Grant Agreement Number: 768953

Project acronym: ICT4CART

Project full title: ICT Infrastructure for Connected and Automated Road Transport

D6.1: SoA & benchmarking of Existing Cyber-security Mechanisms and Technologies

Due delivery date: 29 February 2020

Actual delivery date: 24 March 2020

Organization name of lead participant for this deliverable: ICCS

Dissemination level		
PU	Public	X
PP	Restricted to other programme participants (including the GSA)	
RE	Restricted to a group specified by the consortium (including the GSA)	
CO	Confidential , only for members of the consortium (including the GSA)	

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 768953

Document Control Sheet

Deliverable number:	D6.1
Deliverable responsible:	Panagiotis Pantazopoulos (ICCS)
Workpackage:	WP6
Editor:	Panagiotis Pantazopoulos (ICCS)

Author(s) – in alphabetical order		
Name	**Organisation**	**E-mail**
Danilo Amendola	CRF	danilo.amendola@crf.it
Edoardo Bonetto	LINKS	edoardo.bonetto@linksfoundation.com
Jesus Diaz Vico	IBM-Z	JDV@zurich.ibm.com
Guillemette Massot	AIRBUS	guillemette.massot@airbus.com
Bernhard Monschiebl	ATE	Bernhard.Monschiebl@austriatech.at
Panagiotis Pantazopoulos	ICCCS	ppantaz@iccs.gr
Christophe Ponchel	AIRBUS	christophe.ponchel@airbus.com
Maria Rita Spada	WIND	MariaRita.Spada@windtre.it

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V0.1	12/1/2020	Table of contents and Section 1 inputs	ICCS
V0.2	27/1/2020	Inputs to Section 2 and 4	ICCS
V0.3	13/2/2020	Inputs to Section 2, update of the table of contents	ICCS
V0.4	21/2/2020	Inputs to Section 3 and 4	ICCS
V0.5	24/2/2020	Updates and corrections to Sections 1-3, Conclusions	ICCS
V0.6	5/3/2020	Updates and corrections to Sections 4	ICCS
V0.7	18/3/2020	Edits and corrections in all Sections -Version sent for internal review	ICCS
V0.8	20/3/2020	Internal review	ATE
V0.9	20/3/2020	Internal review	AIRBUS
V1.0	23/3/2020	Final version	ICCS

Abstract
This document presents the outcome of the ICT4CART T6.1. An analysis of a set of existing cyber-security technologies relevant to the ICT4CART focus (i.e., use-cases) is detailed. Furthermore, the deliverable identifies technology gaps and proposes a way to benchmark existing (automotive) cyber-security solutions. Links to the ICT4CART implementation conclude the deliverable.

Legal Disclaimer

Abbreviations and Acronyms

Acronym	Definition
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAD	Connected Automated Driving
CAM	Cooperative Awareness Messages
CAN	Controller Area Network
CMDB	Configuration Management Database
C-ITS	Cooperative Intelligent Transport Systems
EC	European Commission
ETSI	European Telecommunications Standards Institute
GA	Grand Agreement
HD (map)	High Definition (map)
HMI	Human Machine Interface
HW	Hardware
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ITS	Intelligent Transport Systems
ITSM	Information Technology Service Management
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MEC	Mobile Edge Computing
OBU	Onboard Unit
OEM	Original Equipment Manufacturer
PKI	Public Key Infrastructure
PO	Project Officer
PC	Personal Computer
REST	Representational State Transfer
RSU	Roadside Unit
RTIR	Request Tracker for Incident Response
R&D	Research and Development
SoA	State-of-the-Art
SSH	Secure Shell
SIEM	Security Information and Event Management
SIRP	Security Incident Response Platform
SOC	Security Operation Center
SW	Software
TCP	Transmission Control Protocol
TIP	Threat Intelligence Platform
GA	Grant Agreement
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WP	Work Package

Table of Contents

List of Figures

List of Tables

Executive Summary

The deliverable relies on a well-established categorization of the different communication technology areas of connected and automated driving (Section 2) and presents a set of relevant cyber-security technologies to each area (Section 3). The corresponding cyber-security challenges are discussed and the way that they are addressed by the described technology is detailed. Subsequently, the deliverable points to certain technology gaps in the identified cyber-security technology and proposes a carefully-selected set of features that each solution is expected to exhibit (Section 4). This set can serve as recommended benchmarking criteria to comparatively analyze the full spectrum of the various cyber-security tools (which apparently cannot be available to the project). The document concludes providing links from the herein surveyed state-of-the-art cyber-security tools to the actual ICT4CART implementation work in WP6 and furthermore the ICT4CART integrated ecosystem.

1 Introduction

With the emergence of information digitization, ICT infrastructure and data communications gave an unprecedented push towards the realization of truly interconnected and highly-automated vehicles. The emerging notion of CAD supports a plethora of diverse data types and services, a broad set of in-vehicle devices and most notably relies on a mosaic of communication technologies among vehicles (V2V) and/or vehicles and infrastructure (V2I).

Considering the vehicle as the heart of the emerging complex CAD systems, a plethora of relevant interfaces is exposed and leads to the increase of the system's attack surface rendering it vulnerable to cyber-attacks. The key-point, therefore, to unlock the enormous potential this ecosystem can offer towards more efficient and safer transportation lies on the extent to which it remains cyber-secure.

In this deliverable a State-of-the-Art (SoA) analysis of existing automotive cyber-security technologies is presented to lay the ground for the development of relevant mechanisms that will be used in the realization of the ICT4CART use-cases. Furthermore, some hints on relevant technology gaps are provided together with a way to compare (or benchmark) its achievable performance. From a methodological standpoint, D6.1 draws on an available classification (in literature) of the communication and computing technologies for connected and automated vehicles to accordingly categorize the existing cyber-security mechanisms/technologies. Our study covers a broad spectrum of solutions even if a sub-set of them will be actually developed and used to serve the ICT4CART needs.

