D7.2
Market Analysis and Exploitation Potentials

Topic	H2020-SU-ICT-2018-2020
Project Title	Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles
Project Number	833611
Project Acronym	CARAMEL
Contractual Delivery Date	M11
Actual Delivery Date	31/08/2020
Contributing WP	WP7
Project Start Date	October 2019
Project Duration	30 months
Dissemination Level	Public
Editor	Dr. Nicolas Kylilis
Contributors	8Bells, ATOS, ALTRAN, FICOSA, GFX, AVL, PANA

Document History		
Version	Date	Remarks
0.1	1/10/2019	Initial ToC
0.2	1/11/2019	Initial Stakeholder Analysis, Exploitable Assets
0.3	1/11/2019	Stakeholder Analysis
0.4	1/1/2020	Market Entrance Barriers
0.5	1/6/2020	Exploitable Assets Update
0.6	1/6/2020	Exploitation Strategy and Risk Analysis
0.7	1/7/2020	Business Plan update
0.8	1/7/2020	Exploitable Assets Update
0.9	1/8/2020	Exploitation Strategy Update
1.0	1/8/2020	Format Revision
1.1	25/8/2020	Peer Review - Addressing comments and changes
1.2	26//8/2020	Peer Review - Addressing comments and changes

Table of Contents

List of Figures

List of Tables

List of Acronyms

ADAS	Advanced Driver Assistance Systems
AI	Artificial Intelligence
CA	Consortium Agreement
ECU	Engine Control Unit
EIB	Exploitation & Innovation Board
EVSE	Electric Vehicle Supply Equipment
GA	Grant Agreement
HSM	Hardware security module
IM	Innovation Manager
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights
ISP	Internet Service Provider
KER	Key Exploitable Result
ML	Machine Learning
MRL	Market Readiness Level
MT	Management Team
MTRL	Market and Technology Readiness Level
OEM	Original Equipment Manufacturer
OTA	Over the Air
PC	Project Coordinator
PMI	Project Management Institute
SIEM	Security Incident and Event Management
SLA	Service Level Agreement
SME	Small-Medium Enterprise
TB	Technical Board
TM	Technical Manager
TRL	Technology Readiness Level
V2I	Vehicle-to-infrastructure
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything

Executive Summary

The overall goal of this deliverable is to provide a Stakeholder Analysis, Market Analysis and the Exploitation Strategy. The aim is to enhance the understanding of the complex, end-to-end technology and value chain(s) as well as stakeholders/users.

This deliverable consists of 5 sections which are also related to the objective of this work. Section 1 introduces the scope and objectives of the deliverable. Section 2 presents the Stakeholder Analysis and the Barriers. Section 3 describes CARAMEL's Exploitable Assets. Section 4 provides a Market Analysis, Risk Analysis and an in-depth description of the Exploitation Strategy. Section 5 concludes the document by summarizing the scope of this deliverable.

1 Introduction

This deliverable provides a stakeholder analysis, a list of exploitable assets, technology transfer and market analysis in specified sectors. The goal is to create a full understanding of the complex, end-to-end technology and value chain(s) as well as stakeholders/users. This target goes beyond a passive market analysis but involves potential OEMs or other industrial end-users. This entails identification of all the relevant business stakeholders coming from the various industrial sectors likely to benefit from the CARAMEL innovations, either directed at current security needs or anticipative. The CARAMEL Innovations are treated with a SWOT analysis including estimates of potential market share as well as new markets/use-cases potentially unleashed with the introduction of new technologies. Market analysis, business models and exploitation strategy will be updated and further expanded on deliverable "D7.5 Road mapping and Business Modelling Report" on month 30 (M30).

Due to the short innovation cycle in the security sensitive industry as compared to the project duration, the market analysis will be continuously updated by monitoring the activities of the major mobile communications market stakeholders and will ultimately lead to identify market entrance barriers. Building on the market analysis, new business models leveraging on traditional and emerging business roles are developed and road-mapped for the future. This takes into account the features and capabilities of the CARAMEL infrastructure at large. Finally, an accurate model is developed to position CARAMEL technology and use cases in the broader cybersecurity market evolution. In this regard a risk analysis is carried out followed by a technology exploitation roadmap. The existence of suitable business models for key parts of the wider 5G/IoT/Automotive/Embedded System value chain is imperative for the adoption of any solution beyond a single deployment.

2 Stakeholder Analysis and Barriers

CARAMEL considers the needs of the entire cyber-security and automotive value chains, ranging from: (a) the general public that uses digital communications and future automotive products, (b) the cyber-security solution providers, AI and ML methods developers, etc., (c) the infrastructure providers, represented by telecommunication infrastructure providers (telecom operators, ISPs), cloud service providers, and organisations with small, medium and large scale infrastructures that require a low-cost cyber-security investment, (d) vehicle manufacturing industry, i.e. automotive companies, equipment, system and solution providers for automotive industry, etc. CARAMEL further considers the needs of policy makers in EU & Member States for informed decisions regarding the security of modern infrastructures for the future vehicle industry. Additional benefits are considered in the case for standardisation, other special interest groups, open source communities and researchers/academics. Table 1 identifies a stakeholder analysis for CARAMEL's proposed approach.

2.1 Stakeholder Analysis

The innovation capacity provided by the CARAMEL project will strengthen the competitiveness and growth of the consortium partners. As shown in D.7.1 "Dissemination, Communication and Exploitation Plan", CARAMEL outcomes will provide the means for partners to improve not only products and services applied to the project, but also existing products which are part of their portfolio and not used in the project. Therefore, the innovation capacity of partners will be beyond CARAMEL's objectives, as expected from such an interdisciplinary and full value chain targeting project.

Improved situational awareness and decision support for dynamic countering of cyber-attacks on the automotive domain is the major impact expected from CARAMEL. The project does not only leverage on the novel solutions inside the car for advanced response and recovery against cyberattacks, but it also dedicates effort into understanding the threats against modern infrastructure outside the vehicle to support future automotive industry. CARAMEL improves technical capabilities in terms of cyber-attack detection, situation recognition, comprehension, projection and thus decision support. It brings together Intrusion Detection, Security Awareness, Machine Learning and Artificial Intelligence technologies to achieve its aims, and it also considers the needs arising throughout the entire cyber-security value chain. Hence, it provides better situational awareness against multisector, multidisciplinary attacks and it focuses on fortifying against automotive-specific threats, preparing and fortifying next-generation infrastructures (5G/Future Internet).

Target Group	Main Players	Impact/Market Opportunities
Technology Suppliers	Automotive suppliers and partners, automotive integrators, vehicle engineering companies, vehicle manufacturers, charging station component suppliers, manufacturers and integrators, in-vehicle charging infrastructure component suppliers, manufacturers and integrators, payment systems providers, ICT providers, Telematics/data management companies, cybersecurity companies.	Significant cost reduction due to enhanced security features Improved situational awareness, decision support and remediation. Penetration testing methods developed / tested over intelligent and modern testbeds. New cyber security services / products. Simplification of their entry to new markets.
Service providers	EV charge sellers, local EV charge service companies, charging stations owners, specialised consulting companies, mobility service providers, automotive dealers and the aftermarket sector, insurance companies.	

Operations	Telecom operators, road operators, charging station network operators, logistics operators.		Development of business models for cyber-security services / products in future networks, especially for the automotive vertical market.
Research, Academia & Open Source Communities	Researchers and academics from universities, research centres and R&D industry departments, open source communities.		Novel detection methodologies. Open access to an operational environment that allows validation of situational awareness & cyber-security advances in an environment closely resembling actual operations. Ensuring research integrity & credibility by providing medium scale testing. Extension to available open source solutions, maturing them in terms of security. Contributions to Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing (MISP).
Authorities	Public authorities on mobility and cybersecurity, policy makers, regulators, national, local and international governmental agencies (ENISA), cities, GEAR2030, ministries, judiciary systems, national security agencies, national data protection authorities.		Novel improvements and recommendations. Service and data protection methods. Specifications for cyber-security aware services.
Standards organisation bodies	Institute of Electrical and Electronics Engineers (IEEE), National Institute of Standards and Technology (NIST), Society of Automotive Engineers (SAE), International Organisation of Standardisation (ISO), AUTOSAR, ETSI (TC Cybersecurity Group, ITS, MEC), 3GPP, CEN/CENELEC.		
Networks & Platforms	Automotive	5GAA, Car to Car – Communication Consortium (C2C-CC), Connected Motorcycle Consortia (CMC), Auto-	Novel improvements and recommendations. Service and data protection methods.

		ISAC, Auto Alliance, Global Automakers.	Specifications for cyber-security aware services.
	Mobility	ERTICO, ALICE.	Improved synergies among cyber-security and 5G / Future Internet projects Using the CARAMEL testbeds as a solid foundation for the creation of potential interoperable testing facilities across Europe.
	Cybersecurity	ECSO, CSIRTs Network.	
	Telecommunications	5GPPP, 5G Infrastructure Association (5GIA).	
	ICT	BDVA	
End-users	General public, commercial fleets, public fleets, drivers, passengers, society, related associations, fleet customers, vehicle customer.		Better overall situational awareness and cybersecurity protection in future vehicles. Improved protection of systems and data even in cases where endpoints are not sufficiently fortified.

Table 1: CARAMEL Stakeholder Analysis

2.2 Market Entrance Barriers

The barriers to CARAMEL's innovation include many themes which apply across the different work packages; the barriers may be [P]olitical, [Ec]onomic, [S]ocietal, [T]echnological, [L]egislative, [En]vironmental (PESTLE) in their nature. Table 2 identifies such barriers and obstacles which may limit the impact of the project and hinder market uptake, and lists some measures taken to alleviate the possible negative impacts.

Barriers / Obstacles	How it relates with CARAMEL's impact	Mitigation plan
[S, Ec] Lack of investment in continuous human resource training reduces uptake of innovative solutions.	Although there is a large number of professionals active in the cyber- security, Machine Learning, AI and inside car network security market and EU academic and research institutes heavily invest in their education, the realisation of the CARAMEL vision requires continuous education of young professionals with additional focus on future vehicle security specificities.	In order to alleviate the impact of this barrier, CARAMEL partners will invest effort to continuous education. The inclusion of academic and research (I2CAT, UPAT, UCY) partners ensures that these activities will reach a large audience, with additional focus on students and young professionals in the beginning of their careers. Commercial partners will also ensure that CARAMEL knowledge reaches their employees. The road mapping activities, research papers, evidence-based best practices and recommendations to be published by the project are also considered a further step towards the effective dissemination of specialised knowledge.
[T, S, Ec] Lack of trust in research results.	The misalignment of CARAMEL with EU strategies, policies, research activities and well-known standards, would negatively impact the trust in the final project results.	All tasks will take into account the EU regulatory ecosystem, standardisation, research activities, etc. with a view to maximise the innovation potential of the project, while building a proper trust around the obtained results. The extensive validation performed within CARAMEL will enable decision makers and future clients to base their decisions on data, fact and evidence, thus strengthening the project's positioning with respect to large vendors dominating the market. The testbeds will be a major asset that allows CARAMEL to validate all new developments.
[T] Gaps between end user needs and available solutions; [T] Relatively new adoption of cyber-security services in the market; [T] Lack of	The mentioned features would directly impact the adoption of CARAMEL solution by the market.	The cyber-security service market & service chaining proof-of-concepts will enable end users that have identified their needs to reach out to intermediate users in cyber-security, inside/outside the car anti-hacking solutions, and ML/AI solution providers. The decision support tools that will be developed to properly analyse and project the state of the

appropriate decision support for cyber-security incidents; [Ec] Existing long-term service contracts and framework agreements may restrict rapid uptake of new technologies.		internal and external car network under attack will enable end users to properly identify their current and future needs in terms of cyber-security. The creation of the cyber-security services will create a competitive advantage for service providers to negotiate their SLAs and simplify their entry into the 5G/V2X/Future Internet market with tailor made products, thus strengthening their position against large vendors.
[T] Lower-than expected adoption of future connected vehicle technology.	Although the future connected vehicle market perspective is very promising, and it seems like the ones that adopted early use cases of future networks and 5G, CARAMEL solutions' full adoption might take longer than initially anticipated. This may, in some cases, hinder the uptake of some of the CARAMEL innovations, such as in car anti-hacking device.	Other aspects of CARAMEL, such as the situational awareness framework, as well as the enablers for open awareness (ML and AI methods) are still applicable to alternative markets, such as, e.g., IoT, e-health, aviation, and can bring significant value.

