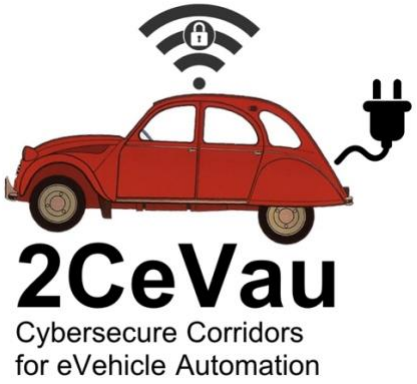
2CeVau - ACTIVITY 1



Cybersecure Corridors for eVehicle Automation

Abstract

2CeVau (Cybersecure Corridors for eVehicle Automation) is a CEF Telecommunication Sector funded project. 2CeVau will develop cybersecurity capabilities for connected vehicles in the context of a complete risk and hazard analysis (threats, vulnerabilities, attacks and countermeasures) focusing on use cases for the "Thessaloniki, Sofia, Belgrade (GR-BG-SRB)" 5G cross-border corridor. It will examine the corridor as a unified set of services, hardware and software components with possible multi-standard, multinational variations exposed to cyber threats. Following this analysis, it will develop a Security Assessment Tool that will increase preparedness for relevant software and hardware components and will facilitate CSIRTs to assess, audit and report security issues for the 5G corridor.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

Milestone & Title:	M1 - "3rd Interim 6-month project report on the progress of 2CeVau."
Activity:	ACT 1
Task:	-
Due Date:	31 January 2021
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR	**DATE**
Leonidas Marantis / UPRC	--/01/2021
CONTRIBUTORS	**DATE**
Konstantinos Maliatsos / UPRC	15/01/2021
Leonidas Marantis / UPRC	18/01/2021
Christos Lyvas / UPRC	20/01/2021
George Efthymoglou / UPRC	22/01/2021
Athanasios Kanatas / UPRC	22/01/2021
Costas Lambrinoudakis / UPRC	25/01/2021
George Drainakis / ICCS	27/01/2021
Panagiotis Pantazopoulos / ICCS	27/01/2021
REVIEWED BY	**DATE**
Konstantinos Maliatsos	28/01/2021
Athanasios Kanatas	29/01/2021
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

Document/Revision history

Version	Date	Partner	Description
V0.1	15/01/2021	UPRC	First draft
V0.2	18/01/2021	UPRC	Activities 1 & 5
V0.3	20/01/2021	UPRC	Activity 3
V0.4	22/01/2021	UPRC	Activities 1 & 5 additions
V0.5	25/11/2021	UPRC	Activities 3 additions
V0.6	27/11/2021	ICCS	Activity 4
V0.7	28/01/2021	ICCS + UPRC	Review
V0.8	29/01/2021	UPRC + ICCS	Proofreading and corrections
V0.9	29/01/2021	UPRC + ICCS	Revised, final version ready

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115

Table of Contents

Table of Figures

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115

List of Tables

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

Acronyms and abbreviations

Abbreviation	Description
5G	5th Generation of Mobile Communications
ACT	Activity
BG	Bulgaria
CCAM	Cooperative, Connected and Automated Mobility
EC	European Commission
GR	Greece
GUI	Graphical User Interface
ITS	Intelligent Transportation Systems
LDM	Local Dynamic Map
RSU	Road Side Unit
RUP	Rational Unified Process
SAT	Security Assessment Toolkit
SDR	Software Defined Radio
SRB	Serbia
UI	User Interface
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle communications
V2X	Vehicle to Anything communications

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115

Executive Summary

This report, entitled "3rd interim 6-month project report on the progress of 2CeVau" specifies all the work that was executed by the project partners during the last 6 months (August 2020 – January 2021) of the 2CeVau project.

2CeVau: "Cybersecure Corridors for eVehicle Automation" is a CEF Telecommunication Sector funded project. 2CeVau develops cybersecurity capabilities for connected vehicles in the context of a complete risk and hazard analysis (threats, vulnerabilities, attacks and countermeasures) focusing on use cases for the "Thessaloniki, Sofia, Belgrade (GR-BG-SRB)" 5G cross-border corridor. It examines the corridor as a unified set of services, hardware and software components with possible multi-standard, multinational variations exposed to cyber threats. Following this analysis, it will develop a Security Assessment Tool that will increase preparedness for relevant software and hardware components and will facilitate CSIRTs to assess, audit and report security issues for the 5G corridor.