Subsequently, the deliverable identifies technologies gaps related to the aforementioned areas of the connected and automated driving technology. Those gaps may serve as incentives to explore the capabilities of the full spectrum of available and shape the benchmarking of the relevant cyber-security (automotive) technologies that follow. It is to be noted that certain limitations (e.g., the lack of availability of an exhaustive set of commercial solutions) lead to the adoption of an approach that retains certain characteristics of generality; even so the recommended benchmarking solution can be effectively applied over cyber-security tools of the automotive provided that one avails their detailed specs and characteristics.

No input from other projects was considered during the compilation of this deliverable while there is no direct dependency of this document on past ICT4CART deliverables. However, the technology developed in the WP6 and the relevant SW technologies presented here will guide the implementation effort which will be reported in subsequent WP6 ICT4CART deliverables.

1.1 Purpose of the document

The document seeks to analyse (in the context of Task 6.1) the State-of-the-Art in automotive cyber-security tools that fall under the ICT4CART scope. Furthermore, it identifies technology gaps and presents a way to devise comparative arguments on the relevant cyber-security tools involved in the ICT4CART use-cases. This work will serve as the (bibliographic) basis for the privacy-preserving mechanisms (PKI) and the supervision functionality that would be developed in WP6; the relevant ICT4CART tools are presented and categorized in this deliverable. Furthermore, the document sheds some light on tools of similar functionality offering a more complete view of the automotive cyber-security landscape.

1.2 Targeted audience

Besides the project reviewers, this deliverable is addressed to any automotive/ITS stakeholder or interested reader in general, as it is of Public dissemination level.

2 A Basic Classification of Automotive Communication and Computing Technology

In what follows we identify/point-to certain to CAD areas (well-established in background studies [1], [2]) out of the full ICT4CART ecosystem (see Figure 1) where cyber-security becomes particularly important. Those areas involve the communication and computing technology required to support the relevant CAD functions. Accordingly, a large set of cyber-security technologies and tools need to be applied (on those areas) to ensure that the cyber-security needs are met.

Those areas are typically characterized in line with the corresponding (whether wireless or mobile) communication technology/link, keeping the connected vehicle as reference. The cyber-security tools that are applied to those areas will be subsequently analyzed.

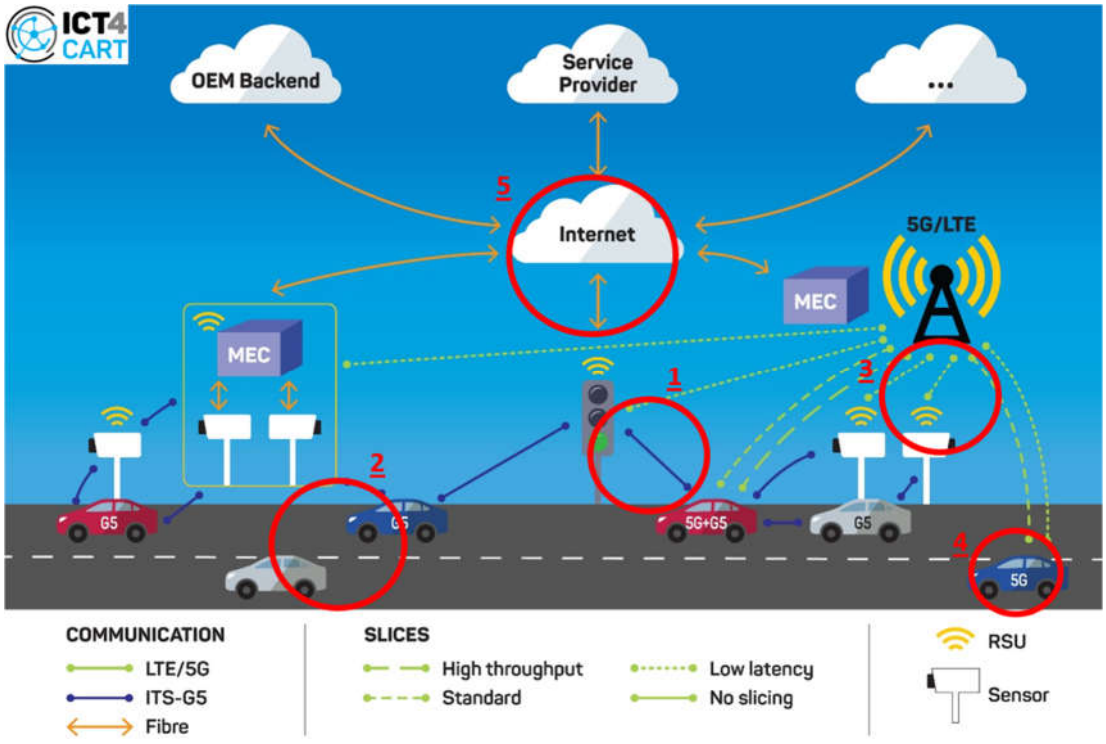

Figure 1 The ICT4CART environment and areas of cyber-security interest

In what follows we elaborate on the high-level description of the four main focus-areas of our study and the relevance of the corresponding communication (and computing) technologies.

2.1 Communication technologies

A number of 'standard' areas in vehicular communications are being highlighted in the following subsections. In each case we identify the "scope of each area" but avoid going into the various technology tools/details since their number is essentially non-tractable and moreover, they remain out-of-scope for the current deliverable. However, the presentation (and classification) of the cyber-security solutions will rely-on this breakdown.

2.1.1 Vehicle-to-Infrastructure technologies

The relevant technologies can be divided into two large areas[1] in line with the infrastructure-end of the corresponding link:

The Vehicle-to-RSU (in circle '1' in Figure 1) communication link. There, information typically originates from the infrastructure back-end (e.g., a Traffic Management Center), reaches the roadside station and becomes relevant in numerous driving use-cases (e.g., intersection crossing) at the vicinity of the RSU.