Table 2: List of barriers and obstacles

3 Exploitable Assets

Within CARAMEL, the project partners work together to come up with an extensible, scalable and market-oriented cybersecurity architecture for the provisioning of situational awareness in CCAM vehicles. To prepare a wide market adoption of CARAMEL outcomes, during the project development phase, the consortium:

- **Will validate three (3) pilots and their benefits**: three case studies will be carried out by the CARAMEL partners to validate and demonstrate the CARAMEL outcomes and provide documentary evidence of their benefits.
- **Formalised a Dissemination and Communication Plan (D7.1)**: The Dissemination and Communication Plan is key to activate communication channels and to increase awareness and interest around the exploitation of the project (e.g. attracting investors).
- **Agreed and adopted an Exploitation Plan and Strategy (D7.2)**: The Innovation Manager and the Exploitation & Innovation Board (EIB) collaborates with partners and advises them, in terms of developing the exploitation strategy, and will liaise with possible partners and stakeholders outside the consortium.

The table below presents a list of the major expected exploitable results from the CARAMEL activities with the highest value for exploitation. This list is and will be continuously updated from the beginning and throughout the project and was also revised for the needs of this deliverable.

#	Exploitable results	Type of result	IP Owner	Exploitation model	Timing for use after the project ends	Market
1	Cyberthreat Detection and Response technologies for autonomous vehicles	Software/ Software with Hardware/ Commercial product	T-SYS, AVL	Product, service	1 Year	T-SYS and AVL's global customer base (OEMs and Tier-1s in Europe, USA, Asia)
2	Multi-modal Data Fusion Module for Responding Reliably to the Threats	Software/ Software with Hardware/ Commercial product	PANA	Product, service	6 Months	PANA's global customer base (OEMs and Tier-1 in Europe, USA, Asia)
3	Cyberthreat Detection and Response Techniques for V2X	Software/ Software with Hardware/ Commercial product	FICOSA, I2CAT	Product, service	1 Year	FICOSA's global customer base (OEMs and Tier-1s in Europe, USA, Asia)
4	PKI-enabled Vehicle Identity Management System	Software/Commercial product	8BELLS, I2CAT	Product, service	6 Months	ALTRAN customer base (automotive sector in Europe) and I2CAT/8BELLS stakeholders in Spain, Cyprus
5	AI-based Context-rich and Context-aware Cybersecurity and benchmarking technologies	Software/Commercial product	0INF	Product, service	1 Year	Autonomous Car Manufacturers, and Integrators in Europe
6	Hardware Security Module and Platform	Software/Soft	T-SYS	Product, service	1 Year	T-SYS' global customer base (OEMs and Tier-1s in Europe, USA)

		ware with Hardware/Commercial product				
7	Automotive solution for Intrusion Detection System	Software/Soft ware with Hardware/Commercial product	AVL, ALTRAN, 8BELLS	Patent licensing, Product	1 Year	AVL's and 8BELLS global customer base (OEMs and Tier-1s in Europe, USA, China)
8	Engineering service and consultancy for designing and implementing automotive intrusion detection	Guideline, Standard contribution	T-SYS, AVL, ALTRAN	New service	Immediate	T-SYS, AVL and ALTRAN's global customer based (OEMs and Tier-1s in Europe, USA, China)
9	Solutions for intrusion detection and consultancy competence beyond CARAMEL activities	Software, Artificial Intelligence Methods, Process competence	ALTRAN	Improved and new engineering consulting services	2-3 years into the project	ALTRAN: Automotive, Rail, Transportation, Telecommunication, IoT (e.g., medicine)
10	Highly secure charge control unit	Hardware solution/ Commercial product	GFX	Product/Service	Immediate	GFX network of customers, charge point manufacturers
11	Anti-hacking device	Software, Commercial product	T-SYS, AVL	Product	1 Year	T-SYS and AVL global customer based
12	Anomaly detection mechanism for EV smart charging stations	Software / Commercial product	SID	Service	1 Year	Charge Point Operators (CPO), E-mobility Service Provider (EMSP), Distribution System Operators (DSO)

13	Improved visualization and security analysis algorithms for highly dynamic automotive systems	Software, Commercial product	CLS	Product/Service	1 Year	CLS's customer base, Automotive, IoT (drones, RC, robotics)
14	Novel and efficient machine learning algorithms for cyber-physical threat detection on autonomous vehicles	Open source software, non-commercial product	CLS	Product	1 year	CLS's customer base, security analysts

Table 3: Major expected exploitable results from the CARAMEL activities

Having in mind the variety of results in CARAMEL and their advanced technological maturity to be achieved by the end of the project (all demonstrated in an operational environment) – methods, hardware prototypes, software tools, guidelines, progress in key enabling emergent technologies in AI, ML, deep learning methods – the exploitation strategies adopted by CARAMEL's partners will put together four main pillars towards their wide adoption and market take-up in order to ensure a viable action plan during and beyond project activities. The four pillars are identified below:

3.1 *Products to be improved using CARAMEL outputs*

Pillar 1: It represents the product market which will be addressed by all CARAMEL industrial partners. The multitude of exploitable assets created in CARAMEL as opportunities arise in the EU and globally, thus requiring a proper pre-commercialisation and business planning analysis. The cooperation of partners is based on common and complementary business interests. The consortium foresees opportunities for commercialisation through two possibilities exemplified below:

- Commercialisation of overall solutions, following agreements between partners, performing activities together in specific tasks and establishing measures for joint exploitation. This will open new market opportunities for the SMEs involved in CARAMEL and will reinforce the market positioning of the big industries involved. These are the exploitation results with highest exploitation value and have been identified in Table 3.
- Integration of solutions, technologies and technical know-how developed in CARAMEL in already existing products or services at the respective individual market. Therefore, the industrial partners will have significant benefits by reinforcing and even extending their market position through the integration with current solutions they already maintain. Table 4 presents a list of the partners aiming to follow this approach. Other possibilities could be identified during the remaining of project, such as the creation of spin-off companies for joint exploitation of results, licensing if partners provide their IP for exploitation by others, open-source projects to ensure third-parties exploitation, among others. The exploitation activities in Task 7.3 "Exploitation of Innovation and Technological Results" will study thoroughly all these possibilities.

Partner	Products to be improved using CARAMEL outputs, while reinforcing Partners position in their current markets	Directly used in CARAMEL
T-SYS	ESLOCKS for anomaly detection and prevention for the in-car CAN bus network	Yes
	TollCollect system to collect toll from commercial road vehicles	No
ATOS	XL-SIEM: it allows detection of intrusions, vulnerabilities in the system and remediation activities, if possible	Yes
	Vulnerability Manager: this tool is a domain-specific solution for identifying, analysing and reporting vulnerabilities detected in a target system; (3) Risk Analysis Engine: this tool executes a risk model-based algorithm in order to provide real time evaluation of the cyber risk of a company.	Yes
AVL	The Device.Connect(TM) data connectivity platform for vehicle on the road for having the right information all the time, while ensuring security & safety with absolute best-in-class protection.	Yes
8Bells	8BELLS aims to understand, evolve and exploit its existing IDS tools for automotive usage.	Yes
UBIWR	Smartlamppost (http://www.smartlamppost.com) - an urban furniture product for municipalities and MNOs interested in 5G deployments;	Yes
	Unicle - a platform for vehicle communication. CARAMEL will help Ubiwhere to enable new innovative applications in this concept, more use cases where latency and bandwidth requirements are key.	No
CLS	DiscØvery is a software for rapidly assessing the unique security threats arising in 5G environments that utilise mobile edge computing and extensive NFV virtualisation;	No
	NIGHTWATCH is software for cyber intrusion detection tailored for vehicles that operate in mobile environments using advanced machine learning techniques.	Yes
GFX	A cloud-based platform GSOP (GreenFlux Service and Operations Platform), with which charge points can be managed and smart charging can be executed, will integrate the Highly Secure charge point control unit validated in CARAMEL activities.	Yes
SID	SiVi© Tool is a human-interactive visual-based anomaly detection system that is capable of monitoring and promptly detecting several devastating forms of security attacks, including wormhole attacks, selective forwarding attacks, Sybil attacks, hello flood attacks and jamming attacks	Yes
	SiVi© Tool is enhanced with the EyeSim, which is a human interactive visual-based anomaly detection system that is capable of monitoring and promptly alerting for the presence of multiple security threats. In addition, it is capable of indicating the malicious nodes that form malicious link.	Yes
FICOSA	Full-fledge V2X (802.11p) HW platform designed for security, which will include secure storage and signing environment.	Yes
PANA	Panasonic Automotive Systems is recognised as a top 20 global automotive supplier and partners with the world's leading vehicle manufacturers in delivering high precision solutions in multiple fields of Automotive ranging from battery innovations and head displays to fully automated solutions on Advanced Driver Assistance Systems (ADAS) and Autonomous Driving. The exploitation plan involves using the outcome of the CARAMEL project for enhancing the stability of the next generation solutions in Autonomous Driving, offered to its customers, mainly Vehicle Manufacturers and fleet management providers. More specifically, Panasonic Automotive aims at exploring the potential and	Yes

	limitations of scene perception technologies towards cyber-attacks and integrating the informed experimental feedback, obtained through CARAMEL validation processes to robustify its products, thus enhancing the safety level of the ADAS and AD function brought to the market.	
ALTRAN	The Vueforge(TM) portfolio contains security elements at all system levels between vehicles/sensors and backend.	Yes

Table 4: Products to be improved using CARAMEL outputs

3.2 *Partners activities benefiting from CARAMEL outcomes*

Pillar 2: It represents the consulting market which will be addressed by the partners that provide consulting and technology transfer activities from the academic, research and industrial areas. Before addressing the “products market” there will be a need for a number of additional steps corresponding to the “productization” phase. The exploitation of the “consulting market” is, however, closer, as the acquired knowledge and developed methodological results can be rapidly used. The CARAMEL partners envisioning these kind of exploitation activities to reinforce their current activities is presented in Table 5.

