



D7.5

Road Mapping and Business Modelling

Topic	H2020-SU-ICT-01-2018-2020
Project Title	Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles
Project Number	833611
Project Acronym	CARMEL
Contractual Delivery Date	M30
Actual Delivery Date	M33
Contributing WP	WP7
Project Start Date	01/10/2019
Project Duration	30 Months
Dissemination Level	Public
Editor	8Bells
Contributors	ATOS, CAPGEMINI, NEXTIUM, GFX, AVL, PANA

Document History

Document History		
Version	Date	Remarks
0.1	01.01.2022	Initial Document Structure, Table of Contents
0.2	30.05.2022	Second draft, compilation of content
0.3	03.06.2022	Third draft, structure and content adjustments
0.4	24.06.2022	Final draft, internal review
0.5	30.06.2022	Final document, consolidated for EC submission

Contributors		
Name	Organisation	Type of contribution
Jordi Guijarro Olivares	i2CAT	internal reviewer
Wael Yahyaoui	Capgemini	internal reviewer
Peter Hofmann	DT-sec	internal reviewer
Thomas Konidakis	8Bells	Editor
Kostas Pilaftsis	8Bells	Editor
Miranda Garcia, Alberto	ATOS	Contributor
Natàlia Porras Mateu	Nextium by idneo	Contributor
Bob Elders	Greenflux	Contributor
Petros Kapsalas	Panasonic	Contributor
Nikos Argyropoulos	CLS	Contributor
Irene Karapistoli	CLS	Contributor
Frantzoglou Vasileios	8Bells	Contributor
Tsagkarinou Natasia	8Bells	Contributor
Skoulaxinos Ilias	8Bells	Contributor

DISCLAIMER OF WARRANTIES

This document has been prepared by CAMEL project partners as an account of work carried out within the framework of the contract no 833611. Neither Project Coordinator, nor any signatory party of CAMEL Project Consortium Agreement, nor any person acting on behalf of any of them:

- makes any warranty or representation whatsoever, express or implied,
 - with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
 - that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
- that this document is suitable to any particular user's circumstance; or
- assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if Project Coordinator or any representative of a signatory party of the CAMEL Project Consortium Agreement, has been advised of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

CAMEL has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833611. The content of this deliverable does not reflect the official opinion of the European Union. Responsibility for the information and views expressed in the deliverable lies entirely with the author(s).

DISCLOSURE STATEMENT

The following document has been reviewed by the CARMEL External Security Advisory Board as well as the Ethics and Data Management Committee of the project. Hereby, it is confirmed that it does not contain any sensitive security, ethical, or data privacy issues.

Table of Contents

List of Figures	6
List of Tables	7
List of Acronyms	8
1. Introduction	11
1.1. Purpose of this document	11
1.2. Focus Areas and Analysis Tools	11
1.3. Document Overview	12
2. Methodology Approach and Tools	13
2.1. PESTLE Analysis	13
2.2. SWOT Analysis	14
2.3. Business Model Canvas	16
3. CAMEL Market Analysis	18
3.1. Automotive Cyber Security - Market Overview	18
3.2. PESTLE	22
3.3. SWOT	37
4. Business modelling and Financial plan	41
4.1. Business Model Canvas	41
4.1.1. Pillar 1 (autonomous mobility) BMC	42
4.1.2. Pillar 2 (connected mobility) BMC	43
4.1.3. Pillar 3 (electromobility) BMC	44
4.2. Business Model Outlines	47
4.2.1. Pillar 1 – The autonomous mobility business perimeter	47
4.2.2. Pillar 2 - The connected mobility business perimeter	48
4.2.3. Pillar 3 – The electromobility business perimeter	49
4.3. Business Model Logic	50
4.4. Pricing, Structure	51
4.4.1. Pricing, Conclusion	53
4.5. Viability	54
4.5.1. Product Lifecycle	54
4.5.2. Sustainability Roadmap	55
4.5.3. Next Steps	56
4.5.4. Potential Commercial Leads	56
4.6. IPR Agreement	58
4.7. Individual Exploitation Plans	59
5. Conclusions	63
References	115

List of Figures

FIGURE 1: PESTLE FACTORS - SOURCE: PESTLEANALYSIS.COM	13
FIGURE 2: COMPONENTS OF SWOT ANALYSIS - SOURCE: WIKIPEDIA.ORG	15
FIGURE 3: BUSINESS MODEL CANVAS - SOURCE: CORPORATEFINANCEINSTITUTE.COM	16
FIGURE 4: THE AUTOMOTIVE CYBER SECURITY ECOSYSTEM - SOURCE: AUTOMOTIVE CYBER SECURITY 2025: THE SECURE CONNECTED CAR, AUTO2XTECH.COM	18
FIGURE 5: THE 18% OF AUTOMOTIVE OEMS ARE LEADING THE CYBERSECURITY DOMAIN - SOURCE ACCENTURE	22
FIGURE 6: CYBERSECURITY ATLAS, COMPETENCY MAP, CYBERSECURITY RESEARCH INSTITUTIONS IN TRANSPORTATION - SOURCE: EUROPEAN COMMISSION	26
FIGURE 7: THE EU CYBERSECURITY TAXONOMY - SOURCE: EUROPEAN COMMISSION	26
FIGURE 8: MOST SIGNIFICANT GOODS BY VALUE IN INTRA-EU EXPORTS. MOTOR VEHICLES TRADE REACHED € 371.7 BILLION IN 2021 - SOURCE EUROSTAT	29
FIGURE 9: CYBERATTACKS WITH A SIGNIFICANT ECONOMIC IMPACT (>1M €) PRESENT, IN THE LAST 5 YEARS, A STEADY MONTHLY RATE OF INCIDENTS - SOURCE (OLIVIA WHITE, 2022).	30
FIGURE 10: STRUCTURE OF ATTACK SURFACE LAYERS AND DISTRIBUTION OF POTENTIAL ENTRY POINTS	34
FIGURE 11: BUSINESS MODEL LOGIC BEHIND CAMEL	51
FIGURE 12: PRICING STRUCTURE BASELINE	52
FIGURE 13: INNOVATION ADOPTION LIFECYCLE	54
FIGURE 14: BUSINESS LIFECYCLE, SOURCE: INTERNAL (ATOS)	55

List of Tables

TABLE 1: PILLAR-1, PRICE STRUCTURE	52
TABLE 2: PILAR 1, LICENSE RANGES	52
TABLE 3: PILLAR 2, PRICE STRUCTURE	53
TABLE 4: PILAR 2, LICENSE RANGES	53
TABLE 5: PILLAR 3, PRICE STRUCTURE	53
TABLE 6: PILAR 3 LICENSE RANGES	53
TABLE 7: CARMEL SUSTAINABILITY ROADMAP	55
TABLE 8: IPR DISTRIBUTION TABLE	59
TABLE 9: PARTNERS' EXPLOITATION PLANS - BASIC OVERVIEW	62

List of Acronyms

AI	Artificial Intelligence
ALKS	Automated Lane Keeping Systems
AML	Advanced Mobile Location
ASDL	Automotive Secure Development Lifecycle
ASIL	Automotive Safety Integrity Levels
ASIL	Automotive Safety Integrity Levels
AUTOSAR	AUTomotive Open System Architecture
B2B	Business-to-Business
B2C	Business-to-Consumer
BMC	Business Model Canvas
BSP	Basic Software Package
CAL	Cybersecurity Assurance Level
CAN	Controller Area Network
CCAM	Cooperative, Connected and Automated Mobility
CEF	Connecting Europe Facility
CERT	Computer Emergency Response Team
CFI	Control Flow Integrity
CPO	Charge Point Operators
cPPP	Contractual Public-Private Partnership
CSIRT	Computer Security Incident Response Team
DC	Direct Current
DCOSS	Distributed Computing in Sensor Systems
DPI	Deep Packet Inspection
DSO	Distribution System Operator
eCall	European Union emergency call service for motorists
ECCC	European Cybersecurity Competence Centre
ECISO	European Cyber Security Organisation
ECUs	Electronic Control Units
eMSP	electroMobility Service Provider
ENISA	European Union Agency for Network and Information Security
EVs	Electric Vehicles
EVSE	Electric Vehicle Supply Equipment
GDP	Gross Domestic Product
GNSS	Global Navigation Satellite System
GUI	Graphical user interface
HMI	Human-Machine Interface
HSM	Hardware security module
ICE	Internal Combustion Engines
ICT	Information and Communication Technologies

IoV	Internet of Vehicles
IPR	Intellectual Property Rights
ISACs	Information Sharing and Analysis Centres
IT	Information Technology
JRC	Joint Research Center
kWh	kilowatt-hour
M2Ms	Machine-to-machine
MEC	Multi-access Edge Computing
ML	Machine Learning
MNOs	Mobile Network Operators
NCAs	National Competent Authorities
NFV	Network function virtualization
NIS	Network Information System
OBU	On Board Unit
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer
OES	Operators of Essential Services
PASEU	Panasonic Automotive
PESTLE	Political; Economy; Social; Technology; Legal; Environment.
PKI	Public Key Infrastructure
PPPs	Public Private Partnerships
RCV	Remote Control Vehicle
RTOs	Recovery Time Objective
SAE	Society of Automotive Engineers
SDN	Software-Defined Networking
SHE	Secure Hardware Extensions
SID	Security Identifier
SOAR	Security, Orchestration, Automation, Response
SPOC	Single Points of Contact
SWOT	Strengths, Weaknesses, Opportunities, Threats analysis
TCOS	Telekom Card Operating System
TRL	Technology Readiness Level
UN	United Nations
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything (X represents everything)
WP	Work Package

Executive Summary

While the global economy becomes more and more dependent on connectivity, digital resources, smart hardware and inter-meshed networks, the need to effectively address the widening exposure to new cyber-threats increases along. Digital transformation technologies spur innovation and growth also in the automotive domain, reshaping the respective value chains, through interactions with terrestrial, wireless and cloud ecosystems, but also attract hackers with increased capabilities to disrupt operations and business lines by exploiting the vulnerabilities in the governance and infrastructure.

The much larger exposure dictates a paradigm shift around how to address cybersecurity threats in automotive systems. Conventional cybersecurity techniques aimed on perimeter defense, access control and accountability seem to be no longer adequate to counter cyber breaches, including insider threats. The automotive cybersecurity model is required to shift to a zero-trust architecture, which will continuously query the security, vulnerability, and reliability at all times.

Deliverable D7.5 explores the unique modalities of the automotive domain and its associated market & business models, within the universality & ubiquity of connected vehicles, identifying the challenges introduced by new disruptions and the solutions available around the fundamental concept of zero trust cybersecurity.

The deliverable provides the necessary market concept that is required to be defined for the implementation of the CAMEL solution and offers a clear view of the CAMEL market by conducting a market analysis using a combination of tools. A PESTLE analysis is used to assess if overall conditions are favorable for launching CAMEL into the market. Followed up by a SWOT analysis, to estimate the level of strategic advantage for the CAMEL solution.

Moreover, a business road mapping is conducted, providing deeper knowledge of the factors that affect CAMEL market adoption and evolution using the Business Model Canvas methodology.

This deliverable also focuses on the project pilot cases, namely Pillar 1, autonomous mobility; Pillar 2, connected mobility; and Pillar 3, electromobility; by offering a value proposition, a Business Canvas and a Business plan activity map for each one of them in order to better describe the consortium's strategy towards bringing the CAMEL solution to the market.

In general, D7.5 is attempting a methodic juxtaposition of the CAMEL solution as a whole, against all institutional, technological and market dimensions that define the complex physical and anthropogenic environment of automotive functions. This operating environment is evolving dynamically and generating constantly multifaceted, omnipresent and mutating cybersecurity risks. The besting of such agile threats starts from the capability of acquiring and maintaining a credible and up-to-date situational awareness and requires moreover an effective management and risk mitigation framework of pre-set protective measures, swift response to counter flaring of incidents and fluid re-structuring of defences.

1. Introduction

1.1. Purpose of this document

This deliverable provides a definition of the CARMEL market with special focus on the project use cases and identifies the key stakeholders taking part in each of them. The report considers the different market possibilities and tools that will make the CARMEL product(s) sustainable and at a time ensure the services will be adaptable and feasible in the energy security market segment.

- The specific objectives of the deliverable are the following:
- Provide a clear picture of the CARMEL market based on the specific information that stems from each use case of the project.
- Conduct a business roadmap analysis to provide a deeper knowledge of the factors affecting CARMEL market adoption and evolution, by using multi-criteria decision-making methods.
- Analyze the specific market of the project, including its definition, segmentation, target market and competitors.
- Analyze the key stakeholders for each use case identifying their characteristics, relations and inter-relations.
- Extract the value chain of each use case, as a result of the market and stakeholder analysis.

For our analysis, we will be considering the EU market as our target market. Thus, we will be assessing the market dynamic and the competitive framework of the EU market environment. Once the above assessment is complete, we will elaborate on how the CARMEL project can create value in that market and which business plan can lead to the optimal value creation. Finally, we will be assessing our business model's competitive advantage and sustainability against our competition.

1.2. Focus Areas and Analysis Tools

This section presents a summary of the focus areas and the analysis tools that are used in this document. Further analysis of the tools and methodologies used can be found in Section 2 of the report.

First, a market environment analysis is conducted, offering insights of the environments of the CARMEL project. This market analysis is conducted using the following environment appraisal frameworks:

- PESTLE analysis:** a framework used to analyze and monitor those environmental factors that may pose a significant impact on an organization's performance. PESTLE offers general insights into the nature of the elements that affect businesses and generally have an indirect impact on the company.
- SWOT Analysis:** a strategic planning technique that offers insights into internal and external factors that a company is expected to face in the market. It is more of a brainstorming technique that provides a compilation of a company's Strengths, Weaknesses, Opportunities and Threats (SWOT).

- c. **Business Model Canvas:** an overview strategy layered out into crucial activities and challenges involved and the correlation of the individual elements.

1.3. Document Overview

This deliverable is structured in 5 distinct sections. After the current Section 1, which introduces us to the scope and focus areas, comes Section 2 to describe the various methodological tools that are applied for the analysis of CARMEL. Section 3 provides the output and findings, from the application of the aforementioned methodologies, specifically for the CARMEL solution, as a whole, in the form of a market analysis. Section 4 explores and evaluates the business modelling and financial plan, in terms of exploitation capacity and potential, for CARMEL's three distinctive Pillars and for each of the individual partners of the consortium. Finally, Section 5 draws the conclusions to be noted.

2. Methodology Approach and Tools

This section concerns the literature survey of the tools and methodologies that will be used for the market analysis, the business road mapping and the business modelling analysis of the deliverable.

2.1. PESTLE Analysis

One of the standard tools used for market analysis is the PESTLE tool¹. PESTLE analysis is used in order to measure the impact of the macro-environment on a company. Investigating the macro-environment enables the identification of different specific factors such as geographical area, market, sector of activity etc., leading to measuring their influence on a company².

The different areas of concern, described in PESTLE and illustrated in Figure 1, are used to identify the factors specific to a situation (geographical area, market, company, sector of activity etc.) and thus able to measure the impact of these factors on an organization. They are briefly summarized below.

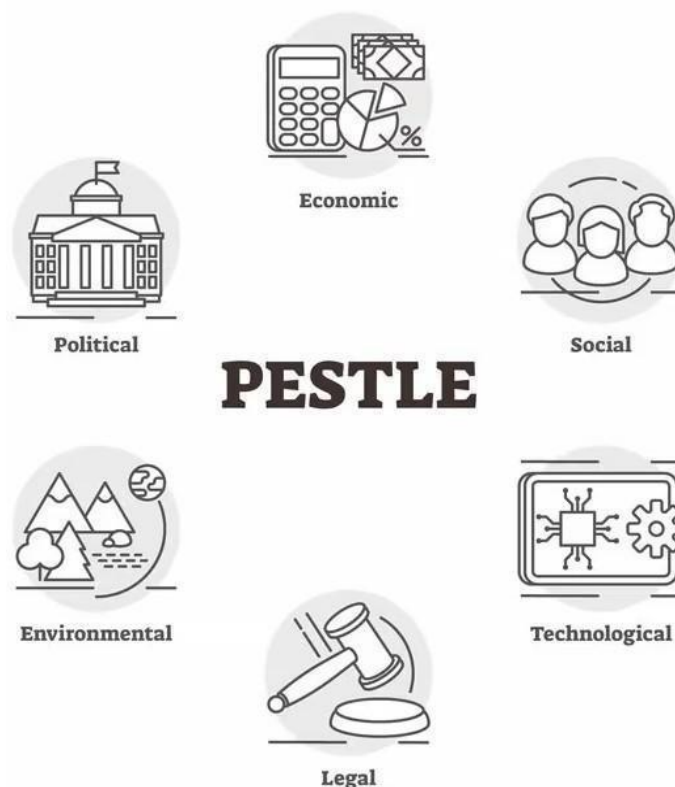


Figure 1: PESTLE factors - Source: pestleanalysis.com

- **Political Environment:** The range of operation of this category covers all levels, from regional to international, regarding mainly institutions, policies and governance instruments. Furthermore, all aspects concerning the political behavior of a society are also included.
- **Economic Environment:** This category involves several different factors such as

¹ "Pestle analysis." <https://pestleanalysis.com/what-is-pestle-analysis/>

² T. Issa, T. Issa, et al., "Sustainable business strategies and pestle framework," GSTF Journal on Computing (JoC), vol. 1, no. 1, 2014.

the purchasing power and consumption expenditure of customers and suppliers. Furthermore, it considers factors that concern the socio-economic area, such as the distribution of wealth.

- **Social or Sociocultural environment:** The different features of the population (age range, size, etc.) are included in this category, together with factors that may pose an impact in the way the population has access to products and services. Some of these factors concern the level of information access, the educational level and the various social and cultural trends.
- **Technological Environment:** This category is about the financial support that is provided to R&D activities. These activities aim at producing new knowledge and creating new products that will set the barrier of innovation of a company.
- **Legal Environment:** This is in direct relation with laws, regulations, controls and standards that impact a company or organization. In addition, and in a more indirect way, it also regards the people within these organizations which are also affected.
- **Environmental or Ecological context:** This category is more about defining all these aspects related to policies of preserving nature and sustainable development that influence an organization and its products and services.

The corresponding PESTLE analysis for the CARMEL project is provided in Section 3.

PESTLE is often used in conjunction with the SWOT analysis tool that is described in the next section.

2.2. SWOT Analysis

SWOT stands for Strengths, Weaknesses, Opportunities, Threats and it is an acknowledged analysis tool directed to formulating a business strategy. This analysis aims to define the objectives of a company/project and to specify all these factors that can affect in a positive or negative way the accomplishment of the objectives of the company/project. SWOT has been described as a proven tool for strategic analysis. Strengths and weaknesses are usually referred as internal factors, while opportunities and threats are referred as external factors. Below we briefly summarize the four different components of the SWOT analysis and in Figure 2 we provide an illustration of the SWOT analysis tool.

- **Strengths:** Aspects of a company/project that give it an advantage over the competition.
- **Weaknesses:** Features that pose a disadvantage to a company/project over the competition.
- **Opportunities:** All these elements that can be exploited and pose an advantage to a company/project.

- **Threats:** All these elements that could potentially harm a company/project.

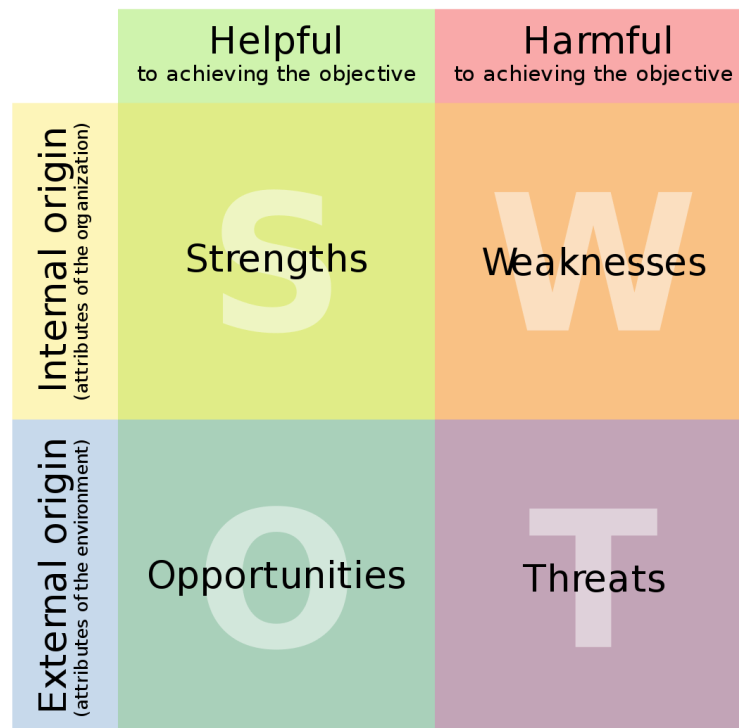


Figure 2: Illustration of SWOT analysis tool.

As mentioned above, when performing a SWOT analysis external and internal factors are identified and are addresses below:

- **External analysis:** It concerns the opportunities and threats present in the environment. A PESTLE analysis can be used in order to identify the opportunities and threats. The outcomes of the external analysis remain the same for all competitive parties.
- **Internal analysis:** It concerns the other two components of the SWOT, namely, the strengths and weaknesses of the business area. The outcomes of the internal analysis are specific to the company/project under study.

The expected result of a SWOT analysis is typically presented in the form of a table with a grid made up of four large boxes (see Figure 2):

- Vertically: two columns.
 - The column on the left collects the list of elements having a positive or favorable impact on the area of the studied strategic activity.
 - The column on the right collects the list of elements having a negative or unfavorable impact on the area of the studied strategic activity.
- Horizontally: two lines.
 - The elements that are related to internal factors are reported in the upper line. These elements - whose causes are internal - can be modified by the organization.
 - In the lower line, the elements that are related to external causes (and are therefore, in general, common to all competitors) are reported. These elements - whose cause or causes are external - are imposed on the leaders of organizations, who have no power over them.

2.3. Business Model Canvas

Business Model Canvas (BMC) was created by Osterwalder and Pigneur³ as a management tool for creating business models. It comes in a graphical form of nine components, as shown in Figure 3 that describe how an organization creates, delivers and captures value from a product or a service⁴. Brief details of the nine components of the BMC are listed below:

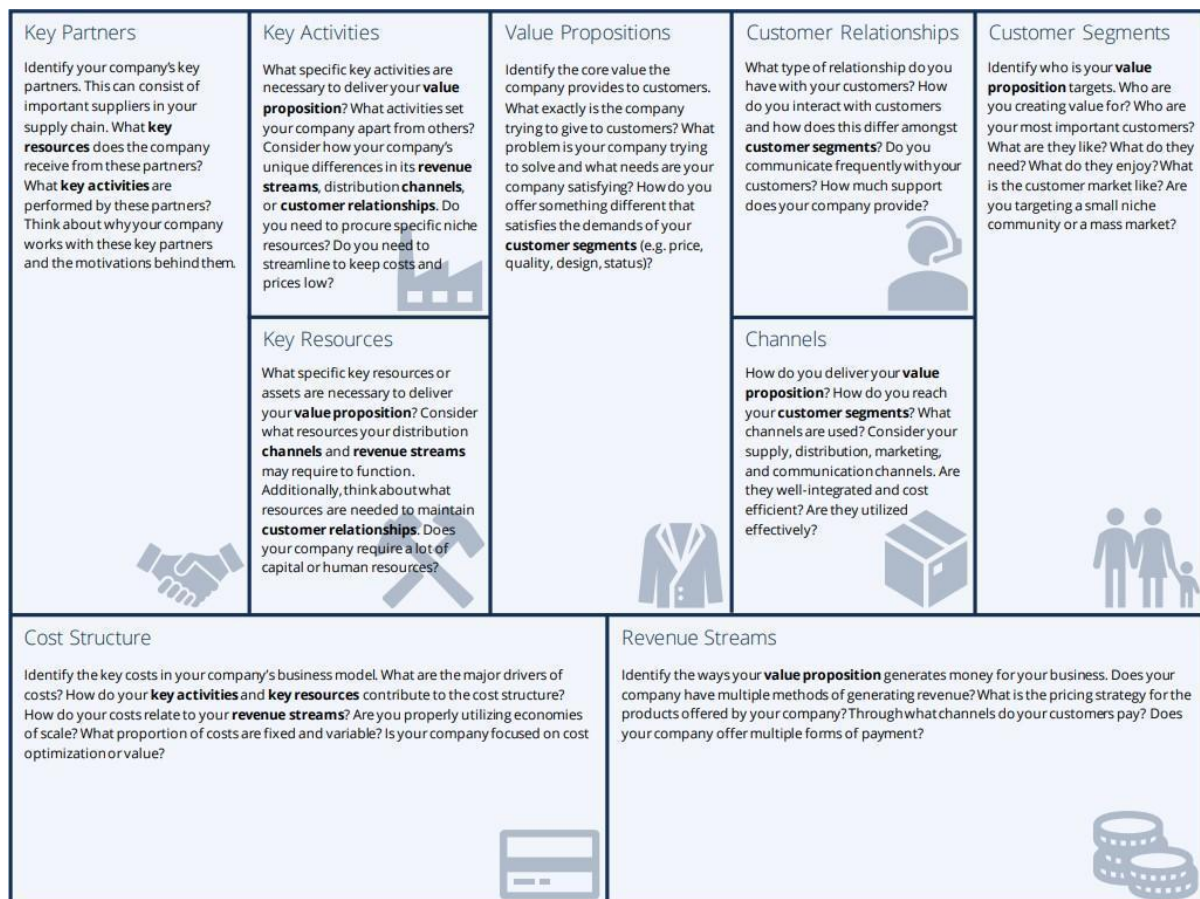


Figure 3: Graphical form of BMC tool.

2.3.1. Key Partnerships: The Key Partnerships Building Block describes the network of suppliers and partners that make the business model work.

2.3.2. Key Activities: The Key Activities Building Block describes the most important things a company must do to make its business model work.

2.3.3. Value Propositions: The Value Propositions Building Block describes the bundle of products and services that create value for a specific Customer Segment.

2.3.4. Customer Relationships: Customer relationships are established and maintained with each Customer Segment. The Customer Relationships Building Block describes the types of relationships a company establishes with specific Customer Segments (Qastharin,

³ A. Osterwalder and Y. Pigneur, Business model generation: a handbook for visionaries, game changers, and challengers, vol. 1. John Wiley & Sons, 2010

⁴ M. A. Toro-Jarrín, I. E. Ponce-Jaramillo, and D. Güemes-Castorena, "Methodology for the of building process integration of business model canvas and technological roadmap," Technological Forecasting and Social Change, vol. 110, pp. 213–225, 2016

2016).

2.3.5. Customer Segments: The Customer Segments Building Block defines the different groups of people or organizations an enterprise aims to reach and serve (T. Pervez, 2013).

2.3.6. Key Resources: Key resources are the assets required to offer and deliver the previously described elements.

2.3.7. Channels: Value propositions are delivered to customers through communication, distribution, and sales channels. The Channels Building Block describes how a company communicates with and reaches its Customer Segments to deliver a Value Proposition.

2.3.8. Cost Structure: The business model elements result in the cost structure. The Cost Structure describes all costs incurred to operate a business model

2.3.9. Revenue Streams: Revenue streams result from value propositions successfully offered to customers (G. Cardeal, 2020).

3. CARMEL Market Analysis

3.1. Automotive Cyber Security - Market Overview

The automotive industry is characterized by long-term relationships between an OEM and its suppliers and very long technology lifecycles. As an example, Bosch's Controller Area Network (CAN bus) technology, was developed in the 1980s as a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer. It was first rolled out in 1987, but today 35 years later, most cars on the road are still using this technology.

The increased connectivity requirements of modern cars come with new risks and challenges in the area of cyber security, as increased number of Electronic Control Units (ECUs), lines of software code, integration of new systems and fragmented supply chain, contribute to making finding countermeasures difficult.

Recent incidents with high public visibility, such as the white-hat hacking of a Jeep's software in 2015 while it was cruising at 70 miles per hour, forced the auto industry to prioritize cyber security.

Even though the market is still at its infancy, many companies in the market are now developing products and offer services in the area of cyber security, and there is increased M&A activity as well.

The Automotive Cyber Security Ecosystem is still evolving and the relevant market will change rapidly over the next decade, especially after the expected mandate for standard fitment of cyber security solutions in modern vehicles. Such mandate will be the catalyst that will drive change as competition will intensify and consolidation continues.



Figure 4: The Automotive Cyber Security Ecosystem - Source: Automotive Cyber Security 2025: the secure Connected Car, Auto2xtech.com

This ecosystem includes: OEMs, Automotive suppliers, Aftermarket vendors, vehicle

owners, dealers, fleet operators, vehicle drivers and passengers, Cyber Security companies in the Automotive and other related industries, regulators, law enforcements agencies, researchers, hackers, organized crime, software and hardware developers, smartphone and tablet manufacturers and many more.