The 2CeVau consortium consists of three eligible partners, involving two prestigious ICT research institutes, i.e. University of Piraeus Research Center – UPRC and Institute of Communication and Computer Systems - ICCS and the Hellenic Ministry of Digital Governance (HMDP). 2CeVau is a 24-month project divided in 5 major Activities.

The description of the work in this report is categorized by activity. Activity 2 is not included in this report since this activity had already been completed since November of 2019.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115

1. Activity 1: Project Management

The main goal of Activity 1 is to keep the activities performed by the partners under control and monitoring, handling all the communication with INEA, and checking that all milestones are delivered in time and are of high quality. The role of the coordinator of the project is assumed by UPRC. The role of the Project Manager (PM) of the project is assumed by Prof. A. Kanatas. Several actions were performed during the last 6 months under the umbrella of Activity 1 concerning the management of the 2CeVau project.

1.1 Activity 1 Actions

Three 2CeVau plenary meetings have been successfully organized during the last six months. It should be mentioned that all the plenary meeting were held online (using the Skype tele-conferencing software), following the Covid-19 health safety instructions and assembly avoidance.

- The 6th 2CeVau plenary meeting was held online on the 3rd of September 2020.
- The 7th 2CeVau plenary meeting was held online on the 6th of November 2020.
- The 8th 2CeVau plenary meeting was held online on the 7th of January 2021.

Many representatives from the three partners participated in all these online events, which involved interesting presentations and critical discussions focusing on the project's progress. The 4th of March 2021 was selected for the next online plenary meeting.

The first Thursday of each month (at 13:00) was selected for the monthly teleconference meeting. The Skype Web Conferencing Tool is used. Two extra telco meetings took place during the last six months.

The technical investigations that were carried out during the last six months focused on Activities 3 and 4. Specifically, Activity 3 of the 2CeVau project was successfully completed with the submission of milestone M6. The activity mainly involved the Reference Modelling – analysis and management over the Risk circle. Moreover, research on Activity 4 involved the definition of penetration tests and the basic design of the Security Assessment Toolkit.

The following project milestones (reports) were submitted to INEA and EC:

Table 1: List of project milestones that were submitted during the last six months.

Milestone Number	Milestone tittle	Submission date
M6	M6 - Specification of Security controls and countermeasures: A list of security services, controls and countermeasures that can be used to mitigate the threats and protect the system from possible attacks. It includes the work of task 3.4. (Activity 3)	31/10/2020
M7	M7 - Penetration tests definition and SAT design completed: The output of the test will be an analytical	31/01/2021

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115

	report with the proposal of specific actions that will help achieve the required level of security. (Activity 4)	

Finally, it should be mentioned that the project coordinator sent an official email to the Project Officer and brought into her attention the necessity of a few internal alterations in the 2CeVau budget. Specifically, Prof. Kanatas described the urgency to shift two amounts of the ICCS budget in order to more efficiently allocate our resources and cover some increased needs. He kindly expressed the following requests:

1. To shift an amount of 7K Euros from the category 'other costs' of the Activity 5 (Dissemination and exploitation) to the personnel category of Activity 4 (Evaluation, penetration tests and SAT development). The successful 2CeVau workshop (of last December) required less amounts compared to what originally planned (i.e., around 11.3K Euros) due to the fact it was organised as an online event (because of the pandemic). On the other hand, our Activity 4 work is currently being *extended beyond* the original plan (i.e., we would incorporate SAT interfaces to external entities and develop advanced functionalities for the dependency of threats among 2CeVau assets).
2. To shift an amount of 5K euros from the 'other costs' category of Activity 2 (Use cases and scenarios for .. the GR-BG-SRB 5G corridor) and 4 (Evaluation, Penetration Tests definition and SAT design) i.e., 2450 Euros and 2550 Euros, respectively, to the personnel category of Activity 4. Same technical reasons as above apply (together with the fact that those funds could not be exploited to cover travel expenses, in view of the pandemic restrictions).

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

2 Activity 3: Reference Modelling – Analysis and management over the Risk circle

Activity 3 includes an elaborate study to identify the vulnerabilities, impacts, mitigation actions and respective security control for the 5G corridors – and especially the defined 2CeVau use cases. The Activity is composed of four basic tasks.

2.1 Task 3.1: Asset Definition

The deliverable M5 regarding Tasks 3.1 and 3.2 of activity 3, entitled "*2CeVau: Vulnerability analysis, Threat analysis and Attack modeling focus on GR-BG-SRB 5G corridor use cases*", identifies the system assets, threats/attacks, vulnerabilities, and security and privacy requirements for the use cases specified in Activity 2. The deliverable mentioned above describes the risk analysis and modeling methodology that has been adopted for the overall 2CeVau risk analysis. The system assets, the communication links, and the involved stakeholders for the use cases specified in Activity 2 were identified. During Task 3.1, the connected, conventional, or electric vehicle assets, as well as all components and modules that participate in the V2X 5G paradigm, were identified. The task includes the specification of all functional and data assets for the connected/electric vehicle, i.e., the radio interfaces, the ITS applications, the Local Dynamic Map, the Vehicle Control system, the set of Sensors and sensor monitor subcomponents, the system controller, the charging stations, etc. In addition, the external critical nodes that play a crucial role in the implementation of the V2X and ITS paradigm were identified and integrated into the model. These include the 5G access network technologies, the roadside units (RSUs), core network infrastructure, cloud-based ITS services and applications, the Traffic Management Centers, and more. The system use cases in interacting assets were also provided in the deliverable, along with the current organizational structure.

2.2 Task 3.2: Threat and Attack Modelling

Task 3.2 includes the specification of the security and privacy constraints and the identification of threats that can affect and compromise the specified assets and components of the connected, conventional or electric, vehicles. A composite threat model was developed, capable of capturing multiple threats while enabling the prioritization of security, privacy, and reliability constraints. The result of the analysis was a set of attacks that materialize the specific threats. One of the main targets within this task was the definition of a dependability model suitable for the Connected Vehicle use cases and environment, aiming at structuring the dependabilities of the complex components, systems, and applications, their connections, and their process/data flow. Special attention was given to the identification of threats and attacks for the cross-border corridor use case.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

2.3 Task 3.3: Vulnerability Analysis – Risk and Hazard management

The deliverable regarding Task 3.3 and Task 3.4 of activity 3, entitled "*2CeVau: Specification of Security controls and countermeasures (focus on GR-BG-SRB 5G corridor use cases)*", is a continuation of the deliverable "*2CeVau: Vulnerability analysis, Threat analysis, and Attack modeling (focus on GR-BG-SRB 5G corridor use cases)*" in the sense that it presents the overall results of the risk assessment for the identified *2CeVau* system assets, threats, and vulnerabilities, for the use cases specified in Activity 2.

More precisely, the deliverable mentioned above reports the final results of Activity 3, entitled "*Reference Modelling – Analysis and management over the Risk circle*." Activity 3 contains all tasks and steps for a complete risk assessment, using as input the set of reference use cases defined in Activity 2. Activity 3 had the objective to perform a full vulnerability assessment, threat and attack modeling. That work was based on a generic methodology developed from UPRC during the H2020 research project SAFERtec. The methodology had been suitably adapted to meet the needs of the current project. It consists of three stages: During the first stage, the system's assets and stakeholders were identified (Task 3.1), while in Stage 2, the security and privacy requirements have been elicited (Task 3.2). In the final stage, MONARC risk analysis methodology has been used for the assessment of the impact of potential security or privacy violation incident (Task 3.3) and the appropriate technical countermeasures were proposed (Task 3.4).

During Task 3.3, vulnerabilities were identified and classified. The vulnerability analysis was extended beyond security, to privacy issues. The analysis was performed for the cross-border corridor use case and the various levels of automation. According to the methodology employed, the vulnerability analysis led to a set of security and privacy requirements and included the development of the risk and hazard management plan. All the information collected from that and previous tasks was jointly modeled in order to proceed in the quantification of risks, identification of threat mitigation and vulnerability satisfaction.

2.4 Task 3.4: Security services, measures and controls

Task 3.4 extended the assessment work by validating the issues raised and identifying a specific set of solutions. Risk management based on MONARC was used to define a set of security controls according to widely accepted best practices (ENISA, OWASP, ETSI-TVRA) and standards (NIST). Services and measures were defined, able to mitigate the identified risks and hazards, as well as able to protect the assets and modules of the Connected, conventional or electric, Vehicle as it moves along the 5G corridor. The security controls and services covered the entire System Development Life Cycle within the Connected Vehicle context as it crosses borders within (GR-BG) or outside (BG-SRB) the EU.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

3 Activity 4: Evaluation, Penetration Tests definition and Security Assessment Toolkit design

3.1 Types and Recommended Penetration Tests for 2CeVau

Penetration tests are classified depending on the available knowledge of the system operation and the level of access granted to the penetration tester. Three generic categories are identified:

- Black box testing:

During a black-box test, the penetration tester assumes the role of a hacker that has no system-specific knowledge for the internal design and implementation of the targeted system. Black box testing includes dynamic analysis and access control of the systems and software that are currently executed within the target network.

- Gray box testing:

Gray-box testing is the next step up from black-box testing. If black-box testing places the evaluator in the place of a hacker, then in gray-box testing, the tester has user's access – possibly with elevated system privileges – and some knowledge concerning the system operation.

- White box testing:

White-box testing has the exact opposite features compared with black-box evaluation. In white-box testing, the testers have full system access. They have: full knowledge of the system architecture, components and modes of operation; full access to source codes, configuration files and log files; administrator and designer accounts, etc. White-box penetration testing offers thorough evaluation of both internal and external vulnerabilities, making it the best option for measurement testing.

In the context of 2CeVau use cases, penetration tests should have the objective to detect vulnerabilities that can be exploited by existing threats, and/or validate the effectiveness of applied security measures and controls. Under these conditions, black-box penetration tests seem to be the more relevant, since it is expected that the vast majority of attackers have not knowledge of the system architecture, functional and data assets and have not direct access to the resources prior to launching an attack. Nevertheless, a hacker may have much more time and computational resources compared with the evaluator, thus by providing a level of information it may be possible to balance the aforementioned trade-off. On the other hand, while white-box testing offers deep access to the implementation details of the system, it is time-consuming and, in many cases, it fails to identify vulnerabilities, since it does not take into account the hacker's view and motivation.

The gap between white-box and black-box testing is covered by gray-box testing that emulates a scenario where the evaluator has the role of a hacker with long-term access to the system. In 5G, V2X and ITS use cases, i.e., as in 5G corridors, gray-box testing seems to be a useful, practical and in most cases implementable mode for penetration tests.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

In the following table, a set of penetration test types applicable to the 2CeVau use cases and the 5G corridors – implementing black and gray box tests are presented.

Table 2: Penetration test types applicable to 2CeVau use cases

#	Penetration test type	Applicable to
1	Man in the Middle Attacks	Network connections; inter-process communication; inter-asset communication
2	Compromised key attacks	Networks; inter-asset communication; web services; access to applications; access to data
3	Distributed Denial of Service Attacks	Network resources; databases; application servers; web services
4	Identity spoofing	Networks; data assets; databases; applications; web services;
5	Password-based attacks	Applications, services, operating systems, computing resources, data assets, network resources.
6	Eavesdropping	Network connections; inter-process communication; inter-asset communication; services.
7	Sniffing attacks	Network connections; inter-process communication; inter-asset communication; services.
8	Data manipulation attacks	Networks; inter-asset communication; web services; access to applications; access to data
9	Application layer attacks	Applications, services, operating systems, computing resources, data assets, network resources.
10	Stateful analysis testing	Networks; inter-asset communication; web services; access to applications; access to data
11	Unvalidated redirects and forwards	Applications, services, web services, databases, data and computing assets.
12	Backup Files Verification	Data assets, data bases
13	Firewall bypass testing	Firewall; routers; computing units; networks
14	Switching or routing messing	Firewall; switches; routers; computing units; networks
15	Remote file inclusion	Web applications and services
16	Cross-site scripting	Web applications and services
17	DNS attacks - Zone transfer testing	DNS servers impacting applications, services and computing units.
18	IPS evasion	Applications, services, operating systems, computing resources, data assets, network resources.
19	SQL/ Database injection	Databases; data assets; operating systems, application servers.
20	Local File inclusion	Web services, applications, sites.
21	SSL/ TLS injection	Web services and applications
22	XXE injection	Applications, services, servers, data assets, databases.
23	Simple AJAX verification	Web services
24	Memory corruption	Applications, services, data assets, operating systems, software components, configuration files.
25	Buffer overflow	Applications, services, data assets, operating systems, software components, configuration files.
26	Application error disclosure	Personal data, Applications, services, data assets, operating systems, software components, configuration files.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

27	Firewall configuration testing	Firewall; switches; routers; computing units; networks
28	LDAP injection	Personal data, Applications, services, data assets, operating systems, software components, configuration files.
29	Command Execution detection	Applications, services, data assets, operating systems, software components.
30	Full Path disclosure	Applications, services, data assets, operating systems, software components.
31	HTTP response splitting	Web services and applications
32	Shellshock or Bash bug	Web services and applications, servers, operating systems, software components.
33	Server-Side Request Forgery	Servers, applications, services.
34	Private IP disclosure	Network, routers, firewalls, Personal data, Applications, services, data assets, operating systems.
35	CRLF injection	Servers, applications, services.
36	CSRF	Web services and applications

3.2 Radio-related tests through Software Defined Radio

Radio communications are a basic 5G-corridor enabler, as highlighted by the 2CeVau use cases. However, as seen in the previous paragraphs, while there are plenty of open-source, dynamic and highly efficient penetration test suites and tools, there are no tests for the radio access network counterpart. More specifically, only Aircrack-ng has relevance with the radio access network, however, it focuses on conventional WiFi, a technology that is only a small subset of the 5G radio ecosystem.

In this section, we present penetration test configurations, implemented by UPRC in the context of the H2020-Safertec project, that were modified in order to also fit the 2CeVau use cases. The penetration tests rely on the Software Defined Radio (SDR) paradigm. An SDR is a radio communication system where all waveform design components that have been traditionally implemented in hardware (e.g., mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system. This means that with the use of generic radio hardware, we are able via software, to implement various wireless interfaces – and also perform tests over-the-air, addressing availability issues – besides integrity and confidentiality.

The following set of tests has the objective to:

- implement radio-related attacks
- apply the attacks on the real-world systems (live, laboratory equipment, test-bench etc.)
- monitor the behaviour of the system
- validate the existence of security controls that are capable to repel the attacks

More specifically, the specific set of tests included the simulated/emulated implementation of the following attacks:

- Replay attack: It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

- Malformed frame attack: The attacker injects malformed frames into the network by violating protocol rules
- Man-in-the-middle attack: The attacker sniffs data from the radio channel and attempts to decode it
- Misbehaviour Detection - False position claim: A legitimate user through valid transmissions claims that its position is different than the real
- Misbehaviour Detection – Sudden position change: A legitimate user (ITS station) through valid transmission claims that it performs irregular/irrational movements that cannot be physically justified in order to confuse other users

3.3 The 2CeVau Security Assessment Toolkit software design

Task 2 of Activity 4 work has been mainly carried-out through the reported semester. The actual work detailed in the 2CeVau Activity 4 report, included the introduction of the software design for the Security Assessment Toolkit (SAT). Taking the 2CeVau modeling work as input, the SAT main objective is to provide an automated way that helps assess the involved levels of risk in the 2CeVau corridor setting (in view of the identified potential threats).

The work as well as the corresponding Activity 4 report, adopted a top-down approach. The starting point was the identification of high-level software requirements (that point to SAT technology needs) of the introduced toolkit. Those requirements are generic and apply for every software tool of relevant scale and complexity.

Then, the conceptual architecture of SAT followed. The effort was to shed some insights on the proposed design by relying on the Rational Unified Process (RUP) that seeks to prescribe the intended reference architecture exploiting relevant best practices[1]. Our systematically SAT software design draws on the earlier 2CeVau modeling work (of Activity 3) and in line with those practices presents the SAT design concept under three views:

3.3.1 Logical view

The logical view describes SAT's functionality, including standards and software tools to support each included operation. Under this view which is thoroughly analysed in the Activity 4 report, the high-level 2CeVau architecture, the required modules and their interconnections are presented. The relevant work has been divided it into four basic layers:

- User Interface (UI), related to presentation services
- Business, related to business logic
- Middleware, related to transaction management and inter-process communication
- System Software layer, related to system's management

In principle, SAT's software components will be developed in line with the conceptual design of the 2CeVau modelling approach depicted in Figure 1.

[1] P. Reed, "IBM Reference Architecture: The best of best practices," 15 September 2002. [Online]. Available: https://www.ibm.com/developerworks/rational/library/2774.html

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

SAT's user-interface refers to the (design of the) log-in functionality and the selection of corresponding software solutions that will be used to implement it. The Business layer analyses the SAT's logic related to design patterns (*e.g.*, SAT software entities that share attributes) and services implementation (*e.g.*, security or authentication mechanisms of the toolkit). The Middleware layer describes communication and messaging mechanisms between the SAT components (and processes).

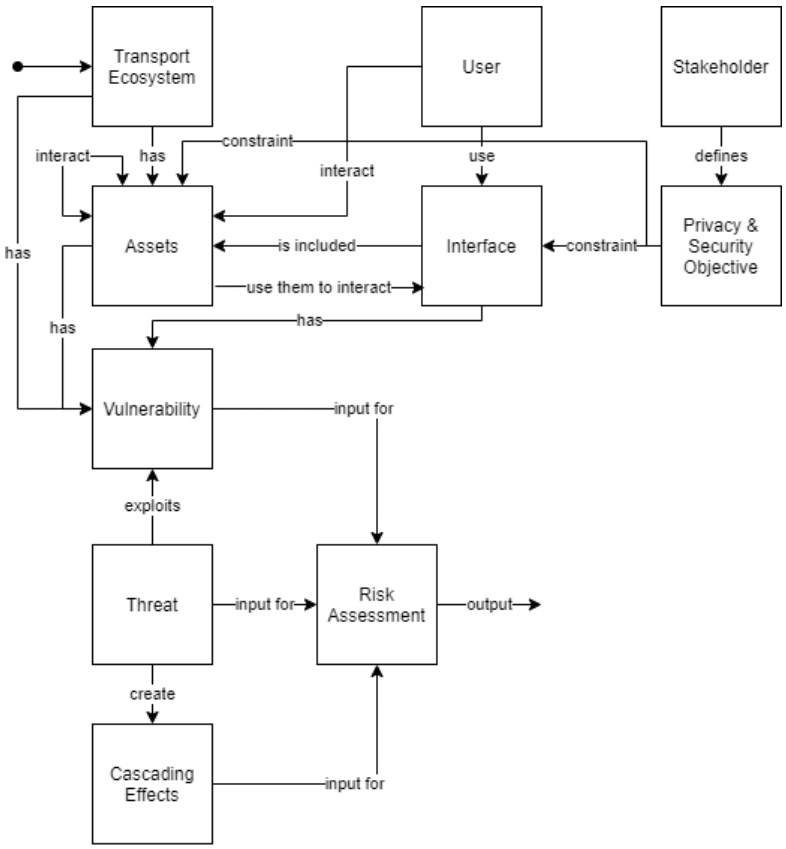


Figure 1. Conceptual design of the 2Cevau modelling work acts as basis for the SAT system design

Finally, the System software layer elaborates on the 'main part' of the proposed software design *i.e.*, the SAT software components, classified into three groups: *The Front end,* including a graphical user interface (GUI) and enabling users to interact with the SAT *back end.* The latter maintains the required data (using a Knowledge Base) to realize all computations and risk assessment functionalities (through an Inference Engine). SAT *interfaces* are means to facilitate the interaction with the user as well as the communication with other external services or security authorities.

3.3.2 Deployment view

The deployment of SAT and the corresponding technical choices are presented and justified under this view. The need for adaptability and extendability points to the usage of virtualization technologies for the SAT deployment. Certain technologies (such as Docker) have been considered and the relevant advantages have been identified.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

3.3.3 Use-cases view

This view clarifies the basic SAT user-roles i.e., common and expert user, each with different functionality. Each role is clearly described and subsequently the respective SAT use-cases (i.e., instances of the SAT usage such as login or viewing entities) are detailed.

4 Activity 5: Dissemination and Exploitation activities

The main objective of Activity 5 is to disseminate the project's results to the relevant audience through a broad range of traditional, online and novel communication channels. In addition, Activity 5 places emphasis on the exploitation of the achieved results. The 2CeVau dissemination and exploitation actions so far, are summarized as follows:

4.1 The 2CeVau workshop

One important milestone (i.e., M10) included in Activity 5 is the project workshop. It was organized during the project month 17 *i.e.*, December 2020 as an online event (due to covid-19 measures). The workshop took place in conjunction with the well-established ITS Hellas Conference (as originally scheduled, see part D of the action) which gathered an important size of attendees i.e., more than 350 registered participants.

Based on its rich agenda (see Figure 2), the 2CeVau workshop efficiently facilitated the dissemination of the project concept and achievements in a broad stakeholders' community. Despite the belayed start, coming after a dense program of the ITS Hellas conference, the workshop attracted the interest of 26 - 42 online participants (in the course of its time duration). In what follows we briefly describe its content.

4.1.1 First part: Presentations from consortium members

A short welcome by the workshop organizer (i.e., ICCS) opened the workshop. Its first part included five short presentations delivered by consortium partners introducing the concept and so-far findings of the project. The introductory presentation delivered by the project coordinator (see Figure 3) provided the means for the audience to familiarize with the project concept and objectives. Four technical presentations followed describing the selected use-cases, the risk analysis methodology as well as the details in identification of involved threats and security/privacy requirements.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

Timeslot	Presentation	Presenter's Name *(Partner)*
15:30 - 15:35 *Duration: 5min*	**Welcoming** (short workshop description)	*Dr. Panagiotis Pantazopoulos*
15:35 - 15:40 *Duration: 5 min*	**Overview of the 2Cevau Project**	*Prof. Athanasios Kanatas (2CeVau coordinator)*
15:40 - 15:50 *Duration: 10 min*	**Use cases of** "Thessaloniki, Sofia, Belgrade (GR-BG-SRB)"	*Prof. Konstantinos Maliatsos*
15:50 - 16:00 *Duration: 10 min*	**Cyber-security challenges in (AD) corridors**	*Prof. Konstantinos Lambrinoudakis*
16:00 - 16:10 *Duration: 10 min*	**Vulnerabilities and Threats of Connected Vehicles**	*Christos Lyvas, Msc*
16:10 - 16:20 *Duration: 10 min*	**Security Assessment Tool** (design & expected functionality)	*George Drainakis, Msc*
16:20 - 16:35 *Duration: 15min*	**Cybersecurity in the connected and automated mobility world**	*Dr. Apostolos Malatras* *Network and Information Security Expert* *ENISA - European Union Agency for Cybersecurity*
16:35 - 17:00 Duration: 25 min	**Round table discussion**	**Moderator**: *Dr P. Pantazopoulos* **Participants** • ***Sophia Papathanosopoulou*** *Head of National Broadband Planning Dept Ministry of Digital Policy, Telecommunications and Media* • ***Prof. Christos Kalloniatis*** *Associate Professor University of the Aegean* • ***Prof. Konstantinos Lambrinoudakis*** *Head of the Department of Digital Systems Director, System Security Laboratory, University of Piraeus* • ***Athanasios Iatropoulos*** *Digital Convergence & Information Systems Dep. Director, Egnatia Odos S.A.*

Figure 2 The 2CeVau workshop agenda

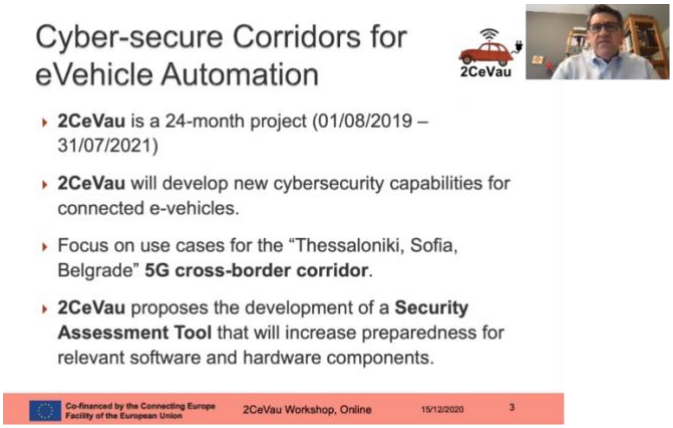


Figure 3 The 2CeVau coordinator introducing the project scope and vision

The first part concluded with a short presentation of the design of the SAT which is currently under-development in the context of the project.

4.1.2 Second part: External expert talk

An invited expert from ENISA (Dr Apostolos Malatras) followed delivering a detailed presentation of the work done by the agency in the area of connected vehicles (see Figure 4).

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

Figure 4 ENISA expert presenting the work carried-out by the agency

Special emphasis was placed on the latest ENISA report (published in late November 2020) that was dedicated to the cybersecurity holistic view of the connected and automated mobility ("CAM") ecosystem.

4.1.3 Third part: Round-table live discussion

Finally, a round-table discussion (see Figure 5) concluded the workshop shading some light in theoretical and practical cybersecurity challenges of the considered environment. Apart from two consortium partners (i.e., Mrs. S. Papathanasopoulou from the Hellenic Ministry of Digital Policy and prof. C. Lambrinoudakis from UPRC) there were two 'external' experts, one coming from academia (prof. C. Kalloniatis) and one coming from the EGNATIA runway (Mr. A. Iatropoulos). The discussion was moderated by Dr. P. Pantazopoulos moving from generic cybersecurity challenges in the connected vehicles and then directed towards dedicated corridor challenges.

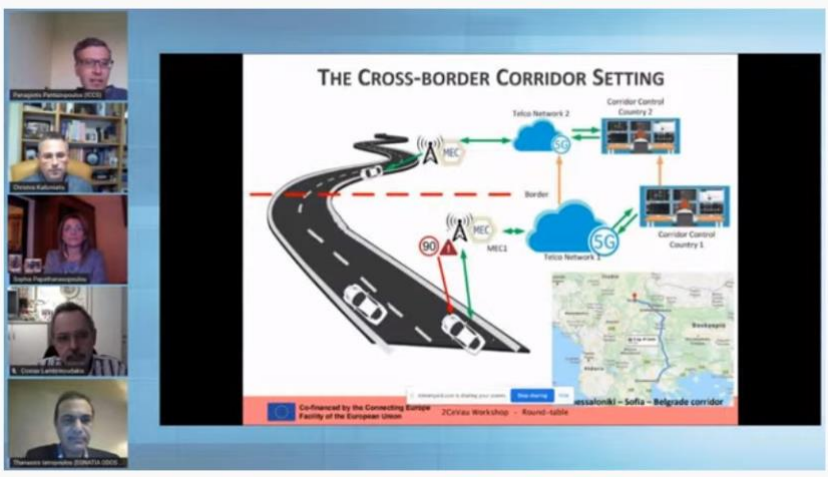


Figure 5 Discussing the cross-border cybersecurity challenges in the round-table

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

Among the interesting ideas discussed, a few noteworthy highlights perfectly in line with the view of 2CeVau work, are the following:

- The notion of "*IoT on wheels*" (used also by the ENISA report) is becoming increasingly relevant to present the way that the connected vehicles paradigm should be considered in terms of cybersecurity challenges.
- The propagation of threats in the complex setting of the connected vehicles and accordingly in the cross-border corridor (and relevant ICT infrastructure) is demanding and remains an open research challenge.
- The role of the end-user (i.e., driver) as a potential source of risk or vulnerability for the whole system was pointed-out both from the research and the highway ICT infrastructure standpoint.

4.2 Additional Activity 5 Actions

Dr. Pantazopoulos represented the 2CeVau project in the 23rd virtual IEEE International Conference on Intelligent Transportation Systems 2020 that was held online on the 20-23rd of September. He specifically participated in the CyberSec Workshop and gave a speech on "Risk Analysis and Security Assurance in Connected Vehicles: The SAFERtec and 2CeVau approach".

Furthermore, Dr. Pantazopoulos was invited as a special guest speaker in the Functional Safety Community (FuSaCom) online event that took place on the 28th of September 2020. Dr. Pantazopoulos gave a virtual oral presentation on "Risk Analysis and Security Assurance in Connected Vehicles", focusing on the research work that is carried out in the 2CeVau project.

Finally, Dr. Maliatsos (Technical Manager of the 2CeVau) participated in the EU CCAM Single Platform virtual meeting that took place online on the 15th of October 2020, in the Working group "WG5 Cybersecurity and Access to Data".

5 Conclusions

This deliverable includes all the research investigations and the work carried out during the last 6 months of the 2CeVau project (August 2020 – January 2021). The description of the work in this report was categorized by activity. Activity 2 was not included in this report since this activity had already been completed in August of 2020.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115.

This project has received funding from the Connecting Europe Facility (CEF) – Telecommunication Sector under grant agreement no. INEA/ /CEF/ICT/A2018/1807631, Action No: 2018-EL-IA-0115