Partner	Activities enhanced by technical know-how gained during CARAMEL implementation
I2CAT	I2CAT is very interested in using the outputs of the CARAMEL to help CESICAT - cybersecurity agency of the Government of Catalonia - (both entities are linked by a close collaboration agreement) to: i) provide consultancy services to companies and organisations in Catalonia, Spain and ii) to protect the Catalan and the Spanish Government's infrastructures and services; these are the two responsibilities of CESICAT. Moreover, I2CAT is a key partner in the 5GBarcelona initiative featuring an integrated metropolitan field and lab environment for testing and trialling future communication technologies / services and validation of end-to-end vertical use cases. It is composed of three field-trial areas in Barcelona and one field and lab-trial area in Castelldefels connected together over an optical metro network. 5GBarcelona test site features MEC nodes in street cabinets, 3.5 GHz Small Cells, SDN enabled WiFi APs mounted on lamp-posts, massive MIMO antennas connected through a high capacity optical access and satellite. It supports live showcasing in an area located near the Mobile World Congress (MWC). I2CAT plans to exploit CARAMEL outcomes to enhance 5GBarcelona testbed for the Internet of Vehicles (IoV) and V2X services with cybersecurity features. In that sense, the target audiences of the initiative such as automotive manufacturers, autonomous transportation ecosystems, cloud and edge computing service providers, IoT solution providers, communication system vendors, smart cities, IoV and V2X technology adopters can benefit from the outcome of their testing activities, taking into account the cybersecurity related aspects.
T-SYS	Telekom Security division will improve its Security Operation Center (SOC) and Security Information and Event Management (SIEM) services to the industry (consulting and operations offering).
8Bells	The activities that 8BELLS will develop in CARAMEL will allow to extend its business in cybersecurity, by providing its clients with consulting services, focused on cutting edge technology that impulses their business in the connected and autonomous vehicles domain.
ALTRAN	As a technology consultancy company, ALTRAN is a top 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). Its wide stock of professional technology consultants, solution design architects and engineers support Automotives (OEMs, Tier-1), telecom operators and enterprises in digital innovation and transformation. ALTRAN's customers cover the entire range of the CARAMEL use cases. This ensures the proliferation of new technologies and consultancy services.
CLS	Consulting services in cybersecurity will be improved by CARAMEL's outcomes.
0INF	CARAMEL will add novel knowledge for consultancy, by enriching 0INF portfolio of data analytics and added-value video solutions.
SID	SID being a newly established SME will benefit from the CARAMEL's results through establishing stronger bonds with cybersecurity experts, manufacturers and automotive stakeholders.
AVL	Consulting is a part of the business offering portfolio. In recent years, AVL has experienced a rapid growth in engineering services including consultancy contracts in relation to dependability features such as system safety according to ISO 26262. Cybersecurity is expected to follow the same growth pattern with the introduction of connectivity and autonomous driving functions and the publication of ISO/SAE 21434 in 2020. CARAMEL will strengthen and expand AVL's cybersecurity capability in the consulting market.

Table 5: CARAMEL Partners activities benefiting from CARAMEL outcomes

3.3 *Partners standardisation activities benefiting from CARAMEL outcomes*

Pillar 3 represents standardisation. Since cybersecurity and the latest changes in the automotive sector have been targeted by several standard development organisations which are followed actively by many CARAMEL industrial partners, CARAMEL activities will bring many opportunities for great contributions in different areas, which are identified in Table 6. Even though it is not directly related to monetary returns, Pillar 3 also represents an important enabler for wider adoption of CARAMEL results. Partners will explore their links to various standardisation bodies and other industrial organisations, in order to influence the adoption of models and guidelines developed by the project. AVL will lead the standardisation activities in T7.4. AVL is a member of the ISO TC22/SC32/WG11 “cybersecurity” working group that is charted to work jointly with SAE to develop road vehicle cybersecurity engineering standard ISO/SAE 21434. The aims of the standard are: to specify requirements for cybersecurity risk management for road vehicles, their components and interfaces throughout engineering (e.g., concept, design, development), production, operation, maintenance, and decommissioning; to define a framework that includes requirements for cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders. The standard is applicable to road vehicles that include Electrical and Electronic (E/E) systems, their interfaces and their communications. The standard is expected to fill the gap of the lack of a cybersecurity standard in the automotive domain. AVL’s planned activities are two-fold. On the one hand side, AVL will inform the CARAMEL partners about the latest and related normative requirements with respect to automotive cybersecurity, which is expected to be followed by OEMs and suppliers around the globe. On the other hand, AVL will disseminate project results in terms of informative recommendations, notes, examples, or references in relevant parts of the standard, such as the section on Cybersecurity Monitoring. Besides fostering collaboration with the standardisation bodies, CARAMEL will also take part on relevant working groups and will put efforts in contributing with relevant documentation and research results. Although the list of relevant working groups is subject to the actual outcomes of the project, the research and industry partners are already involved in a few relevant standardisation activities relevant which will be leveraged by the work developed in the project. Some examples are presented in Table 6.

Partner	SDOs/SSOs	Working Groups	CARAMEL expected contributions
T-SYS	IEEE 801.11 WLAN; WFA/WiFi Alliance; GSMA; NGMN (T-Mobile US) 5GAA (5G Automobile Association) T-SYS provides the Director general of the 5GAA, Dr. Johannes Springer, who is responsible for the 5G Automotive Programme of Deutsche Telekom	T-SYS works in many of the 5GAA working groups, especially in the 5GAA security task force.	Disseminate project results and enhance the security of forthcoming standards and other documents by directly contributing project results. Furthermore, T-SYS will contribute requirements and solutions from the CARAMEL to the relevant 5GAA workings groups and task forces in order to foster a better understanding of security issues and solutions, as well as driving new standardisation activities.
ATOS	European Cyber Security Organisation (ECSO)	WG6 – Strategic Research and Innovation Agenda (SRIA)	ATOS participates actively in the WG6 and, therefore, CARAMEL will be able to disseminate results of, explore possible collaborations with other relevant H2020 projects, participate in the different workshops and events organised by ECSO, etc.
ALTRAN	AUTOSAR (premium m.), ETSI Joint SDOs/Fora Industry Harmonisation Initiative on Unified Standards, 3GPP, IEEE; partly on behalf of customers	ETSI TC Cybersecurity Group, ETSI 5G PoC Consortium on Autonomic Management of 5G Slices: 3GPP, IEEE	New protocol for V2I threat information exchange, Use Cases and Standards Requirements applicable to the automotive.
GFX	OCA (Open Charge Alliance)	OCPP / OSCP	Dissemination of CARAMEL results into the OCPP working group.
UBIWR	ETSI	ETSI's Industry Specification Group on MEC and ITS	Dissemination of CARAMEL results related to the MEC infrastructure applied in the use case.
AVL	ISO, ECSO	TC22/SC 32/WG 11	Dissemination of CARAMEL results within the expert group and in the standard in terms of notes or references.

Table 6: CARAMEL partners standardisation activities benefiting from CARAMEL outcomes

3.4 *Partners research activities benefiting from CARAMEL outcomes*

Pillar 4: Finally, Pillar 4 represents the "research market". Although the research performed in CARAMEL activities is quite limited targeting integration of existing technologies, incremental improvements, adaptations, piloting, and validation, CARAMEL research and academic partners will use the project outcomes to reinforce their skills for future research activities as presented in Table 7.

Partner	Research/Community outreaching using technical and scientific approaches from CARAMEL
I2CAT	Experience and knowledge gained in the European funded project is an essential element to earn the required intellectual capital. I2CAT as a research centre collaborates closely with the universities. This helps to make sure a continuous knowledge transfer to the next generations of experts via offering workshop, courses and scholarships to university students. Moreover, I2CAT contributes to the scientific societies by publishing articles in prestigious and internationally recognised journals and conferences such as, EEE GLOBECOM, IEEE ICC, IEEE/OSA OFC, EuCNC, IEEE Transactions on Wireless Communications, IEEE Communication Magazine, IEEE Vehicular Technology Magazine, Transactions on Emerging Telecommunications Technologies and IEEE Communications Letters. I2CAT private foundation has built a good industrial footprint via its board of trustees, composed of key players in the telecom industry such as Nokia, Cisco, Interoute and Vodafone, among others. Presenting project outcomes is a regular exercise to raise the awareness among important industrial partners and impact the technology evolution. Furthermore, I2CAT is committed to promote and support the open source software communities. In this way, it will try to push as much as possible CARAMEL findings towards Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing (MISP). For example, CARAMEL threat analysis and attack surface modelling can be offered as contributions to MISP. In addition, I2CAT will contribute to the exploitation / extension of open source NFV management orchestration solutions, e.g., OpenStack, ETSI Open Source MANO (I2CAT is an official member), ONAP and SDN controllers, e.g., OpenDaylight (ODL) and ONOS, introducing CARAMEL cybersecurity solutions or future IoV and V2X applications, e.g., PKI /AAA managers as potential extensions to the current available solutions or open-source tools able to simulate CARAMEL cyber-attacks.
UCY	The benefits expected through the participation in the CARAMEL project include: (1) Improve existing knowledge and in-house solutions on the detection, response, and mitigation of cyber-attacks against location services; (2) Extend existing techniques on data validation, fault diagnosis, and anomaly detection; (3) Develop new data-driven methods for enhancing threat intelligence, including advancing personnel skills on machine learning and state-of-the-art data analytics techniques; (4) Disseminate research results and produce high impact scientific publications leveraging on the project's outcomes; (5) Build a SW library of algorithms for autonomous vehicles that can be used to also study the effect of interconnected vehicles. For exploiting the new knowledge and results produced by CARAMEL, UCY will inform academic and industrial partners (both local and international) that are part of the KIOS Innovation Hub to explore opportunities for commercialising our solutions and/or making them available in future proposals to attract funding from local and EU calls.
UPAT	The benefits expected through the participation in the CARAMEL 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 a 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.

Table 7: CARAMEL partners research activities benefiting from CARAMEL outcomes

4 Market Analysis, Business Models and Exploitation Strategy

This section provides a market analysis, business models and exploitation strategy, which define an appropriate exploitation for the CARAMEL results. Market analysis, business models and exploitation strategy will be further expanded on deliverable “D7.5 Road mapping and Business Modelling Report” on month 30 (M30).

4.1 Market Analysis

The cybersecurity market in Automotive is driven mostly by OEMs. Financial impact of reported hacking or even non-safety-critical privacy glitches can be heavy due to image loss, resulting in market share loss. Most of the security incidents impacting vehicles are reported within hours and the news usually associates the incident to the vehicle maker that appears on the headlines across the world. For example, Fiat Chrysler recalled 1.4 million vehicles in 2017 due to a hack [1] and 48% of developers believe that a major overhaul of the car’s architecture is required to make it more secure. The market size is therefore not only to be measured in future economic growth but also in potential loss. The trend to security by design is clearly visible, as part of the learning curve, previously considered a-posteriori to the “actual” engineering.

Globally the market for automotive cybersecurity is expected to grow to €660 million in 2023 [2], at a Compound Annual Growth Rate (CAGR) of 49.5% over the forecast period (2018-2023). This is a huge growth rate which makes absolute predictions obsolete and – if this trend is continuing exponentially – it is the fastest growing technology area. Figure 1 presents a prediction on the number of connected cars. While this statement constitutes the automotive market only, we can expect that the true figure is about double caused via related transportation industry that faces similar challenges and is likely to draw on the same base technology. It is instructive to also consider the IoT market which also constitutes a driver, essentially in system complexity and thus in the number of actual security holes, since one vehicle is likely to connect to a plethora of other “Things”, predominantly phones and infrastructure.

Figure 1: Prediction on the number of connected cars [2]

Such market trends are well aligned with CARAMEL’s implementation timing. Meanwhile, the solution to the problem of cybersecurity is not only technology, but also its organisation. The supply chains are complex and fragmented, and standardisation is underway. We expect that the organisational and regulation effort in economic terms will be significant and increase further, which also constitutes activities by product neutral solution providers like AVL, FICOSA, PANA and ATOS.

CARAMEL positions itself among these growing markets and provides necessary solutions and services in the form of improved situational awareness and decision support, training and penetration testing facilities and a multitude of other exploitable assets, such as CARAMEL's anti hacking solution, ML / AI based cyber-security threats detection and reaction tools. Figure 2 lists a SWOT analysis for the exploitation of CARAMEL's proposed solution.