The Vehicle-to-Cloud (in circle '3' in Figure 1) communication link. There, information typically originates from the infrastructure back-end (e.g., an OEM cloud), reaches the vehicle through the communications network (whether wireless or mobile) and becomes relevant in a variety of driving use-cases; some are those that involve information beyond the RSU or the vehicle vicinity (e.g., an HD map update).

2.1.2 Vehicle-to-Vehicle technologies

The Vehicle-to-Vehicle (in circle '2' in Figure 1) communication link. Information (e.g., CAM messages) typically originates from one vehicle, reaches another and becomes relevant in driving use-cases (e.g., intersection crossing) at the vehicles' vicinity.

2.2 In-vehicle technologies

In-vehicle (in circle '4' in Figure 1) communication links. Connected vehicles integrate a variety of on-board subsystems that consist of the hardware and software needed to support automated driving use-cases. HW may include on-board sensors to sense the environment (e.g., cameras, radars, etc.), actuators and in-vehicle networks (e.g., CAN). On top of those, a SW layer of perception, communications, infotainment and/or HMI applications are hosted.

Over those technologies and their efficient operation, a number of cyber-security tools have been developed and will be analyzed in the following section.

2.3 ICT technologies of general purpose

The last area (indicatively, in circle '5' Figure 1) includes cyber-security tools of more general purpose that can be relevant in numerous ICT products. Here a number of those tools serve the cyber-security purposes of automated driving scenarios.

[1] Other areas such as V2G (Vehicle-to-Grid) may also be categorized here but remain out of the ICT4CART scope.

3 State-of-the-Art of Cyber-security Tools for Connected and Automated Vehicles

Following the section 2 break-down we analyze the State-of-the-Art in cyber-security tools developed in each area pointing also to the relevant ICT4CART tools. We adopt a common and structured way of presentation in each identified area.

3.1 Cyber-security tools for V2I and V2V communications

Table 1 presents the cyber-security technology that becomes relevant in the area of Vehicle-to-Infrastructure and Vehicle-to-Vehicle communications. The 4th column in particular, covers a broad range of open challenges that may extend beyond the ICT4CART research focus; this is for the sake of completeness of the deliverable.

Table 1 – Identification of cyber-security tools for V2I and V2V communications

	V2I / V2V	Cyber-security challenge	Cyber-security Objective	ICT4CART tool	Relevance to ICT4CART use-cases
1	V2I and V2V	The challenges are to ensure the enrolment, authentication and authorization of the connected vehicle without introducing latency in communication. Further challenges are the ability to renew and revoke certificates as well as ensure the service-continuity during roaming.	Identity and Access Management solution i.e., to issue certificates to vehicles that will be used in relevant communications .	CymID	Since it is critical to ensure that only authorized and legitimate users can have access to clouds services and road-side units, the tool is relevant for each ICT4CART use-case.
2	V2I and V2V	ITS messages must be signed to guarantee authenticity and integrity i.e., the ITS-Station must be compliant with all the ETSI standard procedures to guarantee: a) the proper signing of the messages and b) the message signature verification at their reception.	The objective is to guarantee the authenticity and the integrity of ITS messages. Confidentiality can also be guaranteed, but it is not required i.e., all relevant messages are broadcasted.	ITS-Station secured communicatio n tool	It is necessary to guarantee the authenticity and integrity of the ITS messages in the short-range communication s. The involved vehicles need to trust the received information.
3	V2I and V2V	The ITS-Stations need to communicate with a C-ITS PKI to perform the enrollment and authorization tasks for retrieving the required	The objective is to allow the ITS-Station to retrieve the certificates	The Public Key Infrastructure (PKI) is one of the actors of secure V2X	ITS stations involved in use cases and willing to implement the

		certificates needed for a secure V2X communication.	according to the existing relevant ETSI standards.	communication (according to existing standards, e.g., [13], [15]). It mainly aims at producing and distributing certificates to enroll and authorize V2X devices, to manage misbehaviors and revocation lists.	ETSI security standards regarding ITS G5, need to access the PKI to get enrolment and authorization tickets
4	V2I	Data needs to be gathered in a privacy-preserving manner, but without extracting its utility *i.e.*, it can be possible to process the data for the predefined purpose (*e.g.*, detect cyber-security incidents). This should be possible without requiring to leak the identity of involved cars. Still, authenticity of the data needs to be ensured	Implement a variant of group signatures, called Convertibly Linkable Signatures (CLS) or Group Signatures with Selective Linkability (GSSL), that enable to address the described challenge, with low computational and communication costs.	Convertibly Linkable Signatures (CLS) or Group Signatures with Selective Linkability	It is essential to ensure that cyber-security events collected by the supervision service can be processed including those with encrypted data without storing clear data.

3.1.1 Vehicle to road-side unit

In what follows we discuss the background of each entry of Table 1 that falls under the communication link with the road-side unit. We present the required functionality of the relevant technology, the involved data and highlight the available prototype solutions (with a special mention to open-source solutions[2]).

3.1.1.1 Vehicle authentication and authorization

Functionality: The relevant tools need to be compliant with a number of ETSI standards such as TS

[2] Such tools are particularly interesting given their open accessibility as opposed to (potentially numerous) proprietary solutions that cannot easily be known to the authors of this deliverable.

102 731 V1.1.1, TS 103 097 V1.3.1, TS 102 940 V1.3.1, TS 102 941 V1.3.1, TS 102 942 V1.1.1. Such tools need to be able to manage users, devices and permission models (for users' addition or deletion). Authentication and authorization functions able to check the received identity information need to be included; likewise, the capability to validate them is a requirement.

Involved data: the needed information includes authorization tickets and enrolment credentials to grant access to the relevant ITS communication links.

Relevant tools and open-source solutions: CymID is a proprietary solution developed by Airbus CyberSecurity and compared to other solutions it features the Identity and Access management for both users and devices. There is no relevant open-source solution to the best of our knowledge.

3.1.1.2 ITS-Station communications

Functionality: The tools are securing the V2X communication and ensure messages authenticity, integrity and confidentiality. ITS-Stations require the certificates to be used for signing the messages. In their initial configuration, ITS-Stations require a set of information to be used for the enrollment phase and retrieve the certificates from the PKI. Compliance to the relevant ETSI standards such as [13], [15] is needed.

Involved data: The tools exchange information related to secured ITS messages; furthermore, data related to certificates that are used for the ITS messages.

Relevant tools and open-source solutions: Proprietary solutions that secure ITS messages in line with the current ETSI ITS standards have been developed by industrial players within the consortium such as LINKS or outside such as Escrypt [17]. There is no relevant open-source solution to the best of our knowledge.

3.1.1.3 Key distribution infrastructure

Functionality: The relevant technology produces V2X certificates according to the ETSI ITS G5 standards, e.g., (i) Root certificates; (ii) Authorization Authority certificates; and (iii) Authorization Tickets – AT – certificates. When security is enabled, all V2X messages (e.g., CAM and DENM messages) are signed and appended with signed certificates that are added to the message before being sent. The certificates have to be stored by the V2X devices.

Involved data: The configuration for the type of the certificates to be produced (e.g., the list of services and communication types allowed per a given V2X device). For instance, the configuration of the "Service Specific Permissions" (SSP) of the V2X security certificates is needed. The Service Specific Permissions governs the service type a vehicle/entity is allowed to use, thus the PKI can limit the types of requests any entity is able issue. The output of the tools is V2X certificates to be stored in the V2X devices.

Relevant tools and open-source solutions: In the context of a German pilot project, the Escrypt company was commissioned by the Federal Office for Information Security (BSI) to provide the PKI [17]. A limited number of commercial tools can provide offline local services emulating PKI for secure V2X (ETSI ITS G5) communication testing. No data about the existence of comparable open-source solutions are available.

3.1.2 Vehicle to cloud

In what follows we discuss the background of each entry of Table 1 that falls under the

communication link with the cloud services. We present the required functionality of the relevant technology, the involved data and highlight the available solutions.

Functionality: The tool allows to issue privacy-preserving digital signatures which, despite being "anonymous" can be linked when necessary by a special entity called the Converter. The Converter ensures that linking is done only according to the predefined rules (e.g., rules relevant to detect cyber-security incidents.)

Involved data: Vehicles need to communicate with an Issuing entity in order to obtain a credential that enables them to issue group signatures. This credential needs to be renewed periodically. Once the vehicles have the credential, they will be able to issue signatures as desired/required. Compatibility with standards is under analysis. For the linking operation, given a set of anonymously signed messages, the conversion process returns a set of pseudonyms-message pairs such that, every message that has been signed by the same vehicle is associated with the same pseudonym.

Relevant tools and open-source solutions: Other group signature systems require the signer (i.e., vehicles in our case) to decide whether a signature will be linkable or not, before actually issuing the signature. In practice, this typically implies that in order to be able to extract utility, all signatures must be linkable by default (i.e., not privacy-preserving). Alternatively, other schemes allow extracting the identity of the signer but with privacy invasive mechanisms (allowing to link all signatures issued by the same signer). There is no relevant open-source solution to the best of our knowledge.

3.1.3 Vehicle to vehicle

The tools are the same with those used for communications with the road-side units. Please refer to the paragraphs 3.1.1.1 , 3.1.1.2 and 3.1.1.3.

3.2 In-vehicle cyber-security technologies

Table 2 presents the cyber-security technology that becomes relevant in the area of In-vehicle cyber-security.

Table 2 – Identification of in-vehicle cyber-security tools

	Cyber-security challenge	Cyber-security Objective	ICT4CART tool	Relevance to ICT4CART use-cases
1	The main challenge of such CAN gateway modules is to ensure integrity and authenticity of the information (messages) that cross the in-vehicle network, as well as to guarantee authentication and authorization of the sender.	CAN gateway modules aim at guaranteeing integrity and authenticity of each message that crosses the in-vehicle network from components having external connectivity towards the ones that relate to safety functionality.	Vehicle networks CAN gateway modules isolate and therefore protect the OBUs/devices with safety functionality from remote interactions	ECUs have to trust messages propagated from external communications to safely request actions to vehicle actuators.

3.2.1 In-Vehicle isolation gateway

Functionality: Examples of functionality provided by CAN gateway modules are: a) Isolation of the OBUs with safety functionality from the one with remote interactions; b) Monitor the CAN traffic to detect anomalies into normal data-flow workload; c) Provision of the vehicle signals necessary to the V2X OBU for the generation of the CAM messages; d) Provide to the vehicle the needed information coming from the V2X communication links.

Involved data: Relevant data include the CAN messages crossing the in-vehicle network, as well as V2X messages received and pre-processed by the V2X OBU. Configuration information may be also needed by the gateway modules (e.g., to define which messages can pass it). Examples of output of the CAN gateway modules are the CAN messages that are enabled to cross the in-vehicle network, alert messages in case of traffic violations and anomalies and log information.

Relevant tools and open-source solutions: The CAN gateway modules are usually based on proprietary solutions developed by OEMs or companies specialized in embedded cyber-security (e.g., GMV, Arilou, Argus, Trillium Secure) according to the vehicle architecture and in-vehicle network. Often, the CAN gateway modules are composed of a dedicated hardware that has CAN interfaces and that can execute a software for controlling the CAN traffic. SocketCAN is an open-source Linux-based software library composed of CAN drivers and a networking stack implementation that can be used to implement a CAN gateway module in an embedded PC with CAN interfaces.

3.3 Cyber-security technologies of general purpose

Table 3 presents the cyber-security technology that may be relevant in a broad range of ICT instances. Those can be applied in numerous cases of the CAD functionality.

Table 3 – Identification of general-purpose cyber-security tools that are applied in the ICT4CART ecosystem

	Cyber-security challenge	Cyber-security Objective	ICT4CART tool	Relevance to ICT4CART use-cases
1	The main cyber-security challenge is to discover unwanted users that may gain access to the system.	The objective is to act as intrusion detection system.	Fail2ban scans log files and bans IPs that show malicious signs	There is a broad applicability of the tool in automotive SW. In the context of the project, test with the tool will be conducted in a bench lab.
2	Reported events may be numerous per source (vehicle, RSU, services). There are large amounts of sources and the challenge for a supervision service is to cope with the size and the required performance standards due to big data.	The security objective of the supervision service is to detect and report any security issue regarding ITS communications.	Apache Kafka and Graylog products act as event collectors to gather and store security events from vehicles and	The collection system will be demonstrated in scenario 1.1 in Germany and scenarios 2.2, 2.3, 3.1b and 3.3 in Italy

	Detection should be enabled for long-term periods and the targeted event collection should operate without virtually any loss. Storage of the relevant data should be made in a way that allows processing to identify short-term and long-term situations.		road-side units	
3	The challenge here is the detection (of known threats and anomalies) on time in a big data context. The detection system has to support anonymous data in messages from sources while being able to correlate them.	The security objective is to detect cyber-attacks and assess whether the attacked systems are compromised or not.	Graylog correlation plugins to detect cyber-attacks and assess whether the attacked systems are compromised	This detection system of cyber-security issues will be demonstrated in scenario 1.1in Germany and scenarios 2.2, 2.3, 3.1b and 3.3 in Italy.
4	The challenge is the performance of the orchestration of alerts due to big data. (Alerts are the output of correlation analysis over the SIEM-collected security events from the vehicle and/or the road-side units.	The aim is to mainly provide automated incident orchestration.	Cymerius tool (developed by Airbus) to orchestrate alerts generated in line with SIEM-gathered security events	The tool is relevant to enable incident management and proposes situation visualization through dashboards. Cymerius will be used in scenario 1.1in Germany and scenarios 2.2, 2.3, 3.1b and 3.3 in Italy.

3.3.1 Logging tools

Functionality: examples of the logging functionality are: a) Scan constantly the logs of the service under analysis to analyze them; b) Discover anomalies in the analyzed logs; c) Provide mechanisms to react to the discovered anomalies (e.g., limit the number of requests by a given IP, ban a given IP in processing additional requests)

Involved data: Example of inputs are the service to be analyzed (e.g., SSH, in-vehicle networks), log files of the service to be analyzed, tool configuration (i.e., which service to analyze, how to analyze the logs, e.g., frequency of the analysis etc.). Examples of output are alert messages in case of traffic violations and anomalies, or actions performed to limit the discovered potential "attacker" (e.g., ban a given IP in processing additional requests).

Relevant tools and open-source solutions: Alternative log scan tools under the open-source license

exist, e.g., the Auditd [20], but is it of more limited functionality; it is typically used to the scan and/or analyze system-level logs in Linux-based OS (i.e., to check system calls). Fail2ban gives more flexibility and is also open source.

3.3.2 Event collectors

Functionality: Event collectors potentially implemented through a Kafka cluster [14] require to receive logs and events over TCP (under a certain format such as JSON or Syslog messages). Kafka is listening to event messages from vehicles, RSUs, and services. Once received, it makes them available to any system subscribing to this kind of data. A subscriber gets the collected data, normalizes them and stores them. Depending on the kind of data, various indices are used: basically, alerts and events indices. From the OBU/RSU and edge side a module will detect possible security issues and send them to the event collector. The detected events span from known attacks (e.g., the one detectable by an IDS module) to problems related to the ETSI ITS G5 reception of non-authenticated or invalid messages.

Involved data: The output data may be available as JSON structures through a REST API.

Relevant tools and open-source solutions: Tools using SQL bases are limited and lack flexibility: SIEM solutions are used acting as event collectors. Most of them rely on SQL bases. NoSQL technology is preferred for scalability and flexibility. The foreseen tool exploits the capacity to extend the cluster by adding as many servers as needed depending on the context to address scalability. For attacks on cloud services or MEC servers, IDS tools (e.g. Snort) can be used. For the signature verification ad-hoc tools integrated in the stack must be implemented. Apache Kafka, ElasticSearch [23], Graylog [16] and Hadoop [21] are used and are open-source solutions. Snort [22] and others are used for IDS but no one addresses the signature verification.

3.3.3 Detection tools

Functionality: The tools of this category aim to detect cyber-attacks and assess whether the attacked systems are compromised. Tools that fall under this category (such as Graylog [16]) can be used to correlate the collected events and subsequently assist to detect anomalies. The Graylog correlation module works on sliding time windows analyzing the indices (i.e., events and alerts). Based on rules, it verifies if there are matches and if positive it applies the output behavior specified in the rules.

Involved data: Logs and events gathered by the event collector. They are available using REST APIs as JSON data. A correlation alert is produced by Graylog after a rule has matched. Anomaly alerts are generated by Spark. Both are stored in specific indices and accessible as JSON data.

Relevant tools and open-source solutions: Splunk behaves the same as Graylog. According to SPALT [3], alternatives to Spark are: Apache Storm [4], Apache Flink [5], SAS [6], TIBCO StreamBase [7], IBM InfoSphere Streams [8], and Software AG's Apama [9]. Apache Spark and Graylog are open source and so is Apache Storm and Apache Flink.

3.3.4 Alerts orchestration

Functionality: Such tools need to be capable of orchestrating alerts that are generated from the security alerts gathered and inferred by a SIEM platform. Particular care needs to be taken to address vast amounts of data. In ICT4CART, the actual functionalities of the relevant tool i.e., Cymerius are situation awareness incident management, incident response/remediation, dashboard

and reporting.

Involved data: Cymerius compiles information available from the related information system (i.e, SIEM, IDS etc.). The tool provides a unified view of all the gathered information to the operator in charge of the supervision.

Relevant tools and open-source solutions: According to online resources [10], the different tools of similar functionality are depicted in Figure 2.

Figure 2 – Relevant commercial and open-source tools to Cymerius

The left-side solutions are actually IT management solutions that could be customized to become eligible as SIRP platforms. The other solutions are focused on security incident response. The closest solution to ICT4CART tool is IBM Resilient. Open-source are the TheHive [11], FIR [18], RTIR [19], SCOT, and Redmine tools.

4 Comparative Analysis of Cyber-security Automotive Technology

In this section we deal with the exercise to lay a common ground for comparison of the different cyber-security technologies of connected and automated vehicles. Our aim is to ensure that the herein analysis provides the means for a *fair* and *meaningful* comparison of the cyber-security tools present in the automotive arena.

The idea of benchmarking[3] is somewhat highly ambitious for a limited time project that implements (or re-uses) a limited set of cyber-security technologies. Strictly speaking, a benchmarking approach would require a) in-depth exploration of the various features that determine the performance of cyber-security technology and most notably 2) the availability of the exhaustive set of every cyber-security tool in the automotive market (in order to shape any benchmark in line with State-of-the-Art capabilities of the tools). Furthermore, benchmarking typically involves relevant best practices and standards which may differentiate according to their origin such as industrial partners and standardization bodies, respectively.

To overcome this limitation, we follow a more generic approach that allows the identification of areas where improvements (in terms of the cyber-security features and their performance) are needed. More importantly, we elaborate on the tools that have been earlier described and analyze their set of features; we thus, identify an extended set of welcome features that each technology is

[3] According to www.techopedia.com, the typical definition is as follows: "*Benchmarking refers to testing a product or service against a reference point to quantify how it is compared to other products*."

expected to exhibit. This analysis and the corresponding set of features called benchmarking parameters comes from the ICT4CART experts/engineers and it can serve as a basis for any benchmarking effort. With the ICT4CART-proposed list at hand, one who avails all the data in a certain cyber-security automotive area is enabled to compare any tool/technology evaluating the extent to which the ICT4CART benchmarking parameters are present.

Finally, the last paragraph of this section provides some links of the herein reported tools/technology to the actual WP6 implementation work (and further to the WP7 integration).

4.1 Gaps and benchmarking parameters of cyber-security technology

In this section a number of technology gaps related to the aforementioned cyber-security areas and tools are identified. Then, in line with those gaps the document proposes a set of features, occasionally of broader scope than the discussed tools, which can serve as the basis for benchmarking the automotive cyber-security technology.

4.1.1 Identified technology gaps

The ICT4CART ecosystem covers a very broad spectrum of cyber-security (research) areas and the relevant tools. In what follows, a number of technology gaps are highlighted pointing to open research challenges and future directions. In some cases, the identified gaps extend to automotive directions that may even go beyond the ICT4CART reference implementation and render this document of broader value.

4.1.1.1 Privacy concerns against efficient functionality in automotive authentication

Current approaches to authenticate vehicles involved in V2X communications, rely on using fixed-term pseudonyms. Those are pseudonyms used for a fixed number of messages and/or amount of time, before launching some pseudonym-change protocol. These approaches aim at striking a balance between privacy and utility: the more frequently pseudonyms are changed, a higher privacy is reached while at the same time it becomes harder to extract the utility from their associated data. If pseudonyms are changed less frequently, privacy is reduced as vehicles are more easily identifiable, but then it is easier to extract utility from the associated data.

To fill this technology gap, one needs to provide each vehicle with a long-term pseudonymous credential that is randomized for every message that the vehicle needs to send. Therefore, to an external observer, all messages can carry different pseudonyms and are completely un-linkable. However, when the need arises, a (partially trusted) party can process all messages, being able to tell which of the pseudonyms originated from the same vehicle.

In this way, an optimal equilibrium between privacy and utility is achieved: every message has its unique pseudonym and is un-linkable by default, but these pseudonymous messages can be re-linked (by a proper authority) when needed. An approach that seeks to meet those requirements can be found in the Convertibly Linkable Signatures (CLS), or Group Signatures with Selective Linkability (GSSL), presented in section 3.1.

4.1.1.2 Gaps in ITS-Station secured communication technology

4.1.1.2.1 Pseudonym changing

In line with the above thread, one important technology challenge is to appropriately change the ITS-Station pseudonym for privacy protection. At the moment, no solution has been standardized within ETSI standardization framework. ETSI published the Technical Report "*Pre-standardization study on pseudonym change management*" in which several different approaches are illustrated [12]. The pseudonym change involves the periodical modification of all those identifiers of an ITS-Station that may let possible someone to track the ITS-Station. These identifiers can be the Authorization Ticket certificate, the identifier of the ITS-Station, the IPv6 address, the GeoNetworking address, the MAC address and the Path history (i.e., the vector containing the previous positions of the ITS-Station). The main issue is the selection of the timing at which the ITS-Station should perform a pseudonym change. Several different criteria have been proposed mainly related to the number of signatures done with the Authorization Ticket certificate in use, the time elapsed, the distance travelled by the ITS-Station.

The scope of pseudonym changing is to avoid that ITS-Station can be tracked and privacy is then violated. However, tracking is also needed for safety applications in C-ITS (e.g., collision risk warning). It is then required to identify the best criteria for pseudonym changing that can guarantee privacy to ITS-Station, while not compromising the effectiveness of C-ITS safety applications.

4.1.1.2.2 Cyber-event logging system

The current V2X secure communication ETSI-standardization framework does not foresee a specific logging system to report specific cyber-events. The ITS-Stations can log errors that may happen during the communication with the PKI (i.e., enrollment and authorization phases) or during the C-ITS message verification (e.g., not valid message signature, certificate not valid).
The logs should report information of the verified cyber-events providing details for further analysis that may permit the detection of possible cyber-attacks. The logs of cyber-events should be analyzed either by the ITS-Station itself or by an external service. In the latter case, the ITS-Station has to implement a communication system to provide the logs to the external service.

4.1.1.3 Gaps in access rights management

Another technology gap amounts to the provision of certificates complying with ETSI standards to vehicles and road-side units. Relevant tools need to be designed in order to manage users and rights on different applications.
Improved capabilities are needed to allow the handling of certificate requests and authorization tickets from ITS-S devices that essentially fall under the IoT category. At this end, relevant technology should be capable to manage a fleet of ITS-S devices and perform administration tasks such as devices-certificates revocation in case of compromise. Any solution is required to comply with standards such as the ETSI document for PKIs services [13]. This standard defines the format of certificates, communications between PKI and devices and the global architecture while relevant implementations are limited, pointing to an open challenge. The ICT4CART CymID tool has been enhanced to fill the above gaps.

4.1.1.4 Gaps in supervision services for ITS communications

The supervision services challenge in ITS communications is to develop a complex system that provides a full set of capacities such as data collection, event correlation, anomaly detection and reaction. A large part of the required R&D consists of integration activities. For instance, setting the

Kafka [14] cluster to collect data from the fleet management service and OBUs, possibly passing through MEC servers. One of the challenges relates to the support of linkable yet anonymized event data in the correlation process. To fill such a gap, development activities in the frame of the task T6.3 are needed; that is the development of a Graylog plugin to provide linkability of pseudonymized data, relying on a library provided by IBM-Z. To our knowledge, there is no equivalent on the market. Working on the fleet management use case enables Airbus to develop correlation rules and plugins specifically tailored to handle linkable pseudonymized data within the task T6.3.

4.1.1.5 Technology gaps in SIRP capabilities

Open challenges in SIRP solutions typically amount to agility and scalability properties: supported data fields usually come under certain limitations (depending on the application domain) while the underlying data models need to cope with a maximum number of systems (i.e., in the automotive case, a vehicle is considered as a system of devices such as ECUs, sensors, etc.). An important point is the need to efficiently modify the processing workflow of such solutions (mainly for the response orchestration part) in order to cope with vast amounts of data that need to be processed (i.e., alerts and incident tickets). That would mostly ease the work of the corresponding SOC analysts who process the findings.
The ICT4CART Cymerius solution is being totally reworked to meet the above specifications and cover the automotive specificities.

4.1.2 Introducing parameters for benchmarking

Table 4 presents a list of cyber-security parameters i.e., most of them are open research challenges in the area of CAD. Each parameter is explained in the right most column.

Table 4 – Proposed parameters to serve as the basis for benchmarking

Parameter	Description
PKI features: communication messages	The ITS-Station should perform all the initialization procedures with the Enrollment Authority and Authorization Authority of the PKI to be enrolled and authorized in order to obtain the Authorization Ticket certificates to be used for signing and/or encrypting the C-ITS messages. The ITS-Station should periodically interact with the Authorization Authority to get new set of Authorization Ticket certificates when it consumed the ones previously retrieved. Compliance to the standardized PKI communication features is required [13].
PKI features: Pseudonym changing	The ITS-Station should periodically change all the identifiers present in the C-ITS messages. (Those identifiers can render the ITS-Station trackable compromising the privacy of the ITS-Station).
PKI features: Un-linkability properties	Cryptographic schemes provide a high level of privacy in V2X communications, relying on unique pseudonyms to authenticate messages. A third trusted entity may be needed to link pseudonymous messages coming from the same vehicle.
Secured V2X communication: Signatures and encryption	The ITS-Station should be capable to sign and/or encrypt the C-ITS messages to be send and it should be able to verify the signature and/or decrypt the C-ITS messages at their reception. The ITS-Station needs to comply with relevant standardized formats [15].

Privacy-preserving V2X communication	Cryptographic schemes need to provide high levels of privacy in V2X communications, relying on un-linkable unique pseudonyms to authenticate messages.
Vehicular Secure Logging	The ITS-Station should be enabled to log a set of cyber-events that can be used to identify possible cyber-attacks. Furthermore, the ITS-Station should implement a communication system to provide the logs to any relevant external service.
SIEM features: Availability, Auditability	A SIEM system needs to be monitored continually and be able to log all sensitive actions in particular connections and malicious requests. Those are requirements in order to achieve a minimal down-time.
SIEM features: alerts integration	SIEM systems are the main data providers of a SIRP platform. Inputs are alerts, potentially malicious events, provided through an API. Parameters of importance are the number of officially supported event sources, and the extent to which sources are supported. In terms of performance the number of alerts collected per second is of importance.
SIEM features: threat data feeds	Alert analysis is made easier with the ability to link alert data with information found in a threat intelligence base. Relevant parameters of importance are: the number of supported TIP, the type of supported interface (one-way, both ways), the ability to support a new TIP (integration, development, not possible)
SIRP features: incident management workflow, data enrichment, connectors	A SIRP system needs to provide adaptive workflows to handle cyber-security incidents specific to the monitored systems. The relevance of a SIRP can be measured by the number of actions with third systems it supports. Examples of third systems: TIPs, CMDBs, ITSMs, shared services (DNS), LDAP. Another measure is the capacity to let SIRP users extend the list of supported actions. As a result of the analysis of a cyber-security incident, the produced report is crucial for bringing conclusions to the organization requesting the SIRP service. The completeness of reports and facility to produce them are important criteria to assess the relevance of a SIRP.
Access management features: interoperability, availability, reactivity, auditability	- the management service needs to comply with (ETSI, IEEE, ITU) Standards in order to permit data exchange with systems implementing these standards - the management service needs to be assiduously enabled to operate with a minimal down-time due to the criticality of the ITS applications. - the management service needs to be enabled to operate with minimum delays. Latency must be monitored and measured to ensure the appropriate data exchange with vehicles. - the management service needs to log all sensitive actions in view of malicious connections and requests.
Risk analysis and impact assessment [*generic*]	A basic cyber-security feature is the ability to evaluate risk and the impact caused by a cyber-security incident. This information is important as it drives relevant decisions. Relevant parameters to be considered

	are: system availability (i.e., no, internal, through connection to external systems), the exposed API (i.e., none, to request evaluation, to share evaluation), the level of integration with incident tickets (i.e., standalone, integration on-demand, automated integration), the level of integration with the response workflow.

Using the parameters of Table 4 as a basis, one may compare a wide spectrum of automotive cyber-security solutions and provide suggestions (on the appropriateness of each solution). The above list may also drive the further implementation and the relevant extraction best cyber-security practices.

4.2 Links to the ICT4CART implementation

In this section we associate a set of cyber-security tool instances with the actual implementation work that is currently being undertaken and is to be showcased in the context of the ICT4CART project. All relevant data appear in Table 5.

Table 5 – Relevance of cyber-security tools and the ICT4CART prototype development

Cyber-security tool	Implementation effort in ICT4CART
Unlinkability manager	The manager will be implemented as a part of a reference simulator prototype that will be built exclusively for ICT4CART testing purposes.
PKI instance to produce and distribute certificates	The tool that enrolls and authorizes V2X devices according to the ETSI ITS G5 is implemented and will be tested in certain scenarios of the ICT4CART (scenarios 2.2, 2.3, 3.1b and 3.3 in Italy).
V-ITS-S tool (PKI part at the vehicle side)	The tool is implemented and will be tested in certain scenarios of the ICT4CART (scenarios 2.2, 2.3, 3.1b and 3.3 in Italy).
Access management	The tool that manages the access to cloud services and road-side units will be used for each ICT4CART use-case.
CAN gateway to isolate parts of the in-vehicle network	The tool is implemented and will be tested in all ICT4CART use-cases.
Detection and reporting tool of any ITS-communications security issue	The tool is implemented and will be demonstrated in scenario 1.1 in Germany and scenarios 2.2, 2.3, 3.1b and 3.3 in Italy.
Tool to detect cyber-attacks and malicious intrusion	The tool is implemented and will be demonstrated in scenario 1.1 in Germany and scenarios 2.2, 2.3, 3.1b and 3.3 in Italy.
Tool to automatically orchestrate incidents (captured by the SIEM)	The tool is implemented and will be demonstrated in scenario 1.1 in Germany and scenarios2.2, 2.3, 3.1b and 3.3 in Italy.
Instance of group signatures	It will be implemented as a part of a reference simulator

	prototype that will be built exclusively for ICT4CART testing purposes.
Log files scanner (for signs of malicious acts)	To be used for testing in a bench lab (preparing the CRF vehicle use-cases)

5 Conclusions

The document at hand presents a thorough State-of-the-Art analysis of cyber-security technologies applied to various parts of the CAD ecosystem. A broad set of cyber-security tools are systematically described, categorized under well-established areas of the CAD research. Their relevance to the automated driving use-cases that ICT4CART explores, is described.
Furthermore, a number of identified gaps that call for further research and advanced functionalities to address the emerging automotive threats are presented. Importantly, the deliverable identifies a number of technology challenges that may serve as parameters to facilitate the (future) benchmarking of relevant technologies, retaining a certain generality level that goes beyond the scope of the project. Finally, the links to the ICT4CART follow-up work both in the WP6 and the integration/testing tasks suggest a (theoretic yet important) contribution to the coherent ICT4CART body-of-work.

References

[1] W. Viriyasitavat, M. Boban, H. Tsai and A. Vasilakos, "Vehicular Communications: Survey and Challenges of Channel and Propagation Models," in IEEE Vehicular Technology Magazine, vol. 10, no. 2, pp. 55-66, June 2015.

[2] K. Abboud, H. A. Omar and W. Zhuang, "Interworking of DSRC and Cellular Network Technologies for V2X Communications: A Survey," in IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9457-9470, Dec. 2016.

[3] SPALT: https://www.whizlabs.com/blog/apache-spark-alternatives/

[4] APACHE STORM https://storm.apache.org/

[5] APACHE FLINK https://flink.apache.org/

[6] SAS https://www.sas.com

[7] TIBCO STREAMBASE https://www.tibco.com/fr/products/tibco-streambase

[8] IBM INFOSPHERE STREAMS https://www.ibm.com/developerworks/library/bd-streamsintro/index.html

[9] SOFTWARE AG'S APAMA https://www.softwareag.com/au/products/data_analytics/analytics/default.html

[10] SECURITYINSIDER https://www.securityinsider-wavestone.com/2016/12/sirp-la-panacee-de-la-reponse-incident.html

[11] THE HIVE https://thehive-project.org/

[12] ETSI TR 103 415 V1.1.1 (2018-04) https://www.etsi.org/deliver/etsi_tr/103400_103499/103415/01.01.01_60/tr_103415v010101p.pdf

[13] ETSI TS 102 941 V1.3.1 (2019-02) https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf

[14] APACHE Kafka: Distributed Streaming Platform. https://kafka.apache.org/

[15] ETSI TS 103 097 V1.3.1 (2017-10) https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf

[16] Log Management Software https://www.graylog.org/products/open-source

[17] ESCRYPT https://www.escrypt.com/en/solutions/secure-v2x-communications

[18] FIR (Fast Incident Response) management platform http://www.certcg.com/ ; https://github.com/certsocietegenerale/FIR

[19] RTIR https://bestpractical.com/rtir

[20] Auditd or audit daemon, is a user-space component to the Linux Auditing System https://www.linux.com/training-tutorials/auditd-tool-security-auditing-linux-server/

[21] Apache Hadoop software library https://hadoop.apache.org/

[22] Snort open-source network IDS/IPS https://www.snort.org/

[23] Elasticsearch is an open-source search and analytics engine https://www.elastic.co/