Some governments have started to require regulatory bodies to define and deploy a set of guidelines for the industry on cyber security issues, however, most automotive regulatory bodies still have not concretely defined an approach to cyber security.

Therefore, the industry currently is still mostly unregulated with regard to cyber security and industry self-organization is occurring slowly with the first alliances on the topic starting to be established. Some positive first signs come from initiatives at the level of the United Nations.

In particular, UNECE Regulation Automated Lane Keeping Systems (ALKS), which came into force in 2021, will also need to comply with cyber-security and software update requirements (the Working Party on Automated/autonomous and Connected Vehicles 2020) set out in two other new U.N. regulations. UN Regulation 155, on Cybersecurity and Cyber Security Management Systems, and UN Regulation 156, on Software Updates & Software Updates Management Systems, refer to automotive cybersecurity and software updates and establish cybersecurity and software rules together with clear performance and audit requirements for OEMs (United Nations Economic Commission for Europe (UNECE) 2021), (United Nations Economic Commission for Europe (UNECE) 2021).

Given the widespread use of UN Regulations in the automotive sector around the world, the broad adoption of these regulations among and beyond 54 Contracting Parties to UNECE's 1958 Agreement is expected.

More Cyber Security solutions are now available to carmakers as new companies have entered the marketplace in the past 5 years. Most companies are headquartered in developed car markets and in Israel, one of the leading hubs for cyber security globally. Some notable cyber security supplier examples are listed below.

- **Aptiv** (USA) develops software and computing platforms for self-driving vehicles and collaborates with the ride-hailing service Lyft. The company's cybersecurity tools protect everything from a car's infotainment system to its wiring. (<https://www.aptiv.com/home>)
- **NVIDIA** (USA) uses AI-powered data processors and chips to operate and protect self-driving cars. The company's software and cloud-based technologies help autonomous vehicles securely learn and relay driving data. The NVIDIA deep learning systems have been used by Tesla, Mercedes-Benz, Audi, Toyota, Volkswagen and more to power and protect self-driving vehicles. (<https://www.nvidia.com/en-us/>)
- **Centri Technology** (USA) makes cybersecurity solutions for IoT-enabled devices in autotech. The Centri IoTAS installs on chips and mobile apps to protect automobile sensors as well as the data that helps cars learn important driver navigation preferences like optimal routes and addresses. The IoTAS platform requires no internet connection to protect IoT-enabled autotech devices. Instead, it connects to all trusted devices with identity management technology that requires around 40 percent less bandwidth than BLE and TLS. (<https://www.centritechnology.com/solutions-use-cases/automotive/>)
- **Dellfer** (USA) is an automotive cybersecurity startup focusing on coding for autotech software. The company's embedded code helps IoT-enabled cars battle cyber-attacks throughout a car's system. No Internet connection is needed to update critical patches. Instead, the company deploys code execution paths at runtime for security

enforcement. (<https://dellfer.com/>)

- **Argus Cyber Security** (Israel) provides commercial smart vehicles with anti-cyber-attack tools like connectivity and in-car network protection that safeguard everything from a vehicle's infotainment center to the communication networks that run between its software and hardware. Continental, the automotive parts manufacturing company, now owns Argus and integrates Argus' cybersecurity solutions into all of its connected vehicle electronics. Argus's Intrusion Prevention System uses Deep Packet Inspection (DPI) algorithms to detect hacking attempts and prevents them from affecting a vehicle's critical systems. It also notifies car manufacturers in real-time when these attempts are happening and enables seamless integration into any vehicle's production line. The company also offers Cyber Security Vulnerability assessments. (<https://argus-sec.com/>)
- **GuardKnox** (Israel) creates coding architecture for autonomous cars that operates everything from the general vehicle systems (including sensors) to tools that enhance a car's user experience (infotainment systems, center consoles and more). Porsche is using GuardKnox to improve cybersecurity in its new line of vehicles, in order to protect against hacking attacks and act as a foundation for "real-time customization of the vehicle." (<https://www.guardknox.com/>)
- **Harman** (USA) partnered with IBM to develop the Harman SHIELD, which protects key entry points of a car's network from hackers. In addition, it continuously performs a threat analysis to determine which points are most vulnerable at any given moment. In recent years, Harman has acquired Red Bend Software and TowerSec, who were focusing in the area of cyber security. (<https://services.harman.com/>)
- **Intertrust** (USA) makes products that help personalize drivers' cybersecurity needs and overall experience, including tools that protect a vehicle's infotainment center, prevent unauthorized entry and stop the gathering of personal data. One of Intertrust's software products, whiteCryption, speeds up and safeguards content delivery to drivers. Another tool, Personagraph, encrypts a driver's personal data. (<https://www.intertrust.com/solutions/connected-car/>)
- **Britive** (USA) is a cloud-native security software offering API-based integrations and access administration capabilities for applications. Its software is used for securing cloud data and managing user authorization for businesses across multiple industries, including automotive. Toyota was able to shorten the set-up of user authorization and role-based action control privileges for Toyota user accounts from three days to 30 seconds using Britive platform technology. (<https://www.britive.com/>)
- **Thales** (France) provides electrical system engineering services for IoT hardware, software, devices and vehicles. Its services within the transportation and automotive industries operate with an emphasis on cybersecurity and data regulation compliance. In 2021, Thales announced a partnership with Gireve, a company created to further connect electromobility operators in Europe, collaboratively creating the "Plug & Charge" system. This project allows drivers to charge their electric vehicle at any participating compatible charging station, and be automatically billed through a secure card-free transaction. (<https://www.thalesgroup.com/en>)
- **Cisco** (USA) offers both services and software solutions in the Automotive Cyber Security market. Cisco offers the Auto Guard, a holistic security solution for vehicles which includes anomaly-detection, hardening and other Vehicle Area Network security functions. The solution is also set to extend to offer real-time, over the air updates for vehicle ECUs. (<https://www.cisco.com/c/en/us/about.html>)

- **Arilou Technologies** (Israel) offers cyber security solutions in the fields of car cyber security (CAN bus), hacking and penetration testing. Apart from conducting Cyber Security Vulnerability assessments, the company has developed the Security Agent, an IPS and CAN bus firewall that can be integrated into the existing vehicle's CAN network and blocks any attempt to send illegal messages on the network. (<https://ariloutech.com/>)
- **Escript** (Germany), a member of the Bosch Group, is a leading provider of IT security solutions in embedded systems and provides consulting and services for enterprise security and IT-protected production. In the area of automotive security, products from ESCRIPT are chosen by many OEM's and Tier 1 automotive suppliers (<https://www.escript.com/en>)
- **Karamba Security** (Israel) is building deterministic security into the fabric of ECU software, creating the self-defending vehicle. Karamba's Automotive Control Flow Integrity (CFI) doesn't rely on updates and the protection is always on and remains stable over the life of the car or truck, therefore it's safe and secure by design. Karamba XGuard and SafeCAN deliver end-to-end protection—from the external connection points where hackers seek entry to the in-vehicle networks where they take control. This comprehensive solution integrates security into the ECU image build—without developer involvement. (<https://karambasecurity.com/industries/automotive>)
- **NXP Semiconductors** (Netherlands) designs and manufactures semiconductors. They have developed a multilayer approach for automotive security, by employing the 4+1 framework:
 - Secure Interfaces layer, using strong encryption and authentication to ensure that the vehicle is only communicating with known (trusted) entities and that received data can be trusted.
 - Secure Gateway layer acting as a firewall that controls access from the external interfaces (such as the Internet) to the vehicle's inner network, and controls which nodes in the vehicle's network can communicate with each other. As such, it provides domain isolation between for example, infotainment systems and safety-critical systems. It also converts between the different automotive communication protocols.
 - Secure Networks layer protecting the communication over various in-vehicle networks against data manipulation and data theft. It includes intrusion prevention and intrusion containment capabilities.
 - Secure Processors, comprising of a broad portfolio of automotive microcontrollers and processors featuring dedicated automotive (SHE and HSM) security modules that protect software from being manipulated and supporting secure software updates and data protection.
 - Secure Car Access layer, providing traditional physical vehicle protection through anti-theft immobilizer and smart car access functions. Innovations in this area include new features like remote lock and unlock, passive start, remote vehicle monitoring and car access using a smartphone or smart key device.

(<https://www.nxp.com/applications/automotive/functional-safety-and-automotive-security/secure-vehicle-architecture:AUTOMOTIVE-SECURITY>)

- **SBD & NCC.** Automotive technology expert SBD and global information assurance firm NCC Group have announced a unique and strategic partnership to improve

automotive cyber security. The partnership combines the expertise of SBD in connected car architectures and automotive security with NCC Group's expertise in cyber security testing. Together they have created the Automotive Secure Development Lifecycle (ASDL) to help vehicle manufacturers and their suppliers mitigate cyber security risks when developing connected cars. (https://safecarnews.com/staging/sbd-and-ncc-group-form-unique-automotive-cyber-security-partnership_o5153/)

In D7.5 we will use the tools of PESTLE and SWOT analysis, like different cartographic reference systems, in order to map and measure the environment where CARMEL is expected to deploy its comprehensive set of capabilities and services for managing cybersecurity risks, directly or indirectly related with the automotive domain, today and tomorrow.

3.2. PESTLE

With this PESTEL analysis we will examine the Political, Economic, Social, Technological, Legal and Environmental factors that identify and evaluate the market conditions, on a long-term level, for the introduction of CARMEL into the market. This analysis will describe and define the operational framework and provide a useful tool for development of business operations, market penetration activities and strategic placement.

The context for the application of PESTLE is particular to the European Union political, institutional, economic, operational, market and societal aspects of our collective vision, arrangements and activities.

“Some automotive companies were already ahead of the curve in cybersecurity, according to our most recent research. Accenture's detailed modeling of cybersecurity performance identified an elite group—just 18%—that achieve significantly higher levels of performance in at least three of these categories” (Accenture, 2020):

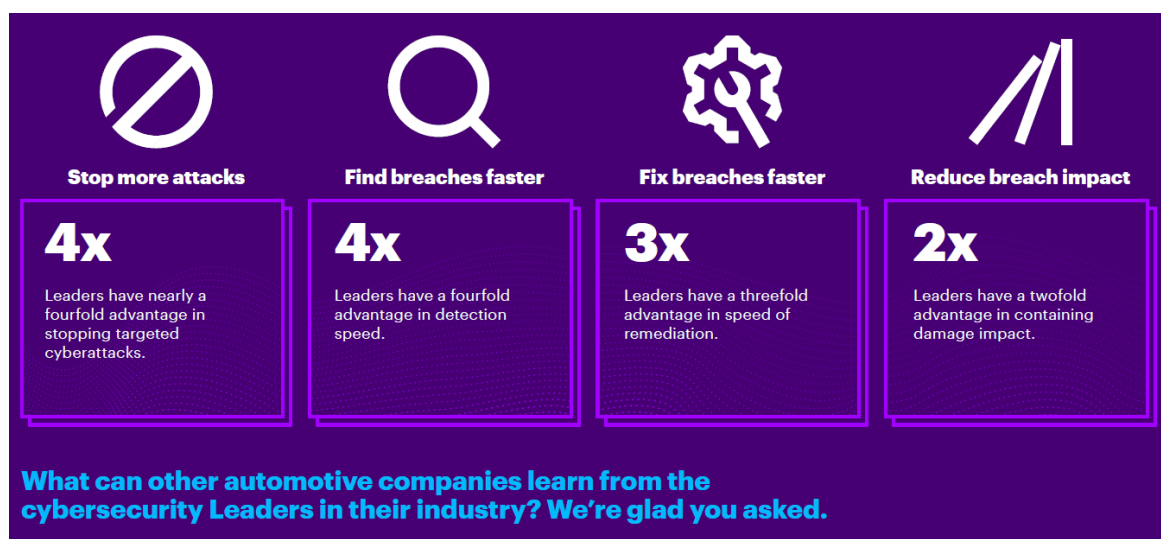


Figure 5: The 18% of automotive OEMs are leading the Cybersecurity domain - Source Accenture

Political	
<i>Instrument</i>	European Commission and the High Representative of the Union for Foreign Affairs and Security Policy: New EU Cybersecurity Strategy (2020)

	<p>"A key component of Shaping Europe's Digital Future, the Commission's Recovery Plan for Europe and of the Security Union Strategy 2020-2025..." It deploys "three principal instruments. These three instruments are regulatory, investment and policy initiatives. They will address three areas of EU action: resilience, technological sovereignty and leadership; operational capacity to prevent, deter and respond; cooperation to advance a global and open cyberspace. The strategy covers the security of essential services such as energy grids, railways and the ever-increasing number of connected objects in our homes, offices and factories." (European Commission 2022)</p>
<i>Institutional</i>	<p>ENISA – Cybersecurity Act – Certification framework</p> <p>A dedicated European Union Agency for Network and Information Security (ENISA) for cybersecurity. Supporting "Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive". The associated Cybersecurity Act is empowering the role of ENISA by providing a permanent mandate and calling for "operational cooperation and crisis management across the EU". Additionally, the EU-wide Certification framework strives to achieve "a single common scheme for certification a product has been checked and certified to conform to high cybersecurity standards". (European Commission 2022)</p>
<i>Instrument</i>	<p>European Commission: Recovery Plan and Support for research and innovation</p> <p>"The Recovery Plan for Europe includes additional investments in cybersecurity Cybersecurity is one of the Commission's priorities". Cybersecurity is a significant and recurring theme in funded research instruments like Horizon 2020 in the past and the ongoing Horizon Europe programmes. "In Horizon Europe, for the period 2021-2027, cybersecurity is part of the 'Civil Security for Society' cluster... As part of Horizon 2020... research and innovation into topics such as cybersecurity preparedness ... cybersecurity for small and medium-sized enterprises, cybersecurity in the electrical power and energy system, and cybersecurity and data protection in critical sectors. These topics fall under the cluster 'Secure societies — Protecting the freedom and security of Europe and its citizens.' In 2016, the Horizon 2020 contractual public-private partnership (cPPP) on cybersecurity was established between the European Commission and the European Cyber Security Organisation (ECISO), an association consisting of members from cyber industry, academia, public administrations and more." (European Commission 2022)</p>
<i>Instrument</i>	<p>European Commission: Cyber capacities and deployment support</p> <p>The Connecting Europe Facility (CEF), 2014-2020, the Digital Europe Programme, 2021-2027 and the InvestEU programmes support "computer security incident response teams, operators of essential services (OES), digital service providers (DSPs), single points of contact (SPOC) and national competent authorities (NCAs)" and invest more than "€1.9 billion into cybersecurity capacity and the wide deployment of cybersecurity infrastructures and tools across the EU for public administrations, businesses and individuals".</p>
<i>Instrument</i>	<p>European Commission: The ECCC and the Cybersecurity Atlas</p> <p>The European Cybersecurity Competence Centre and Network is an industrial, technology and research facility that pools expertise and aligns development and deployment of cybersecurity technologies. It works "with industry, the academic community and others to build a common agenda for investments into cybersecurity, and decide on</p>

	<p>funding priorities for research, development and roll-out of cybersecurity solutions through the Horizon Europe and Digital Europe Programmes". The Cybersecurity Atlas is a "knowledge management platform to map, categorize and stimulate collaboration between European cybersecurity experts in support of the EU Digital Strategy". These mapping activities include a research priorities roadmap, institutions and expertise distribution, taxonomy and competence network (see Figures 6 & 7 below) (European Commission 2022)</p>
<i>Institutional</i>	<p>European Commission: Policy guidance</p> <p>In the form of a blueprint for rapid emergency response in case of cyber incident or crisis, a Joint Cyber Unit to act as a platform for coordinated response and recovery assistance and an EU Toolbox on 5G with measures to strengthen security requirements for 5G networks. (European Commission 2022)</p>
<i>Instrument</i>	<p>European Commission: Skills & Awareness</p> <p>Active stimulation and development of cybersecurity skills through facilities like the European cybersecurity students yearly challenge, the inclusion in the general digital agenda and the awareness schemes for the general public and consumers. (European Commission 2022)</p>
<i>Instrument</i>	<p>European Commission: Cyber community</p> <p>Is formed by ENISA to provide support to Member States, EU institutions and businesses in cybersecurity directives and areas, the Information Sharing and Analysis Centres (ISACs) for advancing collaboration between the cybersecurity community in different sectors of the economy, the Joint Research Center (JRC) that contributes actionable studies & reports, the Computer Security Incident Response Teams that monitor incidents, provide early warning, alerts, risk analysis and response to incidents, the European Cybersecurity Organisation (ECISO) which is a contractual public-private partnership covering Horizon 2020 and the Women4Cyber Registry to acknowledge the importance of women in the European cybersecurity landscape. (European Commission 2022)</p>
<i>Instrument</i>	<p>European Commission: Cyber Policy Areas</p> <p>Dedicated provisions and facilities for the application of a cybersecurity framework and best practices particularly for the domains of Cybercrime, Cyber Diplomacy, Defence and Cyber capacity building in third countries. (European Commission 2022)</p>
<i>Scientific Advice</i>	<p>European Commission: Selected JRC publications (Science for Policy Reports)</p> <p>A curated, by the editor, collection of Joint Research Center's publications that deal directly or indirectly with all aspects Cybersecurity, including automotive, automated mobility, vehicles and transportation in general. These publications are purposed to provide scientific advice to the European Commission for its working with political and societal issues. (European Commission, Joint Research Centre 2022)</p> <ul style="list-style-type: none"> • An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe: Effects of automated driving on the economy, employment and skills (2018) • Place-based Innovation Ecosystems for emerging mobility-based business models: Methodology and a comparative analysis of case studies for mobility-as-a service. (2021) • ERA – JRC Workshop on Safety certification and approval of automated driving functions. (2021) • Innovation capacity in the transport sector: a European outlook.

	<p>(2020)</p> <ul style="list-style-type: none"> • Testing and certification of automated vehicles including cybersecurity and artificial intelligence aspects. (2020) • Research and innovation in transport electrification in Europe. (2020) • Trustworthy Autonomous Vehicles. (2021) • How will vehicle automation and electrification affect the automotive maintenance and repair sector. (2021) • Cybersecurity challenges in the uptake of Artificial Intelligence in Autonomous Driving (2021) • Research and innovation in smart mobility and services in Europe. (2020) • Mobility Imaginaries: Social and Ethical Issues of Connected and Automated Vehicles. (2021) • AI Watch: Revisiting Technology Readiness Levels for relevant Artificial Intelligence technologies. (2022) • On the application of sensor authentication with intrinsic physical features to vehicle security. (2021) • An Experimental Evaluation of Global Navigation Satellite System/Inertial Navigation System Verification Strategies for Vehicular Applications. (2020) • A multi-tier security analysis of official car management apps for Android. (2021) • Standardisation and Certification of Safety, Security and Privacy in the “Internet of Things”. (2022) • Cybersecurity, our digital anchor. (2020) • Digitranscope: The governance of digitally-transformed society. (2021)
<i>Geopolitical</i>	<p>Automotive and National Security</p> <p>Autonomous, connected and electromobility is already openly recognized as a potential risk to national security since “the powerful Cyber Administration of China, along with a suite of security-focused agencies, are rolling out expansive new data security laws, tightening control over data collection and privacy. Samm Sacks, a senior fellow at Yale Law School’s Paul Tsai China Center, said that “Tesla is under tremendous pressure” over data collection in China, in particular from individuals and near military or politically sensitive sites and its cross-border data flows. Last year, Tesla promised to store information collected in China in local data centres, a significant blow to its global data gathering efforts critical to research and development.” (Edward White 2022)</p> <p>Mobility in the digital age means that vehicles are simultaneously sensor platforms, data storage & processing units and network nodes on the move. As such the capacity of data collection, including personal data of drivers and passengers, pose a significant security risk since all collected and inferred information is kept under proprietary status by the vehicle manufacturer. If such manufacturer is owned and controlled by a foreign country, one can plausibly expect that this trove of data -and its inherent intelligence potential- could and would be eventually exploited by the security apparatus against any country of concern.</p>

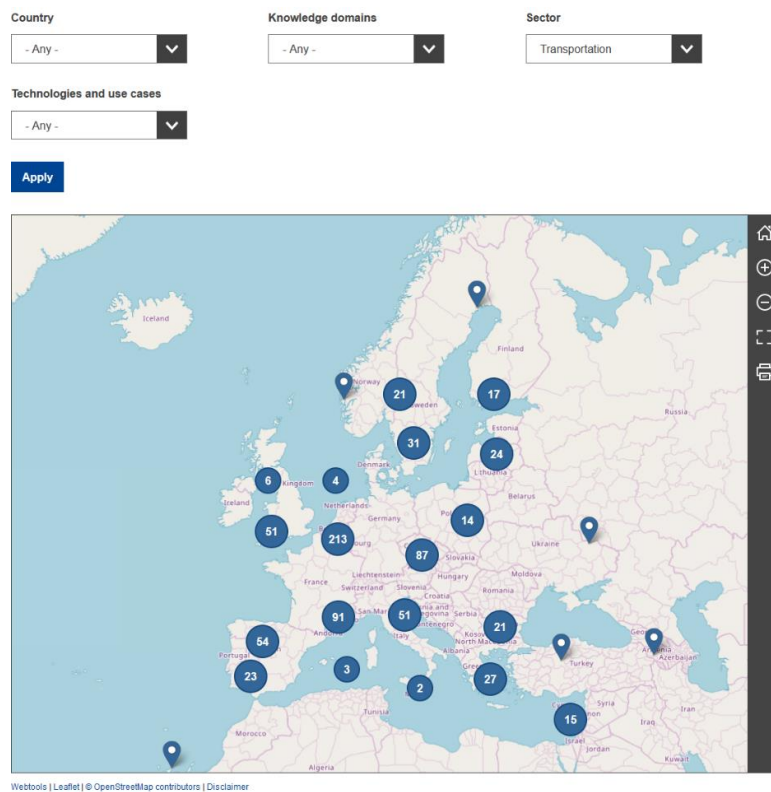


Figure 6: Cybersecurity Atlas, Competency map, cybersecurity research institutions in Transportation - Source: European Commission

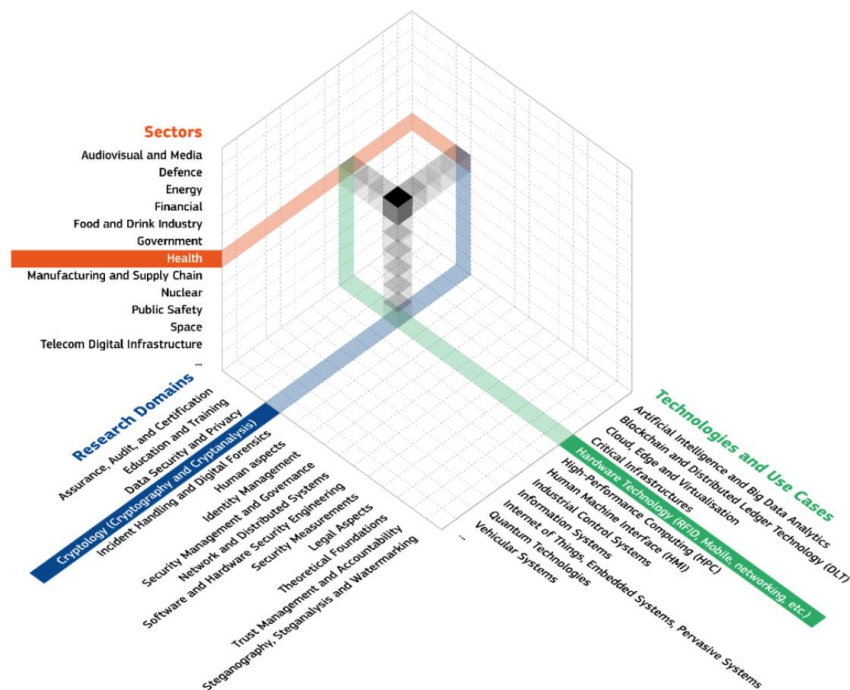


Figure 7: The EU cybersecurity taxonomy - Source: European Commission

Economic	
<i>Macro-level</i>	Condition of the economy <p>After a long period of stable conditions in the economy, where members enjoyed the stability of small -but steady- growth rates and low-interest policies, Europe is feeling the international upheaval which is instigated by the war in Ukraine. The energy and food sectors are already dealing with mitigation and risk management to alleviate disruptions in the respective supply chains. Since the geopolitical environment is currently under flux, also the economy, at collective or individual level, is reflecting these forces of change. The sharp rises in the prices of energy, the hardships of maintaining functioning supply lines, the stock exchange mood swings and the reshaping of markets affect drastically all economic activities including macro and micro economic aspects of the automotive, digital and electromobility industries. Although, these forces have the effect on altering the European Union's economic policies (e.g. inflation drives interest rates upwards) one can expect that Europe will soon find a new kind of equilibrium and recover effectively to install a new stability in terms of economic and market conditions in the business environment.</p>
	Size & metrics of the market <p>The European Union functions as a single market, where the 27 members act individually and collectively towards economic and commercial benefits. In terms of market value, the total, of all goods and services produced (gross domestic product or GDP) in the EU in 2019, when the UK was still part of the EU, was € 16.4 trillion. For the same year (2019), the EU accounted for € 4 071 billion in total global trade and from that the Intra-EU trade was valued at € 3 061 billion, placing Europe second, only to China in terms of absolute figures. See also figure 7 below. (Source: Eurostat)</p>
<i>Macro-level</i>	Demographic factors / Population growth <p>The population of the EU is estimated to be 513 million which categorizes it as the fourth biggest market in the world. Moreover, the EU population is expected to increase in the forthcoming decades reaching an all-time high of 525 million in 2044.</p>
<i>Macro-level</i>	Investments schemes & funded research, innovation and development activities <p>The EU employs a large, complex and multipurpose framework for supporting research, innovation and development activities through a multitude of funding instruments and capability building programs. This is complemented with investment facilities and access to business support tools for enablers of advanced technologies and applications. This is an all-inclusive environment where, private & state actors; Research Technology Organizations & Universities; Industrial Large System integrators & Corporates; along with SMEs & StartUps; are all potential beneficiaries of direct and indirect funding, cooperation and synergies, pooling & sharing platforms and all kinds of benefits that support Europe and its members to maintain technological parity with global state-of-the-art developments and moreover to field operational and commercial solutions of high performance and quality.</p>
<i>Macro-level</i>	Tax policies <p>Different national tax policies are employed within the member states of the EU regarding investments, business & professional activities, commercial transactions and income, regarding, direct and indirect, financial regulations, revenues and fees of the state.</p>

<i>Macro-level</i>	VAT (sales) tax
	Electronic products & services within the EU are susceptible to VAT, ranging from 17% to 27%, depending on the country and goods under consideration. (European Commission 2022).
<i>Industrial</i>	Supply Chain Reliability
	Recent geopolitical developments, global industrial base restructuring, market shifts and the omnipresent environmental factors continuously threaten the stability of any established supply chain. Disruptions and delays are possible and shall be expected at all levels & anytime. They tend to affect the weakest links of the production chain, whether bulk traded raw materials or OEMs who cater sophisticated items to integrators. Supply chain re-routing cost have to be considered and alleviated while mitigation strategies are needed for sustaining production output at planned levels.
<i>OPEX</i>	Compromised vehicles - OEMs
	High cost of recall & re-fit activities. Adverse publicity and brand damage unquantifiable. Cost-saving is expected through prevention instead of higher expenses of damage repair and rehabilitation.
<i>Reparation costs</i>	Compromised vehicles – Users/Consumers
	Financial cost of loss of life, injuries, damages and incapacitation of humans in the case of incidents & accidents caused due to cybersecurity issues of vehicles that directly pose a threat to the physical condition of occupants. Cost-saving is expected through prevention instead of higher expenses of damage repair and rehabilitation.
<i>Reparation costs</i>	Compromised vehicles – Material damages
	Financial cost of reparation and reimbursement activities for damages to material and non-tangible goods due to cybersecurity threat exposures.
<i>Market dynamics</i>	Product affordability & business viability
	Purchasing costs of EVs and charge stations are vital for mass adoption of EVs. Economic dynamics such as inflation and high price of energy impact use of charge stations.
<i>Market dynamics</i>	Justification for OEM, Aftermarket and Consumer cyber-security products & services
	Regulations, Awareness and Requirements establish a new niche market around automotive in terms of prevention, response and compliance.
<i>Market dynamics</i>	Market segmentation – Product variety – Service levels
	All automotive market segments (e.g., private passenger car, professional vehicles, etc.) form a vibrant economy around industrial manufacturers, OEM suppliers, aftermarket solution producers and service providers, who serve their own individual business plans and offer attractive and tailored commercial value to the customer.
<i>Market dynamics</i>	Connectivity services, cyber-security layer
	Extended in-vehicle experience for car occupants, regarding driving & operating, safety & well-being, information & communication, entertainment & assist applications, etc.
<i>Market dynamics</i>	Electromobility framework, cyber-security layer
	All vehicle and infrastructure functions that have to do with efficient electromobility will support resource optimization and energy to mileage yielding.
<i>Market dynamics</i>	Critical safety features, cyber-secured

	Enhanced safety for driver & passengers as mandated by legislation & regulations (emergency/incident alert services, like eCall, location beacon, etc). Functions like eCall and Galileo emergency response service are expected to benefit the
<i>Market dynamics</i>	Cyber-security features as a cost driver Vehicle technology, manufacturing and operating cost is re-structuring pricing policies, especially under revisionist economic conditions that have to adjust to new energy, manufacturing and transport costs.
<i>Market dynamics</i>	Remote/Online metrics, diagnostics, performance monitoring Re-defining the model and cost of servicing and maintenance (predictive, responsive, hybrid)
<i>Market dynamics</i>	Insurances & liabilities Flexible and adaptive insurance business models that rely on continuous vehicle & driver data feedback and smart management of insurance premiums.
<i>Market dynamics</i>	Grand-theft Auto Expanded telemetry & tracking of vehicles against criminal activities to empower services for threat mitigation and reclaim of stolen property.

Top 5 CPA categories in intra-EU exports, 2017 - 2021

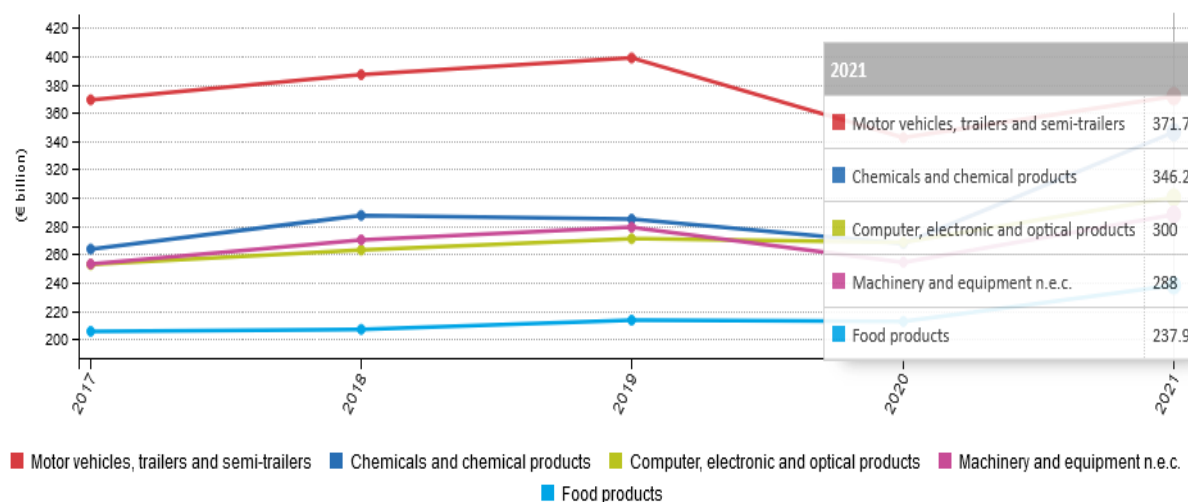
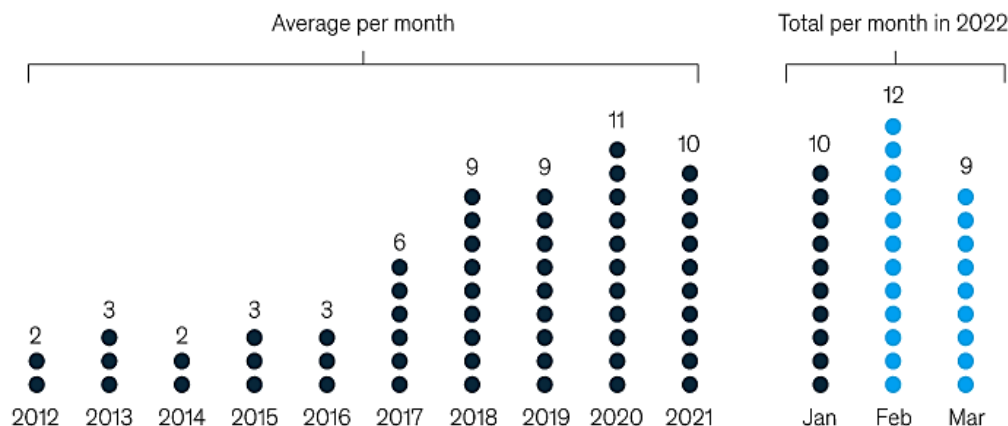


Figure 8: Most significant goods by value in intra-EU exports. Motor vehicles trade reached € 371.7 billion in 2021 - Source Eurostat

Cyberattacks have been rising since 2017.

Significant cyberattacks from 2012–22



Note: Significant cyberattacks are defined as cyberattacks on government agencies, defense, and high-tech companies, or economic crimes with losses of more than \$1 million.

Source: Center for Strategic and International Studies

Figure 9: Cyberattacks with a significant economic impact (>1M €) present, in the last 5 years, a steady monthly rate of incidents - Source (Olivia White 2022).

Social	
Civil Protection	Road Safety support
	Beyond governmental regulations and obligations there is an overarching collective commitment, at societal level, to prioritize measures and practices that upheld and promote safe conduct of vehicles on the road. Protection of human and animal life, bodily injury avoidance and property damage minimization is a funding principle of every society which cares for the safety and well-being of its citizens.
Culture	Access & Cultural trends
	Modern societies have a moral obligation to be inclusive of all its citizens without discriminations regarding a baseline of rights and benefits. This fundamental principle is extended to govern also consumer relationships where the vendor is expected to furnish and offer products of a minimum accepted level of good craftsmanship but also with all the features and functions that are deemed essential for safe and efficient operation by the user. Cybersecurity provisions tend and will be, even more so in the future, an essential safety, functional and privacy outfit for cars and its passengers. Therefore, cybersecurity protection shall be made available from entry-level models and under a universal approach for each and any user of automotive products.
Culture	Increased demand for sustainable mobility
	Social factors may impact demand for EVs. Need for mobility is huge and growing. Demand for sustainable mobility is ever increasing.
Ethics & Responsibility	Awareness level: Automotive OEMs & industrial manufacturers
	Cyber-risk awareness, high. Social & ethical implications of cyber-security are considerable and might incur liabilities.
Ethics & Responsibility	Awareness level: Automotive aftermarket, device and solution providers
	Cyber-risk awareness, medium. Varying degree of cyber-security

	responsibility is observed.
<i>Ethics & Responsibility</i>	Awareness level: Automotive consumers Cyber-risk awareness, low. Consumers start low but present increasing interest about cybersecurity features in automotive
<i>Ethics & Responsibility</i>	Awareness level: Academia & RTOs Cyber-risk awareness, high. Research, experimentation and technology development activities that promote security at all levels against cyber threats.
<i>Ethics & Responsibility</i>	Awareness level: Crime elements Cyber-risk awareness, medium. Prospects of vehicle accessibility and exploitation potential are attracting more and more daredevils that target vehicles and their drivers to be victims of criminal activities.
<i>Ethics & Responsibility</i>	Threat, human Life, injuries, privacy. Notwithstanding legal obligations there are considerable ethical questions pertaining to cyber-protection of vehicles and drivers.
<i>Ethics & Responsibility</i>	Threat, non-human Damages. The same applies for non-living assets and infrastructure.
<i>Ethics & Responsibility</i>	Ethical Questions The wielding of all digital, ubiquitous connectivity, Artificial Intelligence, Data Mining, autonomous drones, etc., generate a valid discourse within the society around ethical issues, safeguarding the principles of humanity and upholding citizen's rights. Autonomous, connected and electromobility provides ample ground for ethical considerations of all sorts, with privacy infringements and safety handling by AI being at the forefront.
<i>Ethics & Responsibility</i>	Driver responsibility issues Beyond legal obligations and regulatory liabilities, the driver might have a conscious position over ethical issues and towards the protection of privacy and security of on-board passengers.
<i>Pandemic challenge</i>	Remote work – Social distancing “...securing personal devices and networks, to protecting collaboration technology like video-conferencing and file sharing, automotive companies will need to make some enhancements in their existing security to close gaps. It is a challenge but one where they can share solutions with thousands of companies the world over.” (Accenture, 2020)

Technological	
<i>State-of-the-Art</i>	Digital Transformation Connectivity, everywhere (place, time, service) & everything, connected (computers, sensors, databases, HMIs, & GUIs, M2Ms, AI operators, systems, devices, etc.).
<i>State-of-the-Art</i>	Mobility System Exposure Digital transformation -through connectivity, industry 4.0, AI operators and drones- allows for the increased exposure of cars to cybersecurity threats and risks. In fact, cars nowadays, present a large and multilayered attack surface, as the sum of all potential attack vectors, where intruders will try their luck with gaining access for malicious purposes. This defines a multi-dimensional space around cars, with numerous possible entry points that can be grouped into the Vehicle, Proximity, Backend & Cloud and Network

	attack surface layers. Cybersecurity strategy and practices should be comprehensive and therefore need to cover meticulously the whole attack surface, throughout all interwoven layers. (DATA, NTT 2021)
<i>Disruptive</i>	Autonomous mobility Digital transformation affects also the automotive industry. Vehicles incorporate complex IT systems, with back-end and front-end functions, running on specific OS and various software applications. Autonomous vehicles comprise a demanding and dynamic informatics & communication framework, dedicated to safe and efficient self-driving functions.
<i>Disruptive</i>	Connected mobility The condition of always & everywhere online vehicles is a fundamental prerequisite for the development and operation of automotive products and services in the digital era. Vehicles are nodes that move, by definition in the spatial but, today also in the digital continuum. The car has become both a data producer and a data consumer system. A clearinghouse for information in the automotive ecosystem and as such also the weakest link within the connected mobility eco-system.
<i>Disruptive</i>	Electromobility Transition towards electromobility adds a layer of physical and digital interactions between vehicles, humans, infrastructure and networks.
<i>Actors</i>	Mobility eco-system From a technological aspect, the complex environment of all involved mobility actors (car manufacturers, back-end & front-end systems, safety & traffic management systems, aftermarket & 3rd party service providers, network operators, other vehicles, etc.) demands complementarity, synergies, integration and responsibility to acquire the critical function of interoperability at system level and through all operating layers.
<i>System level</i>	System specification Cybersecurity has become another important operational and quality parameter that defines the performance and value of an automotive system. Protection against cyber threats & vulnerabilities is considered an essential functional and technical requirement for the respective industry.
<i>Product level</i>	Customer preferences Any tailoring in the outfit and functioning of a connected car, from a certified aftermarket installer or even from a customer daring an unsanctioned hack, potentially changes its overall cybersecurity profile in terms of vulnerability, resilience, integrity and reliability of safety, efficiency and performance parameters.
<i>Product level</i>	Product Adaptation Bring-up-to-speed with Cybersecurity requirements employs special skills and technical resources and is expected to increase the product's lifecycle expenditures (Cost, time, technology, innovation).
<i>Investment</i>	Investment in Innovation "The vast majority of automotive cybersecurity leaders spend more than 20% of their cybersecurity budgets on advanced technologies—the kind that support the innovation their company is baking into their business." (Accenture, 2020)
<i>Disruptive</i>	Prominent Technologies "Artificial Intelligence (AI) and Security, Orchestration, Automation, Response (SOAR) technologies top the list of advanced technologies automotive cybersecurity Leaders are investing in. But others, as you can

	see from the chart, are contributing to their cybersecurity ranking and success.” (Accenture, 2020)
<i>Challenge</i>	EV Charging loads & network Charging powers are increasing, the number of charge stations is increasing as well. DC chargers can now power up to 350+ kW. The load on the grid due to high peaks in power demand (but also peaks in production from renewables) creates technological challenges.
<i>Challenge</i>	Connected cars “unique to the industry. And, it relates not only to privacy and the usual security concerns, but also to a life-or-death matter—the safety of passengers and other drivers.” (Accenture, 2020)
<i>Regulatory</i>	Patents and IPRs Patents and Intellectual property rights remain significant within the technological, industrial and commercial activities of automotive mobility. Even so for the particular field of Cybersecurity systems, equipment, devices, software, applications and services designed and addressed for usage with vehicles. But cybersecurity patents and IPRs have to be also themselves cyber-secured through proper strategies, measures and practices. Because “Beyond the theft of customer data and potential regulatory issues and reputational damage following a cyberattack, it is imperative to understand other less-obvious costs, such as theft of intellectual property (IP) ... IP is the lifeblood of many organizations. It fuels innovation, growth and differentiation IP loss is among the hidden or less visible costs of an attack IP theft differs from customer information theft in that your company owns the IP, whether trade secrets, drawings and plans, or proprietary know-how. Because of this, your company may very well have an obligation to shareholders and stakeholders to identify what has been stolen, assess potential impact and loss, and seek potential recovery of the IP as soon as possible.” (Deloitte 2016)

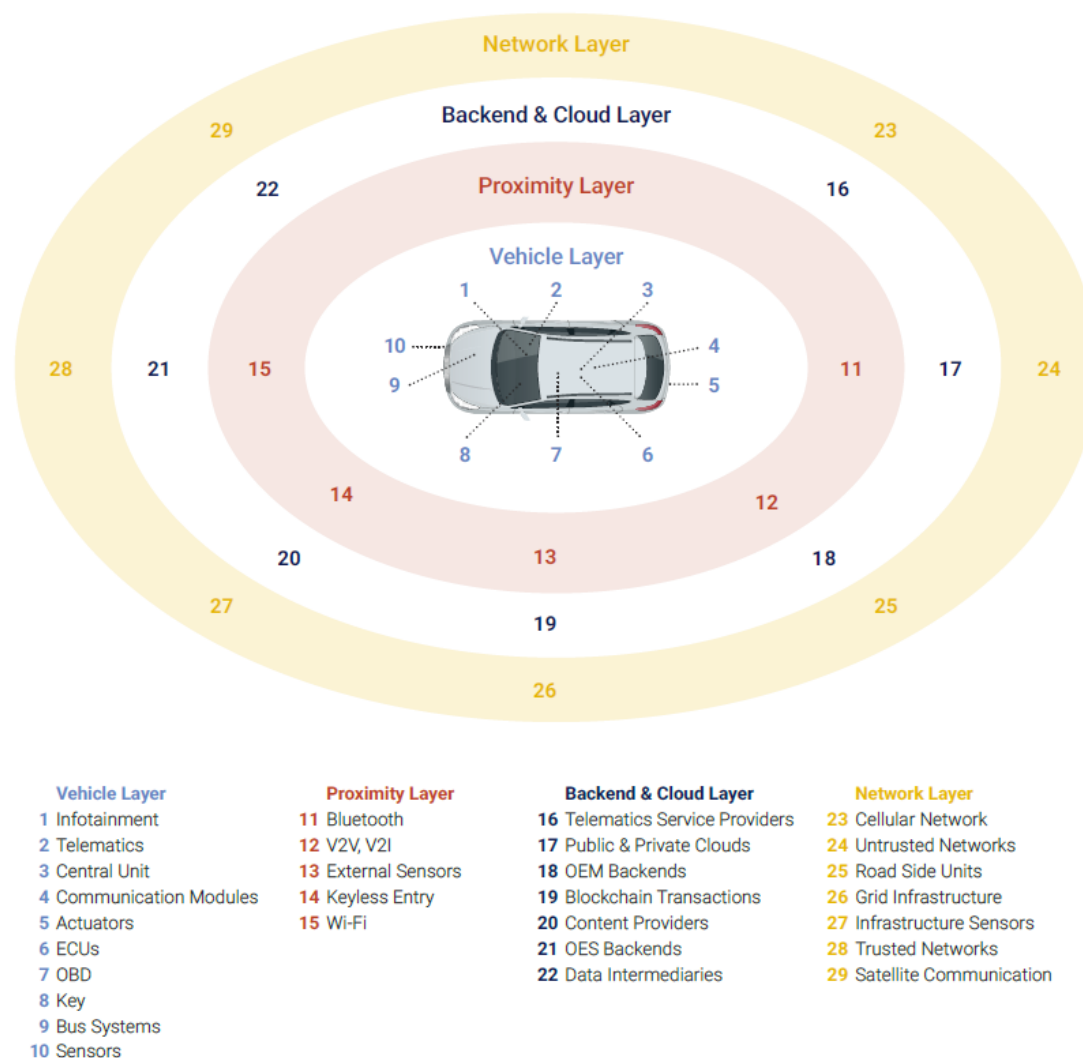


Figure 10: Structure of attack surface layers and distribution of potential entry points – Source (DATA, NTT 2021)

Legal	
Governance	<p>European Parliament and the Council: Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) – (2016)</p>
	<p>It “provides legal measures to boost the overall level of cybersecurity in the EU by ensuring: Member States' requiring them to be with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority. a culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport... and digital infrastructure Businesses identified as operators of essential services have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as cloud computing services and online marketplaces, will have to comply with the security and notification requirements.” Particularly it identifies entities active in road transport like “Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 (11) responsible for traffic management control... Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council”.</p>

Governance	<p>European Commission: Directive (proposal) on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) - (2022)</p> <p>A critical update of rules on the security of network and information systems (NIS Directive, 2020) “because of the increasing degree of digitalisation and interconnectedness of our society and the rising number of cyber malicious activities at global level NIS 2 Directive now covers medium and large entities from more sectors that are critical for the economy and society, including providers of public electronic communications services, digital services manufacturing of critical products also strengthens cybersecurity requirements imposed on the companies, addresses security of supply chains and supplier relationships and introduces accountability of top management for non- compliance with the cybersecurity obligations. It streamlines reporting obligations, introduces more stringent supervisory measures for national authorities, as well as stricter enforcement requirements, and aims at harmonizing sanctions regimes across Member States. It will help increase information sharing and cooperation on cyber crisis management at a national and EU level.”</p>
Standards & regulations	<p>UN ECE WP.29: a new “UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”</p> <p>A United Nations regulation that mandates measures for vehicle manufacturer to:</p> <ul style="list-style-type: none"> a) Detect and prevent cyber-attacks against vehicles of the vehicle type; b) Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type; c) Provide data forensic capability to enable analysis of attempted or successful cyber-attacks. <p>It has to be noted that for the European Union, these cybersecurity regulations on automotive are mandatory for new vehicle types from 2022 and for all vehicle’s types produced from July 2024. It is expected that UN ECE, regulation will be adopted widely on a global scale.</p>
Standards & regulations	<p>ISO 26262: “Road Vehicles Functional Safety”</p> <p>An international standard that addresses specifically the automotive in terms of functional safety of on-board electrical and electronic systems. In particular it takes a risk-based approach to define an automotive risk taxonomy, termed “Automotive Safety Integrity Levels” (ASIL) and how to asses these classes.</p>
Standards & regulations	<p>ISO/SAE 21434: a best practices document</p> <p>Introducing the “Cybersecurity Assurance Level” (CAL) standard, as a way to classify the level of cybersecurity deemed suitable on component or device level. Four steps of CAL are determined against respective threat scenarios and gauging the possible extent of damage and probability of attack.</p>
Standards & regulations	<p>SAE J3061: “Cyber Security Guidebook for Cyber-Physical Vehicle Systems”</p> <p>A release of the Society of Automotive Engineers (SAE), relating to automotive cyber-physical systems and establishing a set of high-level principles for cyber security. SAE J3061, forms a complete and practical approach for the security of the entire lifecycle of a vehicle, including its dedicated parts.</p>
Standards &	<p>AUTOSAR: AUTomotive Open System ARchitecture</p>

<i>regulations</i>	<p>A global partnership initiative of the vehicle manufacturers, suppliers and other companies from the electronics, semiconductor, and software industry.</p> <p>Initially formed in 2003 and counting by now over 280 partners, including Bavarian Motor Works (BMW), Robert Bosch GmbH, Continental AG, Daimler AG (formerly Daimler-Benz, then DaimlerChrysler), Siemens VDO, Volkswagen, Groupe PSA, Toyota and General Motors.</p>
<i>Governance</i>	<p>Insurance policies</p> <p>Are influencing directly and form a governing factor in the automotive market. Liability issues could potentially escalate and draw unwanted attention (publicity, legal, financial) over failures to mitigate and counter cyber threats.</p>
<i>Standards & regulations</i>	<p>Delegated Regulation (EU) 2019/320</p> <p>A new (into effect, 03.2022) EU regulation that mandates that all new mobile phones for the European market need to support Galileo GNSS technology, regarding advanced mobile location (AML) protocol and Wi-Fi communications. This enables emergency response call centers to accurately pinpoint the caller's location, thus reducing response times from rescue services in order to save more lives. We consider and expect this regulation, and the related technologies, to be directly related and utilized also in the automotive ecosystem for the benefit of drivers and passengers of vehicles.</p>
<i>Governance</i>	<p>Legislation differences across EU members</p> <p>National legislation may vary substantially within Europe. Member states, unquestionably, follow and comply with EU regulations but wherever there is room for local adaptation and options to apply selectively we have a situation of differentiation at the level of national laws. This applies and affects certain aspects of the regulatory framework for taxation, road & passenger safety, energy, commercial services, etc. This is indicative in the case of local legislation on EV charging since most of the charging infrastructure is still under development and local governments have a significant impact on the configuration of the services (e.g., how many charge stations are installed and operated).</p>

Environmental	
<i>Sustainability</i>	<p>Decarbonization of Vehicle Manufacturing</p> <p>Net zero strategies of decarbonization will be the driving force for the transformation of industrial production and system manufacturing, affecting almost all technical, operational and administrative activities. This applies to the whole production cycle, from research & development, production planning, assembly, integration and testing.</p> <p>In Automotive, decarbonization practices apply from supply chain, all the way, to the powertrain.</p>
<i>Sustainability</i>	<p>Decarbonization of ICT industries</p> <p>There is a growing realization that ICT systems and services have to meet their own obligations, regarding net zero targets on a global, regional, national and individual responsibility level. Decarbonization is valid equally so for all of CARMEL pillars, namely for the autonomous, connected and electromobility industry & market segments.</p>
<i>Sustainability</i>	<p>EU and global Targets</p> <p>The European Commission, in 2019, set the somehow ambitious target to make Europe "climate-neutral" by 2050.</p>

	The hard facts that drive all mitigation strategies, dealing with reigning in climate change, are represented in the target numbers for keeping the total passenger car CO ₂ emissions under 45 gigatons all the way up to 2050. This is considered to be “a “carbon budget” that would help hold global temperature increases to under 1.5°C” (Julian Conzade 2021)
<i>Sustainability</i>	Climate Change impact Despite resource and performance optimization in conventional vehicles so far there is considerable merit to accelerate transition to electromobility. Operating all kinds of vehicles still results in releasing large amount of carbon emissions into our habitat. “Reducing carbon emissions from vehicles is critical—currently, road transport accounts for 13 percent of global carbon emissions.” (Julian Conzade 2021)
<i>Sustainability</i>	Challenges in automotive According to a credible analysis, the mobility eco-system faces, collectively, five challenges in its effort to meet global targets in the climate change mobilization. These are identified as: 1. Speed the shift to zero-emission vehicles; 2. Leverage the abatement potential of transition technologies; 3. Reduce vehicle miles traveled; 4. Increase share of renewables; and 5. Zero-carbon supply chains. (Julian Conzade 2021)
<i>Sustainability</i>	EV impact The advent of Electric Vehicles (EV) is expected to ameliorate the situation in the fight to constrain Climate Change and to reduce our carbon footprint on the planet. This is based on the combined effect of transforming, both the way cars are produced and the amount of emissions they release while they operate. Especially in the second factor, EVs play a significant role since they present a much lower ecological footprint than Internal Combustion Engines (ICE) cars. The major challenges with this transition are the requirement for cheaper car batteries and the need to efficiently charge EVs with energy that is purely renewable.
<i>Sustainability</i>	EV batteries Understandably, batteries play the most critical role in cutting down mobility emissions and therefore justify focused efforts for optimization in terms of production cost, energy density, control and performance. Prices, for the lithium-ion batteries -the most common type used in EVs- seem to have struck a persistent limit, where manufacturers are challenged to go below the cost of €95 (\$100) per kWh of capacity. Towards this end battery industries are exploring new technologies, mainly on the battery chemistry side with research focusing, among others, on high silicon anodes and solid; foam; gel; states of the units. Another promising field, in battery improvements, lies with the software side of the product since it has been proven that efficient software control systems can shorten overall charging timelines and extend battery life in the long run. (Tom Hellstern 2021)

3.3. SWOT

The SWOT analysis is an established method for assisting the formulation of strategy. It is a business strategy tool for determining the options offered in a strategic business area. It aims to specify the objectives of the company or the project and to identify the internal and external factors that are favorable and unfavorable to the achievement of these objectives. SWOT has been described as a proven tool for strategic analysis. Strengths and weaknesses are often internal, while opportunities and threats generally focus on the external environment.

In this section we present a SWOT analysis for the CAMEL solution. The various components of this analysis are described. These are the main strengths and weaknesses as well as the potential opportunities and the threats that CAMEL might face. This information is important and should be taken into account when a product strategy is being formed.

The results of the CAMEL SWOT analysis can be found below:

Strength	
<i>Know How</i>	Partners Know How
	All partners have gained important know how on providing solutions (hardware and software) for the automotive cybersecurity industry and market.
<i>Reference product</i>	Product is a reference in the sector
	Product has the potential to become innovative in automotive market offering cybersecurity solutions. At least two companies (Nextium, GFX) have developed and proposed complete, innovative product systems. On the other hand, recent market reports mention that cybersecurity innovations in 2022 should seek to appease the immediate threat posed by quantum computers.
<i>Social awareness</i>	Increasing social awareness in road safety
	5GAA's presentation of the latest C-V2X developments means that autonomous vehicles using this technology are becoming closer to reality more than ever. However, this also means stronger and tighter cybersecurity is needed to ensure the security, privacy, and safety of both connected cars and users. While this newer technology will provide better road safety, more convenient driving, and cost efficiency, it also poses some risks that further proves the importance of cybersecurity. Increased road safety ensures higher level of social awareness.
<i>Agnosticism</i>	Hardware agnostic
	There is a high need for hardware agnostic solutions due to the wide variety of hardware devices and expanding IT consumerization. Hardware-agnostic systems do not require any modifications to run on a variety of devices. Thus, hardware agnostic design brings about a high level of compatibility across most common systems. The product is hardware agnostic which encompasses a great advantage for deployment and testing at different hardware platforms.

Weakness	
<i>Dependability with software</i>	Product dependent on the new SW updates
	Hardware and software are mutually dependent on each other. Both of them must work together to make a computer produce a useful output. Even though the product is hardware independent, it still depends on software updates.
<i>Dependability with electronic products</i>	High dependance on electronic products (issue in case of shortage)
	The product is highly dependent to other electronic products. The supply of such electronic products has been affected by the Corona case and the energy (which in turn affects the logistics cost). From the outset of 2021, the outlook for the electronics manufacturing industry has steadily grown murkier. Many PCBs, semiconductors and microchips are still produced in Asia, and with the ongoing supply chain disruptions, some electronics manufacturers are looking at moving their operations back to familiar soil. 2022 is shaping up to be another long wait.

<i>Sensitive to threats</i>	Threats are sensitive to change so the product needs to evolve
	The product needs continuous improvement so that it can be insensitive to future threats. A cyber security threat refers to any possible malicious attack that seeks to unlawfully access data, disrupt digital operations or damage information. Cyber threats can originate from various actors, including corporate spies, hackers, terrorists, hostile nation-states, criminal organizations, lone hackers and disgruntled employees.
<i>Conformity to OCPP</i>	Product can only take data conform OCPP
	The Open Charge Alliance - OCA has launched an independent OCPP certification program, through which the charging point (EVSE) manufacturers and Charging Station Management System providers (CSMS / back office) are now able to conform their OCPP 1.6 implementations according to the official OCPP specification. Product should be compliant with OCPP certification.

Opportunity	
<i>Modular product</i>	Robust Product that can be offered by levels
	The approach in CAMEL is developed and tested in a modular way, following a step-to-step approach. Such an analysis and approach leads to the development of a modular product.
<i>Contact with OEM companies</i>	Contact with direct OEM interested with the product
	OEMs companies have expressed their interest to CAMEL product, so project partners have direct contacts with OEM companies. OEM companies provide solutions for both hardware and software.
<i>Opportunities for new collaborations</i>	New Projects collaboration in related field for partners
	The success of the CAMEL opens opportunities for new collaborations between the partners as follow-up projects.
<i>High demand</i>	High demand for cybersecurity solutions
	According to Fortune Business Insights, the global cyber security market is projected to grow from USD 155.83 billion in 2022 to USD 376.32 billion by 2029, exhibiting a CAGR of 13.4%. The global cyber security market size is projected to reach USD 500.70 billion by 2030, registering a CAGR of 12.0% from 2022 to 2030, according to a new study by Grand View Research Inc. The rise in the number of cyber-attacks during the pandemic kept the cybersecurity solutions' demand upbeat in 2020. The trend is expected to continue post-pandemic and by the forecast period owing to several firms adopting hybrid working resulting in an increase in the number of endpoint devices and anonymous network access, putting the organization's IT systems at risk. More specifically, the global automotive cybersecurity market valued at \$7.23 billion in 2021 and is projected to reach \$32.41 billion by 2030, registering a CAGR of 16.6% from 2021 to 2030.
<i>Remote cyber-attack detection product</i>	Remote cyber-attack detection can become profitable product
	Such a product (with enhanced remote cyber-attack detection functionalities) does not exist in the market. So, it is a great opportunity for commercial use of the product.

Threat	
<i>New competitors</i>	Possible entry of new competitors for another kind of CAMEL product

	<p>The threat of new entrants, or potential for a new business to appear in the industry, is one component to be mindful of when evaluating your company's risks. Marketers and other business professionals consider this when assessing their business's overall health. Understanding how to determine if a new entrant may emerge in cybersecurity sector can help CAMEL partners (SMEs) take preventive measures to still succeed in the marketplace.</p>
<i>Dependance to official standards</i>	<p>High dependance on the official standards</p> <p>NIST and ENISA develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. and European industry, federal agencies and the broader public. Our activities range from producing specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges. CAMEL product should be complaint with every official standard released by both organizations.</p>
<i>Demand's fall</i>	<p>Fall in demand with stabilization in the product market + new competitors</p> <p>This event (threat) has low possibilities to happen since the demand and the forecasts on automotive cybersecurity solutions show a high demand in the next years.</p>
<i>Strong competition</i>	<p>Competition catching up</p> <p>In case that competition catches-up, there are four steps to overcome this. First starting point: Who Are My Actual Competitors? Before you go insane listing out your 50 closest competitors, take a moment to define what you are really competing for and ignore the rest (for now). Second pint: Finding competitors' weaknesses, CAMEL partners able to dig a bit deeper and look at their strengths and weaknesses. A SWOT analysis chart that has competitors names in the left-hand column and title the rest of the columns with website, blog, social media and offline sales. Third point: Make a plan. Once you identify the weak points in your competitors shield, you now have to decide whether or not to exploit them. For example, if your competitors have a massive sales team that is pounding the pavement, see if you can beat them with your online marketing efforts. Finally, fourth step include measure and review. The final step of any new strategic implementation is to look back and see if you are making progress. After 90 days, review your goals and measure your results.</p>
<i>Limitations by regulation</i>	<p>Regulations limiting the potential for remote detection of cyberattacks</p> <p>To comply with increasingly complex cybersecurity regulations, organizations need powerful tools for monitoring cybersecurity risk, managing cybersecurity governance, and implementing cybersecurity best practices. A growing number of cyber security regulations are creating a complex web of compliance requirements for organizations around the world. In analyzing the massive and escalating volume of regulation, a couple of themes emerge loud and clear. Many elements of cybersecurity regulations are directed at establishing accountability and responsibility to ensure that senior leadership in companies are treating security and risk issues seriously and strategically.</p>

4. Business modelling and Financial plan

4.1. Business Model Canvas

Subsequently, we implement the Business Model Canvas over each of the three defined pillars of CARMEL. The prospects and impact of CARMEL's autonomous, connected and electromobility are assessed and evaluated to define plausible business models that could support management of prevailing and emerging cybersecurity risks, as well as offer market valued and adaptive services for both OEMs and consumers in the automotive domain.

The Business Model Canvas (BMC) methodology will be applied to study and produce dedicated and viable business models for each of the three pillars of CARMEL. Each of the three pillars, namely the autonomous, connected and electromobility, will be taken into consideration for the definition of the perimeter and the content of a befitting business model that can be practically applied and provide the marketing framework for the development of products and operation of services.

4.1.1. Pillar 1 (Autonomous Mobility) BMC

KEY PARTNERS <ul style="list-style-type: none"> • Automotive industry and related sectors • Cybersecurity, AI, ML experts • Smart cities • Telecom Operators • Platform-as-a-Service (PaaS) providers • Open-source communities • Big data / 5G / Cybersecurity PPPs • Standardization organizations 	KEY ACTIVITIES <ul style="list-style-type: none"> • Design and development of cybersecurity services • Integration of technologies into products • Testing and Validation • Business model development for new services KEY RESOURCES <ul style="list-style-type: none"> • Test vehicles / Track venues • Anti-hacking IDS/IPS devices • Back-end servers • ADAS systems • Localization services • 4G/5G and IEEE 802.11p wireless networks • Spectrum • ML/AI cybersecurity methodologies • Forensics 	VALUE PROPOSITION <ul style="list-style-type: none"> • Automotive intrusion detection/prevention system • Security monitoring and prompt reaction when incident occurs • AI – Cybersecurity framework for known and zero-day attacks • Comprehensive engineering service, including know-how for intrusion detection • Business evaluation of the security levels 	CUSTOMER RELATIONSHIP <ul style="list-style-type: none"> • Customization • Analytics • Online support • Training support • Consultancy services CHANNELS <ul style="list-style-type: none"> • Direct customer network and sales force • Demonstration and dissemination activities, fairs, events • CAMEL website & GitHub 	CUSTOMER SEGMENTS <ul style="list-style-type: none"> • Automotive industry • EVs charging stations, networks and operators • Cybersecurity service providers
COST STRUCTURE <ul style="list-style-type: none"> • Infrastructure costs for large scale deployments • Personnel costs • Partner costs of services (i.e., PaaS) • R&D costs • Marketing expenditures 			REVENUE STREAM(S) <ul style="list-style-type: none"> • Products sales • After sales services • Security monitoring as a service • Engineering services • Consulting services • License fees, based on software modules, add-ons and tools • Development contracts 	

4.1.2. Pillar 2 (Connected Mobility) BMC

KEY PARTNERS <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • [PRODUCT] OEMs • [NEXTIUM] Integration and infrastructures 	KEY ACTIVITIES <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • HW (OBU) and SW know-how KEY RESOURCES What key resources does your value proposition require? What key resources do you need for distribution? What key resources do you need for customer relationship management? <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • Materials for the HW development - production and SW support. • High qualified engineers with experience. 	VALUE PROPOSITION <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • [NEXTIUM] Experience in the field, product and contact point for some customers/OEMS in the field • [PRODUCT] Cost-effective product focused in life security (road safety) 	CUSTOMER RELATIONSHIP <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • [PRODUCT] Advertising would be the key, together OEMs training - showroom for test CHANNELS Through which channel does your audience want to be reached? How are we reaching them now? How are the channels integrated? Which ones work best? Which ones are the most cost efficient? How are we integrating them with customer routines? <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • Contacts • Social Networks - Marketing 	CUSTOMER SEGMENTS <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • OEMs HW automotive, secured • OEMS Safe communications
COST STRUCTURE <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • Personnel cost • Marketing cost • Manufacturing Process Line Costs • Materials & services costs 		REVENUE STREAM(S) <u>NEXTIUM by Idneo</u> <ul style="list-style-type: none"> • Product Subscriptions - Licenses • Product sale 		

4.1.3. Pillar 3 (Electromobility) BMC

KEY PARTNERS	KEY ACTIVITIES	VALUE PROPOSITION	CUSTOMER RELATIONSHIP	CUSTOMER SEGMENTS
<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Charge station OEMs • Roaming partners <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • Consortium partners. Strategic alliances between the Consortium partners, especially the technology providers who develop technologies and hardware components for Pillar 3, are mandatory for optimizing the allocation of resources and activities. • Hardware and equipment providers. To assure reliable supplies, buyer-supplier relationships with hardware and equipment providers (e.g., EV charging stations) should also be put in place. • Partnerships can help reduce risk in a competitive environment characterized by uncertainty like the one present in the EV charging industry where Pillar 3 of CAMEL is situated. 	<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Software development <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • Software & Hardware development. Design and development of a novel cybersecurity framework for analysing and tracking EV charging data. • Performance evaluation and fine-tuning. Testing and fine-tuning the efficacy of the developed framework in detecting smart charging abuse and EV scheduling abuse attacks targeting the controllers of connected EVs. • Key activities are pivotal in fulfilling the value proposition of Pillar 3 and ultimately in creating revenue streams in the future. 	<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Cloud platform as a service for remote management of charge stations, transaction handling, billing, roaming, smart charging <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • A novel approach to addressing attacks in EV charging stations. Pillar 3 demonstrates how the CAMEL solution can address attacks in EV charging stations using a smart charging control unit as well as sophisticated machine learning (ML)-based anomaly detection mechanisms. • A one-size-fits-all solution for CPOs. It is a one-size-fits-all solution for EV Charge Point Operators (CPO) who want to enhance the integrity of their EVs through the provision of an EV smart charging control unit that protects the EVs against smart charging abuse and EV scheduling abuse attacks. • ML-based anomaly detection on smart charging data. 	<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Extensive cooperation, feature development, daily contact <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • B2B. B2B (business-to-business) relationships will be achieved mainly through contacts with Industrial Energy partners alongside with participation in targeted exhibitions and venues for the Energy Sector. • B2C. Long-term B2C relationships with customers will be achieved through branding activities in different channels aiming to build a trustworthy brand name with a publicly recognized logo. • To achieve customer satisfaction, both B2B and B2C business models will be explored. <p><u>CHANNELS</u></p> <p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Contacts, expos, marketing <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • Direct Contact. Customers will be reached mainly through 	<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Charge Point Operators: usually start/scale-ups or subsidiaries from utilities or large energy companies <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • Manufacturers of EV charging stations. • Charge Point Operators (CPO) • e-Mobility Service Providers (eMSP) • The most important industry targeted by Pillar 3 is the electric vehicle (EV) charging industry. Accordingly, manufacturers of EV charging stations, CPOs, and eMSPs that are part of the smart charging ecosystem are the most prominent customers benefiting from the CAMEL solution. According to a new study conducted by Grand View Research, Inc., the global EV charging infrastructure market size is expected to reach USD 217.06 billion by 2030, growing at a CAGR of 30.6% from 2022 to 2030.
	<p><u>KEY RESOURCES</u></p> <p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Cloud platform • Networks of charge stations • Knowledge/experience <p><u>EXALENS</u></p>			

	<ul style="list-style-type: none"> • The EV smart charging control unit (GFX). The EV smart charging control units developed by GFX is highly secure controller that manages the timing and intensity of the charging vehicles. Among the other responsibilities, this unit embeds algorithms for thwarting smart charging abuse and EV scheduling abuse attacks targeting the controllers of connected EVs. • The Abuse Detection System (SID & CLS). The Abuse Detection System developed by SID & CLS is an algorithmic pipeline installed in each EV smart charging control unit which is capable of collecting suitable EV charging data from the system's database (a database owned by GFX), pre-process this data before applying sophisticated anomaly detection mechanisms for detecting outliers⁵. • The key resources the value propositions of Pillar 3 require pertain to the... 	<p>CAMEL customers will have access to a novel Abuse Detection System that embodies several sophisticated ML techniques for addressing anomaly detection on EV charging data.</p> <ul style="list-style-type: none"> • By catering to the requirements of EV charging industry, the value propositions of Pillar 3 centres around a unique combination of products and services. 	<p>direct contact. Customer communication can include both written communication (e.g., emails, newsletters, etc.), verbal communication (like phone calls), and physical communication (e.g., face-to-face with meetings).</p> <ul style="list-style-type: none"> • Partners' Strategic Partnerships. Through partners' strategic partnerships coupled by active and well targeted dissemination activities. • EU & Government Bodies. Through European Union Bodies, Government Bodies as well as Customer Societies (namely, ENTSO-E, E.DSO, REScoop.eu). • Web/mobile/cloud service channels. Services will be provided through web/mobile/cloud service channels. Partners' social media channels (Twitter, LinkedIn) will also be used. • Both direct and direct marketing channels will be used to reach customers. 	<ul style="list-style-type: none"> • Distribution System Operators. Distribution System Operators (DSO) who manage the electrical grid and are responsible for distributing the energy from the generation sources to the final consumers are also targeted by Pillar 3. • Cybersecurity providers. Finally, the cybersecurity market is a target market for Pillar 3. The cybersecurity market was valued at USD 217.87 billion in 2021. It is projected to grow from USD 240.27 billion in 2022 to USD 345.38 billion by 2026, exhibiting a CAGR of 9.5% during the years 2022-2026. • The addressable market size targeted by Pillar 3 is quite large, which gives a good estimate for a potentially high market share of the CAMEL solution.
--	--	---	--	---

⁵ As an outlier we define a charging process that cannot be grouped into what is called expected behaviour. For example, an EV requests a greater amount of power, or a specific vehicle is charged on a different station from the usual ones, showing an unusual behaviour that should be further investigated.

COST STRUCTURE	REVENUE STREAM(S)
<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • Personnel • Platform costs • Office <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • R&D and integration costs. The key costs concern R&D costs for the development of the CAMEL platform as well as integration costs for integrating the hardware and software components of Pillar 3. • Maintenance costs. Other key costs include costs related to hardware/software, and database maintenance. • Sales and marketing costs. Costs related to customer services and initial commercial operations are also part of the cost structure. • Fixed costs. Fixed costs represent a significant portion of the total costs. Examples include salaries, rents, and physical manufacturing facilities. • Variable costs. Other variable costs include costs related to the acquisition of ICT equipment and components. • All listed costs are expected to be variable and should change with scale. 	<p><u>GreenFlux</u></p> <ul style="list-style-type: none"> • RTU • Monthly subscription fee per charge station • Additional fees for premium functionalities <p><u>EXALENS</u></p> <ul style="list-style-type: none"> • Direct sales. Sources of revenue will be generated directly through the platform licensing (once-off activation and set-up fee), through APIs and SDKs usage fees, monthly account maintenance fees, and volume fees. • After-sales service and support. Other revenue sources will be generated through after-sales services and support. • Engineering services. A fee package can be charged for engineering services such as system enhancements and fine-tuning the implemented CAMEL platform. • Consulting services. Indirect revenue sources will include charging customers a fee per hour or day for consultation about the CAMEL platform. • End-user training. Additional sources of revenue will be generated by organizing training sessions for the users of the platform. • Pillar 3 will generate revenue streams from various sources including direct sales, after-sales support, consulting services and more.

4.2. Business Model Outlines

According to an acknowledged global think tank, in management consulting, there is an upwards trend in the mobility industry, proved by the surpassing of other high performing industries (e.g., semiconductors) in the arena of capital markets. This is thought to be attributed to what mobility start-ups, in particular, bring on, with their agile business models that function along the following six key things (Kersten Heineke 2021):

- **Accessing new value pools.** ... the mobility industry has headed in several promising new directions. Shared mobility, ... is an industry that could double in size by 2030. ... personalized contextual advertising based on driving routes, could create a considerable new subscription business, potentially generating up to \$310 in revenue and \$180 in cost savings per year per car by the end of this decade.
- **Getting software right.** ... the automotive software market will have grown by approximately 250 percent by the end of the decade. This will put software at the very center of new automobile designs.
- **Winning the talent war.** New mobility requires new kinds of talent. ... software- or electronics-first companies and have focused on hiring talent with digital skills ... traditional players will have to reskill up to a quarter of their current workforce.
- **Focusing on green.** New mobility players aim to cut both tailpipe emissions (... two-thirds of the total) and emissions from production (the remaining third). The €1.5 billion European Green Vehicles Initiative supports the effort. Consumers factoring sustainability into buying decisions helped drive EV sales up 43 percent in 2020.
- **Focusing on customers.** ... New mobility players lead with a set of customer-centric solutions that ease the customer journey. It's not just dedicated apps; there are also social networks, flagship showrooms, and lounges for vehicle owners, creating a pleasing environment that envelops consumers from sales to service upgrades.
- **Offering new purchasing options.** ... 50 percent of consumers ... say they are interested in online car purchases, although less than 5 percent of purchases are made that way now. The absence of a traditional dealer structure allows ... to save up to 25 percent (in dealer margins and incentives) on the price of each car. ... two-thirds expect that their OEMs will introduce direct sales channels by 2025.

The partners of CARMEL are reading carefully the new conditions of the market and are posed to offer adaptive business models that capitalize on such winning streaks and performance trends. CARMEL has the ambition to be a viable and credible solution for the Cybersecurity market in automotive and incorporates business modelling requirements for creating additional value, releasing functional software, employing deep tech, pushing-on with net zero practices, keeping the customer engaged and open up sales options.

4.2.1. Pillar 1 – The autonomous mobility business perimeter

Pillar 1 is bringing together a wide range of **key partners**, from the conventional Automotive industry and its related sectors; to cutting edge Cybersecurity, AI & ML experts; Smart cities enablers; Telecom operators; Platform service providers; Open-source communities; Public Private Partnerships in Big data - 5G – Cybersecurity; and Standardization organizations.

The Pillar's **key activities** revolve around Design and development of cybersecurity services;

Integration of technologies into products; Testing and Validation; and Business model development for new services.

Pillar 1 proposes to create **value** in Automotive intrusion detection/prevention systems; Security monitoring and prompt reaction when incident occurs; AI – Cybersecurity framework for known and zero-day attacks; Comprehensive engineering service, including know-how for intrusion detection; and Business evaluation of the security levels.

Customer relationships will rely on tailoring, analytics together with active online support, training activities and bespoke consultancy services.

Respectively, **customer segments** involve the automotive industry, EVs charging stations, networks and operators, as well as cybersecurity service providers.

Key resources will be exploited from areas in Test vehicles & Track venues; Anti-hacking IDS/IPS devices; Back-end servers; ADAS systems; Localization services; 4G/5G and IEEE 802.11p wireless networks; Spectrum; ML/AI cybersecurity methodologies; and Forensics.

Channels include direct customer network and sales force; demonstration and dissemination activities, fairs & events; and CARMEL's website & GitHub.

Cost structure is framed by Infrastructure costs for large scale deployments; Personnel costs; Partner costs of services (i.e., PaaS); R&D funding and Marketing expenditures.

Pillar 1 is counting to install **revenue streams** from Products sales; After sales services; Security monitoring as a service; Engineering services; Consulting services; License fees, based on software modules, add-ons and tools; and Development contracts.

4.2.2. Pillar 2 - The connected mobility business perimeter

The BMC analysis of Pillar 2 shows that the **key partners** involved in connected mobility are the Consortium partners, who either cater as suppliers to the automotive OEMs or are themselves integrators of products and solutions. This includes technology and service providers who develop infrastructure systems, equipment, devices, networks and software tools. Connectivity and content providers are also critical for the business logic of Pillar 2.

Key activities of Pillar 2 include hardware and software research & development both for the definition of proprietary technologies as for the acquisition of technical capabilities. This is based on the formation and retainment of skilled teams of engineers and business administrators.

The **value proposition** of Pillar 2 comes with respect to driver/passenger, vehicle and road safety products and solutions. This integrates the capacity to perform fieldwork -and the experience that comes out of it- and observe cost-effectiveness, as a driver all along the value chain.

Customer relationships are based both in Business-to-Business (B2B) and Business-to-Consumer (B2C) schemes. A key aspect of customer relationships is an extrovert communication program where developers, producers, providers and consumers come together under dedicated branding and marketing activities that support credibility, trust and

functionality of the market.

The **customer segments** here are mainly from the OEM industrial domain. While the automotive OEM domain has its own further segmentation, Pillar 2 business planning addresses distinctively the manufacturers of secure systems and hardware together with the providers of secure communication solutions.

The **key resources** identified for Pillar 2 are the raw materials for the production of hardware, high-tech manufacturing facilities, software development capabilities and most importantly the right people for the job, in the form of high qualified and experienced engineers.

All available **channels** will be used for the promotion of Pillar 2 business purposes. From direct contact of customers, wide dissemination activities and other partners' initiatives but also focused promotion through European Union bodies, governmental programs, professional associations and customer unions. Last-but-not-least, all the digital channels (web/mobile/cloud services, etc.) will be employed accordingly.

In Pillar 2 the following are regarded as defining the **cost structure**: Personnel; Marketing; Manufacturing; and Process Line Costs.

Revenue streams in Pillar 2 are expected mainly from product sales, service subscriptions and license fees.

4.2.3. Pillar 3 – The electromobility business perimeter

All in all, and as detailed in the BMC analysis of Pillar 3, the **key partners** involved in Pillar 3 are the Consortium partners, specifically the technology providers who develop technologies and hardware components for pillar 3. Hardware and equipment providers (i.e., EV charging stations) are also considered as key partners.

Regarding the **key activities** of Pillar 3, CAMEL will design and develop a novel cybersecurity framework for analyzing and tracking EV charging data. Furthermore, it will test and fine-tune the efficacy of the developed framework in detecting smart charging abuse and EV scheduling abuse attacks targeting the controllers of connected EVs. Finally, an extensive analysis will be performed of the ways the developed framework is impacting the EV grid performance and the EV charging business as a whole.

The **core value** proposition of Pillar 3 is that it demonstrates how the CAMEL solution can address attacks in EV charging stations using a smart charging control unit as well as sophisticated ML-based anomaly detection mechanisms.

The use case builds **customer relationships** with both Business-to-Business (B2B) and Business-to-Consumer (B2C) customers. More specifically, long-term B2B relationships will be achieved mainly through contacts with industrial energy partners, alongside targeted exhibitions for the Energy Sector. Long-term B2C relationships with customers will be achieved through branding activities in different channels, aiming to build a trustworthy brand name with a publicly recognized logo.

The main **customer segments** are manufacturers of EV charging stations, CPOs, eMSPs,

DSOs as well as cybersecurity providers.

The **key resources** for Pillar 3 stem from CARMEL's developed tools, namely:

- The EV smart charging control units developed by GFX is highly secure controller that manages the timing and intensity of the charging vehicles. Among the other responsibilities, this unit embeds algorithms for thwarting smart charging abuse and EV scheduling abuse attacks targeting the controllers of connected EVs.
- The Abuse Detection System developed by SID and CLS is an algorithmic pipeline installed in each EV smart charging control unit that is capable of collecting suitable EV charging data from the system's database (a database owned by GFX), pre-process this data before applying sophisticated anomaly detection mechanisms for detecting outliers.

Channels are critical element for the success of Pillar 3. Customers will be reached mainly through direct contact, dissemination activities and partners' initiatives. The value proposition of CARMEL and the Pillar 3 results will also be promoted through European Union Bodies, Government Bodies, Customer Societies (i.e., ENTSOe, EDSO, REScoop). Furthermore, services will be provided through web/mobile/cloud service channels.

The **key costs** in Pillar 3 concern the R&D costs, integration costs, as well as variable costs, such as software and database maintenance, ICT equipment and acquisition of components. Furthermore, fixed costs represent a significant portion of the total costs.

The **revenue streams** of Pillar 3 will come from the customers who will be willing to pay (among others) for: (i) a once-off activation and set-up fee, (ii) monthly account maintenance fees, (iii) subscription service and iv) volume fees.

4.3. Business Model Logic

The total value that CARMEL can bring into the automotive market is better understood through a relevant flow chart that depicts the logic behind the collective business model. CARMEL is positioned to offer its products and services along the entire automotive value chain, both proactive and responsive. Cybersecurity requirements drive security by design beforehand, safeguard it during manufacturing & production of every element and thereafter monitor system functions & performance to respond effectively to incidents and threats.

This scheme below (Figure 11) emphasizes the consolidating effect of the CARMEL solution to the entire automotive eco-system of producers, providers and consumers/users for the benefit of comprehensive cybersecurity in mobility.

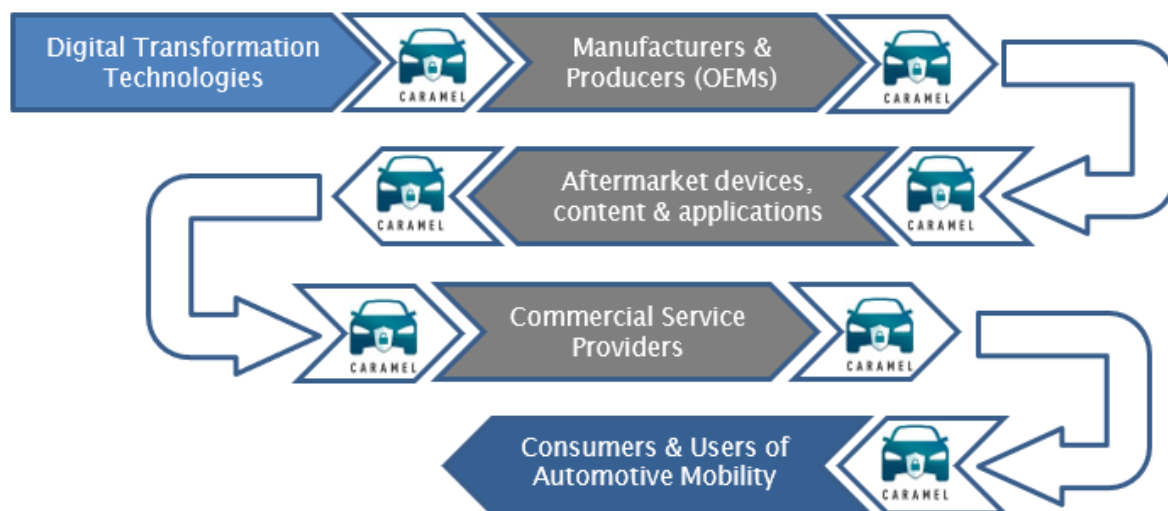


Figure 11: Business model logic behind CARMEL

4.4. Pricing, Structure

As part of an effective transfer to the market of the project results and trying to take into consideration the different sensibilities and customer needs, the consortium has done an exercise to describe in detail its approach to the pricing structure.

With special focus and based on the spirit of a modular approach, which will enlarge the customer segments targeted and better accommodate and adapted these adopters needs.

In order to tackle these particularities, the consortium has evaluated the possibility to generate standalone solutions, apart from the CARMEL as a whole option.

A consensus was achieved when the option to present the current pillar of the project (definition of pillar) was selected to extend CARMEL's commercial offering

This pillar approach includes, as per description in D2.1 Report on Detailed Specification of Use Cases (CARMEL, 2020):

- **Pillar 1: Autonomous Mobility**

"Adversarial attacks seek small perturbations of the input causing large errors in the estimation by the perception modality. The key to all such attacks is that the change to the image should be minor yet have a large influence on the output."

- **Pillar 2: Connected Mobility**

"Address the functional, security and privacy issues of the V2X Communications to provide a secure environment for ITS applications. This technology is relatively new and the security issues are not yet completely studied"

- **Pillar 3: Electromobility**

"Coverage the most important cyber-attacks that exploit known vulnerabilities of the electromobility ecosystem".

As initially described in the design phase, each pillar can operate as a standalone or independent product providing, in that sense, a unique value proposition (description of the value proposition per pillar)

The methodology used to generate the pricing approach to both, CARMEL as a whole and modules (by pillars) follows the R&D (research and development) costs approach. This approach takes into consideration of the research and development costs involved in the generation of each component.



Figure 12: Pricing structure baseline

On top of that costs sum the consortium has agreed to add a margin within the range of percentage that the industry is using on a regular basis for this type of developments. The consensus agreed internally is a range between 15-20% margin.

The tables below represent the exercise done by the consortium partners using the above-described methodology per pillar.

The information contained in that format includes the participant partner per pillar, the individual price per partner contribution + a margin (for that purpose a 20% on top of the Research & Development costs has been added) and the add sum of all costs.

	Price
DEUTSCHE TELEKOM SECURITY	82.720,00 €
CAPGEMINI	135.000,00 €
0 INFINITY	165.200,00 €
UCY	81.600,00 €
UPAT	116.640,00 €
AVL	86.856,00 €
PANASONIC	384.160,00 €
TOTAL	1.052.176,00 €

Table 1: Pillar-1, price structure

Number of licenses	40.000,00	60.000,00	100.000,00	250.000,00
Unit price	52,00€	35,00€	21,00€	10,00 €

Table 2: Pilar 1, License ranges

Pillar 2	Price
I2CAT (infrastructure)	83.300,00 €
I2CAT (2xcon)	41.650,00 €
I2CAT (adaptation)	41.650,00 €
DEUTSCHE TELEKOM SECURITY	155.100,00 €

ATOS	288.000,00 €
CAPGEMINI	135.000,00 €
EIGHT BELLS	240.000,00 €
UBIWHERE	258.692,50 €
UCY	81.600,00 €
UPAT	75.600,00 €
FICOSA + NEXTIUM by Idneo	233.100,00 €
AVL	86.856,00 €
TOTAL	1.720.548,50 €

Table 3: Pillar 2, price structure

Number of licenses	40.000,00	60.000,00	100.000,00	250.000,00
Unit price	52,00€	35,00€	21,00€	10,00 €

Table 4: Pilar 2, License ranges

Pillar 3	Price
CAPGEMINI	56.870,00
CYBERLENS	260.942,50
GREENFLUX	172.000,00
SIDROCO	124.000,00
TOTAL	613.812,50 €

Table 5: Pillar 3, price structure

Number of licenses	10.000,00	20.000,00	50.000,00	100.000,00
Unit price	70,00	30,00	12,00	8,00

Table 6: Pilar 3 License ranges

4.4.1. Pricing, Conclusion

Apart from providing a benchmark reference to potential customer of a price range of the CAMEL solution, the above-described pricing strategy aims to expand the customer segments as not all stakeholders may be interested in the CAMEL as a whole solution. This modularity will capture the attention of other adopter that in under other circumstances will not be interested in a complete solution.

The pricing structure described above corresponds to the year one of deployment. This calculation considers all the R&D costs plus a reasonable margin in the industry (15-20%). As early adopters [as per the innovation or technology adoption lifecycle definition (Bohlen & Beal, 1957)] they may be willing to pay an extra cost to obtain a cutting-edge technology and be the first to benefit from the value proposition provided by CAMEL.

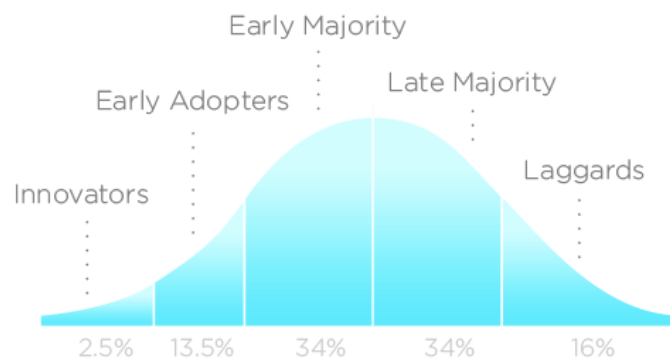


Figure 13: Innovation adoption lifecycle

The following years, this initial license may experience a price reduction as the technology will be more mature and an early majority has initiated its adoption and the added value is widely distributed among the industry. In summary, the unfair advantage that the adoption of this technology generated after the first year will not pay the extra price of year 1.

All these calculations are based on the assumptions agreed between the consortium partners and always considering the most adequate and fair approach. Nevertheless once a commercial opportunity pops up and during the negotiation period, the customer needs and the particularities of the project will be accommodated as long as the pricing proposal.

4.5. Viability

4.5.1. Product Lifecycle

One of the key objectives for CARMEL project is to extend its commercial “life” beyond the project lifespan itself. The following subsection tries to summarize the 5 phases of the Business Lifecycle (Corporate Finance Institute, 2022) (a short description per phase is included). At the time this report has been written, CARMEL is consolidating the phase one, **Seed**, and has set up the first steps towards its progress into phase two, **Start-up**.

Business lifecycle

a. Seed

This is the first step of the business lifecycle. Technical development and pilots have been run, ready for an effective transfer to the market.

b. Start-up

Once the business concept has been validated and contrasted, it comes the next step moving forward and initiate the commercial activities trying to transfer to the market the project outcomes. Several action lines are ongoing, described in the next step section, although there is not a solid commercial opportunity at the moment. CARMEL is now in the entering in this phase.

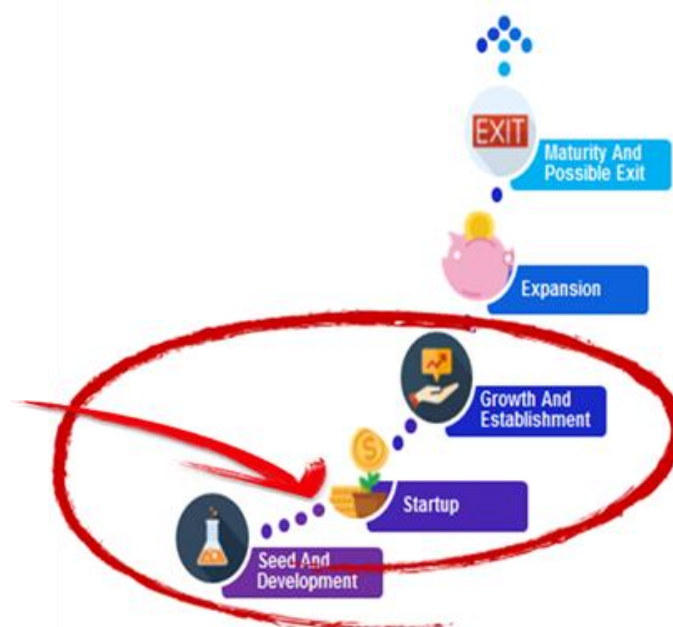


Figure 14: Business lifecycle, Source: Internal (Atos)

c. Growth

In this phase, the commercial exploitation of the project results is generating regular incomes. Customer's onboarding is part of the business-as-usual activities.

d. Expansion

Once a business is placed in this stage revenue and cashflow experience a rapid growth.

e. Maturity

After the expansion stage, the new legal structure should be receiving stable benefits on a yearly basis.

4.5.2. Sustainability Roadmap

Sustainability beyond the project lifespan is one of the key drivers of the CAMEL project and it is directly linked to exploitation plans (considering both perspectives: joint and individual).

The table below represents a 5-year -high level- roadmap plan for CAMEL. It consists of three phases, initial steps of the business life cycle (Seed, Start-up and Growth):

CAMEL 5-year sustainability plan	2019		2020		2021				2022		Y4-2022	Y5-2023	
	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2		
													Startup
Definition of CAMEL technical concept													
Solution set-up													
Pilots phase													
Evaluation and validation													
CAMEL offering													
Ramp-up													
CAMEL offering extension													
Target users identification													
Communication & Dissemination activiti													

Table 7: CAMEL sustainability roadmap

- The first phase covers the duration of the CAMEL project during its three years duration.
- The second phase starts during the second half of year 2022 (Q3 and 4). Not all components have a TRL mature enough and their development will continue during this phase which will match the commercial offering and the starting client's portfolio (at least a commercial opportunity consolidated).
- The beginning of year 5 represents the starting point of the Growth phase

This roadmap is based on a fair assumption of the project partners and may vary depending on the progress of the activities once the project ends.

4.5.3. Next Steps

To support the described above sustainability of CAMEL project and continuing with the exploitation strategy, consortium partners have initiated several work lines that will contribute to pave the way to the project results adoption beyond its lifespan. These strategies focus on initiate commercial contacts with potential adopters using internal (consortium partners customer portfolios) and external (referees or direct contact from interested potential end uses.

“Offering CAMEL solution as a modern vehicles’ protection against cybersecurity breaches related to automated driving, communication flows with other vehicles and the roadside infrastructure, and smart charging”.

The consortium has used all the events and dissemination activities to promote the project results and specially during Y3, once physical meeting has started again after the pandemic impasse, several commercial leads have been identified and initiated in its initial contact phase.

Although in its infancy, these commercial leads will be followed up in order to achieve a satisfactory end for all the participants.

4.5.4. Potential Commercial Leads

US Army

Goal: Meeting to gain familiarity with the European Union 's CAMEL Project and contributing organizations to develop cybersecurity solutions for the new generation of cars.

Main topics of interest:

- Autonomous mobility Cyberattacks do not require physical access to the vehicle or tampering with the communication system.
- 5G connected mobility V2X applications interconnect not only vehicles but also infrastructure and pedestrians, hence it is critical to protect V2X functions from misuse.
- Electromobility Unauthorized access and control of EVSE stations and firmware modifications should be prevented. iv) Remote Control Vehicle (RCV) Intrusion detection and estimation algorithm in the Gateway & RCV controller is necessary to avoid misuse.

Next steps:

- They asked for more details about partners and their expertise (proposal DOW specific section of partners profiles could be an option)
- Include the main contact into our mailing list to be informed of next dissemination actions.
- They will consider the IOTWorld Congress as a possible next stage to see demonstrations in action.
- They asked for accuracy figures about AI use cases from Pillar1 mainly

Main Contact: Confidential

Deloitte

Another lead triggered as part of CARMEL participation in the IOTWSC in Barcelona, a Deloitte Risk Advisory partner (involved in inCAR cybersecurity) had a meeting with some consortium partners.

Main topics of interest:

The main objective of this meeting was specifically to see in some additional detail and particularities of the CARMEL project. In particular activities related to Pilar 1 and Pillar 2. During the meeting objectives both parts share their objectives and questions around the involved partners expertise (i2CAT, DT-SEC, NEXTIUM, PANASONIC, CAPGEMINI) were clarified.

- hacking device collection of data...

Contact: <https://>Deloitte expressed their main interest in Antihacking device and inCAR technology.

Next steps: share results of the final demo and continue with the conversations to identify potential commercial cooperation.

Main Contact: Confidential

Other

During the event I collected a few contacts from people whom I gave explanations to and people to whom I visited their booth.

Summary of the main contacts obtained during the IOTSWC meeting hold in Barcelona.

- **Idiada:** interested in collaborating. They are working on charging units / electronic cybersecurity. They invited us to visit their testing area.
- **Build38:** an AI-based protection and management platform. They are working on a use case focusing on healthcare data security.
- **DevlinLand:** a UK contact focusing on connectivity, they are partners with multiple

international companies. They are interested mainly in HE participation.

- **Ruptela:** a telematics company providing fleet management and GPS tracking solutions. They expressed their interest in CAMEL's technology, especially the anti-hacking related.
- **VBH:** a company for installing and servicing luxury technologies in superyachts. Potential collaboration by accessing to new and innovative use cases.

All the above-mentioned initiatives and contact are directly coordinated by the consortium and followed up to identify realistic commercial opportunities or collaboration that will enhance the CAMEL value proposition in its aim for an effective transfer to the market.

4.6. IPR Agreement

During the last period of the project (M24-36), the joint exploitation has been a continuous activity to smooth the path of the consortium to an effective impact creation in the market and potential adopters.

As part of these activities, and as the final stage of the work conducted during the previous period (M12-M24, the consortium validated started and conclude the signature process of the Intellectual Property Rights agreement (IPR). All partners with relevant exploitable assets validated and signed (a legal representative of each organization) this document.

The sole purpose of this document, articulated under the structure of an internal agreement between the partners, is to reflect the distribution (in %) of the intellectual property rights per component.

The document considers two different owners depending on the type of contributions conducted during the asset development. Namely the distribution can be:

- A single partner developing the component (100% of the IPR assigned).
- Two or more partners contributing (% distributed among all contributors based on their individual efforts) in the development of the component.

The information on the contributions is summarized in Table 1.

Name of Component	Lead Developer	Contributing Parties	IPR (%)
Robustification of Scene analysis for Responding Reliably to adversarial threats			
	UPAT		100%
Multi-modal Data Fusion Module for Responding Reliably to the Threats			
		PANA	70%
Fusing of 2D and 3D segmentation modules		UPAT	30%
Cooperative Multimodal Localization for Reliably Estimating the Vehicle Location			

	UPAT		100%
--	------	--	------

Table 8: IPR Distribution Table

The rationale behind this document is to coordinate document and agree the distribution of the IPR ownership percentage that each party claims, in relation to the assets (components susceptible to be commercialized) the parties have developed during the project duration.

The inputs of this agreement can be used as part of the compensation schemes generated ad- hoc in a later exploitation or commercialization agreement (a draft version of this agreement has been also described in this final report). The economic distribution of the benefits of any potential commercial action can therefore easily distributed among the participants in such commercial opportunity.

The final version of this document, with the signature of all partners, is attached in this document as Annex A.

4.7. Individual Exploitation Plans

This subsection includes the last version of the CAMEL partners' individual exploitation plans. These plans are the result of the evolution from the initial version presented at the very beginning of the project. The content presented by each partner follows a template that asked several questions (see Table ??) organized around three (3) main topics namely:

- Profile and motivation. Four (4) questions
- What and why. Three (3) questions
- Roadmap with timeline. Three (3) questions.

A description of those question is found below.

Questions

<p>PROFILE & MOTIVATION</p> <p>1. Partner Profile</p> <p>Brief introduction about your organization, explaining your background (technical or business) and what is your field of operation.</p> <p>2. Your motivation to participate in the project and commitment:</p> <p>Why did you join the consortium and what is your role in the project.</p> <p>3. Means to achieve your objectives:</p> <p>Show that you have necessary background (resources, dedicated department or working group, infrastructure).</p> <p>4. Opportunity which appeared/appears:</p> <p>Your participation is the result of the real need of your customers (for industrial partners) or internal needs (for user partners). For academic partner mention if CAMEL is in line with other projects (continuation) and reuse of know-how. Are there any other opportunities in the pipeline when project finished?</p> <p>WHAT & WHY</p>
--

5. Exploitable assets and results:

Describe what assets (whether this involves specific components, tools, knowledge, methodologies, skills, etc.)

6. Rationale:

Explanation of why you are interested on those assets (the added- value they provide), how do you plan to exploit them (academically or industrially: e.g., provide as commercial solution, certification services, standardization, consultancy, further R&D, positioning).

7. Your Value Proposition towards Joint Exploitation of CARMEL:

What do you expect from project partners, what benefits will you deliver to the rest, what components/interest do you share with other partners.

ROADMAP WITH TIMELINE**8. Roadmap: the timeline plan you have for using those assets:**

The timeline plan you have for using those assets: (what, where, to who, e.g. meeting with board to present them in 6 months, inclusion in your portfolio etc.). Provide concrete actions for months M22-M30 and maybe for after the project.

9. Measurement

How do you plan to measure impact of planned actions for the last year of the project.

10. Positioning

If you can provide any comparison to competitors or alternatives to your asset or market figures as a reference point it would be more than appreciated.

The consortium consists in wide range of partners who come from different domains (industrial SMEs, academic and RTOs). This variety helps to capture different perspectives in the individual exploitation plans and also cover multi-angle approach for the exploitation strategy of the project results. A basic overview of the involved partners & their role, profiles & capacity, motivations, opportunities and value propositions can be gleaned in Table 9 below. The complete and in detail individual exploitation plans of the partners of CARMEL can be found in Annex B.

CAMEL Exploitation Plans						
			Profile % Motivation		What & Why	Pillar
Partner	Profile	Capacity	Motivation	Opportunities	Value Proposition	
i2CAT	RTO	ICT	to manage the Future Internet networks, the connectivity of elements such as cars, infrastructure, sensors and IoT to enable new functionalities and new infrastructure business models	design algorithms and applications enabling the future connected and autonomous cars	Asset development, cooperative exploitation, future project participation	Trans-Pillar
NEXTIUM by IDNEO	Industry	connectivity, in-cabin sensing & biometrics	implement cyber-security in the logical and physical domains	On-Board Units (boxes within the CCAM) and all items related to physical security, Secure Boot and Keys Management	growing in knowledge and setting alliances for current CAMEL and future experiences and products.	Pillar 2 - connected mobility
UBIWHERE	SME	Smart City and Future Telco areas	will be the MEC solution provider for the autonomous connected car use case in CAMEL	potential synergies and overlapping areas with existing products such as Unicle (http://unicle.io), a platform for vehicle communication and Smartlampost ...to leverage Smartlampost into effectively launching a new private and dedicated 5G network for V2X communication, while using the distributed edge computing resources to deploy a specific software stack	SW components to include in V2X solution to include in Smartlampost platform	Pillar 1 - autonomous & Pillar 2 connected mobility
OINF	SME	AI driven company mainly focusing on Machine learning (Deep Learning), Virtual, and augmented reality	contribute and improve our knowledge on Machine learning especially in the Deep learning field enhancing the security aspects of autonomous and connected vehicles	establish research in physical adversarial attacks on camera sensors	share a mutual understanding of the challenges that lie in autonomous vehicles and have worked together to produce innovative solutions for anomaly detection. There is possibility for collaborations that could aim to the integration of multiple solutions and approaches (e.g. GPS based AD) into a single commercial product	Pillar 1 - autonomous mobility
ALTRAN	Industry	ICT, High-Tech Engineering and R&D Consulting	from hardware development (including sensor hardware) to the Internet of Things and large- scale data analysis and Cyber Security for different industrial purposes. This combination of skills and proprietary software is partly marketed as a portfolio of Vue Forge (TM) services by Altran. The ability to offer the full range of competencies and technologies is a unique selling point.	Due to exceedingly high demand in security solutions by OEMs we expect significant business increase in this area in any case. Innovative solutions and competence demonstrations are adding on top. Since we are product neutral, we expect proliferation of CAMEL technologies and thus further indirect business.	Building internal capacities. Getting more people on board. Forming new business opportunities and partnerships	Pillar 1 - autonomous & Pillar 2 connected mobility
AVL	Industry	largest independent company for development, simulation and testing in the automotive industry	a major contributor to e-mobility, AVL drives innovative and affordable systems to effectively reduce CO2 by applying a multi-energy carrier strategy for all applications – from hybrid to battery electric and fuel cell technologies. an automotive engineering company, AVL will provide know-how and support in automotive cybersecurity. Specifically, our role in the project includes to develop distributed automotive intrusion detection system integrated with backend SIEM solutions, with a focus on security of automotive E/E systems and in-vehicle network, to conduct threat modelling and risk assessment of connected car use cases, from V2X to EV charging, to lead system integration and validation in WP6 and demonstrate feasibility of the solutions against cyberattacks on in-vehicle network and components including	The whole pipeline of intrusion detection system for GPS also includes hardware in loop along with the HackRF and Ublox receiver. For now, the whole test setup (testbed) is created by considering the requirements from CAMEL. As an idea for the future improvements and improvising the already existing system from CAMEL the idea is to bring the whole setup into the real vehicle and to work towards making this as a one-step solution for intrusion detection system for GPS in the near future.	AVL has offered free one year trial of AVL Model.CONNECT for partners from academic institutions or research institutes. Along with PANA AVL has also offered to provide Gratkorn Test Track (in Austria) as one of the pilot sites if incase any unseen issue comes up with the scheduled test sites	Pillar 2 - connected mobility
Exalens (ex CyberLens)	SME	next generation threat detection, response, and recovery for IT, OT, IoT and IIoT systems	protect digital manufacturing against downtime and safety events through early warning of both system malfunctions and cyber security incidents. With our ground-breaking "cyber-physical" security analyst AI, manufacturers enhance their operational resilience with automated incident detection and response	surging concerns of advanced threats targeting autonomous vehicles and EV charging infrastructures, the need for increased cyber hygiene in the automotive industry, etc.	integration of our cyber- physical intrusion detection tool with GreenFlux's EV charging platform which would see the two companies launch into the market an enhanced cybersecurity- aware EV charging solution	Pillar 3 - electromobility
University of Cyprus	RTO	Research and Innovation Center of Excellence for Intelligent Systems and Networks	to become a center of excellence in the field of Information Technology and Communication, with emphasis on the design of intelligent systems and networks. The KIOS CoE addresses some of the most important research and technological challenges of monitoring, control, management and security of Critical Infrastructure (CI) systems, by advancing ICT research towards intelligent systems and networks, able to produce smart decisions from large volumes of data	to continue the project activities by participating in a number of research project proposals relevant to cybersecurity for connected and autonomous vehicles	The is common interest with other partners on cybersecurity solutions against camera attacks and GPS location spoofing attacks	Pillar 1 - autonomous mobility

CAMEL Exploitation Plans						
Profile % Motivation					What & Why	Pillar
Partner	Profile	Capacity	Motivation	Opportunities	Value Proposition	
University of Patras	RTO	Visualization and Virtual Reality Group	Department of Electrical & Computer Engineering, University of Patras. The activities of the Group include Teaching, Research, and Development in the areas of Computer Graphics, Virtual Reality, Visualization, Biomedical Engineering, Virtual Physiological Human, Computational Geometry, Human- Computer Interaction, and Computer Vision - Build an SW library of algorithms for detection of fault data injection using sparse and deep priors that can be used to also study the effect of	other projects that are closely related to autonomous vehicles	UPAT will provide integrated solutions that could be used for attack detection and mitigation on autonomous vehicles	Pillar 1 - autonomous mobility
Deutsche Telekom Security	Industry	highly qualified solutions from the security technology and services sector	DT-Sec is the market leader in Germany and one of the industry leaders in Europe. DT-Sec builds the same protective wall for its customers that successfully secures Deutsche Telekom AG itself. DT-Sec provides security and data protection "Made in Europe" - Almost all large European car manufacturers and suppliers are customers of DT-Sec or Deutsche Telekom. DT-Sec has identified automotive security as a growth area, given that more and more domains in the automotive sector are governed by IT	an urgent need for all stakeholders and specifically our customers in the automotive domain to increase the security level of their products	the collaboration of partners well versed in artificial intelligence and machine learning with partners coming from a security background	Trans-Pillar
ATOS	Industry	ICT global leader in digital transformation	European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry	transition from research results to Atos global portfolio and service lines	project partners (I2CAT and UBIWHERE) provide the connectivity between the PKI servers and the PKI client installed on the vehicle. Additionally, I2CAT provides the communication module which allows the PKI client to access secure functions of the HSM of the vehicle	Trans-Pillar
Eight Bells	ICT	independent Research and Consulting company	business analysis and automotive threat modelling	Further and deeper involvement in similar activities	automotive threat modelling tutorial has been created and is available for everyone. Moreover, a detailed business model and market analysis plan	Trans-Pillar
GreenFlux	Industry	market leader in the international EV charging market	providing an advanced cloud-based platform for managing charging infrastructure for electric vehicles. GreenFlux offers this solution to energy companies, network operators, parties in the automotive industry and fleet managers. With the platform, our customers are able to manage charging stations remotely, give EV drivers access to a large network of charging stations (through roaming), process charging transactions and use our smart charging technology - The AI & ML nature of this project ties in well with the hardware agnostic and cloud functionalities of our platform. With the developed ML components, GFX can centrally detect whether an attack is being carried out on one of the connected charge stations. For us, CAMEL is a springboard to	applying the detection from the cloud, cyber attacks on these legacy charge stations can still be detected	the focus of our use case is on the EV Charging Station and less on the car	Pillar 3 - electromobility
SIDROCO	SME	Research, Development and Inspiration. New Generation Internet of Things (NG-IoT)	brings a whole range of New Generation Internet of Things (NG-IoT) features and capabilities for creating, supporting, and managing ultra innovative solutions, products, and services, by providing efficient, effective, and secure NG-IoT solutions for various heterogeneous environments, including Critical Infrastructures like Energy and Healthcare	led by market needs	disseminate CAMEL results and exploit the assets developed during CAMEL	Pillar 2 - connected mobility
PANASONIC	Industry	leading companies on AI, Sensing, embedded optimization and trajectory planning technologies	provided solutions to be robust across a wide range of attacks ranging from attacks to each individual sensing modality to the system of sensors. For PASEU, the co-conception with the consortium partners and development of the CAMEL cyberattack mitigation engine is completely aligned with PASEU's Research-strategy design	CAMEL cyberattack mitigation engine is completely aligned with PASEU's Research-strategy design	the manufacturing and automotive market, are investigated as to whether it is feasible and financially sustainable to turn ideas and the CAMEL concept of solution into a marketable product that abides by the standards	Trans-Pillar

Table 9: Partners' Exploitation Plans - Basic Overview

5. Conclusions

The future of mobility is clearly delineated by the increased support of capital markets, the high demand of private cars in the emerging markets (e.g. China, India, etc.), the global expectations to hold down climate change and the possibilities that open up by the application of new technologies, available from now to automotive industries. Cybersecurity is a defining aspect of the automotive and mobility eco-system in the digital age, mainly by its purpose to maintain awareness of risks and threats and its operational capacity to ensure defenses against attacks to our privacy, safety and well-being during driving and riding.

The most pivotal observation of this analysis is the universal acknowledgement of Cybersecurity as a critical factor in automotive. Consumers, OEMs and regulators all contribute from their standpoint to a heightened awareness over Cybersecurity issues, along and across the automotive domain. Although, those different actors perceive and present different levels of cybersecurity awareness they all agree that we now have an additional layer of concern, risk and threat to deal with, while being in the production and operating environment of autonomous, connected and electromobility.

Digital transformation, with its disruptive technologies in Artificial Intelligence & Machine Learning; high performance networks & connectivity of anything; integration & efficiency of sensors; big data analytics & knowledge management; together with the prospect of electromobility being the dominant scenario of future mobility; all contribute to enlarge and multiply the attack surface that vehicles will be exposing from now on to all kinds of intentions and involuntary acts.

This has created an awareness and a momentum for cybersecurity in the automotive industry and market, where actors are willing to take on the complex challenges that come along with autonomous, connected and electromobility in the digital age.

Followed up by considerable investments in research and innovation, transformation efforts to get the right mix of people, technologies and methodologies, expressed willingness to cooperate and find synergies and above all the readiness to meet efficiently and effectively the security, safety, reliability and compliance requirements in the automotive industry.

The appraisal of the status and prospects of the mobility market have revealed the particular conditions that describe and set the playground for industrial, commercial and operational activities in the automotive domain in Europe. More specifically:

- At the political level Cybersecurity is institutionally acknowledged, at the highest level (European Commission), with a new dedicated strategy, an empowered specialized agency (ENISA), ample support for research & innovation and a multidimensional regulatory, administrative and consultancy framework that provides reference and guidance to industrial and commercial activities with respect to social and environmental responsibilities.
- The economics of the EU, regarding growth conditions, size & metrics of the market, demographics & institutions, resources & sales, as well as funding & costs, all favor and support practically the integration of cybersecurity practices, products and

services in the automotive domain, who is expected to develop in full and by large numbers in the next decades.

- Socially there is a clear awareness, albeit with varying specific gravity, of the critical role that cybersecurity plays in future mobility, concerning passenger & road safety, sustainability & inclusiveness, ethics & culture and defenses against criminal activities and damages of all kind.
- Technologically, the powerful momentum of digital transformation, together with other disruptive technologies and challenges provide an operating environment for adapting and adopting industrial, commercial and business innovations to the high-tempo of developments in the automotive domain.
- The legal and regulatory framework for engaging in cybersecurity activities in mobility is a dense and evolving set of EU directives, UN regulations, industrial & business standards, related with national legislation and administrative practices, which defines the rights and obligations of all involved actors and stakeholders.
- Environmental awareness becomes an overarching principle in automotive, since EU and global decarbonization targets together with Climate Change strategies are expected to be benefited by restraining car emissions and the road & transport impact altogether through electromobility, digital transformation of manufacturing and efficient usage of vehicles.

Cybersecurity becomes a holistic concept that runs throughout the digital and physical continuum of automotive mobility. A design and function requirement that simply cannot be ignored because of the potential grave implications in human life & health, individual well-being & social community, economy & production and at first most consumers & markets.

The eco-system is in need, as the consortium of CARMEL well understands, of a comprehensive cybersecurity strategy & practices, engaging directly and throughout the product, software and services development life cycle and thereafter enabling a vigilant eye on the functions and operations of systems, platforms and networks.

CARMEL advocates to design, develop and operate a risk-aware, process-driven solution that integrates cybersecurity, as an end-to-end concept, that has to be taken into consideration in safety provisions & regulations, engineering & administration, manufacturing & assembly and usage & services.

Moreover, the CARMEL consortium brings along a range of complementary multi-disciplinary areas of expertise, including direct knowledge of autonomous, connected, electromobility and cybersecurity and the explicit willingness to cooperate in a synergistic fashion under the banner of catering for the cybersecurity of the whole domain.

CARMEL can be Europe's springboard to the next level of cybersecurity for autonomous, connected and electromobility by employing our collective resources in industrial capacity, technological prowess, social responsibility and market leverage.

Annex A: CAMEL Intellectual Property Rights Agreement

This Annex contains the effective, complete and duly undersigned -by all participants of the consortium- Intellectual Property Rights agreement that is applicable for CAMEL at the collective level. A total of 22 pages, including in-page images of the original signature pages, for each of the 18 participants of CAMEL.

CAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

IPR AGREEMENT

BETWEEN:

Description of partners detailed in the Consortium Agreement

1. **FUNDACIO PRIVADA I2CAT, INTERNET I INNOVACIO DIGITAL A CATA- LUNYA (I2CAT)**, established in CALLE GRAN CAPITA 2-4, EDIFICI NEXUS I, BARCELONA 08034, Spain,
2. **DEUTSCHE TELEKOM SECURITY GmbH**, Bonner Talweg 100 53113 Bonn, Germany
3. **ATOS IT (ATOS)**, established in CALLE DE ALBARRACIN 25, MADRID 28037, Spain,
4. **ALTRAN DEUTSCHLAND SAS & CO KG (ALTRAN)**, established in FRANKFURTER RING 81, MUNCHEN 80807, Germany, ,
5. **EIGHT BELLS LTD (8Bells)**, established in 23 Agias Paraskevis, Strovolos, Nicosia 2002, Cyprus,
6. **UBIWHERE LDA (UBIWR)**, established in TRAVESSA SENHOR DAS BARROCAS 38, AVEIRO 3800 075, Portugal, ,
7. **CYBERLENS BV (CLS)**, established in SCHOOTSESTRAAT 14, EINDHO- VEN 5616 RD, Netherlands,
8. **GREENFLUX ASSETS B.V. (GFX)**, established in MAURITSKADE 63, AM- STERDAM 1092 HA, Netherlands,
9. **SIDROCO HOLDINGS LIMITED (SID)**, established in Petraki Giallourou 22, 1077 Nicosia, Cyprus,
10. **O INFINITY LIMITED (OINF)**, established in 2A HEIGHAM ROAD IMPERIAL OFFICE, LONDON E6 2JG, United Kingdom,
11. **UNIVERSITY OF CYPRUS (UCY)**, established in KALLIPOLEOS STREET 75, NICOSIA 1678, Cyprus,
12. **PANEPISTIMIO PATRON (UPAT)**, established in UNIVERSITY CAMPUS RIO PATRAS, RIO PATRAS 265 04, Greece,
13. **IDNEO TECHNOLOGIES, S.A.U.**, with tax address GRAN VIA CARLOS III 98 PLANTA, BARCELONA 08028, Spain
14. **AVL LIST GMBH (AVL)**, established in HANS-LIST-PLATZ 1, GRAZ 8020, Austria,
15. **PANASONIC AUTOMOTIVE SYSTEMS EUROPE GMBH (PANA)**, established in ROBERT-BOSCH-STRASSE 27-29, LANGEN 63225, Germany,
16. **Korea Automotive Technology Institute (KATECH)**, established in 303 Pungse-ro, Pungse-Myeon, Cheonan-Si, Chungnam, Republic of Korea
17. **Electronics and Telecommunication Research Institute (ETRI)**, established in 218 Gajeong-ro, Yuseong-gu, Daejeon, 34129, Republic of Korea
18. **MOBIGHEN CO LTD (MOBIGHEN)**, established in C-16th Floor, 128, Beobwon- ro, Songpa-gu, Seoul, Republic of Korea,

hereinafter, jointly or individually, referred to as "Parties" or "Party" relating to the Action en-titled

Artificial Intelligence based cybersecurity for connected and automated vehicles
in short

CAMEL

corresponding to the Grant Agreement number **833611** and hereinafter referred to as "Project" or "Action"

WHEREAS:

The Parties, having considerable experience in the field concerned and are conducting the Project to the Funding Authority as part of the Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020).

The Parties wish to specify or supplement binding commitments regarding intellectual property rights (IPR) handling among themselves in addition to the provisions of the specific Grant Agreement and Consortium Agreement.

NOW, THEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1. Purpose

1.1 The purpose of this IPR Agreement is to specify with respect to the Project the IPR ownership of all results developed within the Project.

1.2 The "CAMEL" Grant Agreement and the "CAMEL" Consortium Agreement are integral parts of this agreement and its content prevails should this agreement contain clauses contradicting them.

1.3 The agreements made herein settle only the purpose defined in section 1.1 and not any future contracts or contracts which are currently negotiated between some Parties.

2. Definitions

Words beginning with a capital letter shall have the meaning defined either herein, in the Rules Rules for Participation Regulation No 1290/2013 or in the Grant Agreement including its Annexes, or in the Consortium Agreement.

Component: each result (whatever kind or nature, including hardware, software, etc.) developed during the Project lifespan by one or several Parties (Lead or contributing parties).

Lead Developer. means the Party that has developed or led the development of a Component

Contributing Parties: means all Parties that have helped to the development of a Component.

IPR %: Is the respective share of property of a Component by a Party contributing to the development of it.

3. IPR Ownership

Section 8 and specifically subsections 8.1 and 8.2 of the Project Consortium Agreement, and Grant Agreement Art. 26 settle the ownership of Results.

In addition to the Grant Agreement and the Consortium Agreement, this document settles that “*Generation of Results*” means that an owner has developed through substantial effort, re-search, time, and expense, specific software components (Components).

A Result developed solely by one party shall be owned wholly by the Party that generates it. However, if a Result is jointly generated by two or more parties and it is not easy to ascertain the share of work of each Party; or separate each party’s intellectual contribution to the creation of the Result, then the Result will be jointly owned by the parties in their respective contribution.

The following table lists the percentage of ownership for all Components generated in the Project, whether owned by a single Party or distributed among several contributing Parties.

Name of component	Lead developer	Contributing parties	IPR %
Robustification of Scene analysis for Responding Reliably to adversarial threats			
	UPAT		100%
Multi-modal Data Fusion Module for Responding Reliably to the Threats			
		PANA	70%
Fusing of 2D and 3D segmentation modules		UPAT	30%
Cooperative Multimodal Localization for Reliably Estimating the Vehicle location			
	UPAT		100%
Cyberthreat Detection and Response Techniques for V2X (HW in the vehicle side) Hardware in the vehicle side (OBU)			
	IDNEO		100%
Cyberthreat Detection and Response Techniques for V2X (BSP in the vehicle side) BSP (Basic Software Package): low level routines to manage alarms and generic basic software to manage hardware devices			
	IDNEO		100%
Cyberthreat Detection and Response Techniques for V2X (SW in the vehicle side)			
	I2CAT		100%
Cyberthreat Detection and Response Techniques for V2X (SW in the infrastructure side) Software in the infrastructure side (RSU + MEC) to manage V2X messages and to provide different radio technologies interoperability			
	I2CAT		100%
AT scheduler for anti-tracking of V2X messages Software			
	I2CAT		100%
PKI-enabled Vehicle Identity Management System			
(PKI Servers, PKI Client)	ATOS		80%
		I2AT	15%
		UBIWHERE	5%
Multi-access edge infrastructure			
	UBIWHERE		50%
		I2CAT	50%
AI-based Context-rich and Context-aware Cybersecurity and benchmarking technologies			

Name of component	Lead developer	Contributing parties	IPR %
	OINF		100%
Hardware Security Module and Platform			
	DT-Sec		100%
Automotive solution for Intrusion Detection System			
GPS Intrusion detection and integration into the vehicle'		AVL	100%
Backend Solution		ALTRAN	100%
Highly secure charge control unit			
	GFX		100%
Anti-hacking device			
	DT-Sec		100%
Anomaly detection mechanism for EV smart charging stations			
EV smart protection		SID	60%
		GFX	25%
		8Bells	15%
Improved visualization and security analysis algorithms for highly dynamic automotive systems			
	CLS		100%
Novel and efficient machine learning algorithms for cyber-physical threat detection on autonomous vehicles			
	CLS		100%
Evaluation Framework for Automotive Threat Modelling			
		8Bells	70%
		ALTRAN	30%
In-vehicle sensor fusion for detecting GPS location spoofing attacks			
	UCY		100%
DriveGuard: Robustification of Automated Driving Systems			
	UCY		100%
Combination of External and Internal Camera Attack Detection Solution			
	UCY	UCY	60%
		OINF	40%
Combination of in-vehicle and cooperative solutions for detecting GPS location spoofing attacks			
	UCY	UCY	50%
		UPAT	50%

Table 1: Software components and other materials of CARMEL

4. Signatures

The Parties have caused this Agreement to be duly signed by the undersigned Authorised Representatives in separate signature pages the day and year first above written.

The signature of a Party by means of a scan or digitization of the original signature (e.g. a scan in PDF format) or an electronic/digital signature (e.g. via AdobeSign, via digital certificate...), counts as an original signature with the same validity, enforceability and permissibility. In case of signature using a digital certificate, it must have been issued by a trusted provider at EU level listed in <https://webgate.ec.europa.eu/tl-browser/#/>

Each Party receives a fully signed copy of this Agreement. The transfer of this copy by e- mail or via an electronic signature system will have the same legal force and legal effect as the transfer of the original copy of this Agreement.

Date:

Name: Joan Manel Martín Almansa Function: Managing Director

Representing the following body: **FUNDACIÓ PRIVADA I2CAT, INTERNET I INNO- VACIÓ DIGITAL A CATALUNYA (I2CAT)**, CALLE GRAN CAPITÀ 2-4, EDIFICI NEXUS I, BARCELONA 08034, Spain,

Signature:

52166299E
JOAN MANEL
MARTIN
(R:G63262570)

Digitally signed by
52166299E JOAN
MANEL MARTIN
(R:G63262570)
Date: 2021.10.22
14:34:46 +02'00'

CAMEL (No. 833611)

D7.5

June 2022

CAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 16.11.2021

Name: Stefanie Unkelbach

Function: Legal Entity Appointed Representative (LEAR)

Representing the following body: **DEUTSCHE TELEKOM SECURITY GmbH**, Bonner Talweg 100 53113
Bonn, Germany

Signature: Stefanie Unkelbach Digital unterschrieben von Stefanie Unkelbach
Datum: 2021.11.16 08:51:24 +0100

CARMEL (No. 833611)

D7.5

June 2022

CARMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date:

Name: Fernando Mediavilla Basabe Function: Head of Iberia BDS

Representing the following body: **ATOS IT (ATOS)**, established in CALLE DE ALBAR- RACIN 25,
MADRID 28037, Spain,

Signature:

CAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 22.10.2021

Name: Peter Fintl

Function: Director Technology & Innovation

Representing the following body: **ALTRAN DEUTSCHLAND SAS & CO KG (AL-TRAN)**, established in FRANKFURTER RING 81, MUNCHEN 80807, Germany,

Signature:

A handwritten signature in black ink, appearing to read 'Peter Fintl', written over a light gray background.

Date: 25 Oct 2021

Name: Dr Ioannis Giannoulakis

Function: H2020 L.E.A.R., Pr. Management Director

Representing the following body: **EIGHT BELLS LTD (8Bells)**, established in 23 Agias Paraskevis, Strovolos, Nicosia 2002, Cyprus

CARMEL (No. 833611)

D7.5

June 2022

CARMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date:

Name:

Function:

Representing the following body: **UBIWHERE LDA (UBIWR)**, established in TRAV
ESSA SENHOR DAS BARROCAS 38, AVEIRO 3800 075, Portugal,

Signature: *Rui Arnaldo Tereza Pinheiro Novo de Góia*

Date: 27 September 2021 Name: Georgios Alexopoulos Function: Managing Director

Representing the following body: **CYBERLENS BV (CLS)**, established in KASTANJELAAN 400,
EINDHOVEN, 5616 LZ, Netherlands,

Signature:

A handwritten signature in blue ink, consisting of a large, stylized 'G' followed by a horizontal line and a small flourish at the end.

CARAMEL IPR AGREEMENT

Confidential


version 14 2021-09-27

Date: 14-11-2021
Name: J.J. van Oort
Function: Director

29-11-2021
R.A. Plantinga
Director

Representing the following body: **GREENFLUX ASSETS B.V. (GFX)**, established in
MAURITSKADE 63, AMSTERDAM 1092 HA, Netherlands,

Signature:



CAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 4/10/2021

Name: ELISAVET GRIGORIOU

Function: OFFICE DIRECTOR

Representing the following body: **SIDROCO HOLDINGS LIMITED (SID)**, established in
Petraki Giallourou 22, 1077 Nicosia, Cyprus,

Signature:



CAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

CAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 28/09/2021

Name: George Efthymiou Function: Director

Name: Dr Marios Demetriades

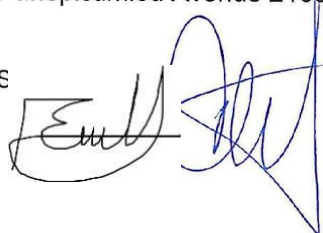
Function: Head of Research and Innovation Support Service

Representing the following body: **O INFINITY LIMITED (OINF)**, established in 2A HEIGHAM ROAD
IMPERIAL OFFICE, LONDON E6 2JG, United Kingdom,

Representing the following body: **UNIVERSITY OF CYPRUS (UCY)**, established in 1
Panepistimiou Avenue 2109 Aglantzia, 2109, Nicosia, Cyprus,

Signature:

S



CAMEL IPR AGREEMENT

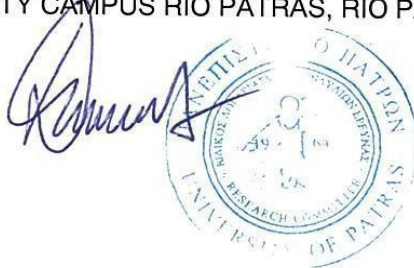
Confidential

version 14 2021-09-27

Date: 20/12/2021
Name: Panagiotis Dimopoulos
Function: Vice Rector

Representing the following body: **PANEPISTIMIO PATRON (UPAT)**, established in
UNIVERSITY CAMPUS RIO PATRAS, RIO PATRAS 265 04, Greece,

Signature:



CARMEL (No. 833611)

Date: Name: Function:

46578151T JOSE
MARIA PUJOL
(R:A08320384)

D7.5

Firmado digitalmente por June 2022

46578151T JOSE MARIA

PUJOL (R:A08320384)

Fecha: 2021.10.08 15:35:31

Representing the following body: ~~HOME TECHNOLOGIES, s.l.u.~~, with tax address GRAN VIA
CARLOS III 98 PLANTA, BARCELONA 08028, Spain

Signature:

CARAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date:
Name:
Function:

Representing the following body: **AVL LIST GMBH (AVL)**, established in HANS-LIST-PLATZ 1, GRAZ 8020, Austria,

Signature:




AVL List GmbH
Hans-List-Platz 1
A-8020 Graz, Austria
Phone: +43 316 287-0
www.avl.com

CARAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 09/11/2021
Name: Petros Kapsas
Function: ADAS Technical Leader, LEAR

Representing the following body: **PANASONIC AUTOMOTIVE SYSTEMS EUROPE GMBH (PANA)**, established in ROBERT-BOSCH-STRASSE 27-29, LANGEN 63225, Germany,

Signature:



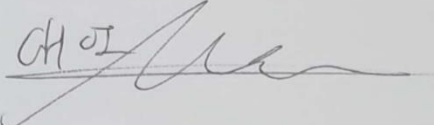
CARMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 19. Oct. 2021
Name: You-Jun CHOI
Function: Principal Researcher

Representing the following body: **Korea Automotive Technology Institute (KATECH)**,
established in 303 Pungse-ro, Pungse-Myeon, Cheonan-Si, Chungnam, Republic of
Korea

Signature: You-Jun CHOI 

CARAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 19 Oct 2021
Name: Taesang Choi
Function: Principal Researcher

Representing the following body: **Electronics and Telecommunication Research Institute (ETRI)**, established in 218 Gajeong-ro, Yuseong-gu, Daejeon, 34129, Republic of Korea


Signature:

CARAMEL IPR AGREEMENT

Confidential

version 14 2021-09-27

Date: 19. Oct. 2021
Name: Moon Kook, Park
Function: Director

Representing the following body: **MOBIGEN CO LTD (MOBIGEN)**, established in C-16th
Floor, 128, Beobwon-ro, Songpa-gu, Seoul, Republic of Korea

Signature:



Annex B: Participant's individual Exploitation Plans for CARMEL

This Annex contains, in full detail, the Individual Exploitation Plans of each one of the 18 participants of CARMEL.

I2CAT Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

i2CAT is a non-profit research and innovation centre located in Barcelona, Spain. We focus on promoting mission-driven knowledge to solve business challenges, co-create solutions with a transformative impact and contribute and lead collaborative research and innovation projects in the European and national context.

We base our added value on sound knowledge of digital technologies, and we promote R+D+i activities in Internet Technologies within the ICT industry. The centre stands up for a new model in a new conception of innovation: the collaboration between companies, public administration, the academic environment, and end-users.

i2CAT seeks actively this collaboration with the environment and the society, through our Board of Trustees, we have strong connections with the principal industrial, administration, and academic sectors. Our Board is formed by companies like Cisco, Orange, Fujitsu, Telefonica, Vodafone, Juniper and Cellnex between others plus four Catalan government departments and the three main technical universities of Catalonia.

i2CAT's activities are concentrated around, but not limited to, Cybersecurity, network development (5G, Mobile wireless networks, software networks with special focus on NFV and SDN, open access networks and recursive Internet network architecture), Distributed Artificial intelligence, virtual and immersive technologies, and sensor networks (IoT and M2M) i2CAT is participating on more than 32 competitive projects from H2020 including

16 5GPPP projects (3 of them as Project Coordinators and 3 as Technical Coordinators) expanding our experience on the applied research.

2. Your motivation to participate in the project and commitment:

i2CAT focus on exploring and defining new ways to manage the Future Internet networks, the connectivity of elements such as cars, infrastructure, sensors and IoT to enable new functionalities and new infrastructure business models. i2CAT considers the experience and knowledge gained in the European funded project as an essential element to earn the required intellectual capital. CARMEL project is an excellent mean to grow the knowledge and experience on cybersecurity and artificial intelligence to improve the new connected world.

i2CAT is the project coordinator of CARMEL, leading WP1 and contributing to WP2 where the requirements, specifications and architecture of the CARMEL are identified. We will also participate intensively on the WP3 on the cyber threat detection and response techniques for cooperative automated vehicles are defined for the on boarded unit as well as for the infrastructure units. We are also participating in WP4 (on the PKI enabled vehicle identity management) and on WP5 (on the sw for the security module and the defence protecting the chain of trust). We are also participating on WP6 for the integration, validation, and evaluation activities.

3. Means to achieve your objectives:

i2CAT has at the end of 2021 more than 140 professionals dedicated to fulfilling its applied research mission. Mainly composed by researchers and with approximately a 22% of PhD, i2CAT has a strong human team that ensures its ability to perform the tasks required in this project.

i2CAT has created its own cybersecurity area with dedicated professionals that together with the Distributed Artificial Intelligent area are involved in CARMEL to reach the goals of the project. The Mobile Wireless internet and Software Defined areas have also dedicated resources to this project.

4. Opportunity which appeared/appears:

i2CAT has participated in previous H2020 projects like SHIELD, 5GCity, 5GPicture, Charisma, 5GHAUL and V2xArch that set the base for the current development on CARMEL. We have also worked together with the local administration in cybersecurity programs and mobility challenges that grounded our knowledge.

The focus of Shield research was to increase the efficiency of the current cybersecurity solutions with the objective to understand attacker's behaviour and predict vulnerabilities and threats. CARMEL is a continuation on the work done in this and other projects.

i2CAT as an applied research centre is working on the research challenges posed by the vehicular communications, a market that will be of capital importance in the next years. We have a strong group of researchers dedicated to this topic in a horizontal CCAM group that includes researchers in the cybersecurity, distributed artificial intelligence, software networks and mobile wireless teams. The goal of this researchers is to design algorithms and applications enabling the future connected and autonomous cars.

We are also participating in other European founded projects such as 5GMED and PLEDGER and Spanish founded ones as Red.es projects where we want to develop further and test the assets we are working on in CARMEL.

WHAT & WHY

5. Exploitable assets and results:

i2CAT is working in obtaining five different assets, either owned by i2CAT or jointly owned together with CARMEL partners, as a result of this project. i2CAT has identify 3 exploitation items developed exclusively by i2CAT as output of the CAMEL project:

Cyberthreat Detection and Response Techniques for V2X on the infrastructure

Cyberthreat Detection and Response Techniques for V2X onboarded on the vehicle

AT scheduler for anti-tracking of V2X messages

And has also identify two future assets in a join development:

The PKI-enabled vehicle Identity Management System with ATOS and Ubiwhere and the Multi-access edge infrastructure together with Ubiwhere

i2CAT is working on a reference V2X kit that include different features that facilitate the developers of the apps to get to a viable point decreasing the complexity of the ecosystem by managing the V2X messages ant to provide different radio technologies interoperability. In CARMEL we focus on the Cyberthreat detection and response part, for the infrastructure & MEC as well as for the on-board unit. We also work on an innovative approach to the V2X identity tracking, using ML to better detect the traceability of vehicles on the platforms.

i2CAT also works with other partners in defining sw solutions for the vehicle identity management systems and the MEC edge infrastructures that will also be key on the V2X ecosystem.

6. Rationale:

i2CAT aims to impact the society and invests great efforts into deploying assets that can bring innovation and improvements to them.

We will use the assets as background for the future research projects we are already securing and where we would aim to improve them. We will also continue fostering the academia environment to better understand the challenges we work on in CARMEL project through our different collaborations with the principal universities in Spain, via offering workshop, courses and

scholarships to university students.

i2CAT wants to use the outputs of CARMEL to help CESICAT (cybersecurity agency of the Government of Catalonia) with whom we have collaboration agreements as well as fostering closer collaboration with the Automotive industry, telecommunication operators and integrators ecosystems. We also belong to organizations like the CIAC (Catalonia Automotive Industrial Cluster) where we will scout technological transfers.

We are also a key partner in the 5GBarcelona initiative where there is a test ecosystem including MEC facilities. There we will have the possibility to further test and develop the different SW assets. i2CAT plans to exploit CARMEL outcomes to enhance 5GBarcelona testbed for the Internet of Vehicles (IoV) and V2X services with cybersecurity features.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

i2CAT has also identify two future assets in a join development:

The PKI-enabled vehicle Identity Management System with ATOS and Ubiwhere and the Multi-access edge infrastructure together with Ubiwhere

We will seek a joint exploitation plan with the two partners where we take advantage of our mutual particular forces in an aim to reach the major number of possible transfer targets at the same time that we use the results for future research.

i2CAT is already working in MEC applications life cycle management and other possible assets related with the Edge orchestrations that could be exploited jointly with the results of this projects. We will individually evaluate the assets and then put in place a project to trace the next steps.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

i2CAT has a dedicated team, Knowledge and Technology Marketing, that evaluate each result of the projects and provide an evaluation report for each technology. This process will be started when the assets are mature enough to evaluate the technical problem solved and the added value given. This process may take between 4 and 6 weeks, where the team and the researchers work together to define and characterize each asset.

This report evaluates different aspects of the asset such as Technology Readiness Level (TRL), difficulties to further advance this TRL, replicability, and competitive advantages together with market perspectives such as market size or industry maturity. This report is presented to the company board and the next steps are decided. The technology is also included in i2CAT portfolio at this stage.

As a result of this report i2CAT defines an exploitation plan for each one of the assets, either investing on further development, actively seeking a company to transfer the technology and support the process to transform it into a product, creating a spin-off that can foster the transformation in case of emerging markets and fostering community adoption of the new knowledge on the European community.

In case of future development, the first step is to start an internal valorisation project where the required steps to bring the results as close as possible to transference stage are defined and timely scheduled. At the same time there are continuous meetings with relevant stakeholders on the ecosystem to ensure the alignment between the research efforts and the market needs. i2CAT also plan to showcase the assets internally and also to work on communication and dissemination actions that can enforce the assets value. As project coordinators we are already monitoring the defined KPI and carrying out actions like the workshop preparation.

9. Measurement

Inside the project we, as project coordinators, are following up the action plan and KPI planned for the whole project impact such as trainings, webinars, white papers.

i2CAT, as individual partner, measures the impact of each asset individually depending on the actions decided upon evaluation.

i2CAT considers dissemination actions such as papers and publications related to the assets, as well as workshops prepared on the result context.

For those assets where a valorisation project is set up after evaluation, i2CAT sets milestones to be measured like the number of interviews with relevant stakeholders carried out, the follow up meetings with relevant companies, in case of transfer proposes or the license contracts obtained.

We also take into account other communication KPI like digital attraction to the information or assets publicly available on our web page and traffic routed to the web from social network communication posts.

10. Positioning

The global market for V2X is forecasted to grow with a CAGR between 42-45% for the period 2021-2026 or 2021-2028 depending on the sources a, b, c. The COVID19 pandemic was especially hard on this market due to the considerable decrease on vehicle production and sales, nevertheless the reports consider that the V2X market will cope with the issues one the pandemic is over due to the boost on the demand for cars including connected technologies. There are still few reports on the impact of the silicon shortage on the V2X market, but the forecast may be impacted due to this current contingency.

If we take into consideration the submarket of cybersecurity associated to V2X the CAGR on the period 2020-2025 d or 2020-2030 e is expected to be of the around the 33%. The grow in this market is also attributed to the growing trend in the cyber-attacks in the automotive industry and the increase of connected cars present on the market. The reported cyber-attacks around the world has spike in the last 3 years, with reported increases of more than 80% year over year. Another interesting driver for the market is the amount of data generated by the sensors, network elements and other devices on the vehicles that will need to be analysed. The data protection, to ensure proper personal data protection and security concerns, will also be a key factor in the developing of the cybersecurity market. The AT scheduler for anti-tracking of V2X messages solution that i2CAT is developing will help coping with this security concern. The access point for the attackers are not just the vehicles and its components but also the infrastructure. That is why i2CAT finds of capital importance to work simultaneously in the protection techniques for both elements.

The segmentation on the platforms, due to the OEMs policy of developing its own electronic components, software, connectivity modules and platforms can lead to cybersecurity exposure due to the integration interfaces between the elements. This element can be an opportunity in the market and also an element that delay the adoption of some improvements. One of the challenges of the market will be to keep up with the continuous evolutions in the ecosystem. The changes on the standards as well as the existence of different protocols cohabitating the ecosystem poses major load on the technology solutions.

There are some companies offering V2X stacks, which can be divided into several groups being the two most relevant the OEM themselves who have close implementations and the Big consultancy or other companies that seek the adoption of their version f, g. Further study of the possible product on the market will be needed upon the internal evaluation of each asset.

- a. <https://www.businesswire.com/news/home/20210730005345/en/Global-V2X-Market-Forecasts-2021-2026-A-6.5-Billion-Market-by-2026---ResearchAndMarkets.com>
- b. <https://www.fortunebusinessinsights.com/automotive-v2x-market-103320>
- c. <https://www.globenewswire.com/news-release/2021/09/06/2291733/0/en/Automotive-V2X-Market-to-Exhibit-a-CAGR-of-42-1-and-Hit-USD-7-351-9-Million-by-2028-Qualcomm-Technologies-and-GM-s-Extension-of-Their-Partnership-to-Amplify-Growth-Fortune-Business.html>
- d. <https://www.marketsandmarkets.com/Market-Reports/v2x-cybersecurity-market-194480977.html>
- e. <https://www.researchnester.com/reports/v2x-cybersecurity-market/3586>
- f. <https://capgemini-engineering.com/es/es/brochure/v2x-stack/>
- g. <https://www.cohdawireless.com/solutions/v2x-stack/>

NEXTIUM by IDNEO Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

NEXTIUM by Idneo is an innovation partner for connectivity, in-cabin sensing & biometrics solutions. Its passion is to design, develop and deliver next generation products and services for automotive, mobility and industrial sectors.

2. Your motivation to participate in the project and commitment:

Cyber-Attacks are one the most important problems nowadays and together the topic that cars are everyday more connected to Internet (CCAM), this is translated to a cyber-security issue associated to the road security, which means a possible impact within the driving experience and society. CARMEL project born as European project with the aim to address security to CCAM in the European area.

As FICOSA and NEXTIUM by Idneo are companies located in Europe and with a robust experience within the automotive hardware and software. Cyber-security has gained a lot of attention in recent years due to ever increasing communication channels. It is on our aim to maintain a high level of cyber-security in our products, so we entered CARMEL project with two objectives: implement cyber-security in the logical and physical domains.

Our position is with the On-Board Units (boxes within the CCAM) and all items related to physical security, Secure Boot and Keys Management with the aim to help to look for a better society protection.

3. Means to achieve your objectives:

Our experienced hardware and software automotive engineers together prepared laboratories and knowledge give us the enough tools for this collaboration, all this up to the experience on the automotive sector, collaboration with automotive companies, grants and products industrialization.

Also, it is very important to remark, that we have members in our team with experience in cyber-security banking sector.

4. Opportunity which appeared/appears:

NEXTIUM by Idneo - also FICOSA- takes care of the product (hardware and software) with its automotive know-how and the business opportunity is with the automotive dedicated product production.

We think that the knowledge developed in CARMEL grant will be of interest for any automotive company.

WHAT & WHY

5. Exploitable assets and results:

The three pillars where NEXTIUM by Idneo can contribute on CARMEL project are the know-how on components related to the product and technologies required, enough knowledge based on the experience & background, and methodologies & tools to make the product feasible, secure and affordable.

6. Rationale:

Cyber-security is a very actual, important and essential topic for CCAM due to its impact on the driving's security, and it represents a must-have pillar to focus on for NEXTIUM by Idneo.

Our interest and exploitation are both industry and R&D oriented. We provide commercial solutions and contribute to new product and technologies developments, integrations and validations.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

NEXTIUM by Idneo shares the hardware and software security know-how and components against logical and physical attacks being feasible the product production in our facilities.

Our expectations from the rest of the partners are growing in knowledge and setting alliances for current CARMEL and future experiences and products.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

The final part of the project comprises seeing the result and effort effectiveness of all the work of the project with the Demonstration on car.

NEXTIUM by Idneo collaborates with the hardware and software which will be introduced within the car and together with other partners such as Panasonic, i2cat and ATOS we will test the different use cases defined at Panasonic's parking lot in Germany around April – May 2022.

After the demo, all the documentation depending on it will be finished presenting the results and also during these months, collaboration on Congresses is being defined (e.g., IoT Solutions World Congress in Barcelona on May 2022 where performing a demo is being evaluated).

9. Measurement

The objective is that actions defined for CARMEL give the expected results and are reliable, secure and robust as an automotive product in the market according to the standards.

10. Positioning

Cyber-security is everyday more requested by the official entities, customers and the market itself. This means that being present in the sector with a dedicated team, with continuous improvements and benchmarking is very important to be able to offer an excellent working and affordable product.

UBIWHERE Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

Ubiwhere is a Portuguese SME founded in 2007, has been well-renowned for its R&I activities in the Smart City and Future Telco areas, having already been involved in more than 15 H2020 projects. Ubiwhere's activity focuses on the research and development of technologies across several markets, namely: Telecom and Future Internet; Smart Cities; Sustainable and Efficient Resource Management (Energy, Environment, and Natural Resources); Transportation, Travel, and Tourism.

2. Your motivation to participate in the project and commitment:

Ubiwhere intends to leverage and increase its know-how in solutions related with Smart Cities and V2X communication, particularly using technologies like 5G and MEC. CARMEL represents an opportunity to explore new innovative applications in this area, especially for use cases where latency and bandwidth requirements are key.

Ubiwhere will be the MEC solution provider for the autonomous connected car use case in CARMEL and participate in all tasks related to this use case.

In WP2, Ubiwhere will contribute for the overall design activities while following the cybersecurity outcomes implementation in WP3 to WP5.

In WP6, Ubiwhere will integrate its solution in the pilot for validation.

Finally, Ubiwhere will be active in dissemination, communication and exploitation activities.

3. Means to achieve your objectives:

Since 2007, Ubiwhere has fostered a culture of innovation and creativity by delivering the solutions that its clients need in order to succeed, offering a vast portfolio of products, services and solutions for the Telecom and Future Internet sectors.

For Smart Cities, Ubiwhere has been developing solutions since 2014 for improving the mobility and the environment, with the strategy of going from R&D Projects up to commercial joint ventures (like Citybrain) or even spin-off companies, such as Bikeemotion for electric bike sharing, Parkware for smart parking systems, Thumbco Corporate for fleet and car sharing and UNICLE for V2X communication.

Responsible for these achievements, Ubiwhere's key ingredient is a multi-faceted, dynamic, passionate and highly qualified team composed of Senior Executives, Researchers, Consultants, Project Managers, Creative Designers, Programmers and Quality Assurance Technicians.

4. Opportunity which appeared/appears:

The acquired knowledge from Ubiwhere's participation in CARMEL is extremely relevant due to the potential synergies and overlapping areas with existing products such as Unicle (<http://unicle.io>), a platform for vehicle communication and Smartlamppost, a piece of urban furniture which can host multiple equipments such as 5G nodes, EV charging systems and surveillance systems, just to name a few. V2X initiatives such as CARMEL need 5G connectivity closer to the vehicles, which can help to leverage Smartlamppost into effectively launching a new private and dedicated 5G network for V2X communication, while using the distributed edge computing resources to deploy a specific software stack.

WHAT & WHY

5. Exploitable assets and results:

Currently, the Smartlampposts have been installed for smart lighting, electric vehicle charging, and network connectivity. However, the product has the potential to be a vehicle for rapid and cost-effective 5G network deployment as it allows for a massive Small Cell rollout.

6. Rationale:

With previous "G's" relying more on macro site deployments for wide coverage, it is expected that 5G will be much more dependent on small cells due to the use of higher frequency bands with much shorter coverage range. This will result in an increased node capillarity and in the installation of radio equipment in urban landscapes, leading to unwanted equipment creating visual pollution. Smartlamppost aims at solving these problems, by providing urban furniture that can host small cells in a non-intrusive way. Additionally, SmartLamppost's Neutral Host Platform capabilities allow Mobile Network Operators (MNOs) and Neutral Hosts to rent existing infrastructure, sharing maintenance and deployment costs.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

SW components to include in V2X solution to include in Smartlamppost platform

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

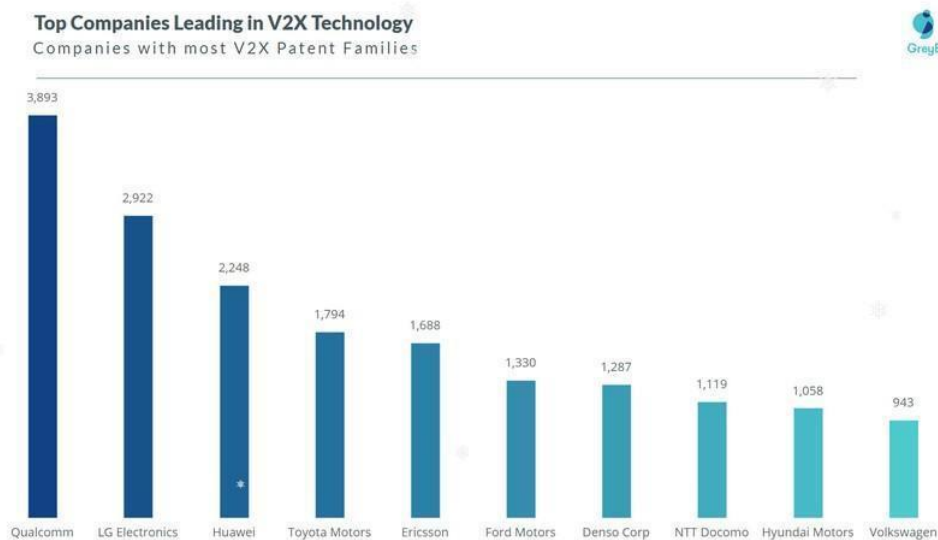
- New Business leads generated directly or indirectly by the project outcome
- Participating in other EC funded projects related with V2X

9. Measurement

The objective is that actions defined for CARMEL give the expected results and are reliable, secure and robust as an automotive product in the market according to the standards.

10. Positioning

Top 10 companies leading in V2X technology (taken from <https://www.greyb.com/v2x-companies/>):



Top start-ups in V2X (taken from <https://tracxn.com/d/trending-themes/Startups-in-V2X>):

- <https://auto-talks.com/>
- <https://www.visteon.com/>
- <https://en.derq.com/>
- <https://www.valerann.com/>
- <https://www.commsignia.com/>
- <https://www.haasalert.com/>
- <https://www.kapsch.net/>
- <https://seesense.cc/>
- <https://connectedsignals.com>
- <https://www.cohdawireless.com/>

OINF Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

OInfinity Ltd is a SME based in London, UK. We are an AI driven company mainly focusing on Machine learning (Deep Learning), Virtual, and augmented reality.

2. Your motivation to participate in the project and commitment:

Our aim is to contribute and improve our knowledge on Machine learning especially in the Deep learning field enhancing the security aspects of autonomous and connected vehicles. We concentrated our effort on the physical adversarial attacks on the environment (i.e., camera related attack) and led the task 4.2 in CARMEL project.

3. Means to achieve your objectives:

We are a group of distinguished scientists with extensive experience in various UK/European projects and have proven track record on AI solutions for cybersecurity and anomaly detection. Likewise, all the necessary resources for completing CARMEL project are in place such as GPUs, embedded devices, libraries and human power.

4. Opportunity which appeared/appears:

Our main contribution towards the CARMEL project is to establish research in physical adversarial attacks on camera sensors. This is mainly reflecting the internal needs of our group to extend our background and tools on cybersecurity moving from power grids to include also autonomous

vehicles. The physical adversarial attack is a real world challenge that needs to be solved in order to have fully autonomous vehicles. Hence, our research in the field as well as the proposed solutions produced in CARMEL is highly relevant in this field.

WHAT & WHY

5. Exploitable assets and results:

During the CARMEL project, the proposed solutions for physical adversarial attacks as well as the developed pipeline can be integrated to our cyberattack benchmarking tools which can be considered as exploitable assets. Furthermore we published our results in various conferences and journals that helps to demonstrate the novelties and the over potential of the developed solutions.

6. Rationale:

The developed solutions for autonomous vehicles have both commercial and research applications. Therefore, the potential of the anomaly detection framework is high and aims to offer a complete solution in autonomous systems with real-world products focusing on the safety validation and benchmarking of autonomous vehicles and critical infrastructures.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

Our goal in the project is to share knowledge and increase the collaborations with other involved partners in the near future. We share a mutual understanding of the challenges that lie in autonomous vehicles and have worked together to produce innovative solutions for anomaly detection. There is possibility for collaborations that could aim to the integration of multiple solutions and approaches (e.g. GPS based AD) into a single commercial product.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

Based on current plans we aim to participate and if possible contribute to workshops and expos the following 6 to 9 months. Specifically we aim to present part of our latest systems and innovation in the International Conference on Distributed Computing in Sensor Systems (DCOSS 2022) and IoT cybersecurity related workshops. Also we aim to participate at the Autonomous Vehicles Expo Sep 2022 The International Centre, Telford, UK and if possible to be involved and present tools and systems developed in this project during related workshops part of ECCV 2022 in Oct. 2022.

9. Measurement

Participation to relevant expos and workshops; Novel contributions and publications; New collaborations and new business partners; Funding to complete the development of our tools.

10. Positioning

An Increasing amount of research is being carried out in similar fields, plus the interest of large organisations in this field and area of innovation including McAfee. Hence in the near future there will be an increased market potential for business and products in this area of topics and problems we investigate in CARMEL.

ALTRAN Individual Exploitation Plan

PROFILE & MOTIVATION

11. Partner Profile

ALTRAN is a global High-Tech Engineering and R&D Consulting company whose mission is to improve technologies throughout their lifecycle and directly drive the Digital Transformation of its clients in the ICT industry. The consolidation of a unique set of advanced engineering and R&D capacities has the largest distribution network in the world, with a presence in all principal engineering centres. Many clients also benefit from ALTRAN's ability to implement large-scale

technologies, its broad product engineering expertise, and industrial expertise.

12. Your motivation to participate in the project and commitment:

Given the technologies to be developed within CAMEL, ALTRAN's objective is to make the most of the knowledge and software generated and to develop more knowledge internally. The use cases considered in the CAMEL project are well established in the company as part of a wider arc of topics ranging from hardware development (including sensor hardware) to the Internet of Things and large- scale data analysis and Cyber Security for different industrial purposes. This combination of skills and proprietary software is partly marketed as a portfolio of Vue Forge (TM) services by Altran. The ability to offer the full range of competencies and technologies is a unique selling point.

The specific consultancy services w.r.t. the technologies involved in CAMEL are characterized as follows:

- Altran is considered an established contractual supplier of experts and solutions to Telecoms and Automotive (Carriers in particular, and vendors as well), and has experts driving Projects globally (including Vodafone Group, Orange, Telefonica, Deutsche Telecom; Verizon, BT and BMW, Daimler, PSA, Audi) that range from Solution Design Architects; Engineers; Project Managers; Experts driving RFIs/RFPs/RFPs Solutions Bidding and Vendor Solutions Selections and Vendor Management; Standardization Experts and Innovators for new products and services.
- Upscale existing cooperation with telecom operators, Auto motives and vendors. Altran supports its customers in the selection of technologies and components, deploying the solutions, and building roadmaps for products and services innovation.
- Solution development on demand, as Altran also develops own IP as well as in partnerships with manufacturers ALTRAN is represented in most European countries as well as USA and Asia.

13. Means to achieve your objectives:

Altran has a wide range of professionals with expertise in CAMEL's core areas, such as 5G technology, cyber security, and marketing experts for WP7 activities, and proven experience in artificial intelligence, machine learning, embedded software and IoT.

All this collection of expertise in conjunction with the participation in the project makes Altran a partner capable of strengthening its market presence in automotive cybersecurity.

14. Opportunity which appeared/appears:

The participation in the project permits to Altran generate relevant expertise in cyber security research, thanks to the effort in developing simulations for testing cyber security systems. Furthermore, the knowledge acquired can be exploited in internal business projects where simulations and artificial intelligence become central in their development. Due to exceedingly high demand in security solutions by OEMs we expect significant business increase in this area in any case. Innovative solutions and competence demonstrations are adding on top. Since we are product neutral, we expect proliferation of CAMEL technologies and thus further indirect business.

WHAT & WHY

15. Exploitable assets and results:

- IoT
- Cyber Security
- System integration
- Automotive Embedded Security
- Simulations for autonomous driving
- Collection, detection, and analysis information on suspicious activities

- Threat visualization

16. Rationale:

ALTRAN seeks to improve its IoT and Automotive Cyber Security service portfolio by building on the knowledge from its participation in CARMEL. As a technology consultancy company, ALTRAN has a vast stock of professional technology consultants, solution design architects, and engineers to support the automotive industry, telecom operators, 5G related enterprises, Cyber Security, Intrusion detection, and other emerging technologies.

This guarantees a proliferation of innovative technologies or consulting services. Furthermore, ALTRAN might take advantage of the generated knowledge from its participation in the project to integrate them into its range of services and provide help to customers in other fields of application.

17. Your Value Proposition towards Joint Exploitation of CARMEL:

The CARMEL consortium includes a range of complementary multi-disciplinary areas of expertise, including direct knowledge of autonomous mobility and cybersecurity.

Building internal capacities. Getting more people on board. Forming new business opportunities and partnerships

ROADMAP WITH TIMELINE

18. Roadmap: the timeline plan you have for using those assets:

Steps to support the GTM of the solution:

- Autonomous Mobility (system integration. Simulation for testing AI-based apps under controlled environments,) → present it to clients.
- Electromobility (focus on sustainable solutions. Using it for ev alike.)
- Connected Mobility (Using the backend (cooperative information) for increased security of the CCAM)
- Remote Controlled Vehicles (safe AI, Connecting modules.)

Additional selected points from our development plan related to the CARMEL use cases:

- Leverage enterprise IT (Information Technology) processes for data protection and data decommissioning.
- Push further the implementation of encryption and software source-code signing to protect the integrity of system software.
- Develop standards of practice for secure development of critical vehicle systems.

19. Measurement

- First three solutions: focus on the end user. Increasing safety criteria. Based on the integration of the backend solution by other partners.
- Success rate of served clients
- Rate of implemented solutions
- Rate of "clients"/ partners adapting to some cybersecurity label.. ISO/SAE 21434

20. Positioning

AVL Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

AVL List GmbH ("AVL") is the world's largest independent company for development, simulation and testing in the automotive industry, and in other sectors. Drawing on its pioneering spirit, the company provides concepts, solutions and methodologies to shape future mobility trends. As a major contributor to e-mobility, AVL drives innovative and affordable systems to effectively reduce CO2 by applying a multi-energy carrier strategy for all applications – from hybrid to battery electric and fuel cell technologies.

AVL constantly evolves its ecosystem of high-end methodologies and innovative technologies in the area of vehicle development and testing which provides real world solutions to support customers' future mobility ambitions. From the ideation phase to serial production, the company covers future vehicle architectures and platform solutions including the impact of new propulsion systems and energy carriers.

By digitizing the vehicle development with state-of-the-art and highly scalable IT, software and technology platforms, AVL creates new customer solutions in the areas of Big Data, Artificial Intelligence, simulation and embedded systems. In the field of ADAS and autonomous driving, AVL has built comprehensive competences to accelerate the vision of smart and connected mobility.

2. Your motivation to participate in the project and commitment:

As an automotive engineering company, AVL will provide know-how and support in automotive cybersecurity. Specifically, our role in the project includes to develop distributed automotive intrusion detection system integrated with backend SIEM solutions, with a focus on security of automotive E/E systems and in-vehicle network, to conduct threat modelling and risk assessment of connected car use cases, from V2X to EV charging, to lead system integration and validation in WP6 and demonstrate feasibility of the solutions against cyberattacks on in-vehicle network and components including CAN bus and ECUs, to develop and disseminate automotive cybersecurity best practices leveraging AVL's participation in road vehicle cybersecurity engineering standard ISO/SAE 21434 and the involvement in various industry groups. • Altran is considered an established contractual supplier of experts and solutions to Telecoms and Automotive (Carriers in particular, and vendors as well), and has experts driving Projects globally (including Vodafone Group, Orange, Telefonica, Deutsche Telecom; Verizon, BT and BMW, Daimler, PSA, Audi) that range from Solution Design Architects; Engineers; Project Managers; Experts driving RFIs/RFQs/RFPs Solutions Bidding and Vendor Solutions Selections and Vendor Management; Standardization Experts and Innovators for new products and services.

- Upscale existing cooperation with telecom operators, Auto motives and vendors. Altran supports its customers in the selection of technologies and components, deploying the solutions, and building roadmaps for products and services innovation.
- Solution development on demand, as Altran also develops own IP as well as in partnerships with manufacturers ALTRAN is represented in most European countries as well as USA and Asia.

3. Means to achieve your objectives:

AVL provides comprehensive engineering service and innovative technical solutions to protect connected cars against cyberattacks. With more than 65 years of experiences in the development and improvement of all types of powertrains as well as in the field of measurement and test technology, AVL offers know-how of the best methods and technologies for the safety and security of road vehicles, with a deep understanding of best practices in both automotive and cybersecurity. The security activities cover the whole engineering lifecycle, including threat analysis and risk assessment, specification of security requirements, design of functional and technical security concepts (e.g. security architecture and cryptographic schemes), security implementation (e.g.

secure coding, security gateway and system integration), security verification and validation (e.g. static & dynamic code analysis, vulnerability test, fuzzing test, pen testing), as well as remote software update and continuous security care.

As an engineering service provider, AVL has the know-how, tools and equipment needed for mastering complexity in powertrain development, covering the entire development life cycle. Most of the tools are developed and manufactured by AVL itself, including full simulation environments e.g., for security testing of connected vehicles, which allows a high degree of flexibility also for new systems. For research and development in realistic settings, AVL will use test cars at the company test track in Gratkorn in Austria and on the road. The test cars are equipped with CAN interfaces for injecting CAN packets and connecting to vehicle internal networks.

4. Opportunity which appeared/appears:

The intrusion detection system for GPS which is being developed from AVL is a combination of AI and ML techniques along with AVL's own simulation tool named Model.CONNECT. The whole pipeline of intrusion detection system for GPS also includes hardware in loop along with the HackRF and UBlox receiver. For now, the whole test setup (testbed) is created by considering the requirements from CARMEL. As an idea for the future improvements and improvising the already existing system from CARMEL the idea is to bring the whole setup into the real vehicle and to work towards making this as a one-step solution for intrusion detection system for GPS in the near future.

WHAT & WHY

5. Exploitable assets and results:

Intrusion detection system for GPS solution uses the tool Model.CONNECT™ is AVL's open model integration and co-simulation platform, connecting virtual and real components into one functional prototype. The AI and ML techniques used for the training of the network for intrusion detection system is developed by taking few of the ideas from the already existing works at AVL. Results of the trained networks also improved by considering the ideas and knowledge from experts and from some of the existing works at the company. Lessons learnt from other projects also added value in the whole development and integration process.

6. Rationale:

The assets from CARMEL project (tools, hardware and software components) are developed in a way that they can be adapted to other projects which has similar ideas involving around intrusion detection, AI and ML concepts and need of a simulation environment. AVL foresee to improvise its intrusion detection system to bring it as a one stop solution of Anti-hacking system-GPS for the future autonomous vehicles. AVL is in active discussion with the potential partners to deploy the intrusion detection system in one of the upcoming projects.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

AVL as mentioned earlier has a motto to share its knowledge and assets with other potential partners to have a healthy and fair competition in the market. In CARMEL project AVL has offered free one year trial of AVL Model.CONNECT for partners from academic institutions or research institutes. Along with PANA AVL has also offered to provide Gratkorn Test Track (in Austria) as one of the pilot sites if in case any unseen issue comes up with the scheduled test sites. AVL also had few meetings and interactions with UCY to discuss and share their experience about the intrusion detection system for GPS since both the partners were working on the similar topic. AVL is eagerly looking forward collaborating with other CARMEL partners to be a part of RnD projects and to learn and share the knowledge of their expertise from other partners as well.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

As an initial plan AVL would like to present the testbed setup for intrusion detection system to all the partners in one of the upcoming technical meetings. Since AVL is following its own pipeline for integration and validation of the work AVL would like to receive comments from partners/experts from CARMEL project to improvise its results by considering the final review meeting as the priority. The result from CARMEL is being presented internally to other teams to find the potential projects to reuse or adapt the CARMEL work. Active discussions are happening with academic institutions to continue the further development of the existing intrusion detection system.

9. Measurement

For now, the measure of impact of planned actions can be done by evaluating as for how many potential projects the results of CARMEL was considered to be a part of the item for the project. As mentioned earlier there are active discussions happening around to extend the results by collaborating with the academic partners.

10. Positioning

CyberLens B.V. Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

CyberLens B.V., traded as Exalens™ since September '21, is an innovative cybersecurity SME pioneering in next generation threat detection, response, and recovery for IT, OT, IoT and IIoT systems. At Exalens, we protect digital manufacturing against downtime and safety events through early warning of both system malfunctions and cyber security incidents. With our ground-breaking "cyber-physical" security analyst AI, manufacturers enhance their operational resilience with automated incident detection and response (www.exalens.com).

2. Your motivation to participate in the project and commitment:

Exalens joined the CARMEL consortium aiming at extending its experience in the field of automotive cybersecurity. Based on its expertise Exalens contributes to the specification of the security and privacy requirements of the CARMEL platform, the identification of the CARMEL use cases and the definition of the overall CARMEL architecture. Exalens also contributes to the task of automotive threat modelling as well as to the development of machine-learning algorithms for the passive detection of attacks or intrusions on the vehicles' systems. Finally, Exalens contributes to the integration and pilot validation activities of the CARMEL project and provides support to the overall exploitation and business planning of the project in addition to contributing to the project's dissemination and communication activities.

3. Means to achieve your objectives:

Exalens originally established in London in May 2015. Since 2018, the company extended its presence in the Netherlands. This strategic decision facilitated the expansion of the company's team of experts and elevated the quality level of the business services offered. Currently, the Exalens team consists of 24 in-house experts with a combined over 50 years of experience in academic and industrial research and innovation, over 200 publications, and an insatiable desire for developing entirely new solutions for the most challenging technologies. The team is therefore in an excellent position to support a wide range of cybersecurity needs within research and innovation projects. Finally, a properly configured development environment of workstations allows for the efficient coordination of the company's R&D activities.

4. Opportunity which appeared/appears:

As part of the SWOT analysis the company has contacted, there are plenty of opportunities that

have arisen in the automotive cybersecurity market. These include, among others, the surging concerns of advanced threats targeting autonomous vehicles and EV charging infrastructures, the need for increased cyber hygiene in the automotive industry, etc. Accordingly, and given the fact that our participation in the CARMEL project is the result of the real need of our customers, exploiting these opportunities can make a huge difference to our company's ability to compete and take the lead in the market it serves.

WHAT & WHY

5. Exploitable assets and results:

In the context of CARMEL, Exalens brings NightWatch, a cyber-physical intrusion detection tool for advanced and novel threats to autonomous systems and vehicles. NightWatch (a by-product of Retina™) leverages Exalens' proprietary artificial intelligence technologies for accurately and rapidly determining the likelihood that an autonomous system has been compromised.

6. Rationale:

The primary benefit of a cyber-physical intrusion detection tool is to ensure IT and OT personnel is notified when an attack or network intrusion might be taking place in the monitored system and/or infrastructure. Exalens was fast to see that Retina™ (the company's exploitable asset / product) could deliver value to its customers and contractors. Hence, in November 2021, the company started to pursue the opportunities and took steps to exploit Retina™. Exalens's exploitation plan included the onboarding of an efficient exploitation team, the crafting of a thorough market analysis (aimed at defining the market potential, the target end-users, and all market competitors), the definition of the product's concept and value proposition, the efficient management of the company's IP, the derivation of a business model and a focused financial plan as well as the definition of targeted dissemination activities (through the onboarding of a marketing team).

7. Your Value Proposition towards Joint Exploitation of CARMEL:

A potential joint exploitation activity could result from the integration of our cyber-physical intrusion detection tool with GreenFlux's EV charging platform which would see the two companies launch into the market an enhanced cybersecurity-aware EV charging solution. By targeting the cybersecurity of EV charging infrastructures, this collaboration will provide a substantial contribution to the "EV charging networks of the future" paradigm. In addition, this collaboration has the potential to increase the offer proposed by Exalens and GreenFlux to their customers and improve the revenues for both companies.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

As part of the company's ongoing fundraising strategy, Exalens has created a tight roadmap to bring Retina™ to the market by June 2022, which includes, among others, the following: (i) introduction to customers, business partners, suppliers, and investors (VCs), (ii) establishment of sales and partnership opportunities with strategic service providers and vendors, and (iii) development of the company's market engagement strategy. Exalens expects to make this a reality by capitalizing on connections and intensive sessions on investment, branding, PR, diversity, pitching and other innovation streams that the Cyber Runway programme the company participates to offers to support the growth of innovative cyber start-ups across the UK (<https://www.plexal.com/cyber-runway/>).

9. Measurement

Our plan to measure the impact of the planned actions for M22-M30 of the CARMEL project relies on measuring KPIs relevant to our ongoing fundraising strategy. Accordingly, this plan will include KPIs related, for example, to the number of active users secured by Q2 2022, the number of paying customers or strategic service provider partnerships established by Q2 2022, resulting in at least X

MRR revenue by Q4 2022, etc.

10. Positioning

Without doubt, the last couple of years, cybersecurity has become a significant challenge for all critical sectors of our economy, including the automotive industry. Since then, the automotive cybersecurity market has gained a lot of traction. This is indicated by a recently published market research report by MarketsandMarkets™ entitled “Automotive Cybersecurity Market by Form, Offering, Security, Application Type, Vehicle Type, Propulsion, Vehicle Autonomy, Approach, EV Application, and Region - Global Forecast to 2026”, which presents the market competition landscape and provides a detailed analysis of the global players in the market.

University of Cyprus Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

The University of Cyprus (UCY) is a leading educational, research institution, and a center of excellence in the Mediterranean region. It is the leading university and the most active research institution in Cyprus. The KIOS Research and Innovation Center of Excellence for Intelligent Systems and Networks (KIOS CoE) is a large research center within the University of Cyprus which has been operating since 2008, with an ambitious goal to become a center of excellence in the field of Information Technology and Communication, with emphasis on the design of intelligent systems and networks. The KIOS CoE addresses some of the most important research and technological challenges of monitoring, control, management and security of Critical Infrastructure (CI) systems, by advancing ICT research towards intelligent systems and networks, able to produce smart decisions from large volumes of data.

2. Your motivation to participate in the project and commitment:

By participating in the CARMEL project KIOS will:

- Improve existing knowledge and in-house solutions on the detection, response, and mitigation of cyber-attacks against location services
- Extend existing techniques on data validation, fault diagnosis, and anomaly detection
- Develop new data-driven methods for enhancing threat intelligence, including advancing personnel skills on machine learning and state-of-the-art data analytics techniques
- Disseminate research results and produce high impact scientific publications leveraging on the project's outcomes
- Build a SW library of algorithms for autonomous vehicles that can be used to also study the effect of interconnected vehicles.

3. Means to achieve your objectives:

KIOS researchers have the expertise to work on the detection and cyber threat intelligence to counter cyber-attacks targeting network localization services that follow a Global Navigation Satellite System (GNSS)-based approach. Moreover, location spoofing attacks can be reproduced using existing Software Defined Radio (SDR) equipment, e.g., HackRF. Such attacks have been demonstrated against the GPS receivers of Unmanned Aerial Vehicles (UAV) that are part of KIOS' technical equipment.

In addition, KIOS researchers have the expertise to investigate the effect of attacks on the camera sensors for autonomous vehicles and work on the detection and mitigation using current deep learning techniques.

4. Opportunity which appeared/appears:

KIOS has identified and pursued opportunities to continue the project activities by participating in a number of research project proposals relevant to cybersecurity for connected and autonomous vehicles.

WHAT & WHY

5. Exploitable assets and results:

- DriveGuard deep-learning solution for detecting and mitigating attacks on camera image frames
- In-vehicle GPS location spoofing attack detection solution

6. Rationale:

The above assets will be mainly exploited academically by doing further R&D to increase their TRL
Potential commercialization of the assets will be explored

7. Your Value Proposition towards Joint Exploitation of CARMEL:

- Partners can provide realistic data and platforms to test and validate the developed approaches.
- The two exploitable assets and associated results will be delivered as part of the CARMEL holistic offering.
- There is common interest with other partners on cybersecurity solutions against camera attacks and GPS location spoofing attacks.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

- Include the IP of the two assets as part of the KIOS Innovation Hub IP list
- Leverage the assets in research project proposals

9. Measurement

- Number of new research project proposals that the IP has been included
- Number of research publications stemming from the IP and/or extensions
- Number of citations to the associated research publications
- Number of views of the videos created for the IP under the CARMEL YouTube channel

10. Positioning

University of Patras Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

UPAT, as an academic and research institution, has a strong interest in advancing its knowledge. The research group responsible for CARMEL is Visualization and Virtual Reality Group (VVR). The (VVR) was established in 2012 and is one of the eight separate research groups of the Wire Communications Laboratory (WCL), Department of Electrical & Computer Engineering, University of Patras. The activities of the Group include Teaching, Research, and Development in the areas of Computer Graphics, Virtual Reality, Visualization, Biomedical Engineering, Virtual Physiological Human, Computational Geometry, Human- Computer Interaction, and Computer Vision.

2. Your motivation to participate in the project and commitment:

The benefits expected through the participation in the CARMEL project include:

- (1) Improve existing knowledge and in-house solutions on the detection, response, and mitigation of cyber-attacks against computer vision systems;
- (2) Disseminate research results and produce high impact scientific publications leveraging on the project's outcomes;
- (3) Build an SW library of algorithms for detection of fault data injection using sparse and deep priors that can be used to also study the effect of cyberattacks in autonomous vehicles.

3. Means to achieve your objectives:

UPAT has done a lot of work toward the CAVs domain and indicative factors are the recent publications presented below:

- Kloukiniotis, A. Papandreou, A. Lalos, P. Kapsalas, D. . -V. Nguyen and
- K. Moustakas, "Countering Adversarial Attacks on Autonomous Vehicles Using Denoising Techniques: A Review," in IEEE Open Journal of Intelligent Transportation Systems, vol. 3, pp. 61-80, 2022, doi: 10.1109/OJITS.2022.3142612.
- N. Piperigkos, A. S. Lalos and K. Berberidis, "Enabling Online Cooperative Awareness in CAV via Graph Laplacian Processing," in IEEE Transactions on Vehicular Technology, 2021, submitted.
- Vitale, N. Piperigkos, C. Laoudias, G. Ellinas, J. Casademont, J. Escrig, A. Kloukiniotis, A.S.Lalos, K. Moustakas, R.D. Rodriguezm D. Banos, G.R. Crusats,
- P. Kapsalas, K.P. Hofmann, P.S. Khodashenas, "Caramel: Results on a Secure Architecture for Connected and Autonomous Vehicles Detecting GPS Spoofing Attacks", Eurasip Journal on Wireless Communications and Networking, vol. 115, May 2021.
- C. Kyrkou, A. Papachristodoulou, A. Kloukiniotis, A. Papandreou, A.S. Lalos, K. Moustakas and T. Theocharides, "Towards Artificial-Intelligence-Based Cybersecurity for Robustifying Automated Driving System Against Camera Sensor Attacks", IEEE ISVLSI 2020, Limassol, Cyprus, July 2020.
- N. Piperigkos, A. Papandreou, A. Kloukiniotis, J. Casademont, G. Arvanitis, A.S. Lalos, K. Moustakas, C. Vitale, C. Kyrkou, C. Laoudias, T. Theocharides, G. Ellinas and P.S. Khodashenas, "CARMEL: Artificial Intelligence based cybersecurity for connected and automated vehicles", ITS European Congress 2020, Lisbon, October 2020.

4. Opportunity which appeared/appears:

UPAT has participated in many other projects that are closely related to autonomous vehicles such as

- Trustonomy (The vision of Trustonomy is to maximize the safety, trust, and acceptance of automated vehicles by helping to address the aforementioned technical and non-technical challenges through a well-integrated and inter- disciplinary approach, bringing domain experts and ordinary citizens to work closely together.),
- CamECar (GameECAR aims to develop a highly innovative and interactive Serious Games platform that will empower and guide users to adopt an eco- friendly driving style.).
- Another ongoing project UPAT participates in is
- Cyber-physical Systems of Systems (CPSoS). (CPSoSaware project aims at developing the models and software tools to allocate computational power/resources to the CPS end devices of the system by determining and generating autonomously what cyber-physical processes will be handled by a device's heterogeneous component (processor cores, GPUs, FPGA fabric, software stacks).)

WHAT & WHY

5. Exploitable assets and results:

UPAT from CARMEL project outputs consist of separate components which could be used as standalone products, but all together form an integrated system that provides situational awareness and decision support to the driver. Codes repositories/ simulated datasets produced during

CARMEL for training and penetration testing of deep learning models used for perception can be used for further research and educational purposes.

6. Rationale:

The interest of UPAT in those assets is mainly for further Research and to be used in the training of postgraduate, graduate, and undergraduate students of computer engineering. Moreover, UPAT focuses on research and its dissemination by publishing results in well-known and widely read international scientific journals, as well as by presentations in international scientific conferences, workshops and exhibitions, web-based publishing, standards submissions, and small seminars and talks organized for specialized audiences. Furthermore, part of the UPAT business plan is to participate in a number of new spin-off commercial companies capable of exploiting its research when new market needs and solutions are identified. UPAT targets accomplishing Technology Transfer, encouragement of entrepreneurship and innovation. UPAT will set up discussions with the Corallia cluster (<http://www.corallia.org/>), initiated by the University of Patras could potentially lead to commercialization of the CARMEL outcomes.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

UPAT expects the partners to share results that will be used for validation and benchmarking of the proposed solutions. UPAT will provide integrated solutions that could be used for attack detection and mitigation on autonomous vehicles.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

Our future plan is to exploit the work done for Caramel to support scientific publications. More specifically we are planning to:

- Publish an adversarial Dataset to investigate the effect of adversarial noise on Deep Learning models in complex scenarios produced using the autonomous driving simulator Carla.
- Develop a distributed learning-based scheme for enhancing and robustifying cooperative awareness of each vehicle, against location spoofing attacks.

9. Measurement

As a research center one of the basic measures to assess the impact of the planned action is publishing results in well-known and widely read international scientific journals, as well as by presentations in international scientific conferences, workshops and exhibitions, web-based publishing, standards submissions and small seminars and talks organized for specialized audiences.

10. Positioning

Our basic competitors are:

- W. Wei, L. Liu, M. Loper, S. Truex, L. Yu, M.E. Gursay, Y. Wu, Adversarial Examples in Deep Learning: Characterization and Divergence, 2018.
- S. Chen, X. Huang, Z. He, C. Sun, DAmageNet: A Universal Adversarial Dataset, CoRR. abs/1912.07160 (2019).

In terms of cooperative localization, our goal is to achieve sub-meter positioning accuracy for the vehicles in a variety of traffic and weather conditions, as indicated by the relevant literature and standards about autonomous driving.

Deutsche Telekom Security GmbH (DT-Sec) Individual Exploitation Plan**PROFILE & MOTIVATION****1. Partner Profile**

Deutsche Telekom Security GmbH (DT-Sec) is an independent company of the Deutsche Telekom Group and offers highly qualified solutions from the security technology and services sector with 1,600 specialists and over 25 years of experience. With annual revenue of over of over EUR 250 million in cyber security, DT-Sec is the market leader in Germany and one of the industry leaders in Europe. DT-Sec builds the same protective wall for its customers that successfully secures Deutsche Telekom AG itself. DT-Sec provides security and data protection "Made in Europe". On a worldwide scale DT-Sec is active on two continents and 5 countries with more than 30 locations. DT-Sec cooperates with leading global companies to offer digital security from a single source.

2. Your motivation to participate in the project and commitment:

Almost all large European car manufacturers and suppliers are customers of DT-Sec or Deutsche Telekom. DT-Sec has identified automotive security as a growth area, given that more and more domains in the automotive sector are governed by IT

– may it be the connected car itself, the roadside infrastructure, or the backend systems. This increasing reliance on data communication and processing inside the car, the edge, and the cloud dramatically widens the attack surface and therefore the market for security solutions. Given this background, DT-Sec focuses on delivering tailor-made secure IT solutions to the connected vehicle such as the anti-hacking device or the embedded secure element (or HSM, hardware security module).

3. Means to achieve your objectives:

DT-Sec runs the Deutsche Telekom trust center for the whole Deutsche Telekom group and many external customers. Additionally, DT-Sec has its own product line of smart card and secure module products based on the Telekom Card Operating System (TCOS) that is used for the German identity and healthcare cards, for example. DT-Sec has the engineering and software development ability to integrate this HSM solution into a range of embedded devices – the anti-hacking devices of the CARMEL project – and to help partners deploy this technology into their respective security scenarios and showcases developed for the project. DT-Sec is also running the Deutsche Telekom CERT (Computer Emergency Response Team) for the whole Telekom group which is also networked to the ENISA CSIRT network.

4. Opportunity which appeared/appears:

As outlined before the propagation of information technology in the automotive sector widens the attack surface.

Therefore, there is an urgent need for all stakeholders and specifically our customers in the automotive domain to increase the security level of their products. Results and experiences of the CARMEL project will influence the roadmap of the DT-Sec product portfolio development for years on end and will drive the development of innovative product offerings for the automotive security market.

WHAT & WHY**5. Exploitable assets and results:**

Specifically DT-Sec will re-use the methodology of integration of hardware security elements into in-car control units as showcased in the anti-hacking device. Leveraging its membership in the 5GAA (5G Automotive Association), specifically the working group 7 on security and the work in the misbehavior detection work item to integration results from CARMEL into forthcoming 5GAA documents. Additionally, DT-Sec will steer the direction of development of the TCOS platforms such to enable more compatibility with automotive standards, eg. by supporting elliptic curve

cryptography to enable secure handshakes with automotive control units and on-board units such as showcased in the project. The multi-layered approach to security taken in the anti-hacking device will be adapted as a blueprint for the development of future hardware solutions for the automotive product portfolio and forthcoming customer projects.

6. Rationale:

As a subsidiary of a Telecom operator, DT-Sec has a vested interest in strengthening the connected car ecosystem and therefore supports the 5GAA standardization work. DT-Sec is also a large player in security market in Europe and is committed to expand its existing business in the automotive security sector. In order to succeed, innovative approaches are necessary for the development of the product portfolio as well as references for successful activities in the automotive security sector. DT-Sec also has a security consulting department that benefits from the experiences gained in the CARMEL project.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

A unique aspect of the CARMEL project is the collaboration of partners well versed in artificial intelligence and machine learning with partners coming from a security background. This special work relationship in the project will be able to provide partners with new and innovative approaches beyond their normal line of work, therefore enhancing their ability to innovate into new and future-proof product development directions.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

The Architecture & Innovation department inside DT-Sec carrying out the work is committed to constant dissemination of work results to the whole of Deutsche Telekom Group in Germany and internationally. Members of the CARMEL project team take also part in the internal product portfolio process and meet with members of the board on a weekly basis. Therefore, transmission of project results into the portfolio and the product roadmap is guaranteed. Project results will be preserved and made available to all of Deutsche Telekom groups employees by using the widely accepted internal knowledge management platform "YAM United" where they are prominently displayed and easily be found by the advanced search functions of this platform.

9. Measurement

On the one hand a simple measure of success will be the increased turnover in the automotive security segment. In addition to that, and more specifically related to the project team in the Architecture & Innovation department, will be the success of the internal dissemination activities (YAM United page views, CARMEL presentations and demos to internal stakeholders and our customers).

10. Positioning

As pointed out in the company introduction, DT-Sec is the security market leader in Germany and also a strong force in Europe. We strive to extend that position by continuously extending our product portfolio, one of these activities being the expansion of our automotive security market presence.

ATOS Individual Exploitation Plan**PROFILE & MOTIVATION****1. Partner Profile**

Atos is a global leader in digital transformation with 120,000 employees in 73 countries. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions through its Digital Transformation Factory, as well as transactional services through Worldline, the European leader in the payment industry.

Within Atos Research & Innovation (ARI), node of R&D at Atos in Spain, there is technology transfer and business development team that works on transition from research results to Atos global portfolio and service lines.

2. Your motivation to participate in the project and commitment:**3. Means to achieve your objectives:****4. Opportunity which appeared/appears:****WHAT & WHY****5. Exploitable assets and results:**

PKI infrastructure: The PKI infrastructure, composed of the PKI servers and the PKI client, seeks to facilitate the secure electronic transfer of information and aims to solve the security requirements of the VANETs. The PKI infrastructure fulfills the general security requirements for PKI are authentication, confidentiality, integrity, availability and non-repudiation. It additionally handles VANET specific requirements: anonymity and scalability.

6. Rationale:

Atos is particularly interested in the outcomes of the CARMEL project as it will bring anonymity and scalability improvements to the standard PKI infrastructure. These additional features could be implemented in environments different from the VANET scenario used in CARMEL, such as smart grids.

(Atos acquired a company which develops PKI services for vehicles and perhaps these findings could be integrated. It is called IDnomic)

7. Your Value Proposition towards Joint Exploitation of CARMEL:

The project partners (I2CAT and UBIWHERE) provide the connectivity between the PKI servers and the PKI client installed on the vehicle. Additionally, I2CAT provides the communication module which allows the PKI client to access secure functions of the HSM of the vehicle.

ROADMAP WITH TIMELINE**8. Roadmap: the timeline plan you have for using those assets:****9. Measurement**

Eight Bells Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

Eight Bells LTD is an independent Research and Consulting company specializing in selected parts of Information and Communication Technologies (ICT) as well as in modelling and analysis for businesses, based in Nicosia, Cyprus and Athens, Greece. Areas of expertise include 5G, AI, Cybersecurity, IoT and Sensors.

2. Your motivation to participate in the project and commitment:

Interest in the area of automotive cybersecurity. The role is mainly on business analysis and automotive threat modelling.

3. Means to achieve your objectives:

Expertise on business analysis as part of the key areas of interest in 8Bells.

4. Opportunity which appeared/appears:

Further and deeper involvement in similar activities.

WHAT & WHY

5. Exploitable assets and results:

Cybersecurity is one of the key areas of 8Bells Ltd. Through CARMEL we would like to enhance our experience and expertise on automotive cybersecurity and get familiar with new methodologies.

6. Rationale:

They are in-line with the areas of interest of 8Bells. We would like to provide consulting services in cybersecurity and this way we will enrich our knowledge on the specific area. Furthermore, R&D activities may be initiated as in-house projects so as to investigate potential solution for future projects/products etc.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

An automotive threat modelling tutorial has been created and is available for everyone. Moreover, a detailed business model and market analysis plan will be offered in collaboration with other partners involved in the task.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

- Automotive Threat Modelling tutorial
- Market/Business Analysis

9. Measurement

10. Positioning

GreenFlux Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

GreenFlux has been the market leader in the international EV charging market since 2011, providing an advanced cloud-based platform for managing charging infrastructure for electric vehicles. GreenFlux offers this solution to energy companies, network operators, parties in the automotive industry and fleet managers. With the platform, our customers are able to manage charging stations remotely, give EV drivers access to a large network of charging stations (through roaming), process charging transactions and use our smart charging technology. Internationally, GreenFlux is active in 21 countries, and we have an ecosystem of more than 185,000 charging stations (including roaming) and we support more than 1.8 million EV drivers.

2. Your motivation to participate in the project and commitment:

By participating in CARMEL we hope to take our services to the next level. The AI & ML nature of this project ties in well with the hardware agnostic and cloud functionalities of our platform. With the developed ML components, GFX can centrally detect whether an attack is being carried out on one of the connected charge stations. For us, CARMEL is a springboard to the next level charge station security.

3. Means to achieve your objectives:

The GreenFlux team largely consists of the Development department (30 FTE). Security is an item that affects all domains within our platform, which means that it is relevant for the entire development team.

4. Opportunity which appeared/appears:

Several tens of thousands of charge stations are currently connected to our platform via our customers. Part of this consists of so-called legacy charge stations from the first generations in which few or no security measures have been taken. By applying the detection from the cloud, cyber attacks on these legacy charge stations can still be detected.

WHAT & WHY

5. Exploitable assets and results:

The main result is the anomaly detection tool that makes it possible to detect compromised charge stations from the cloud.

6. Rationale:

Applying the anomaly detection tool is a piece of security that we can add to our platform. This is mainly so that we can prevent further damage to our infrastructure in case of an attack. We see this as a core functionality of our platform and will not charge our customers an additional fee for this.

7. Your Value Proposition towards Joint Exploitation of CARMEL:

Unlike the other CARMEL use cases, the focus of our use case is on the EV Charging Station and less on the car. This may make the outcomes less relevant for other partners. The partners who have co-developed this tool are free to further develop and commercially exploit this tool.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

The functioning of the tool is demonstrated within this project. In its current form, the tool will be rolled out to a select number of charge stations, starting with charge stations next to or close to the GFX head office. The next step is to apply the tool on a larger scale. This requires further development of our platform. This will be continued from 2022.

9. Measurement

The GFX platform consists of several separate environments. The tool developed within CARMEL will be deployed on one of these environments, parallel to the standard Azure security package that claims to detect anomalies in communication as well. In addition, the operations department keeps a log of all charge stations that required a site visit and whether there was a cyber attack/vandalism/other issue. As soon as sufficient data has been collected, both methods are compared with each other so that the impact of these tools.

10. Positioning

there is no competitor or market alternative for the remote detection of cyberattacks on charge stations through OCPP communication monitoring.

SIDROCO Individual Exploitation Plan

PROFILE & MOTIVATION

1. Partner Profile

SIDROCO Holdings Ltd (SID) is a creative SME focusing on Research, Development and Inspiration. SIDROCO brings a whole range of New Generation Internet of Things (NG-IoT) features and capabilities for creating, supporting, and managing ultra innovative solutions, products, and services, by providing efficient, effective, and secure NG-IoT solutions for various heterogeneous environments, including Critical Infrastructures like Energy and Healthcare. SID designs, develops and implements novel and innovative products, frameworks and tools. SID can support a variety of research solutions and integrated products in multiple domains such as network and system security, modelling and simulation, optimization, visualization, machine learning solutions, risk analysis and assessment, market analysis and business modeling.

2. Your motivation to participate in the project and commitment:

SID was interested to Electric Vehicles domain in order to improve its know-how. SID participates in several tasks of CAMEL. Apart from its participation in WP1 (Project Management) and WP7 (Dissemination, Communication, and Exploitation of Results), where SID will actively participate in the scientific and technical coordination of the project by contributing to the technical and financial reports, and promoting CAMEL's achievements through publications at high quality ranked international conferences and journals in the fields of Security, Privacy, and Software Engineering, SID will also participate in WP1 (Project Management) and WP7 (Dissemination, Communication, and (T2.4). In WP3 (Countermeasures and Mitigation Techniques for Advanced Cybersecurity), SID will participate in the definition of practical and efficient approaches for modeling automotive domain threats (T3.1), investigate and define in the foreseen cyberthreats aligned with the autonomous use case (T3.2), facilitate the IDPS definition that will be included over a secure HW ECU with Hardware Security Module (HSM), and how charging stations can be made tamper-proof and secure (T3.3). SID plays a minor part in establishing the immutable two-way information exchange protocol between vehicle and infrastructure in WP4 (Cross-cutting Intrusion Detection and Cyberattack Prevention) (T4.4). SID's contribution to WP5 (Development of Antihacking Device and In-depth Defense) is in addressing the hardware specification of the HSM as well as strategies for provisioning cryptographic keys into the HSM at manufacturing and later a deployment time (5.3), as well as increasing the resilience against software modification. WP6 (System Integration, Validation, and Demonstration) will conduct a comprehensive set of penetration tests (T6.2), while also contributing to the integration of the outputs from the preceding technical WPs (T6.1). SID will also be involved in verifying the novel project developments, examining their functional features, and evaluating their performance (T6.3), in addition to contributing to the overall CAMEL demonstration applications.

3. Means to achieve your objectives:

SID has the necessary human resources to achieve the objectives, since a Software Engineer and Cybersecurity analysts are supporting the corresponding tasks of SIDROCO in CAMEL.

4. Opportunity which appeared/appears:

Our participation in CAMEL was led by market needs. A market analysis conducted in the past was mentioning that the global electric vehicle market was valued at \$162.34 billion in 2019, and was projected to reach \$802.81 billion by 2027, registering a CAGR of 22.6%.

WHAT & WHY

5. Exploitable assets and results:

SID participated in the Machine-learning anomaly detection component in WP6. Specifically, the software component that was developed named "Anomaly detection mechanism for EV smart

charging stations” in collaboration with GFX and 8bells.

6. Rationale:

This asset is an innovation that deals with the issue of the unlabelled datasets that contain normal and abnormal data. It can detect data in order to build a model for the classification of any new incoming data without class bias. This asset intends to extend the capabilities of SID's AI4CI tool which is a powerful AI suite of customisable frameworks, tools and processes designed to help customers/organizations effectively utilize AI's potential.

7. Your Value Proposition towards Joint Exploitation of CAMEL:

As mentioned, SIDROCO expects to keep the successful collaboration with CAMEL partners in order to disseminate CAMEL results and exploit the assets developed during CAMEL.

ROADMAP WITH TIMELINE

8. Roadmap: the timeline plan you have for using those assets:

The plan is to re-factor the code of the component mentioned earlier and dockerize it as a service to increase its re-usability.

9. Measurement

This has not yet been included into SIDROCO's internal processes.

10. Positioning

PANASONIC Individual Exploitation Plan**PROFILE & MOTIVATION****1. Partner Profile**

Panasonic Automotive (PASEU) as one of the leading companies on AI, Sensing, embedded optimization and trajectory planning technologies. PASEU In Europe sees a business case in CARMEL by deepening the expertise in those areas in order the provided solutions to be robust across a wide range of attacks ranging from attacks to each individual sensing modality to the system of sensors. For PASEU, the co-conception with the consortium partners and development of the CARMEL cyberattack mitigation engine is completely aligned with PASEU's Research-strategy design. The commercial opportunities, as well as the manufacturing and automotive market, are investigated as to whether it is feasible and financially sustainable to turn ideas and the CARMEL concept of solution into a marketable product that abides by the standards.

2. Your motivation to participate in the project and commitment:**3. Means to achieve your objectives:****4. Opportunity which appeared/appears:****WHAT & WHY****5. Exploitable assets and results:****6. Rationale:****7. Your Value Proposition towards Joint Exploitation of CARMEL:****ROADMAP WITH TIMELINE****8. Roadmap: the timeline plan you have for using those assets:****9. Measurement****10. Positioning**

References

- Accenture. *Automotive Cybersecurity: Shifting into Overdrive*. Accenture, 2020.
- Alonso Raposo, M., Grosso, M., Després, J., Fernandez Macias, E., Galassi, M., Krasenbrink, A., Krause, J., Levati, L., Mourtzouchou, A., Saveyn, B., Thiel, C. and Ciuffo, B. *An analysis of possible socio-economic effects of a Cooperative, Connected and Automated Mobility (CCAM) in Europe*. Luxembourg: Publications Office of the European Union, 2018.
- ALTRAN. *CYBERSECURITY IN AUTOMOTIVE: HOW TO STAY AHEAD OF CYBER THREATS?* ALTRAN, part of CAPGEMINI, 2020.
- Anderson, R., Leverett, E. and Clayton, R. *Standardisation and Certification of Safety, Security and Privacy in the 'Internet of Things'*. Luxembourg: Publications Office of the European Union, 2022.
- Baldini, G. *Testing and certification of automated vehicles including cybersecurity and artificial intelligence aspects*. Luxembourg: Publications Office of the European Union, 2020.
- Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiataakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, G. *Cybersecurity, our digital anchor*. Luxembourg: Publications Office of the European Union, 2020.
- Baldini, G., Giuliani, R., Gemo, M. and Dimc, F. "On the application of sensor authentication with intrinsic physical features to vehicle security." *COMPUTERS and ELECTRICAL ENGINEERING, PERGAMON-ELSEVIER SCIENCE LTD*, 2021: 107053.
- Borio, D. "An Experimental Evaluation of Global Navigation Satellite System/Inertial Navigation System Verification Strategies for Vehicular Applications." *IEEE INTELLIGENT TRANSPORTATION SYSTEMS MAGAZINE, IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC*, 2020: 25-35.
- Chatzoglou, E., Kampourakis, G. and Kouliaridis, V. "A multi-tier security analysis of official car management apps for Android." *FUTURE INTERNET, Multidisciplinary Digital Publishing Institute (MDPI)*, 2021: 58.
- Corporate Finance Institute. *Business Life Cycle: The five stages of a business' life*. Januray 24, 2022. <https://corporatefinanceinstitute.com/>.
- Craglia, M., Scholten, H.J., Micheli, M., Hradec, J., Calzada, I., Luitjens, S., Ponti, M. and Boter, J. *Digitranscope: The governance of digitally-transformed society*. Luxembourg: Publications Office of the European Union, 2021.
- DATA, NTT. *Automotive Cybersecurity: An End-to-End Automotive Cybersecurity Solution Combining NTT DATA's Intrusion Detection System for CAN Bus with its State-of-the-Art Vehicle-Security Operation Center*. NTT DATA Deutschland GmbH, 2021.
- De Urquía, M.Á., Compano, R. and Díez, S. *Place-based Innovation Ecosystems for emerging mobility-based business models*. Luxembourg: Publications Office of the European Union, 2021.
- Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A. and Sanchez Martin, J.I. *Cybersecurity challenges in the uptake of Artificial Intelligence in Autonomous Driving*. Luxembourg: Publications Office of the European Union, 2021.
- Deloitte. *5 insights on cyberattacks*. Deloitte Development LLC, 2016.
- Edward White, Eleanor Olcott. *Elon Musk's Starlink aid to Ukraine triggers scrutiny in China over US military links: 'Silicon Valley Iron Man' is under pressure over satellites as Chinese rivals close in on Tesla*. June 21, 2022. <https://www.ft.com/content/df032357-51e7-4635-baaa-f053dcc0c4c1?>

- European Commission. *Cybersecurity Policies*. May 28, 2022. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies>.
- . *The Cybersecurity Strategy*. May 28, 2022. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>.
- . *The EU Cybersecurity Act*. May 28, 2022. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>.
- European Commission, Joint Research Centre. *Joint Research Centre*. May 28, 2022. <https://publications.jrc.ec.europa.eu/repository/>.
- Fernandez Llorca, D. and Gomez Gutierrez, E. *Trustworthy Autonomous Vehicles*. Luxembourg: Publications Office of the European Union, 2021.
- Galassi, M.C., Lagrange, A., Guido, P., Mele, R., Ciuffo, B., Piron, O. and Malfait, W. *ERA – JRC Workshop on Safety certification and approval of automated driving functions*. Luxembourg: Publications Office of the European Union, 2021.
- Grosso, M., Ortega Hortelano, A., Marques Dos Santos, F., Tsakalidis, A., Gkoumas, K. and Pekar, F. *Innovation capacity in the transport sector: a European outlook*. Luxembourg: Publications Office of the European Union, 2020.
- Grosso, M., Raileanu, I.C., Krause, J., Alonso Raposo, M., Duboz, A., Garus, A., Mourtzouchou, A. and Ciuffo, B. "How will vehicle automation and electrification affect the automotive maintenance and repair sector." *TRANSPORTATION RESEARCH INTERDISCIPLINARY PERSPECTIVES* (ELSEVIER, TRANSPORTATION RESEARCH INTERDISCIPLINARY PERSPECTIVES), 2021.
- Julian Conzade, Russell Hensley, Patrick Schaufuss. "The irresistible momentum behind clean, electric, connected mobility: Four key trends - Part 3: Can electric vehicles put the brakes on climate change?" *McKinsey Quarterly*, April 2021: 6-7.
- Kersten Heineke, Timo Möller, Asutosh Padhi, Dennis Schwedhelm, and Andreas Tschiesner. "The irresistible momentum behind clean, electric, connected mobility: Four key trends -Part 1:Why capital markets love mobility." *McKinsey Quarterly*, April 2021: 2-3.
- Martinez Plumed, F., Caballero Benítez, F., Castellano Falcón, D., Fernandez Llorca, D., Gomez Gutierrez, E., Hupont Torres, I., Merino, L., Monserrat, C. and Hernández Orallo, J. *AI Watch: Revisiting Technology Readiness Levels for relevant Artificial Intelligence technologies*. Luxembourg: Publications Office of the European Union, 2022.
- Olivia White, Kevin Buehler, Sven Smit, Ezra Greenberg, Mihir Mysore, Ritesh Jain, Martin Hirt, Arvind Govindarajan, and Eric Chewing. "War in Ukraine: Twelve disruptions changing the world." *McKinsey & Company, strategy & Corporate Finance Practice*. May 09, 2022. <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/war-in-ukraine-twelve-disruptions-changing-the-world>.
- Ponemon Institute. *Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices*. Synopsys, Inc. and SAE International, 2018.
- the Working Party on Automated/autonomous and Connected Vehicles, UN Economic Commission for Europe. "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system." *United nations, Economic and Social Council, Economic Commission for Europe, Inland Transport Committee*. June 23, 2020. <https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>.
- Tom Hellstern, Kimberly Henderson, Sean Kane, Matt Rogers. "Innovating to net zero: An executive's guide to climate technology." *McKinsey Sustainability*, October 2021: 1-11.
- Tsakalidis, A., Van Balen, M., Gkoumas, K., Haq, A., Ortega Hortelano, A., Grosso, M. and

Pekar, F. *Research and innovation in smart mobility and services in Europe*. Luxembourg: Publications Office of the European Union, 2020.

Tsakalidis, A., Van Balen, M., Gkoumas, K., Marques Dos Santos, F., Grosso, M., Ortega Hortelano, A. and Pekar, F. *Research and innovation in transport electrification in Europe*. Luxembourg: Publications Office of the European Union, 2020.

United Nations Economic Commission for Europe (UNECE). "UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system." *United Nations Economic Commission for Europe (UNECE)*. 2021.
<https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>.

—. "UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system." *United Nations Economic Commission for Europe (UNECE)*. 2021.
<https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update>.

Van Wynsberghe, A. and Martinho Guimaraes Pires Pereira, A. *Mobility Imaginaries: Social and Ethical Issues of Connected and Automated Vehicles*. Luxembourg: Publications Office of the European Union, 2021.