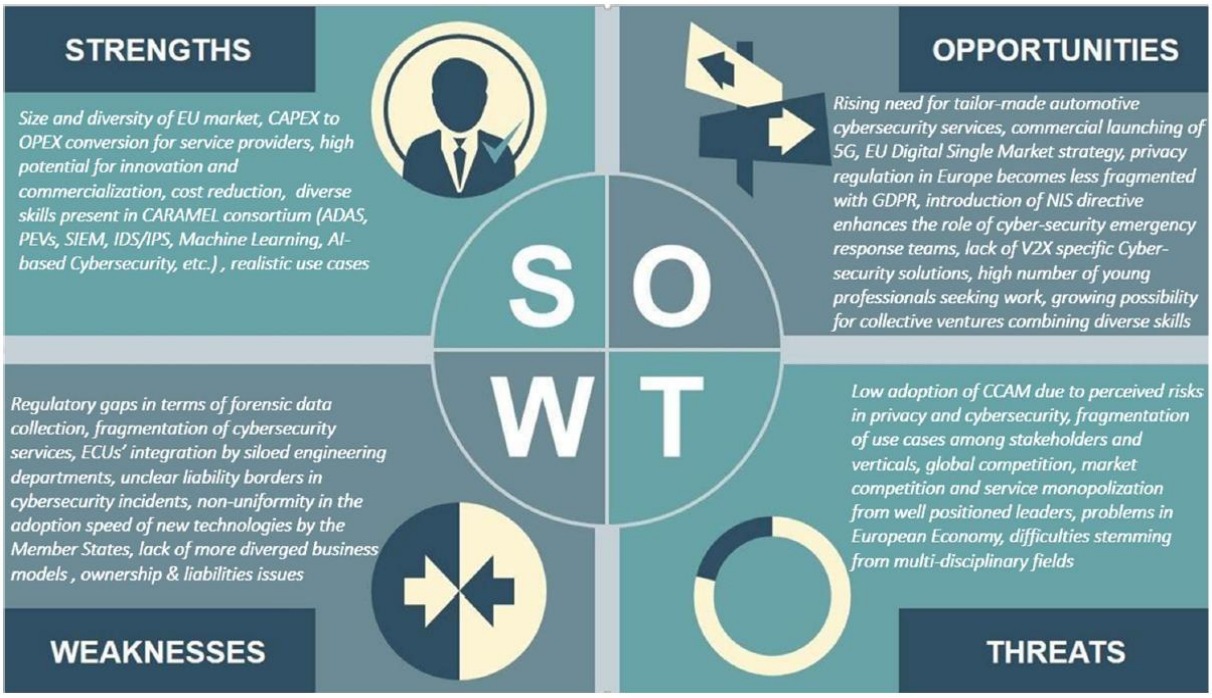

Figure 2: SWOT analysis

4.2 Risk Analysis

Bearing in mind that some risks (both technical and managerial) on the execution period of the project may cause an impact on the project schedule or/and objectives, it is essential that the management process identifies, monitors and takes appropriate measures upon them. Internal risks can stem from:

- The technical nature of the R&D: Unexpected technical difficulty or key technologies not available
- Problems with partners: partner underperforming or key partner leaving the project
- Project execution risks: key milestones or critical deliverables delayed
- Poor communication and cooperation between the partners
- Overly ambitious objectives (in terms of budget) or feasibility

External risks essentially come from the existence of other industrial technology solutions as well as from worldwide competing R&D. Mitigation will be undertaken therefore at the appropriate level in the project organisation: TB, PC or GA in accordance with the rules defined in the Consortium Agreement. Preventive corrective actions will be applied on the structure of the work plan and the project consortium to mitigate or eliminate the most probable risks, and those with the most negative impact on the project success.

Management will continuously monitor and control (i.e., taking corrective actions) expenses, resources and schedules versus plans (i.e., technical and financial annexes to the EC Grant Agreement). A list of precise success criteria for the project will be set-up and maintained during the project life. Root causes for deviations, be it shortages or excesses, in costs, resources and schedules shall be identified, recorded and used as input for continuous improvement. Possible impacts of schedule changes on the budget and resources of the project and on the quality of the product shall be

determined. Deliverables prepared by any member of the project will be first reviewed and then submitted to approval following the process described above.

In order to avoid risks and mitigate its possible consequences, a risk management plan will be set up at the very beginning of the project. The risk management process includes identification, evaluation (probability and impact), reduction actions (plans to avoid risks, manage and reduce them), monitoring and revisions (continuous revision of the risk plan during the entire project duration) and success/failure feedback. Some preliminary strategic, organisational and technical risks have been identified and discussed by the consortium, and a possible contingency solution is formulated for each of them. These critical risks are summarised in Table 8, where risks have been ordered as Technical (T), Management (M) and Financial (F) risks. Also, the likelihood (low – L, medium – M, high - H) of the corresponding risk has been assessed in the table.

Description of risk and associated WPs	Type	Likelihood	Risk mitigation plan, justification on probability level and contingency plan
Partner Risks			
Underperformance of one or more partners, not able to fulfil responsibilities according to project agreement (WP1)	M,F, T	L	This risk has been highly mitigated through the careful selection of all the partners, all of them with recognised expertise in similar projects. The well-structured Project Management approach followed by the project will allow spotting these possible issues very early (through Task 1.2); partners would receive a timely warning from the GA; not fulfilled engagement would be shifted to another partner according to the Consortium Agreement. If not possible, then outsourcing of concrete tasks will be pursued.
A partner leaves the Consortium for unforeseen reasons (All WPs).	M	L	Given the good reputation of the project partners, most of them with proven success records in European Projects, we consider this possibility unlikely. In that case, the GA will decide whether the uncovered project activities can be covered out by one of the existing partners. If this is not possible another partner will be recruited.
Project partner goes bankrupt (All WPs)	M, F	L	Advanced allocation of funding will be carefully organised, so as to minimise risk of a funding shortfall. Gaps would be filled, where possible, with existing partners. Back-up partners would be kept in mind.
Overspending of one of the partners (WP1)	M, F	L	This situation will be detected early via management reports. If this risk occurs, actions will be considered by the MT such as the escalation to the management of the affected partner(s), to mobilise more experienced or better skilled resources capable of working more efficiently.
Agreement and project management risks			

High management overhead due to medium/large CARAMEL Consortium, (All WPs)	M	L	In CARAMEL, each of the 15 partners has a clear and valid role, as well as adequate resources for conducting its commitments. The coordinating organisation and the project management team have substantial and proven experience in the coordination of both scientific and H2020 projects involving many partners and complex research goals. The PC has been involved in decision-making positions in other past research projects, while the TM has big experience in managing multi-people teams. At any case, the principles of PMI management will be in effect. If difficulties in the management arise, further experienced personnel will be involved.
Consortium partners cannot agree because of different interests, (all WPs)	M	L	This has been addressed by the careful selection of the partners, which will be further ensured by signing a comprehensive CA, and by developing an appropriate conflict resolution strategy. Besides, the project has already defined a specific procedure for conflict resolution in the GA in Section 3.2.1.1 to help mitigating this risk.
Financial difficulties and gaps between project phase and budget expenditure. (All WPs).	M, F	L	The MT will evaluate potential gaps in the financial expenditures and project advancement in order to prevent a potential risk in project. If some problems occur, they will work promptly with project partner/s in order to understand the reasons of the gaps and follow up on the problem/s resolution.
Difficulties to identify and/or engage with the External Innovation Advisory Board (EAB), (All WPs).	M	L	Several project partners are already collaborating with key stakeholders and have experience in handling user requirements at a major level, and such a risk can adequately be addressed by the involved partners, particularly, the partners involved in the use cases demonstrations.
Regulatory limitations or safety constraints prevent from deploying Connected and Automated Driving Use Cases in realistic conditions, (WP2, WP3, WP6)	M, T	L	In the case that new regulatory and safety constraints come into force, through Task 1.2, CARAMEL will become aligned with the updated exemption procedures. At any case, the CARAMEL platform will be deployed in private tracks and not in public roads, i.e., in the Test Area Autonomous Driving Baden-Württemberg.
The standardisation impact is not sufficient (WP7).	T	L	The consortium plans to monitor and contribute to standardisation bodies as well as to find any relevant fora that CARAMEL outcomes can be used to provide valuable contributions. This includes the ECSO, MISP, 3GPP, IEEE, ETSI, as well as, SAE, AUTOSAR, EuroNCAP, 5GAA, C2C-CC. To maximise the impact of standardisation activities, CARAMEL industrial partners have already agreed

			to contribute in the standardisation bodies that they are already engaged, in tight cooperation with WP7 leader and the PC. Cooperation with 5G Automotive Working Group will be also encouraged
The assessment of the business models shows poor viability, (WP7).	T	L	Multiple variations from the scenarios and use cases defined in WP2 will be studied, and relevant business roles and models will be compared accordingly, as well as their respective profitability perspectives, each with an adapted and realistic timeline. The EIB team has specific experience and commercialisation strategy for the CARAMEL concepts and will act upon defining a clear and transparent business strategy.
Exploitation achievements lower than expected, (WP7).	T	L	The Consortium is based on recognised EU leaders in cybersecurity and automotive industries, supported by partners heavily involved in the definition and implementation of Future Internet in Europe. In addition, the product development departments of industrial partners will evaluate the possible application of CARAMEL outcomes to car models of 2022 and beyond. All the above will be utilised so as to prevent this risk from taking place.
Technical risks			
Diverging orientations, (All WPs)	T	L	The technical approach for CARAMEL has been carefully discussed among partners and is clearly stated in this proposal. Project management structure and the work plan, which includes the specific Task 1.2 on technical management, have been specifically designed to minimise this risk and to ensure correct collaboration between the work packages and the partners. PC, TM and WP Leaders will ensure that the partners are working on the achievement of the common planned goals.
The developed architectural framework does not match with the expected benefits planned in the proposal, (WP2, WP3, WP4, WP5).	T	L	The CARAMEL platform requirements will be formulated in WP2 following on the early outcomes of WP3, 4 and 5 to be included in the architecture. However, due to different evolution of each WP it may happen that some expected requirements are not met. If this risk happens, the involved partners will analyse the component(s) that cause the failure and assess whether this can be circumvented, or the constraints driving the system design relaxed.
The analysis does not fully cover the range of use cases / scenarios and so key requirements are left out, (WP2).	T	L	The CARAMEL Consortium consists of industrial leaders both in the cybersecurity, automotive and in the telecom industries. Thus, they are fully aware of the needs and requirements of the challenging

			CARAMEL use cases. Moreover, the EIB will support the Consortium in order to properly analyse all the key scenarios and requirements.
Delays in the acquisitions of the hardware/software components (e.g., MEC servers, 4G/5G small cells, SOBUs, RSUs) that cause significant delays in integration and are required for the pilots, (WP6).	T	L	The CARAMEL consortium is well-balanced, and it includes partners that can supply all the individual components of the CARAMEL platform (i.e., Radars, Lidars, Cameras, V2X onboard units, PEVs smart charging controllers, IDS/IPS modules, Penetration testing tools, test vehicles, etc.) In addition, by the start of the project it is reasonable to expect that further advances will give access to the products, hence making this risk minimal. As regarding the 4G/5G small cells I2CAT will subcontract an appropriate European company (e.g., Accelleran, IP. Access, Casa Systems), in order to provide to the consortium eNBs capable to serve FICOSA UE's based on LTE Cat 16 FDD configuration. This is a widely used configuration and a subcontracting cost has been already reserved, so the risk in the delay of the purchase of the equipment is minimal. Also, the MT will constantly monitor project activities, and identify in advance any obstacle and will set the necessary correcting actions.
Vehicular CAN-bus data collected to be used by AI/ML algorithms do not follow a concrete data format or have been captured after some steps of data aggregation.	T	L	CARAMEL is in favour of standardised and interoperable data and file formats when possible. In cases of unstructured, non-standardised data, the consortium will implement a data format to be published as a CARAMEL specification, where data sets will be described explicitly. The consortium is aware that some specific car models aggregate data in order to deliver a standardised information to the OBDII interface. In case that the attacks are not detected at this aggregation level, CARAMEL consortium has the appropriate packet analysers (and packet sniffers) to digest further all the data.
Actual test vehicles do not allow to showcase all technologies (WP6)	T	M	CARAMEL consortium has agreed with PANA to provide a state-of-the-art test vehicle equipped with all modern AUTOSAR compatible ADAS components (see Section 4 for the full description of the test vehicle). In case of incompatibilities or missing functionalities, AVL can provide also with an alternative test vehicle platform for the purposes of CARAMEL.
Diverse interests between the participating vehicular Tier-1 equipment providers, (WP2, WP3, WP4, WP5, WP6)	T	M	It is not unusual that different automotive industries have very different business interests, which can be reflected in the technical developments of the project. In the scope of CARAMEL, AVL, PANA, and FICOSA have agreed in an optimised balance that

			offers them competing advantages and at the same time it is beneficial for the end customers.
Use of initially planned pilot site (Test Area in Baden-Württemberg) is not possible due to issues reported from committed partners or due to the restrictions imposed by the venue owners, (WP6).	T	L	Multiple validation sites for CCAM vehicles will be considered from the beginning of the project. In case one of those sites becomes unavailable the pilots will be rescheduled on another site. The project can also leverage on the Test Track in Gratkorn in Austria (owned by AVL).
Difficulties to engage with the relevant end-users, to obtain feedback on the developing work on user requirements. The developed solution has problems in stakeholder acceptance, (WP2, WP6).	T	L	Several project partners are already collaborating with key user groups and have experience in handling user requirements at a major level, and thus such a risk will be adequately addressed by the involved partners, in particular, the Tier-1 equipment providers. In addition, periodical exchanges between stakeholders will be conducted during the entire course of the project. In any case, the appearing problems, if any, will be detected and addressed in an early stage of it. The project management structure includes also an EAB of independent experts that will provide feedback and help to steer project activities.
Severe problems arise during interfacing and integration of components (e.g., the CARAMEL onboard sensors, ADAS modules, IDS/IPS, backend servers, PEV charger controllers), (WP6, WP3, WP4, WP5).	T	M	The interfaces among the modules will be mostly based on AUTOSAR APIs and will be strictly defined from the very early stages of the project. Pre-integration actions will be taken, if possible, remotely. If not sufficient, integration will be concentrated in one physical site with the participation of engineers from involved partners, for as long as needed. All software development will follow a rigorous software development lifecycle with detailed (interface) requirements specification, detailed design guidelines, unit and sub-system testing; for relevant parts, automatic concurrent (unit) testing facilities are used along with the development process. In any case, automotive providers' value chain is fragmented and Tier-1 equipment providers (PANA and AVL) and automotive integrators (FICOSA) have long experience in integration with the involvement of siloed engineering departments.
The deployment of too many and diversified tools and products on the same platform causes instability, (WP2, WP6)	T	M	The CARAMEL partners will warn the PC and TM as early as possible about the issue so as to be able to act proactively. This will provide the time required to find a suitable functional replacement.
Not enough valid data provided by partners, especially when dealing with real cost data, to make a profound techno-	T	L	Big industrial partners will provide a detailed analysis contributing to economic aspects that are beneficial for them (achievable cost reduction can be demonstrated). Since damages resulting from a bad

economic assessment, (WP2, WP7)			risk analysis can cause greater damage and a clear competitive disadvantage, with higher financial risks, this risk has very low probability.
Conflicting requirements across safety, security, privacy and performance, (WP2, WP3, WP4, WP5, WP6)	T	M	The consortium will prioritise the project objectives (technology development) and it will provide different variants and alternatives with different scenarios and costs.

Table 8: Project Risks

4.3 Business plan and Exploitation Strategy

4.3.1 Business plan

The Business Plan is a key enabler for the success of this project. The current section presents the plan of the common grounds for the business plan for the main CARAMEL outputs. Market positioning of the automotive domain and smart transportation in general is a key industrial sector for Europe [3], securing 12.2 million jobs, producing 22% of the vehicle worldwide (out of 90 million vehicles produced yearly worldwide), and generating a yearly trade balance over €100 billion. It also impacts major societal challenges including reduction of pollutant emissions [4], reduction of traffic fatalities [5], or increased mobility for an ageing population. These societal challenges are strongly supported by the following main technology trends:

- Vehicle electrification [6], with the introduction of e-mobility (hybrid, pure electric vehicle) to optimise or even completely remove the internal combustion engine, finally reducing the resulting pollutant emissions.
- ADAS and autonomous driving functions [7], spanning from providing more comprehensive information to the driver for better context awareness to taking over specific driving manoeuvres, finally reducing the demands on the driver and reducing number and impact of accident.
- Connected vehicles enabling optimisation of vehicle's operation while relying on external information Digitalised manufacturing (Industry 4.0) [8] with the target of optimising production in terms of higher customisation (better variant management), reduction of production costs and higher product quality.

The project's business plan can thus be summarised in the form of the following Business Model Canvas, presented in the Figure 3.

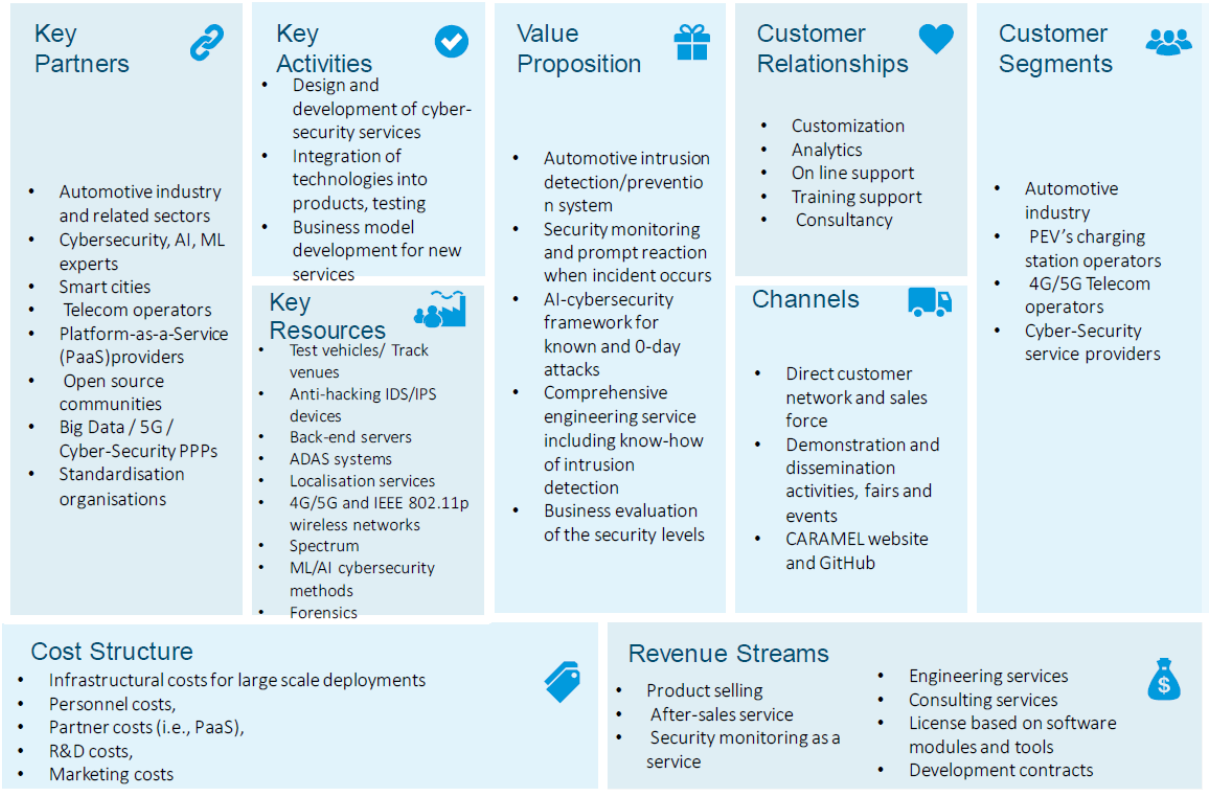

Figure 3: Business model canvas for CARAMEL

4.3.2 Exploitation Strategy

A brief outline of the envisioned activities to ensure a successful exploitation plan for all CARAMEL assets by the end of the project and their market uptake in all corresponding pillars is presented in the **Error! Reference source not found.**. These activities are covered by WP7. A more detailed description of the Exploitation Plan can be found in deliverable "D7.1 Dissemination, Communication and Exploitation Plan".

Exploitation Action Plan	
Vision	Definition of the mission, identification of the key factors for success and main drives.
Market Analysis	Identify key trends and challenges, segment of markets, potential clients, related sectors and subsectors, convenient geographical concentrations for commercial efforts, approach end-users and industry.
Sales and Marketing Strategy	Fully define the value proposition, perform competitive analysis, define sales strategy, identify strategies for market traction (such as free demos, premium features).
Implementation Strategy	While identifying CARAMEL outcomes relevant for exploitation, an exploitation pipeline will be prepared acting as roadmap for the activities to be performed and the required focus and priorities to be defined. Different outcomes have different timings for market approach activities (which could be short, mid-term or long term) and commercial models.
Joint Exploitation Models	Collaboration opportunities will be identified and the IPR management principles for joint outcomes will be established. Different possibilities for joint exploitation will be assessed.
Financial Plan	Economic and financial issues will be assessed for a period of 5 years, such as economic assumptions, break-even, analysis, envisioned profit and loss, cash flow, balance, and operational business ratios.

Table 9: CARAMEL Exploitation Action Plan

All these activities will follow a multi-step iterative approach during the project monitored by the EIB to ensure that optimisation and sustainability principles are followed while keeping a cycle of continuous improvement. Therefore, regular outputs will be released by partners working on the exploitation of specific CARAMEL results, while trying different models that will be evaluated by the EIB increasing their chances of successful implementation beyond the project timing. CARAMEL milestones will be important to assess these exploitation plan exercises, not only to refine them, but also to provide feedback which can be relevant for other CARAMEL activities.

4.3.2.1 Vision

The main goal of CARAMEL is achieving modern vehicles' protection against cybersecurity breaches related to automated driving, communication flows with other vehicles and the roadside infrastructure, as well as smart charging in the case of PEVs. For preventing, detecting and mitigating cyber-attacks, CARAMEL plans to develop and validate secure ADAS modules, trusted V2X Electronic Control Units (ECUs), and smart charger components, but also to demonstrate the effectiveness of an onboard Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS) as a second layer of protection. The later will be hosted over a secure hardware ECU with HSM to store the private keys and any other valuable information, and it will be built upon the advances of ML and AI for efficiently protecting the vehicles against various types of attacks that have not addressed by previous the countermeasures. The ultimate target is to offer anomaly and fault detection in an automated way, being at the same time a trusted tamper-proof black box for CAN-bus data collection.

CARAMEL follows an automotive cybersecurity layered approach that deals with attestation of vehicular hardware, software, and network infrastructures. Through trusted computing, chains of trust will be created, which are necessary for fully automated autopilots with no driver's supervision, the interoperability of V2X communications, and the cyberthreat protection and assurance for EVSE chargers. Understanding the notion of Defence in Depth, one of the cybersecurity core pillars, CARAMEL will extend and integrate advanced security technologies for securing the attack surface that is created by: a) the autonomous vehicle, b) the connected vehicle and c) the plug-in electrical vehicle. As a second line of defence, tailored intrusion detection and prevention tools will be designed and deployed. In particular, for 0-day attacks, CARAMEL will employ an AI-based Security Incident and

Event Management (SIEM) software that will be in charge for real-time monitoring, correlation of events, and sending notifications and alarms. Afterwards, proactive vulnerability discovery and penetration testing will be performed. Last but not least, cybersecurity best practices will be formalised across the involved industrial segments, providing feedback to various regulatory bodies with respect to automotive cybersecurity.

4.3.2.1.1 Key Factors for Success and Main Drives

The key factors for success and main drives are closely related to the main measurable objectives and expected results of Caramel. Caramel's measurable objectives are:

- To identify cybersecurity threats and vulnerabilities in the context of cooperative, connected and automated mobility vehicles (including electrical plug-in vehicles).
- To design and develop a successful extensible, scalable and market-oriented cybersecurity architecture for the provisioning of situational awareness in CCAM vehicles.
- To model cyberthreats, detect cyberattacks and to identify appropriate responses for each modern vehicle category considered in CARAMEL.
- To consider and fuse different data sources of information in order to achieve contextual and situational awareness and to facilitate the decision-making process.
- To create an anti-hacking device that will be able to disable higher level functions in case of a cyberattack.
- To perform penetration testing, validate and demonstrate the CARAMEL solution.
- To ensure the long-term success of the project through standardisation and dissemination in commercial and industrial fora and by exploring synergies with other EU initiatives and projects.
- To design and develop a successful market-oriented, AI-driven and extensible cybersecurity framework for modern vehicles / Business Models to exploit findings in partners' future product/service portfolios.

Regarding Caramel's expected results, the system prototypes will be integrated and demonstrated in an operational environment in the "Test Area Autonomous Driving Baden-Württemberg", as well as in the GFX premises. The TRL expected for the majority of the CARAMEL components and for the integrated platform is 6, i.e., "technology demonstrated in relevant environment (industrially relevant environment in the case of key enabling technologies)". The main expected technical outcomes of the CARAMEL project, as well as their target TRL levels are summarised in Table 10. The following categorisation applies: PRO: Prototype, OP: Open-source project to be initiated, OS: Open Specification, R: Report, DEM: Pilot, demonstrator.

CARAMEL Outcomes	Relevant consortium's existing tools and technologies	Verification	Target TRL
Implementation and deployment of the CARAMEL automotive-grade, on-board and backend IDS/IPS and event data analytics. It will detect intrusion and anomaly caused by cyberattacks on the in-vehicle network, especially CAN communication and data in and out of the Telematics Unit.	Based on the T-SYS existing solution in the market "ESLOCKS", CARAMEL will design and build an anti-hacking IDS/IPS service for the in-car CAN bus data. The software is available as ESLOCKS core and it is continuously developed and maintained with focus on "Software as a Service" aspects.	D5.4 (R/DEM/PRO)	7
Provision of contextual and situational awareness through a fully operational control loop.	The CARAMEL operational control loop will be based on the XL-SIEM product of ATOS, allowing detection of intrusions, vulnerabilities in the system and remediation activities. It can handle large volumes of data and notify about security alerts from a business perspective thanks to its analysis and event processing. Its main functionalities are: i) real-time collection and analysis of security events, ii) prioritisation, filtering and normalisation of the data gathered from different sources and iii) consolidation and correlation of the security events to carry out for a risk assessment, generation of alarms and reports. Finally, it also provides a multilevel web-based visualisation framework for security monitoring and incident response.	D3.3, D4.3 (R/DEM)	6
Collection, detection and remediation of cyberthreats through ML-based techniques.	Collection of real-time service information from the infrastructure elements (e.g., network flow data, DNS queries, HTTP transactions, etc.), storing them in a Big Data infrastructure. The analysis will be made in real time using tailored made ML algorithms through the novel tools of 8BELLS (based on Apache Spot). The goal will be to identify anomalies (deviations from the normal operation) in the running	D5.3 (R)	6

	applications and network services, which would imply either a malfunction or a security incident.		
Development of an in-vehicle Hardware Security Module (HSM) that will serve as a repository for private key data.	The CARAMEL prototype will use a high security embedded device, currently under product development at AVL for several international OEMs for over-the-air connectivity from the OEM site to AVL backend. CAN and Ethernet interfaces, as well as HSM and end-to-end secure communication are already integrated and implemented. AVL will leverage the availability of the embedded hardware and software platform to add IDS and IPS functionalities.	D5.6 (R/DEM)	7
Risk assessment tools for CCAM usage to execute a risk model-based algorithm that provides real time evaluation of the cyber risks. This will be a key asset, able to inform CARAMEL infrastructure about the detected cyber incidents.	ATOS' Vulnerability Manager is a domain-specific solution for identifying, analysing and reporting vulnerabilities detected in a target system, which will be a good basis for CARAMEL's purposes. The discovery of vulnerabilities is supported by domain-specific techniques and rules, which are created and maintained by experts. The vulnerabilities are also correlated with historical data of the system, making the information of vulnerabilities and recommendations more useful and supporting interdependencies between vulnerabilities and solutions recommended.	D3.1 (R)	6
Development of ETSI MEC compliant platform to enable interoperability between 4G/5G and 802.11p (WAVE) wireless networks.	This outcome will be based upon the development of UBIWR's MEC server, which offers both the virtualised environment for MEC apps to be instantiated on, as well as the required V2X physical interfaces to the different underlying radio access technologies.	D3.3 (R/DEM)	6

Table 10: CARAMEL Expected Results and Technology Readiness Level

4.3.2.2 Market analysis

A detail description of Market Analysis is presented in Section 4.1. However, further business models tools and processes will be utilised. Caramel will follow the RACE 2050 vision for the European automotive sector that imagines the industry as a Responsible Automotive Customer-centric Ecosystem. This shared vision was based on the results of the study of McKinsey & Company, Inc [9]. that Caramel plans to pursue and follow in future iterations and studies. Caramel vision aligns with the aforementioned that aims to leverage "Europe's diversity of mobility realities and strengths in technological innovation, talent, skills, and collaborative spirit to make the region the gateway of the global automotive future" [9]. In addition, Caramel will align with the EARTO Recommendations from "The TRL Scale as a Research & Innovation Policy Tool, EARTO Recommendations" [9].

4.3.2.3 Sales and Marketing Strategy

The value proposition for understanding and defending against cyber threats in autonomous vehicles is that CARAMEL will develop and validate different mitigation mechanisms for cyber threats, by focusing on co-registering and processing data from multiple sources located at different strategic points on the vehicle. This type of defence will make it challenging and potentially unlikely for an attacker and a natural event to compromise multiple sources and vehicle points simultaneously. Moreover, different camera filters will be designed for removing laser light and preventing blinding. Furthermore, different pre-processing approaches with the ability to distinguish adversarial samples that lie outside of the data manifold learned by a generative adversarial network will be implemented and tested. For secure multi-technology V2X communications Caramel adds value by addressing the interoperability of legacy IEEE 802.11p and Cellular C-V2X technologies, and the securitisation of V2X. These aspects are critical for the successful market adoption of CCAM technologies. For cyberthreat detection and response techniques for Plug-in Electrical Vehicles (PEVs) value will be added by mitigating known and zero-day attacks and developing model-based and statistical intrusion detection methods, respectively. The first ones rely on the characteristics of known attacks (modelled by rule-based languages, and state transition analysis toolkits), while the later are based upon detection of activities that deviate significantly from system normal behaviour.

Moreover, CARAMEL will research and develop an anti-hacking IDS/IPS device as a second layer of protection with an onboard Intrusion Detection System / Intrusion Prevention System (IDS/IPS) solution that targets a CAN-based automotive E/E system architecture. The system consists of distributed IDS/IPS components and a backend cloud-based IDS/IPS component. The on-board IDS/IPS detects attacks from the in-vehicle network traffic including CAN messages and the traffic in and out of the vehicle through the telematics unit and it also generates vehicle log data based on selected features of the In-Vehicle Network (IVN).

4.3.2.3.1 Results Exploitation Strategy

Part of the Results Exploitation included the marketing strategy as well. This section describes the current and planned activities that are implemented by CARAMEL for an effective and successful exploitation, marketing and technology transfer of CARAMEL's results. The overall Exploitation Potentials Strategy is descripted bellow and the results are to be presented in deliverable "D7.5 Roadmapping and Business Modelling Report" on month 30 (M30).

(1) Cyberwatching (https://cyberwatching.eu/)

Cyberwatching [10] is the European observatory of research and innovation in the field of cybersecurity and privacy. CARAMEL will collaborate with Cyberwatching to share the projects outputs and products in terms of exploitation either by the project itself or by others who may reuse CARAMEL's outputs. This is to be achieved by:

- The inclusion of CARAMEL to the European Project Radar
- An evaluation of the project's Market and Technology Readiness Level.

As it is shown in Figure 4, CARAMEL has already registered to the European Project Radar, however this will be updated after the project's outputs are evaluated in terms Market and Technology Readiness Level. The project's roadmap is to adopt Cyberwatching's Market and Technology Readiness Level Calculator (Annex 1) by adjusting it to CARAMEL first and then have all involved partners provide their inputs. The aforementioned calculator is in the form of a questionnaire and the overall aim is to receive recommendations based on the resulting MTRL scoring (Figure 5). The collaboration with Cyberwatching and participation in Cyberwatching's Market and Technology Readiness Level Calculator are already agreed by all partners within CARAMEL's consortium.

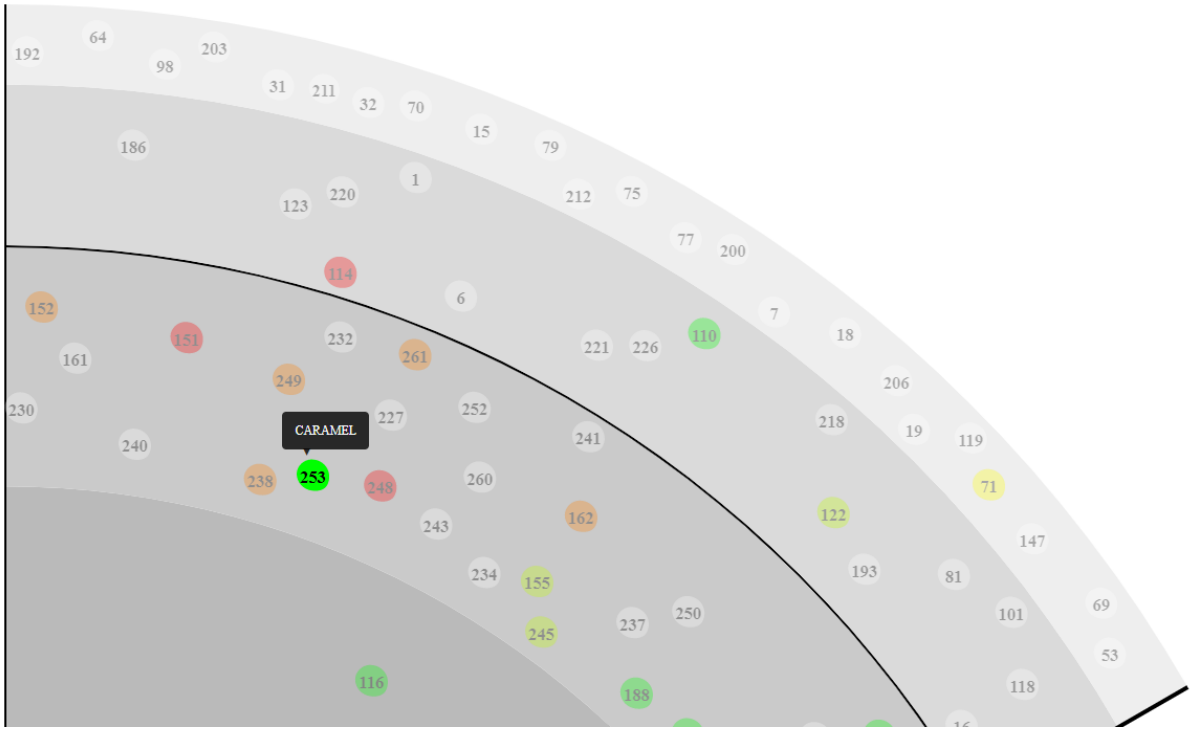

Figure 4: CARAMEL in the European Project Radar

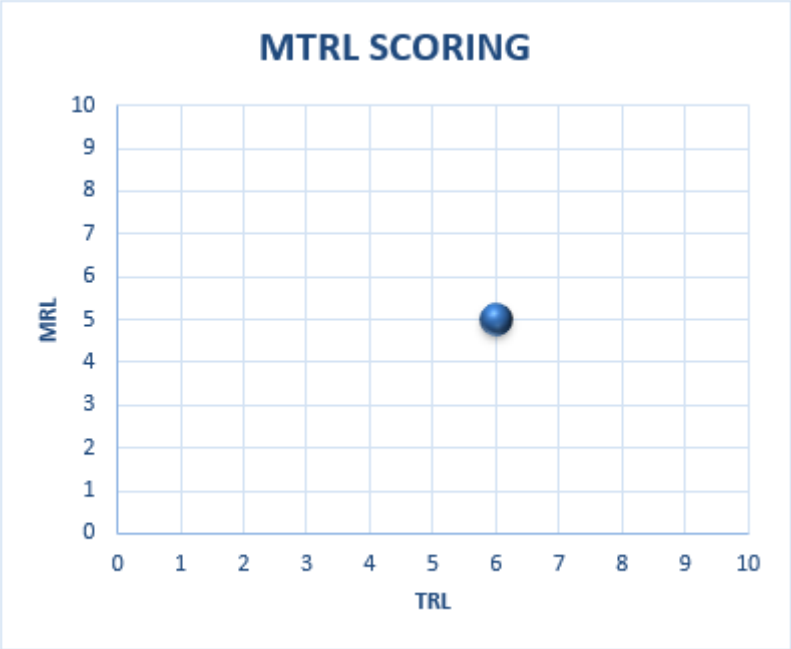

Figure 5: MTRL Score Calculation

(2) Horizon Results Platform (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform)

The Horizon Results Platform [10] is a platform by the European commission where Framework Programme Participants present their results for interested parties to search, contact their owners, and hopefully form fruitful partnerships that will eventually generate the desired value. CARAMEL will collaborate and make use of this platform to publish and advertise its Key Exploitable Results (KER's) based on the degree of innovation, exploitability and impact.

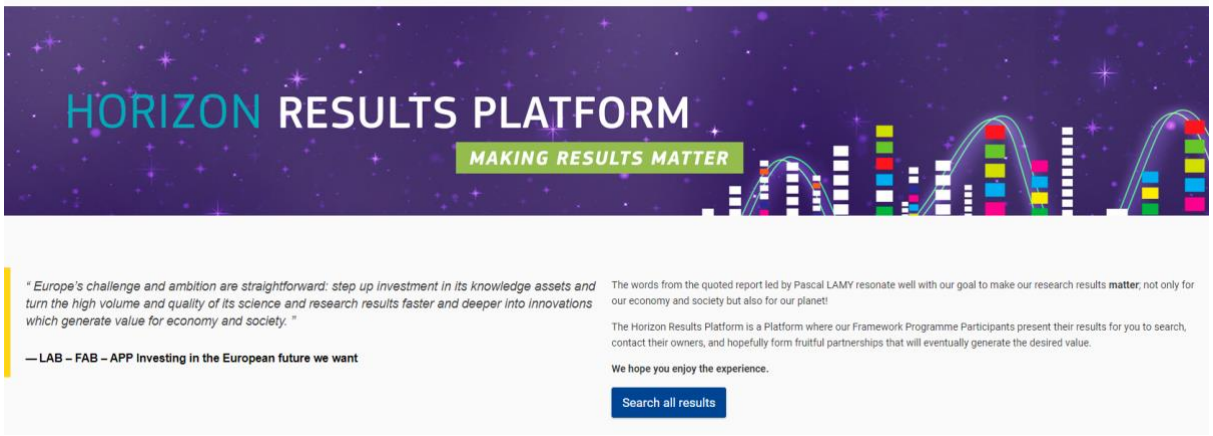

Figure 6: HORIZON Results Platform

To successfully achieve the desirable results, a template is currently under construction in order to capture CARAMEL's results and provide additional details on their type, Business Domain, Applications and Technologies, Target Sector and Target stakeholders. A draft of the template can be found in Annex 2. The collaboration with the HORIZON Results Platform is already agreed by all partners within CARAMEL's consortium.

(3) Horizon Results Booster (https://www.horizonresultsbooster.eu/)

Horizon Results Booster [12] is a package of specialised services that is fully supported by the European Commission. The purpose is to maximise the impact of Research and Innovation public investment and further amplify the added value of the Framework Programmes (FPs). It helps to bring a continual stream of innovation to the market and beyond. It will help to speed up the journey towards creating an impact, providing support to remove bottlenecks. The services provided are designed to build the project's capacity for disseminating research results. CARAMEL will seek to get support in order to further increase the project results' exploitation potential and improve access to markets. All three types of services provided are offered free of change:

- Portfolio Dissemination & Exploitation Strategy
- Business Plan Development
- Go To Market

Figure 7: Horizon Results Booster Services

4.3.2.4 Implementation Strategy

For the implementation strategy, a business plan is summarised in the form of the following Business Model Canvas, presented in the Figure 3. Furthermore, as a complementary action to the business plan in Section 4.3.1, Caramel will adopt the 7P's of the Marketing Mix Model. The seven (7) "P"s reflect the Product, Price, Place, Promotion, People, Process and Physical evidence (Figure 8). The motive of adopting the 7P's of the Marketing Mix model is due to the simplicity to handle, the flexibility of the separation of marketing from other activities of Caramel and the delegation of marketing tasks [13]. The components of the marketing mix can change an organisation's competitive position [14].

Figure 8: 7 Ps of the Marketing Mix [16]

The main components of the 7 Ps of the Marketing Mix are elaborated below as it is described in the Marketing Theories [15], [16]:

- Product - The Product should fit the task consumers want it for, it should work and it should be what the consumers are expecting to get.
- Place – The product should be available from where your target consumer finds it easiest to shop. This may be High Street, Mail Order or the more current option via e-commerce or an online shop.
- Price – The Product should always be seen as representing good value for money. This does not necessarily mean it should be the cheapest available; one of the main tenets of the marketing concept is that customers are usually happy to pay a little more for something that works really well for them.
- Promotion – Advertising, PR, Sales Promotion, Personal Selling and, in more recent times, Social Media are all key communication tools for an organisation. These tools should be used to put across the organisation's message to the correct audiences in the manner they would most like to hear, whether it be informative or appealing to their emotions.
- People – All companies are reliant on the people who run them from front line Sales staff to the Managing Director. Having the right people is essential because they are as much a part of your business offering as the products/services you are offering.
- Processes –The delivery of your service is usually done with the customer present so how the service is delivered is once again part of what the consumer is paying for.
- Physical Evidence – Almost all services include some physical elements even if the bulk of what the consumer is paying for is intangible. Even if the material is not physically printed (e.g. Software source code) they are still receiving a "physical product" by this definition.

To relate each "P" with CARAMEL, the Product refers the major expected exploitable results from the CARAMEL activities (e.g. Automotive solution for Intrusion Detection System) which can be found in detail in Table 3. The Place is mainly to be available via e-commerce and other platforms mention in Section 4.3.2.3.1. There are multiple products improved from CARAMEL and multiple exploitable results. As such the Price is heavily dependent on the IP Owner. For the Promotion, CARAMEL already promotes its product, results and progress through the project website (https://www.h2020caramel.eu),

Social Media (Table 11) and an elaborate dissemination strategy that can be found in "D7.1 Dissemination, Communication and Exploitation Plan". The People refers to the consortium and to ensure the quality of the results a Risk Analysis in Section 4.2 was conducted. The processes of CARAMEL's implementation in specific are defined in the Grand Agreement. The details for delivering services outside of CARAMEL project is up to negotiation between to IP owners and the potential customers. The Physical Evidence of CARAMEL results are going to be Software source code, Documents and Physical products.

Social medium	URL
LinkedIn	https://www.linkedin.com/company/caramel-project
YouTube	https://www.youtube.com/channel/UCX9JMlToA5U1CRWwNMnwTYQ
Twitter	https://twitter.com/caramel_project

Table 11: Social media channels

4.3.2.5 Joint Exploitation Models

Joint Exploitation Models are described in Section 4.3.2.1.4 in the results Exploitation Strategy with the utilization of the three platforms:

- Cyberwatching.
- Horizon Results Platform.
- Horizon Results Booster.

4.3.2.6 Financial Plan

The services and tools used by CARAMEL for Market Analysis and Exploitation Strategy are provided either free of charge by European Commission (e.g. Cyberwatching, Horizon Results Platform, Horizon Results Booster) or are provided by the project's partners. The expenditure for activities related to exploitation are in accordance with the Grand Agreement budget allocation.

5 Conclusion

This document presented the Stakeholder Analysis, Market Analysis and the Exploitation Strategy for CARAMEL. An understanding of the complex, end-to-end technology and value chain(s) as well as stakeholders/users was developed, nevertheless deliverable “D7.5 Road mapping and Business Modelling Report” on month 30 (M30) will update the Market Analysis, Business Models and Exploitation strategy.

The Stakeholder Analysis provided the means for partners to improve products and services applied to the project, and existing products which are part of their portfolio. The Exploitable Assets were identified considering a wide market adoption of CARAMEL outcomes. A Market Analysis studied the attractiveness and the dynamics of the Cybersecurity in CCAM and developed a Risk Analysis that evaluate the technical and managerial risk during the execution period of CARAMEL. Various Business Models that are adopted by CARAMEL were presented and lastly the Exploitation Strategy Plan was elaborated in detail.

References

[1] BBC, “Fiat Chrysler recalls 1.4 million cars after Jeep hack”, Available online: https://www.bbc.com/news/technology-33650491

[2] Cybersecurity Market For Cars - Segmented by Solution (Software Based, Hardware Based, Professional Services), Type of Security (Network, Application, Cloud), and Region - Growth, Available online: Trends and Forecasts (2018 - 2023), Mordor Intelligence, March 2018: https://www.mordorintelligence.com/industry-reports/global-market-for-cyber-security-of-cars-industry

[3] Automobile Industry Pocket Guide 2016 - 2017, Available online: http://www.acea.be/publications/article/acea-pocket-guide

[4] The Paris Protocol. European Commision. 2015 Available online: https://ec.europa.eu/clima/sites/clima/files/international/paris_protocol/docs/com_2015_81_en.pdf

[5] Road safety in the European Union. European Commission, Mar 2015, Available: https://ec.europa.eu/transport/sites/transport/files/road_safety/pdf/vademecum_2015.pdf

[6] European Roadmap Electrification of Road Transport, ERTRAC Working Group, Jun 2017, Available: http://www.ertrac.org/uploads/documentsearch/id50/ERTRAC_ElectrificationRoadmap2017.pdf

[7] Automated Driving Roadmap, ERTRAC Working Group May 2017, Available: http://www.ertrac.org/uploads/documentsearch/id48/ERTRAC_Automated_Driving_2017.pdf

[8] Factories 4.0 and Beyond, European Factories of the Future Research Association, Sep 2016, Available: https://www.effra.eu/sites/default/files/factories40_beyond_v31_public.pdf

[9] McKinsey & Company. Race 2050 – A Vision For The European Automotive Industry. 2019 Available online: https://www.mckinsey.com/~/media/mckinsey/industries/automotive%20and%20assembly/our%20insights/a%20long%20term%20vision%20for%20the%20european%20automotive%20industry/race-2050-a-vision-for-the-european-automotive-industry.ashx

[10] Cyberwatching. The European Watch on Cybersecurity & Privacy. European Commission. Available online: https://cyberwatching.eu/

[11] Horizon Results Platform. European Commission. Available online: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform

[12] Horizon Results Booster. European Commission. Available online: https://www.horizonresultsbooster.eu/

[13] Manoj Kumar Jain. An Analysis of Marketing Mix: 7Ps or More. Asian Journal of Multidisciplinary Studies. Volume1, Issue 4, November 2013. Available online: http://www.ajms.co.in/sites/ajms2015/index.php/ajms/article/view/73

[14] Grönroos, C. From Marketing Mix to Relationship Marketing: Towards A Paradigm Shift in Marketing. Management Decision ISSN: 0025-1747. 1994. Available online: https://www.emerald.com/insight/content/doi/10.1108/00251749410054774/full/html

[15] Marketing Theories – The Marketing Mix – From 4 Ps To 7 Ps. Available online: https://www.professionalacademy.com/blogs-and-advice/marketing-theories---the-marketing-mix---from-4-p-s-to-7-p-s

[16] The Marketing Mix 7P’s. Marketing Mix Definition of the 4P's and 7P's. Available online: https://marketingmix.co.uk/marketing-mix-7ps/

Annexes

Annex 1

cyberwatching.eu - Market and Technology Readiness Level Calculator

Instructions
This questionnaire has been adapted to be used within the cyberwatching.eu project.
* The questionnaire has 9 questions, the first two are oriented to obtain the current TRL (Technology Readiness Level) of your R&D project, the others are focused on the MRL (Market Readiness Level).
* Each answer is assigned a numerical value, from 1 (less ready) to 5 (more ready).
* For each question you must select the answer that best suits the current status of your project. Choose the appropiate numerical value in the box that appears to the left of each question (dark blue).
* At the end you will get a pair of values (between 1 and 9) showing how ready your project is, and a graphic representation of this values.

The score obtained with this questionnaire provides a first evaluation of the Market and Technology Readiness of a R&D project within the scope of the cyberwatching.eu project. It is highly recommended to consult a professional advisor before taking any action.

GENERAL INFORMATION	
Project name	CARAMEL - ARTIFICIAL INTELLIGENCE-BASED CYBERSECURITY FOR CONNECTED AND AUTOMATED VEHICLES
Website	https://www.h2020caramel.eu
Full name	Pouria Sayyad Khodashenas
Email	pouria.khodashenas@i2cat.net
Project outcomes	The EU-funded CARAMEL project is developing cybersecurity solutions for the new generation of cars: i) autonomous cars, ii) 5G connected vehicles, and iii) electromobility. T
Authorization	☑ I authorize cyberwatching.eu to publish the results of this questionnaire and use them for statistical purposes ☑ I authorize cyberwatching.eu to publish the contact email in the cyberwatching.eu site ☑ I authorize cyberwatching.eu to publish the name of the contact person for the project in the cyberwatching.eu site
Comments	(Any comment about the questions or your answers)

2	**1. PROJECT MATURITY**
1. Project work is beyond basic research and technology concept has been defined. Principles postulated and observed but no experimental proof available. 2. Applied research has begun and practical applications have been formulated. 3. Preliminary testing of technology components has begun in a laboratory environment. Proof of concept. 4. Initial testing of integrated product has been completed in a laboratory environment. Early prototype. 5. Integrated product demonstrates performance in the intended environment. Large scale protoype.	
	2. Applied research has begun and practical applications have been formulated.
2	**2. PRODUCT/SERVICE DEVELOPMENT**
1. Initial "product/service - market" fit has been defined 2. Pilot scale product/service has been tested in the intended environment close to the expected performance. Prototype System. 3. Demonstration of a full scale product/service prototype has been completed in operation environment at pre-commercial scale. 4. The manufacturing issues has been solved and you have a first commercial product/service. 5. Product/service is available for all consumers/beneficiaries.	
	2. Pilot scale product/service has been tested in the intended environment close to the expected performance. Prototype System.
3	**3. PRODUCT/SERVICE DEFINITION/DESIGN**
1. One or more initial product/service hypotheses have been defined. 2. Mapping product/service attributes against customer/beneficiaries needs has highlighted a clear value proposition. 3. The product/service has been scaled from laboratory to pilot scale and issues that may affect achieving full scale have been identified. 4. Comprehensive customer/beneficiary value proposition model has been developed, including a detailed understanding of product/service design specifications, required certifications, and trade-offs. 5. Product/service final design/definition optimization has been completed, required certifications have been obtained and product/service has incorporated detailed customer/beneficiary and	
	3. The product/service has been scaled from laboratory to pilot scale and issues that may affect achieving full scale have been identified.
2	**4. COMPETITIVE LANDSCAPE**
1. Market research has been performed and basic knowledge of potential applications and competitive landscape have been identified. 2. Primary market research to prove the product/service commercial feasibility has been completed and basic understanding of competitive products/services has been demonstrated. 3. Comprehensive market research to prove the product/service commercial feasibility has been completed and intermediate understanding of competitive products/services has been demonstrated. 4. Competitive analysis to illustrate unique features and advantages of the product/service compared to competitive products/services has been completed. 5. Full and complete understanding of the competitive landscape, target applications, competitive products/services and market has been achieved.	
	2. Primary market research to prove the product/service commercial feasibility has been completed and basic understanding of competitive products/services has been demonstrated.
4	**5. EXPLOITATION TEAM**
1. No specific exploitation team defined in the project. 2. Solely technical or non-technical partners within the consortium with no outside assistance. 3. Solely technical or non-technical partners within the consortium with assistance from outside (advisors, mentors, incubator, accelerator, etc.). 4. Balanced team with technical and business experience within the consortium. 5. Balanced team with all capabilities onboard (sales, marketing, customer service, operations, etc.) within the consortium.	
	4. Balanced team with technical and business experience within the consortium.
3	**6. DOCUMENTATION**
1. Solely technical descriptions have been elaborated, i.e., software documentation, architecture diagrams, components, etc. 2. User-oriented documentation has been created, such as user manual, installation guides, reference manual, etc. 3. Media demonstration resources have been developed (recorded videos, website with link to demo, etc.). 4. Position papers, press releases, posters, etc. have been elaborated for the dissemination of the project outcomes. 5. Marketing documentation has been created, such as a Business Model Canvas, etc.	
	3. Media demonstration resources have been developed (recorded videos, website with link to demo, etc.).
5	**7. INTELLECTUAL PROPERTY MANAGEMENT**
1. No IPR have been defined (nor exploitable assets has been identified). 2. Initial means of protection have been considered (or initial definition of exploitable assets has been considered). 3. A proper and clear definition of shares has been elaborated (or each partner knows who will explode what). 4. An assignation of exploitation rights has been developed (or an exploitation agreement is in process). 5. A contractual obligation regarding IPR has been established (or an exploitation agreement has been signed).	
	5. A contractual obligation regarding IPR has been established (or an exploitation agreement has been signed).

Annex 2

Result name		Analysis of Security and Privacy Requirements of CCAM
Expected TRL		5
Expected delivery date (MM/YY)		
Overview		The security and privacy aspects of the next generation mobility ecosystem
Result Type	☐	Blueprint
	☐	Commercial solution
	☐	Data set / data pool
	☐	Demonstrator
	☐	Feasibility study
	☐	Framework (e.g. software environment, policy document, legal framework)
	☐	Hardware (e.g. chip, appliance, drone, sensor)
	☐	Infrastructure (e.g. IT infrastructure, transport infrastructure, energy infrastructure, water infrastructure, building etc.)
	☐	Methodology
	☐	Model (e.g. risk model, mathematical model, data model, physical model, business model etc.)
	☐	Patent (e.g. utility, design patents and plant patents)
	☐	Policy report
	☐	Prototype
	☐	Proxy/broker service
	☐	Research and/or virtual environment
	☐	Scientific publication (Refereed)
	☐	Scientific publication (Non-refereed)
	☐	Software (e.g. routine, integrated platform, library, plugins)
	☐	Standard (e.g. norms, policies)
	☑	Taxonomy / Ontology
	☐	Tool / Toolkit / toolbox
	☐	Training (e.g. learning tools, services, modules)
	☑	White paper or similar publication
	☐	Other. Please specify:
Business domain	☑	Data security (including GDPR)
Business area to which the result belongs	☐	Identity & access management
	☐	Network security
	☐	Security compliance
	☐	Application security
	☑	Mobile security
	☑	Threat analysis
	☐	Risk management
	☐	Cloud security
	☐	Biometrics
	☐	Forensic
	☐	IoT
	☐	Cyber physical systems
	☐	Certification and accreditation
	☐	Cyber and security testing infrastructure
	☐	Other. Please specify:
Applications and Technologies	☑	Artificial intelligence
Used in your result or that can benefit from this result	☐	Big Data
	☐	Blockchain and Distributed Ledger Technology (DLT)
	☑	Cloud and Virtualisation
	☐	Embedded Systems
	☐	Hardware technology (RFID, chips, sensors, routers, etc.)
	☐	High-performance computing (HPC)
	☐	Human Machine Interface (HMI)
	☐	Industrial Control Systems (e.g. SCADA)
	☐	Information Systems
	☐	Internet of Things (including Connected and Wearable Devices)
	☐	Mobile Devices
	☐	Operating Systems
	☐	Pervasive Systems
	☐	Quantum Technologies
	☐	Robotics
	☐	Satellite systems and applications
	☑	Vehicular Systems
	☐	Virtual Reality / Augmented Reality
	☑	5G
	☐	Other. Please specify:
Target Sector	☐	Audiovisual and media
The target sector that can benefit from this result	☐	Defence
	☐	Digital Infrastructure
	☐	Energy
	☐	Financial
	☐	Government and public authorities
	☐	Health
	☐	Maritime
	☐	Nuclear
	☐	Public Safety
	☐	Tourism
	☑	Transportation
	☐	Smart Ecosystems
	☐	Space
	☐	Supply Chain
Target stakeholder	☑	Research& academia
Stakeholders are parties that will be affected by a project's execution or results (clients, suppliers, partners...) Stakeholders can have their own expectations and objectives and have the potential to strongly influence a project's outcome in positive or negative directions.	☑	Innovation platforms & clusters
	☐	ICT operators / service providers
	☐	Standard Development Organizations (SDOs)
	☑	SMEs & Start-ups
	☐	Large enterprises
	☐	Policiy experts & activists
	☐	Policy makers, funding agencies including EU & national digital agencies
	☐	Civil society, NGOs, citizens
	☐	Other. Please specify: