



D7.1

Dissemination, Communication and Exploitation Plan

Topic	SU-ICT-01-2018 - Dynamic countering of cyber-attacks
Project Title	Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles
Project Number	833611
Project Acronym	CARMEL
Contractual Delivery Date	M07
Actual Delivery Date	M07
Contributing WP	WP7
Project Start Date	01/10/2019
Project Duration	30 Months
Dissemination Level	Public
Editor	ALTRAN
Contributors	I2CAT, T-SYS, ATOS, ALTRAN, 8BELLS, UBIWR, CLS, GFX, SID, 0INF, UCY, UPAT, AVL, PANA

Version	Date	Remarks
0.1	14/02/2019	First Draft
0.2	25/01/2020	New sections added
0.3	14/02/2020	Format improved
0.4	01/03/2020	New sections added
0.5	09/03/2020	Content filled
0.6	15/03/2020	Content improved
0.7	05/04/2020	Second Consolidated Draft
0.8	14/04/20	Final Draft for internal and SAB review
0.9	27/04/20	SAB review received
1.0	29/04/20	Final version

DISCLAIMER OF WARRANTIES

This document has been prepared by CAMEL project partners as an account of work carried out within the framework of the contract no 833611.

Neither Project Coordinator, nor any signatory party of CAMEL Project Consortium Agreement, nor any person acting on behalf of any of them:

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

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

DISCLOSURE STATEMENT

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

Table of Contents

LIST OF FIGURES	6
LIST OF TABLES.....	7
LIST OF ACRONYMS	8
EXECUTIVE SUMMARY	9
1 INTRODUCTION.....	10
1.1 AUDIENCE	10
2 GOALS AND OBJECTIVES.....	14
2.1 TARGET AUDIENCE	14
3 COMMUNICATION STRATEGY	17
3.1 PROJECT LOGO.....	17
3.1.1 <i>Proud display of EU support</i>	18
3.2 TEMPLATES	18
3.3 PROJECT WEBSITE AND MAINTENANCE	21
3.3.1 <i>Website latest news</i>	24
3.3.2 <i>Website statistics</i>	24
3.4 SOCIAL MEDIA COMMUNICATION.....	25
3.4.1 <i>Twitter</i>	26
3.4.1.1 Twitter Analytics.....	27
3.4.2 <i>LinkedIn</i>	28
3.4.3 <i>YouTube</i>	29
3.4.3.1 The first promo video of CAMEL.....	30
3.5 COMMUNICATIONS PLAN	31
4 DISSEMINATION STRATEGY	33
4.1 DISSEMINATION ACTIVITIES TEMPLATE	34
4.2 EXHIBITIONS.....	35
4.3 SCIENTIFIC PUBLICATIONS.....	35
4.4 WHITE PAPERS.....	36
4.5 WORKSHOPS	37
4.6 WEBINARS	38
4.7 DISSEMINATION IN OTHER EVENTS	38
4.8 LIAISON WITH THE EC INITIATIVES.....	39
4.9 INTERACTION WITH THE EXTERNAL ADVISORY BOARD	41
5 INTERACTION WITH THE STANDARDIZATION BODIES.....	42
5.1 PARTNERS STANDARDISATION PLANS:.....	43
6 MARKET ANALYSIS, BUSINESS MODELS AND EXPLOITATION STRATEGY	44
6.1 MARKET ANALYSIS.....	44
6.2 BUSINESS PLAN	45
6.3 EXPLOITATION ACTION PLAN	46
6.3.1 <i>Liaison with open source community</i>	48

7 CONCLUSION..... 49

8 REFERENCES 50

List of Figures

<i>Figure 1: CAMEL logo.....</i>	<i>17</i>
<i>Figure 2: European flag [3].....</i>	<i>18</i>
<i>Figure 3: Copyrighted acquired images.....</i>	<i>19</i>
<i>Figure 4: Snapshots of the first created flyer.....</i>	<i>21</i>
<i>Figure 5: Screenshot of CAMEL website.....</i>	<i>22</i>
<i>Figure 6: Website structure tree.....</i>	<i>23</i>
<i>Figure 7: Location of visitors to CAMEL's website.....</i>	<i>24</i>
<i>Figure 8: Official twitter logo [6].....</i>	<i>26</i>
<i>Figure 9: Snapshot of twitter account from 20 - Feb 2020.....</i>	<i>27</i>
<i>Figure 10: Snapshot of impressions earned from 14 January 2020 to 15 April 2020.....</i>	<i>28</i>
<i>Figure 11: Official LinkedIn logo [7].....</i>	<i>28</i>
<i>Figure 12: Snapshot of LinkedIn CAMEL account from 20 Feb 2020.....</i>	<i>29</i>
<i>Figure 13: Official YouTube logo [8].....</i>	<i>29</i>
<i>Figure 14: Snapshot of YouTube CAMEL account from 20 - Feb 2020.....</i>	<i>30</i>
<i>Figure 15: Screenshot of CAMEL's first promo video.....</i>	<i>31</i>
<i>Figure 16: Dissemination activities template.....</i>	<i>34</i>
<i>Figure 17: Prediction on the number of connected cars.....</i>	<i>44</i>
<i>Figure 18: SWOT analysis.....</i>	<i>45</i>
<i>Figure 19: Business model canvas for CAMEL.....</i>	<i>46</i>

List of Tables

<i>Table 1: CARMEL Project Stakeholders</i>	<i>13</i>
<i>Table 2: Goals and objectives</i>	<i>14</i>
<i>Table 3: Dissemination and communication approaches</i>	<i>15</i>
<i>Table 4: CARMEL stakeholders</i>	<i>16</i>
<i>Table 5: Summary of created print material</i>	<i>21</i>
<i>Table 6: Social media channels</i>	<i>25</i>
<i>Table 7: Set of possible hashtags to be used on tweets</i>	<i>26</i>
<i>Table 8: Communication plan</i>	<i>32</i>
<i>Table 9: Specific Dissemination activities and its expected KPI.....</i>	<i>34</i>
<i>Table 10: Proposed exhibitions to be attended by partners.....</i>	<i>35</i>
<i>Table 11: Scientific publications compilation.....</i>	<i>36</i>
<i>Table 12: White papers compilation</i>	<i>37</i>
<i>Table 13: Proposed workshops</i>	<i>38</i>
<i>Table 14: Proposed webinars.....</i>	<i>38</i>
<i>Table 15: Dissemination in other events.....</i>	<i>38</i>
<i>Table 16: Identified groups</i>	<i>40</i>
<i>Table 17: External advisory board members</i>	<i>41</i>
<i>Table 18: CARMEL exploitation action plan.....</i>	<i>47</i>

List of Acronyms

CCAM	Cooperative, connected and automated mobility
DGPS	Differential Global Positioning System
EC	European Commission
ECCV	European Conference on Computer Vision
EU	European Union
EV	Electric Vehicles
IEEE 802.11p	Wireless access in Vehicular Environments (WAVE)
LiDAR	Light Detection and Ranging
OEM	Original Equipment Manufacturer
V2X	Vehicle to Everything
ICT	Information and communications technology
EV	Electrical Vehicle
MISP	Malware Information Sharing Platform and Threat Sharing
IEEE	Institute of Electrical and Electronics Engineers
NIST	National Institute of Standards and Technology
SAE	Society of Automotive Engineers
ISO	International Organization for Standardization
AUTOSAR	Automotive Open System Architecture
ETSI	European Telecommunications Standards Institute
3GPPP	3rd Generation Partnership Project
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
5GAA	5G Automotive Association
C2C-CC	CAR 2 CAR Communication Consortium
CMC	Connected Motorcycle Consortium
ALICE	Alliance for Logistics Innovation through Collaboration in Europe
ECSO	European Cyber Security Organisation
CSIRTs	Computer Security Incident Response Team
5GPPP	5G Infrastructure Public Private Partnership
5GIA	5G Infrastructure Association
BDVA	Big Data Value Association

Executive Summary

Deliverable D7.1 (Dissemination, Communication and Exploitation Plan) aims to present the dissemination and communication strategies of CARMEL project to purposefully share its outcomes to different audiences. Additionally, the activities that have been carried out during the first period of the project are being presented.

The first section of this document introduces the goals and objectives for the dissemination activities, followed by a list of approaches to execute the communication and dissemination activities in the chapter three the communication plan and the use of social media channels are being introduced, continuing with the dissemination strategy to address the three main industrial areas covered by the project, namely: Mobility, Telecommunication/ICT, Electric charging in chapter four. The next section consists of the initial ideas of standardisation, the last chapter consists of a summary regarding the exploitation strategy.

Different deliverables belonging to the same work package will address in a more detailed way the ideas presented in this document, namely D7.2, D7.3, D7.4.

Note that, the presented material in this document does not apply to the classified EU restricted results of CARMEL.

1 Introduction

This deliverable presents the communication, dissemination and exploitation strategies for the project CARMEL as part of the Work Package 7 (WP7). The activities described in this document aim to spread the gathered knowledge during the whole duration of the project, additionally, comply with the articles Art.28, Art. 29 and Art 38.1 of the Grant Agreement between the European Commission and the Consortium Partners.

Note that, the presented material in this document does not apply to the classified EU restricted results of CARMEL.

Although related, communication, dissemination and exploitation activities are very diverse and create value to the project stakeholders in different ways. The communication strategy and activities will focus on the planning process that starts at the outset of the action and continues throughout its entire lifetime, aimed at promoting the actions and their results [1]. Communication will not be a single output but a constant activity within the project lifetime. Thus, to keep stakeholders informed and CARMEL project relevant. A main objective, therefore, is to reach out to society and show the impact and benefits of EU-funded activities.

Dissemination is the public disclosure of the results, including by scientific publications in any medium as mentioned by EU Commission [1]. Such activities are important for transferring knowledge and results to third parties. As one of CARMEL's objectives, dissemination activities enable sharing the knowledge at a general and scientific level multiplying the impact of the output of CARMEL's project.

The main objectives are:

- the utilization of the results in further research activities other than CARMEL,
- or in developing, creating and marketing a product or process,
- or in creating and providing a service,
- or in producing either societal and/or economic benefits.
- or in standardization activities

The CARMEL strategic communication, dissemination and exploitation plan includes different tools such as website, social media, participation in events, industry-related conferences, the release of scientific documents, among others. These activities will be explained in detail in this document.

1.1 Audience

The information in this document is intended for the general public to inform them about the planned communication and dissemination activities. All interested parties as well as project partners are expected to benefit from the activities laid out in this document so that the scope of the project can be maximized.

CARMEL 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. CARMEL further considers the needs of policy makers in EU & Member States for informed decisions regarding the security of modern infrastructures for future vehicle industry. Additional benefits are considered in the case for

standardisation, other special interest groups, open source communities and researchers/academics. CARMEL stakeholders are listed on Table 1.

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 Development of business models for cyber-security services / products in future networks, especially for the automotive vertical
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	
Operators	Telecom operators, road operators, charging station network operators, logistics operators	

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-ISAC, Auto Alliance, Global Automakers	Improved synergies among cyber-security and 5G / Future Internet projects Using the CAMEL testbeds as a foundation for the creation of potential interoperable testing facilities across Europe.
	Mobility	ERTICO, ALICE	

	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: CARMEL Project Stakeholders

2 Goals and Objectives

CAMEL is an ambitious project sponsored by the European Commission under the Horizon 2020 program. Moreover, as an important pillar of the project, the work package 7 has the aim to achieve a high and measurable impact of the project results and to ultimately lead to successful adoption of the disruptive capabilities and innovative features into the cybersecurity ecosystem. The objectives related to this plan can be seen in Table 2.

General Objective	Specific Objectives
Tailored and interactive communication outreach and dissemination of the CAMEL project results towards the various stakeholders and integrating their feedback at key points of the project development.	<ul style="list-style-type: none"> - To create a website to centralize CAMEL information. Including objectives, consortium details, project resources, and other contract details. - To create CAMEL's logo to generate a brand identity. - To create a brochure that simplifies the socialization of CAMEL project. - To establish social media channels to build a community. - To create a YouTube channel where videos will be shared. Including cybersecurity, artificial intelligence, CAMEL progress among other topics.
High impact-driven exploitation of the project results prioritizing contributions that can pave the way for the adoption of the CAMEL technological components and solutions into future related standards and innovative products.	<ul style="list-style-type: none"> - To publish CAMEL's results in an open access repository for funded projects (listed some options): https://dmponline.dcc.ac.uk https://dmp.csuc.cat http://pgd.consorciomadrone.es https://about.zenodo.org/ - To organize at least 3 workshops to position CAMEL consortium as industry experts - To develop training material - To release 2 white papers

Table 2: Goals and objectives

2.1 Target audience

To keep the project relevant among a wide public is important to identify the targeted audience for both communication and dissemination activities. The communication activities are more focused to the general public as EU citizens, while on the other hand, the dissemination activities imply interaction with

the specialized audience, i.e. with experts in the fields of cybersecurity, telecommunications, mobility, and artificial intelligence.

From the previous categorization into target audiences, CARMEL can identify appropriate ways to connect to and provide them with processed information based on the interest of each cluster, and also spreading the information in the most efficient and/or effective manner as can be seen in Table 3.

Target Dissemination Groups: The cluster of experts considered, is composed of professionals working for leading companies in electromobility, communications, and mobility, researchers at private institutions and at universities. Scientific events, industrial fairs, congresses are proper events on which those experts may be reached. The specialized audience may and also ideally belong to one or more of the three pillars addressed by the project, which encourages wide dissemination.

EU citizens: It is of great importance that this group is informed or at least can easily pull information about how the goals of the project can increase the security of connected cars and autonomous mobility through the deployment of artificial intelligence techniques or mitigate hacking attempts in future generations of vehicles.

Target Dissemination Groups	Communication Tools for EU Citizens
Expert groups	Website
Industrial fairs	Twitter
Scientific event	YouTube
Workshops	LinkedIn
Policy makers	Flyers
Synergy with other projects	Interviews
Specialized clusters	Brochures

Table 3: Dissemination and communication approaches

By identifying CARMEL's target audience, the consortium partners will be able to focus their efforts to provide dedicated information when communicating and disseminating it to the stakeholders. The use of Artificial Intelligence in cybersecurity for automotive is a new and developing topic that attracts interest in the industry. Therefore, as there is a high number of participants in the automotive value chain, CARMEL must clearly define which of them will be targeted as part of this communication, dissemination and exploitation plan as presented in Table 4.

Stakeholder	Description	Objectives
Original Equipment Manufacturer (OEM)	<p>OEM that provides or uses the following components to the automotive industry:</p> <ul style="list-style-type: none"> • Radar • LiDAR • Camera • Sonar • DGPS • software driving above types of sensor systems • connectivity devices and connectivity in general 	To create awareness of cybersecurity risk factors that OEM should be considered when designing this vehicle component

Connectivity Providers/Telecoms Operators	<p>In today's automotive industry, connectivity is essential. Therefore, companies providing this service should be aware of the CARMEL project. The most popular protocols are:</p> <ul style="list-style-type: none"> • V2X • IEEE 802.11p • ITS-G5 • 5G 	To emphasize the importance of connectivity services for connected vehicles and the threat that both, vehicle and service provider, will be exposed. Furthermore, to stress the urgency to invest in cybersecurity resilience and attack detection
Plug-in Electrical Vehicles (PEVs) Providers	Electric Vehicle (EV) charging infrastructure providers	To reinforce the risk that electric charging points represent to connected vehicles if suitable security measures are not considered
Charging Infrastructure providers	Providing elements in the charging technology and services chain, partly software driven	as above
Vehicle Manufactures	Vehicle manufacturers rely on several OEM to have a final product in the market. They should be involved and educated in cybersecurity topics that will impact their business	<p>To present the research results to educate vehicle manufactures and propose a process how to detect and mitigate attacks.</p> <p>To describe vulnerability areas and risk management solutions</p>

Table 4: CARMEL stakeholders

3 Communication strategy

A proper plan and rationale shall be followed to interact successfully with the targeted audience presented in the previous chapter. This section introduces the strategy to be implemented to achieve outstanding communication and dissemination.

Each result achieved during the entire project lifetime shall be publicized to the general audience or a group of specialized people, presented with a clear project brand, a defined targeted audience, a proper identified activity to spread the results and a proper schedule.

3.1 *Project Logo*

As part of CARMEL's brand and reputation building initiatives, a logo has been designed to be included in all communication and dissemination activities. The logo represents a link between all Consortium Partners and other stakeholders that will be participating as the project evolves.

The CARMEL logo (Figure 1) contains three representative elements:

1. Vehicle (represents automotive in general): probably one of the most advanced and complex IoT in today's world on which CARMEL is focused on
2. Shield: a symbol of strength, control and protection
3. Padlock: as a representation of privacy and security



Figure 1: CARMEL logo

3.1.1 ***Proud display of EU support***

All communication related to the project (including electronic communication, using social media, etc.) and all infrastructure, equipment or major results funded under the grant must provide a visible information to acknowledge the received support [2]:

- (a) display the EU emblem (Figure 2)



Figure 2: European flag [3]

- (b) include the following text:

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833611

3.2 ***Templates***

Different templates have been produced to be used by members of the consortium when presenting information internally, to other project partners or externally when the information is shared to a wider audience.

The idea of such documents is to facilitate the creation of content as well as to maintain a constant set of documents that includes the official format and CARMEL's logos.

Deliverable template - The deliverable template serves as the basis for reporting the project activities and includes official brand colours within the entire template and the official logo on the first page.

PowerPoint template - The PowerPoint template serves as the basis for presentation creation and includes official brand colours within the entire template, official logo on the first slide, and logos from all members of the consortium on the last slide.

Licensed images – While communicating results, a correct use of images on official documents can improve the acceptance and therefore the successful spread of the message being transmitted to the audience.

As an attempt to maintain an official format on each communication and dissemination activity of CARMEL a set of graphics with a royalty-free license has been acquired allowing to safely promote

the project with high-quality infographics. This database is available for all members and can be used in any document created to share insights obtained from CARMEL outcomes.

The set of images were acquired with the vision of CARMEL in mind that includes artificial intelligence, cybersecurity, connected cars, and electromobility, attempting to reflect the principles graphically, as can be seen in Figure 3.



Figure 3: Copyrighted acquired images

Flyer - The participation in congresses, events, industrial fairs, brings an excellent opportunity to reach potential users interested in topics addressed by CARMEL, for that reason a flyer can work as an optimal element to be physically shared among users.

CAMEL will try to deliver a set of different flyers during the project lifetime which can be easily shared with all audience, that include not only EU citizens but may reach university members, professional staff, students, European commission members and even members from other consortia that may like to join forces.

The flyer shown in Figure 4 presents the CAMEL goals and challenges toward cybersecurity issues mitigation through artificial intelligence and contact details of the coordinators of the project. The flyer consists of a two-sided page with four different areas. The first section consists of the name of the project and official logos over a royalty-free acquired image that conveys the goal to address cybersecurity issues. In a further section, the goal and challenges of the project are introduced briefly. The next section explains where the pilot demonstrations will occur. On the last page, the name of the project coordinators is included as well as the social media channels and address to our website. Additionally, the logos of each project partner are displayed. As an official document the flyer includes the grant agreement from the European Commission and the name of the program that provides the funding as can be seen on the Figure 4.

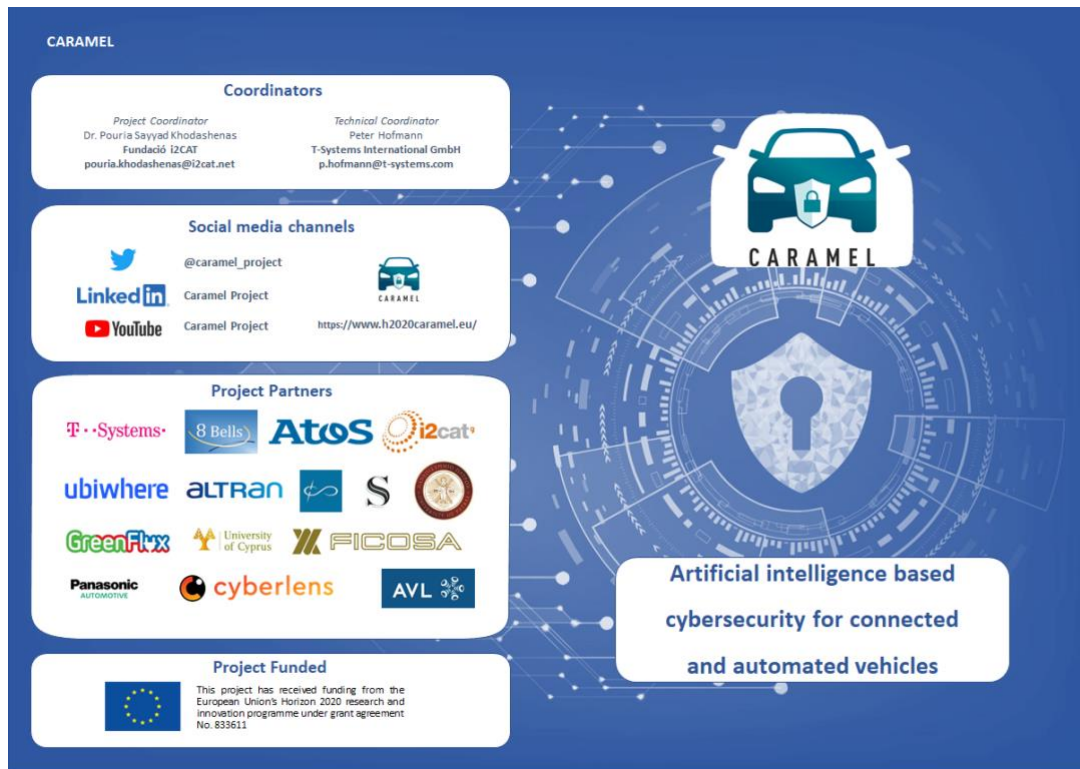




Figure 4: Snapshots of the first created flyer

Leaflet and Poster - For successful communication of CAMEL outcomes, a set of printable media has been created and is ready to be shared among the interested audience. The summary of the already created content can be seen in Table 5

Material	Description
Leaflet	First leaflet of CAMEL project presenting the goal, challenges and pilot demonstrations.
Poster	The first poster will include general information about the project for a general audience.

Table 5: Summary of created print material

3.3 Project Website and Maintenance

The project website holds all publicly relevant information about CAMEL on <https://www.h2020caramel.eu> independently of location and time of day.

CAMEL's website is very important as it centralizes all the information related to the project from the beginning to the completion. Since the release of the Website, information such as objectives, partners, project plan, and deliverables has been shared. Consequently, additional dissemination material will be linked with the data source and the website to facilitate the location of all CAMEL's outcomes. Figure 5 shows a screenshot of the CAMEL website.

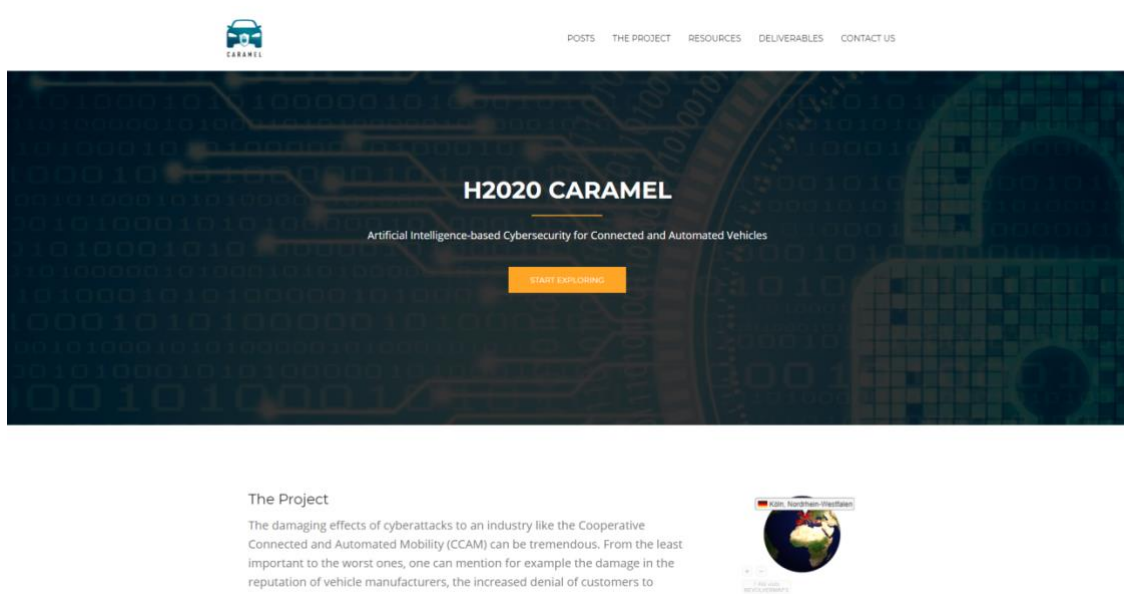


Figure 5: Screenshot of CAMEL website.

CAMEL's website uses a modern, easy to use, flexible, open-source and secure platform called WordPress. This Software provides multiple accessibility levels and high performance [4]. As a content management system WordPress allows us to visualize the content on smartphones, tablets and desktops. It supports a wide range of plug-ins that provide tailored visualization of specific content. All of those characteristics represent an effective way to manage the content and allows maintenance.

The website was deployed in April 2019 with a very simple structure that included direct access to news, project description, a dedicated section for upload the deliverables, and a special section to contact the consortium. Since then, the webpage has been updated and will continuously be improving to include all relevant outcomes from the project.

This content advanced information serves as a basis to spread all kind of information to a general audience but also provide augmented with technical content for the experts on the field.

The website highlights and provides direct access to the latest posts, project description, resources, deliverables and a contact us formula while maintaining an easy to follow structure as can be seen on the site tree in Figure 6.

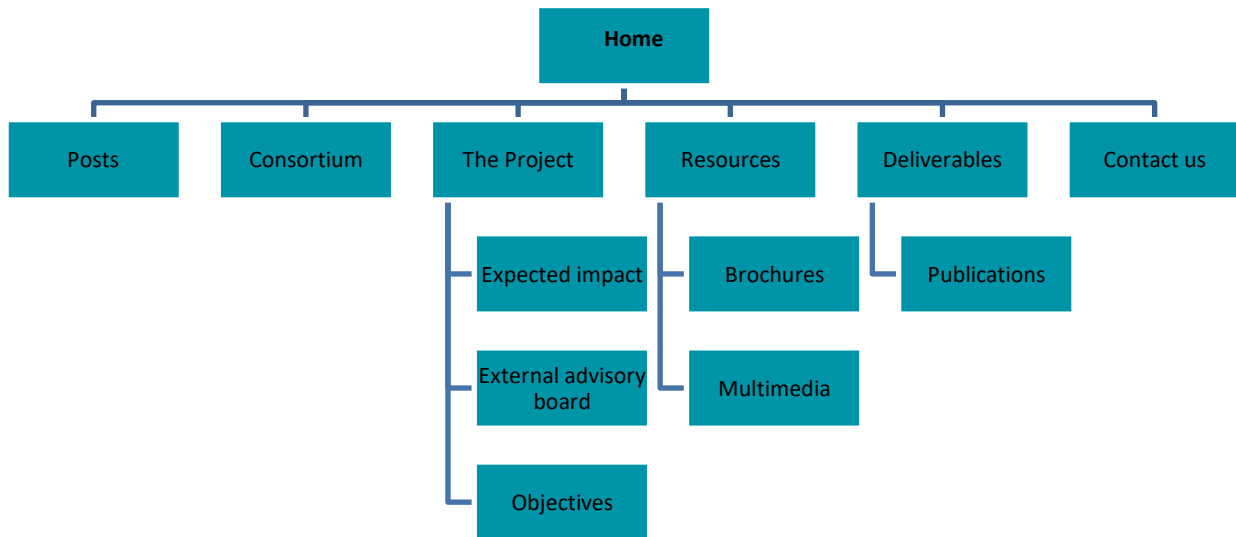


Figure 6: Website structure tree

Home: This section serves as the anchor point for the CARMEL website and points directly to the project page, which consists of a small abstract of the Project.

Posts: This section includes all relevant actions that have been carried out by the members of the consortium, includes all the latest news, as well as relevant events.

Consortium: This page aims to introduce each of the project partners of the consortium, including its official logo and a short abstract. Additionally, it includes a map pointing to the locations from our partners.

The project: The objective of this section is to provide an introduction to the CARMEL goal, what we are addressing and the main pillars of the project.

Expected impact: On this page, some specific outcomes from the project are being introduced.

External advisory board: This section introduces external experts to serve as a support committee with respect to the overall status and direction of CARMEL.

Objectives: The page summarizes the specific objectives of the CARMEL project.

Resources: This section serves as a repository of self-explanatory files.

Brochures: Repository for ready to print versions of brochures or flyers.

Multimedia: All infomercials produced by CARMEL can be found in this section.

Deliverables: During the timeline of the project a set of public deliverables will be produced and shared on this site.

Publications: This section will recompile each outcome produced and already presented to a wider audience; all of those publications will be available for download.

Contact us: In this site, there is provided a contact form that will allow us to keep a record of comments from the viewers.

3.3.1 *Website latest news*

During the life of the project, a series of relevant news items have been reported on CARMEL's website, covering events like face to face meetings, registration of CARMEL in specialized databases and dissemination activities on not planned events. The specific events are:

- CARMEL kick-off meeting which represents the official start of CARMEL's activities and took place in Barcelona, Spain in October 2019.
- The second general assembly which took place at the end of January 2020 in Aveiro, Portugal. In that meeting representatives of each of the project's members worked together defining strategies to achieve the proposed goals.
- Registration of CARMEL in Cyberwatching's database, which provides a compilation of projects that provide research and innovation throughout Europe in the field of cybersecurity.
- Registration of CARMEL in ARCADE database which promotes the exchange of knowledge on innovative solutions in the field of CCAM.
- H2020 CARMEL Project Coordinator gave a talk to UPC students, he shared information about the Next-Generation Mobility: Protecting the new generation of cars from cybercriminals.

3.3.2 *Website statistics*

CARMEL's website was provided with a tool called revolver maps that allows tracking the number and locations of visits made to the page. **Figure 7** shows the locations that have visited the page since the website was uploaded.



Figure 7: Location of visitors to CARMEL's website

The widget attached to the website allows us to track through its live statistics the countries that have visited CARMEL's website most frequently. Until 15-April-2020 the website has registered 1836 visits. Spain leads the major number of visitors on the website with 22%, Germany and the United States are in the top 3 representing 19% and 10% respectively. Additionally, countries like Korea with 3% of the total amount of visits reach ninth place. Special mentions to China, Australia and Nigeria, which its visits allow us to mention that the project has been visited globally.

3.4 Social Media Communication

This project will leverage social media channels as much as possible as these are inexpensive and widely used tools. Overall, the project will focus on communicating to the public, this means, not using scientific but more common language to attract and keep the attention of a broader audience. As mentioned previously, CAMEL touches several trending topics such as Artificial Intelligence, Deep Learning and Cybersecurity for connected vehicles. Therefore, not just the scientific community will be interested in CAMEL, but many other organizations and individuals will be.

The messages will follow the Golden Circle framework as mentioned by Sinek [5]. This theory explains why some organizations and leaders can inspire by communicating from a **Why- How- What** approach. Besides, Sinek described its relationship with the human brain to drive behaviour. CAMEL messages will emphasize first on **Why** this project is important: increasing Cybersecurity risk and potential impact to the world's safety and economy. Second, **How** the project desires to tackle this issue: researching and exploring how AI and Deep Learning could be implemented as risk prevention and mitigation techniques. And finally, the **What**: actual software and hardware outcomes that enhance security, e.g. an anti-hacking device. This was just a simple example but shows how CAMEL will use the Golden Circle in the communications.

The social media has become one of the most important communication channels for many industries, including the scientific community. Taking advantage of its increasing acceptance by users, CAMEL project will use the following social media channels:

1. **Twitter**: the 280 "Tweet" characters limitation results in a sufficient space to communicate effectively over social media.
2. **LinkedIn**: considering that CAMEL is a Research & Innovation (R&I) each outcome can be communicated to a particular audience; LinkedIn is the most professional-oriented social media that CAMEL will be using.
3. **YouTube**: by leveraging this social media channel, CAMEL will be able to release informative videos on the internet and create a stronger spreading of knowledge. Additionally, these videos will be rebroadcast in the other CAMEL platforms. The multimedia material will simplify the communication with interested audiences.

The social media official channels of the project are presented in Table 6.

Social medium	URL
LinkedIn	https://www.linkedin.com/company/caramel-project
YouTube	https://www.youtube.com/channel/UCX9JMIToA5U1CRWwNMnwTYQ
Twitter	https://twitter.com/caramel_project

Table 6: Social media channels

3.4.1 *Twitter*

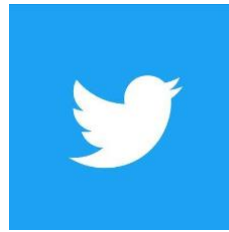


Figure 8: Official twitter logo [6]

To have an effective social media communication, the CAMEL twitter account (Figure 9) will be actively following users in this industry/knowledge domain. This measure intends to grow CAMEL social media connections and to increase the rebroadcasting. Besides, by following related accounts, CAMEL will be able to share (repost) external content, correlated to the research, to increase engagement with stakeholders and to build the CAMEL brand.

One of the strategies followed by twitter users is to use different hashtags achieving maximum diffusion through searches over twitter. This strategy will be adopted using some hashtags and handles when posting in Twitter as presented in Table 7.

Required by	Hashtags/Handles
European Commission	#H2020 @EU_H2020
Caramel Project	#caramel_project @caramel_project
Consortium	@Cyberlens1 @8Bells_research @UCYOfficial @panaauto @Greenfluxinfo @FICOSA_Int @AVL_List @upatras @ALTRAN_DE @Atos @ubiwhere @i2CAT @tsystemscom
Miscellaneous	@5GPPP @ecso_eu @MShuaibSiddiqui @sfiguerola #AI #ML #Machine_Learning #Cybersecurity #Connected_Vehicles

Table 7: Set of possible hashtags to be used on tweets

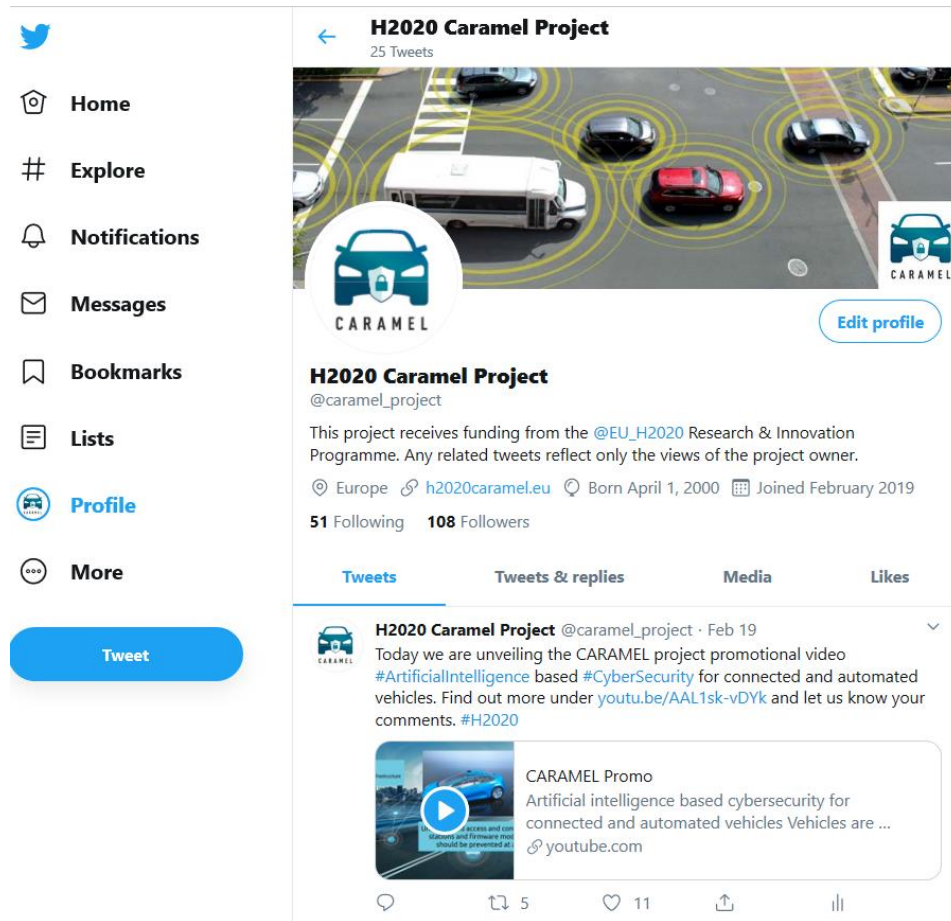


Figure 9: Snapshot of twitter account from 20 - Feb 2020

3.4.1.1 Twitter Analytics

Twitter provides an analytic dashboard that allows obtaining detailed information about how many times CAMEL tweets showed up in people's feeds which are called impressions. It also provides the number of interactions made on tweets for example likes, retweets, etc. such activities are called engagements. **Figure 10** shows the impressions gathered from 14 January 2020 to 15 April 2020.

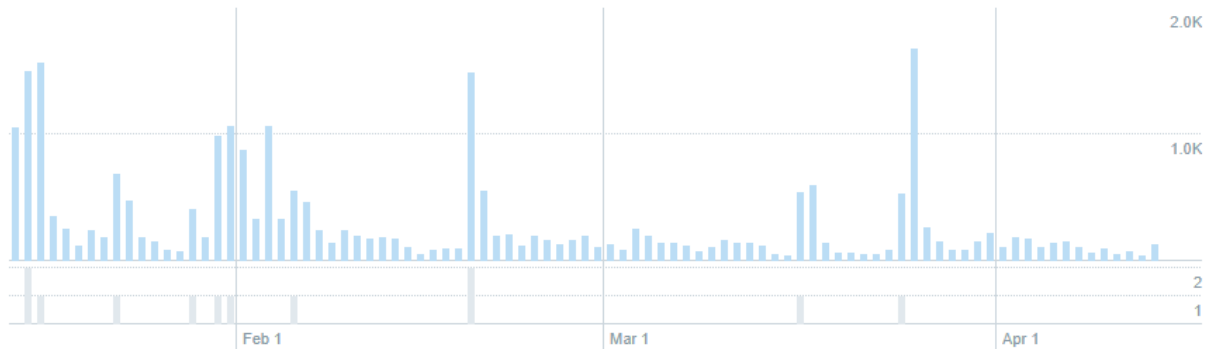


Figure 10: Snapshot of impressions earned from 14 January 2020 to 15 April 2020

From the second week of January until the beginning of the third week of April our TWEETS earned 25.8K impressions and reached on average 267 impressions per day. It even reaches peaks of 1500 impressions even without making tweets those days. This represents interest from the users in the topics addressed by the project.

In the same period, the engagement achieved by our last tweets reaches a total of 360 interactions.

Until 15-April CARMEL's official twitter account is being followed by a total of 18 H2020 projects and EC initiatives, from those projects at least 50% belong to the 5G communication sector.

3.4.2 *LinkedIn*



Figure 11: Official LinkedIn logo [7]

LinkedIn has become one of the most successful networks between professionals making it a suitable way to reach a specialized audience.

CARMEL project will (in parallel to the website and twitter posts), publish in the linked website to get in touch with professionals from the interested sectors related to the CARMEL project. Figure 12 presents CARMEL LinkedIn account.

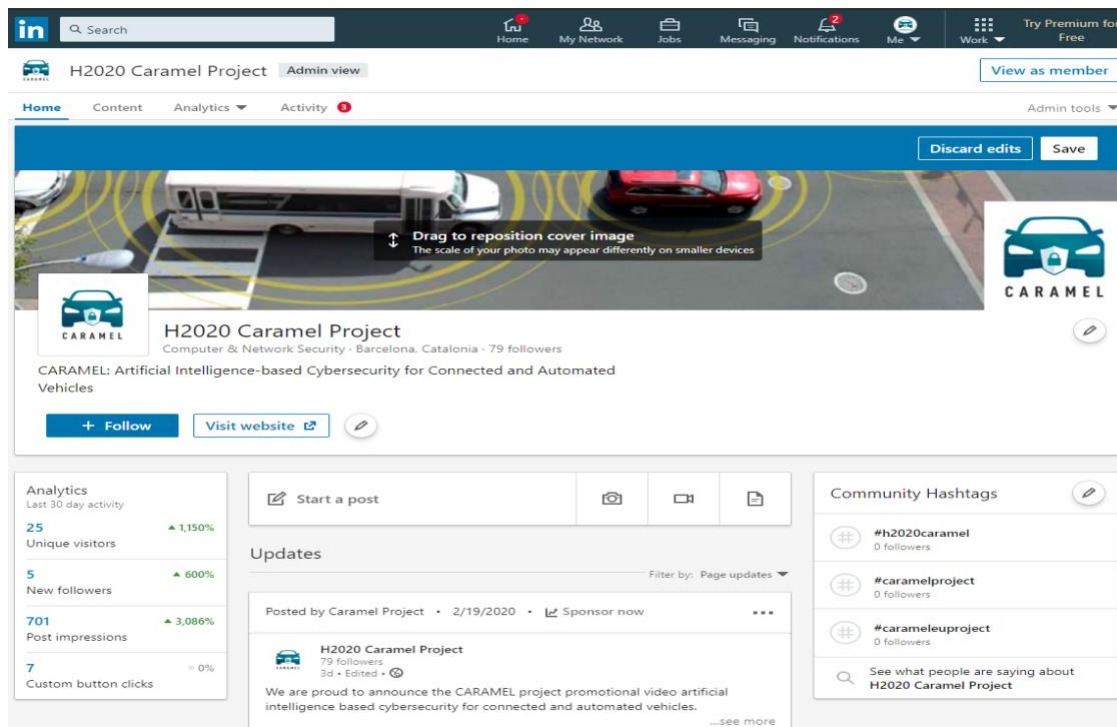


Figure 12: Snapshot of LinkedIn CARMEL account from 20 Feb 2020

3.4.3 YouTube



Figure 13: Official YouTube logo [8]

YouTube is a network that enjoys popularity among all internet users, mostly because the videos are entertaining, and a short video may be enough to transmit very small news or interesting facts.

CARMEL will create and publish a set of videos that introduce basic concepts in a concise way and trying to be consistent but entertaining. The use of the YouTube account (Figure 14) will allow us to provide self-explanatory content through a widely accepted service.

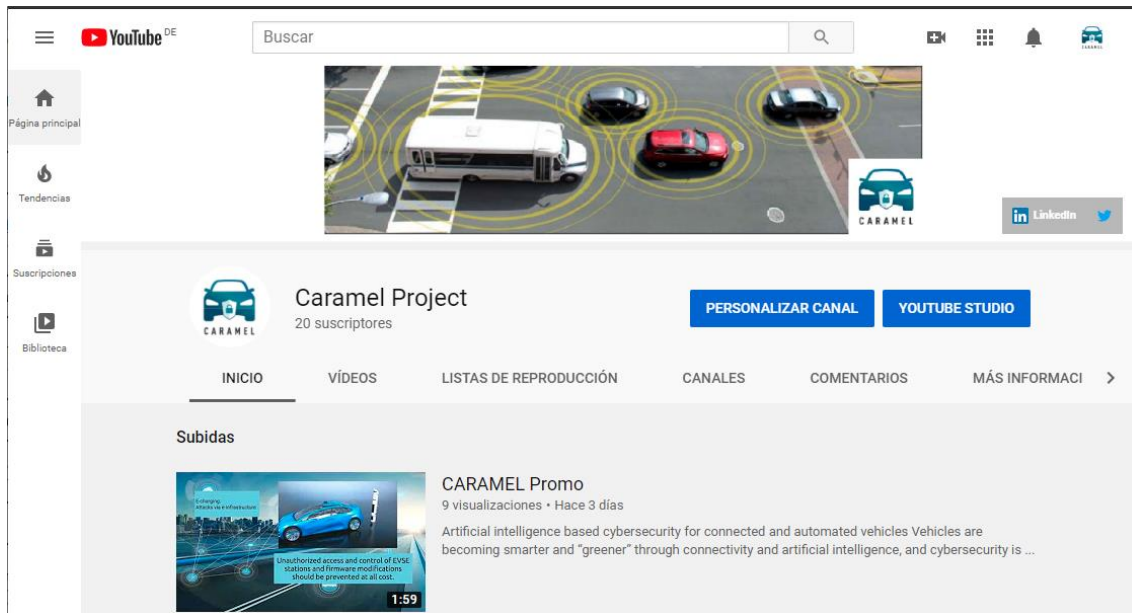


Figure 14: Snapshot of YouTube CAMEL account from 20 - Feb 2020

3.4.3.1 *The first promo video of CAMEL*

CAMEL's first video introduces the aiming of the project toward dealing with the modern cybersecurity gaps, including information about how it plans to combat hacking attempts through the use of artificial intelligence. Besides, it explains how each of the possible attacks identified can affect the integrity of the vehicle. Finally, it mentions the training of a device that will be able to identify possible attacks. Figure 15 shows a pair of screenshots from the official video, which can be accessed from the official YouTube account or at the following link <https://youtu.be/AAL1sk-vDYk>.

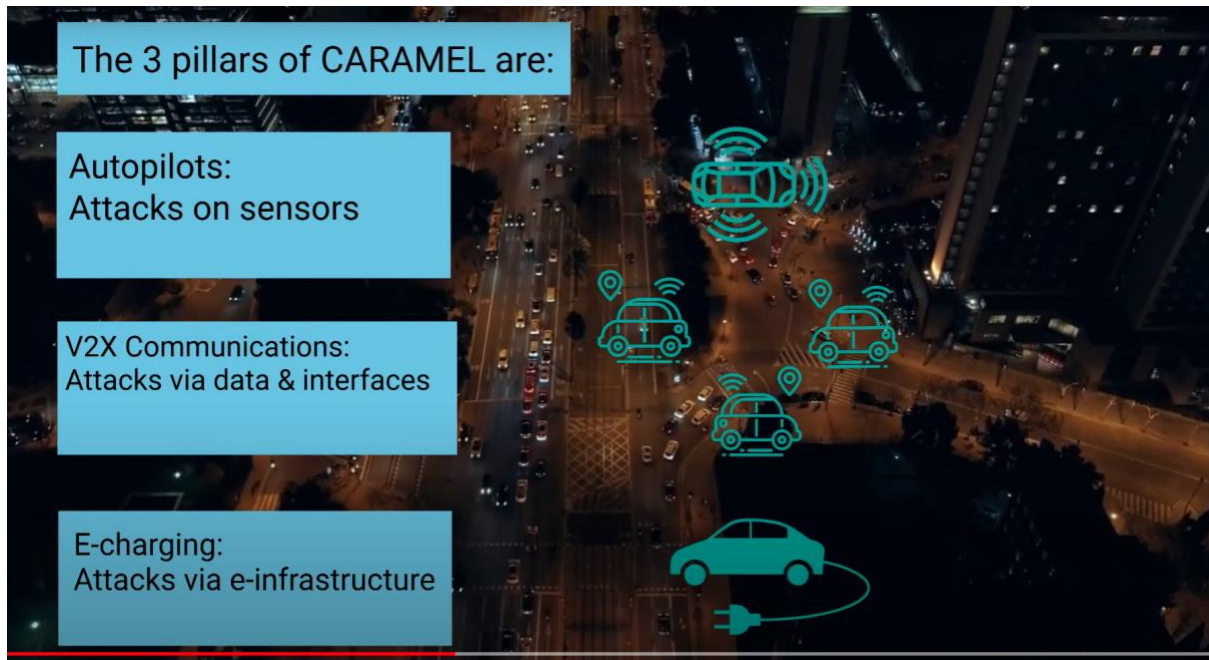


Figure 15: Screenshot of CARMEL's first promo video

3.5 Communications plan

The following communications plan shown in Table 8, describes at a high level, the activities that CARMEL will carry to reach its audience.

Communications Plan
<p>Project objectives and key message points (high level):</p> <ul style="list-style-type: none"> • To create awareness in cybersecurity risk factors. • To keep CARMEL project relevant. • To describe vulnerability areas and risk management solutions. • To present the research results.
<p>Stakeholders – target groups:</p> <ul style="list-style-type: none"> • Public/citizens • Cybercrime-related policing organization • Automotive OEMs • Suppliers • Telecommunication/Connectivity providers (industry) • Infrastructure providers (public) • Mobility providers (Public or car sharing) • E-Charging infrastructure providers • E-Charging payment providers • Scientific community

a. AI/ML b. Cybersecurity c. ADAS and advanced autonomous systems (driving or generally)			
Proposed Timeline	Target (groups)	Tool	Message Points
M01-M07	ALL	LinkedIn Twitter	Position Consortium Partners as experts in their field and highlight their contribution to the project
M03	ALL	YouTube	Present cybersecurity challenges and CARMEL research goals
M03	ALL	YouTube	Automotive Cybersecurity - State of the Art
M01-M30	ALL	LinkedIn Twitter	Biweekly Tweet – project status
M01-M30	OEM	LinkedIn Twitter	Vulnerability research
M01-M30	ALL	LinkedIn Twitter	Blog/News report of participation in conferences

Table 8: Communication plan

4 Dissemination strategy

CAMEL is a project that foresees three major areas on which cybersecurity developments are required, namely mobility, telecommunications and electric charging stations. Such aspects will be complemented aiming to mitigate cyberattacks through the integration of state-of-the-art technologies from the field of artificial intelligence.

The Dissemination strategy of CAMEL targets the superset of three industrial areas:

- a) Mobility
- b) Telecommunication/ICT
- c) Cybersecurity

To push the technology across the boundaries for typically siloed innovation. The unique selling point of CAMEL shall be exploited by targeting actions/events/audiences that also touch more than one of the above areas. Furthermore, this allows us to reach out farther and more efficiently because essentially the same material can be (re-)used, more than one sector is listening.

During the project, different activities are being identified to disseminate the results of combating the cybersecurity attacks for the newest generation of vehicles. The activities to perform the dissemination are listed in Table 9: Specific Dissemination activities and its expected KPI.

This implies a dissemination strategy that should cover the results achieved by the project in the main concepts aimed at by CAMEL.

The European conference and community landscape provide different events that cover at least 2-3 of the above core concepts from the project.

Specific activity	Key performance indicator
Conferences	At least 3 oral presentations per year.
Journals and conference proceedings	All presented work shall be shared and be available to everyone (open access).
Industrial Fairs	Partners will participate in at least 8 different exhibitions per year
Training	A tutorial package about threat analysis and cyber-threats in the automotive sector shall be shared in project website.
Workshops, Seminars	3 workshops are foreseen at academia and industry
Webinars	3 webinars are expected from the research made by CAMEL.
White papers and standard contributions	2 white papers shall be provided as well as 5 joint white papers. 2 standard contributions are expected.
Workshops	Some workshops shall be presented aiming at OEMs

Table 9: Specific Dissemination activities and its expected KPI

To purposefully monitor all related communication and dissemination activities with stakeholders, it is important to have the support of the partners, who must notify in a timely manner to the work package leader and/or use the proposed standardised collection mechanism for communication and dissemination activities.

This procedure will enable a common strategy toward maintaining coherence and providing a proper method to monitor all activities.

A template has been designed by the WP7 leader to provide a document easy to fill by the partners in which they may introduce relevant information about the planned activity.

4.1 *Dissemination activities template*

Dissemination activities are tracked by a web-based table for online and conflict free editing, see Figure 16.


<div>  <div>CAMEL</div> </div> <div>Dissemination activities template</div>								
Dissemination date	Name of event	Lead partner	Event owner	Event country	Targeted audience	Action type Dissemination description	URL to official webpage	URL to produced content

Figure 16: Dissemination activities template

The template lists a set of useful columns that summarize the most important information from a planned dissemination activity, including:

- **Dissemination date:** Allows easy display on a timeline.
- **Name of event:** Full name of the event, congress, industrial fair.
- **Lead partner(s):** Partner is in charge of participation/presentation/content.
- **Event owner:** Entity that organizes the event.
- **Event country:** Country on which the planned activity will take place, useful to track the geographical reach of the dissemination activity.
- **Targeted audience:** Useful to monitor the group of stakeholders reached with the dissemination activity. Those may include but not limited to specialized audience, industry, European citizens, standardization members, media.

- **Action type dissemination description:** This column is reserved to provide a brief description of the planned activity.
- **URL to official webpage:** A link to the official website of the event.
- **URL/link/location to produced/published content:** Information presented as part of the dissemination activity and are publicly available (brochures, published articles, agenda, CARMEL presentations, videos presented during the activity)

4.2 Exhibitions

Participation in exhibitions is part of the dissemination activities, such events provide an opportunity to showcase the results of the CARMEL project, additionally, it is possible to create networks through direct contact with the potentially interested audience.

The right selection of an exhibition, trade show, conferences may be based on addressing some of the major areas pointed out by the project, firstly identifying the main topics of such events and then planning how to participate, what to show, aiming to connect with a wider audience.

Each of the participations in events can be led by any project partner and is encouraged to advise in a timeline manner to the WP7 leader to properly execute the tracking activities.

Some of the identified expos are summarized in Table 10.

Event	Partner
Mobile World congress	I2CAT
ITS European Congress	UBIWR I2CAT
EuCNC	I2CAT
ICTON	I2CAT, Ubiwhere, UCY, UPAT
IEEE ICME	UPAT
ECCV	0INF
EWGT	UCY, 0INF, SID
ITSC	UCY, PANA, UPAT
ICT 2020 Exhibition	I2CAT, 0INF, ALTRAN

Table 10: Proposed exhibitions to be attended by partners

4.3 Scientific publications

Scientific publications are a useful way to expose the obtained results from CARMEL project to a diverse group of stakeholders. This document section focuses on presenting a clear strategy toward the preparation of scientific publications covering contributions as conference papers or journals.

While the WP7 is led by a specific partner, the contributions made for publications can be led by any of the members of the CARMEL consortium, leaving open the decision to participate in specific events. The main idea is to plan all contributions with enough time in order to maintain a set of recurrent interactions by means of online teleconferences, shared repositories and in case of necessary planning

physical meetings toward the successful creation of scientific publications collaboration among a subset of the CARMEL partners.

One of the main tasks of this plan will be to correctly find and select the most appropriate venues on which the CARMEL consortium can participate and at the same time, spread the outcome to a larger interested audience. All the publications made by CARMEL can be seen in Table 11.

Lead partner	Event owner	Title	URL to official webpage
UCY	EuCnC20	The CARMEL project: a secure architecture for connected and autonomous vehicles	https://www.eucnc.eu/
CLS	EWGT2020	Addressing cybersecurity in the next generation mobility ecosystem with CARMEL	http://ewgt2020.eu
UPAT	EUSIPCO2020	Graph-based cooperative localization for connected and semi-autonomous vehicles	https://eusipco2020.org
UPAT	IEEE-ITSC	Vanishing point detection based on the fusion of lidar and image data	https://www.ieee-itsc2020.org
UCY	ICTON	GNSS location verification in connected and autonomous vehicles using in-vehicle multimodal sensor data fusion	https://icton2020.fbk.eu
i2CAT	ICTON	Multi-Radio V2X Communications Interoperability Through a Multi-access Edge Computing (MEC)	https://icton2020.fbk.eu

Table 11: Scientific publications compilation

4.4 White papers

The white papers created by the consortium will disseminate the vision and challenges from the CARMEL project point of view. All of those white papers shall be presented within the project lifetime expecting to have a more robust outcome at each iteration.

Additional to the CARMEL white papers, it is expected to work together with external partners from specialized clusters, like 5g PPP Automotive WG, 5GAA or ongoing EU H2020 projects. A precise interaction with external projects will allow to purposefully plan and create a publishable joint white paper with the visions of both projects and intentions correctly shared into a single publishable document.

The planned white papers to be produced are listed in Table 12

Title	Date	Lead partners
ECSO Transportation report, Cybersecurity for road, rail, air, sea.	3/03/2020	I2CAT
CARMEL: Artificial intelligence-based cybersecurity for connected and automated vehicles	20/06/2020	UPAT

Table 12: White papers compilation**First CARMEL whitepaper**

The first CARMEL whitepaper will be led by UPAT.

Title: CARMEL: Artificial intelligence-based cybersecurity for connected and automated vehicles

Abstract

Modern vehicles require about 100 million lines of code, more than e.g., a Boeing 787 (14 million) or Facebook (61 million), transforming them to some of the most complex systems. The new capabilities increase dramatically the complexity of a vehicle's systems, and although these complex systems have significantly improved vehicle performance, the probability of impairments has also increased. The damaging effects of cyberattacks to the automotive industry can be tremendous. One can mention for example the damage in the reputation of vehicle manufacturers, the loss of working hours, increased environmental pollution due e.g., to intentional traffic jams, and ultimately the great danger for human lives, either they are drivers, passengers or pedestrians. CARMEL is a European Project that aims to proactively address modern vehicle cybersecurity challenges exploiting Artificial Intelligence (AI) and Deep Learning (DL) techniques, and to continuously seek methods to mitigate associated safety risks.

4.5 Workshops

One of the main topics included within CARMEL scope is cybersecurity, such theme has enjoyed popularity in recent years, making it an attractive topic to be spread as part dissemination activities.

As opposed to seminars, a workshop serves as a starting point to learn about a definite topic with hands-on oriented activities, typically for a small group. Additionally, discussions and exercises are encouraged, to apply the learned concepts.

The workshops usually last longer compared to a seminar, due to the time required to apply the learned concepts.

As part of CARMEL activities for dissemination, three workshops are foreseen to spread all scientific or technical knowledge gathered from the produced outcomes.

Table 13 shows a summary of each planned workshop to be presented within the lifetime of the project.

Title	Date	Venue	Partner
Cybersecurity Challenges in Connected, Automated, and Electric Vehicles	18/09/2020	EWGT 2020	UCY
Advanced Cybersecurity Approaches for connected, automated and electric vehicles	20/09/2020	IEEE ITSC2020	UCY

Table 13: Proposed workshops

4.6 Webinars

An additional campaign to disseminate information regarding the newest technological achievements produced by CARMEL is via web-based seminars (webinars), the information can be presented in real-time and interactively thanks to the streaming capabilities of any video conferencing software [9].

The advantages of webinars are that they allow an interactive session, without the necessity to be physically present in the same room. This enables a discussion, exercises, sharing of files, etc.

Webinars can be recorded; a broadcasted video stream can be further published via the CARMEL YouTube account.

The proposed webinars are summarized in Table 14:

Title	Partner
Use of CARLA Simulation Environment for CARMEL	T-SYS

Table 14: Proposed webinars

4.7 Dissemination in other events

Some members of CARMEL may be invited to give an oral presentation and present any scientific or technical information in front of a large interested audience. It is important to keep tracking of events that were not previously planned.

All the events that were not previously scheduled as a CARMEL activity are presented in Table 15.

Title	Date	Venue	Partner
Protecting the new generation of cars from cybercriminals [10]	18/09/2019	Politécnica de Catalunya (UPC), Barcelona, Spain	I2CAT
Artificial intelligence: The revolution of artificial intelligence in the real world	13/02/2020	Foro Transfiere 2020	ATOS

Table 15: Dissemination in other events

4.8 *Liaison with the EC Initiatives*

As a part of the dissemination activities is to identify conglomerates of experts for which the topic of the project may be relevant. A list of identified groups is presented on Table 16.

CAMEL will take part in relevant 5G PPP working groups (indirectly – via common partners like i2CAT), ECSO (directly – CAMEL is a member), and CCAM initiative (directly – CAMEL is a member). The non-extensive list of relevant bodies is presented here: 5GPPP/5GIA Architecture WG; 5GPPP/5GIA Network Management WG; 5GPPP/5GIA Software Networks WG; 5GPPP/5GIA SME WG; 5GPPP/5GIA Trials WG; 5GPPP/5GIA Vision and Societal Challenges; 5GPPP/5GIA Automotive WG. A particularly relevant contribution to the long-term impact of CAMEL will be contribution of project visions and results to the ongoing structuring activities of future Safe and Automated Road Transport and Smart Networks vision of EC. CAMEL is contributing to the Safe and Automated Road Transport roadmap through the EU Single Platform for CCAM, in particular WG5: EU-CCAM-WG-DATA-CYBERSECURITY. Regarding ECSO, CAMEL is a member and contributor of WG3: Sectoral Demand (Industry 4.0, Energy, Financial, Public Services / e-Government, Health, Transportation, Smart Cities, Telecom - Media & Content).

In addition, with the help of external advisory board CAMEL will interact with initiatives like ERTICO (see the next section). CAMEL also enjoys the presence of common partners with 5GAA (in particular PANA). This will help the project to create a communication channel with them.

Cluster	Description
ERTICO	ITS Europe is a public-private membership driven organization promoting, developing and deploying Intelligent Transport Systems (ITS) in Europe to save lives, protect the environment and sustain mobility in the most cost-effective way [11]
ENISA	The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. The Agency is located in Athens, Greece and has a second office in Heraklion, Greece [12]
IEEE ComSoc	Is a leading global community comprised of a diverse set of professionals with a common interest in advancing all communications and networking technologies [13]
ECSO	ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centers, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations, countries part of the European Economic Area (EEA) and the European Free Trade Association (EFTA) and H2020 associated countries [14]
5G PPP	The 5G Infrastructure Public Private Partnership (5G PPP) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions) [15]
Autosar	Is a worldwide development partnership of vehicle manufacturers, suppliers, service providers and companies from the automotive electronics, semiconductor and software industry [16]
CEN/CENELEC	CEN and CENELEC are business catalysts in Europe, removing trade barriers for European industry and consumers. Their mission is to foster the European

	economy in global trading, the welfare of European citizens and the environment. Through their services they provide platforms for the development of European Standards and other technical specs [17]
CSIRTs Network	The NIS Directive in Article 12 establishes the CSIRTs Network “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation”. The CSIRTs Network is a network composed of EU Member States’ appointed CSIRTs and CERT-EU (“CSIRTs Network members”). The European Commission participates in the network as an observer. ENISA is tasked to actively support the CSIRTs cooperation, provide the secretariat and active support for incident coordination upon request. The CSIRTs Network provides a forum where members can cooperate, exchange information and build trust. Members will be able to improve the handling of cross-border incidents and even discuss how to respond in a coordinated manner to specific incidents [18]

Table 16: Identified groups

CAMEL is registered on the following EC databases:

- **ARCADE**

The Knowledge Base on Connected and Automated Driving (CAD) is a great tool to share and exchange knowledge on innovative solutions for CCAM [19].

<https://knowledge-base.connectedautomateddriving.eu/projects/findproject/>

- **Cyberwatching**

European observatory of research and innovation in the field of cybersecurity and privacy. This action was made as an effort to consolidate an online hub of the projects that with its work provide research and innovation activities across Europe in the field of cybersecurity [20].

<https://cyberwatching.eu/projects/1737/artificial-intelligence-based-cybersecurity-connected-and-automated-vehicles>

Regarding the computer security incident response team (CSIRT) network, leveraging on its strong consortium network contacts and CAMEL relevant expected results for “strategic threat radar” and cyber-incident management for connected autonomous cars, CAMEL foresees to generate an impact on CSIRT network across Europe. As a matter of fact, CAMEL’s Technical Coordinator, T-SYS, is a highly recognised partner for its expertise, experience and high-quality impact on CSIRT / ENISA ecosystem. T-SYS is active in three levels: (1) at internal level: local CSIRT team of T-SYS (and Dutch telecom) in different locations in Germany; (2) at national level: in Germany, T-SYS is active in CSIRT teams including mainly German large corporations (e.g., Volkswagen), while participating also in a large German group of 100 CSIRT teams; (3) at European / International level: T-SYS is the 3rd highest ranked member, according to the ENISA website information on the CSIRTs European network. T-SYS performs information exchange with other members, makes presentations of relevant technical content for CSIRT and, more importantly, T-SYS is a widely known for its team receiving multiple contacts for pushing forward new issues. Such contacts are triggered on incident bases, i.e., whenever a party identifies an incident and finds a way to mitigate it, T-SYS is the reference contact point to push the issue forward. Therefore, CAMEL outcomes impact in different CSIRT’s networks at different levels (i.e., local, national and International/European) will be ensured by such an important technical and operational role of T-SYS in the CSIRT / ENISA ecosystem.

4.9 *Interaction with the external advisory board*

The External Advisory Board (EAB) has been established with the idea of improving the efficacy of CAMEL deliverables by assessing and providing feedback about the status of the outcomes produced during the project's timeline. The board is composed of a group of experts in at least one of the main pillars addressed by CAMEL and is being formed by the people whose names appear in Table 17.

Name	Title
Jesus Alonso-Zarate	PhD. Senior Researcher Manager, the communication technologies division Head of the machine-to-machine communication department at CTTC, 5G-PPP H2020 5GCroCo Project Coordinator Chair of the 5G-PPP Automotive working group
Antonio M. López Peña	PhD. CVC Principal Investigator & UAB Associate professor
Johanna Tzanidaki	Dr. Director innovation & deployment of ERTICO
Pedro Dias Rodriguez	Security Operations Center Manager of EDP

Table 17: External advisory board members

The interaction with the EAB is made through the project coordinator which will organize remote conferences or interact by email providing updates about CAMEL activities.

Depending on the project needs on different fronts EAB will be extended with the new members linking the project to proper expert networks and clusters.

5 Interaction with the Standardization Bodies

One of the project objectives is to contribute to the standardisation activities where relevant. The Standardization Strategy of CAMEL predominantly targets the intersection of three industrial sectors:

- Mobility
- Telecommunication/ICT
- Cybersecurity

CAMEL partners are continuously monitoring and following relevant standardisation bodies.

The project tries to incorporate lessons learned in terms of requirements, characteristics and specifications experienced in the CAMEL scenario to proper standardisation activities. However, without directly being members of the standardization bodies creating such an impact might not be that easy. Nevertheless, via publishing recommendations in the form of white papers and by participating on pre- standardisation activities done at EU initiatives, CAMEL tries to create an impact on this front.

In order to boost the possibility of creating awareness which is crucial for an impactful contribution on standardisation activities, CAMEL invited / will invite some key figures from Cybersecurity, ICT and Mobility communities on its advisory board and put in place an interactive framework between the project and them.

Typical candidates for standardization are therefore fora covering more than one of the three areas, e.g. ETSI-ITS, ITU-T, IEEE, and others, each providing work groups stretching between, for example, automotive scenarios treated from the perspective of Telecommunication and Cybersecurity.

CAMEL already identified some potential venues:

3GPP: 3GPP is formed by seven telecommunications standard development organizations (from Asia, Europe and North America) known as “Organizational Partners”. It aims to produce reports and specifications for the cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities – covering topics such as work on codecs, security, and quality of service. In this sense, 3GPP supports complete system specifications. It also takes into account the non-radio access to the core network and interworking with Wi-Fi networks [21].

ETSI: ETSI is a European independent standardization group with a key role in developing standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies. In 1988, the European Conference of Postal and Telecommunications Administration (CEPT) established ETSI as a non-profit organization, now representing more than 800 member organizations, over 64 countries [22]. Under ETSI, in particular these items are interesting:

- Technical Committee (TC) Intelligent Transport Systems (ITS)
- Automotive Intelligent Transport Systems (ITS)

ISO TC 204: It is the responsible body for the overall system and infrastructure aspects of intelligent transport system (ITS). Individuals or companies cannot become ISO members, but there are ways to take part in standardization work. The mechanism is based on the indirect contribution via member bodies. Full member is the highest level that sell and adopt ISO international standards nationally [23].

5GAA: 5G Automobile Association is a global cross-industry organization of companies from the automotive, technology, and telecommunications industries to develop end-to-end solutions for future mobility and transportation services [24].

CAR2CAR: leading European community of vehicles manufacturers, equipment suppliers and research institutions who join forces for the deployment of cooperative Intelligent Transport Systems and Services

(C-ITS). It aims on ensuring the interoperability of cooperative systems, spanning all vehicle classes across brands and borders [25].

IETF/IRTF: Internet Research Task Force (IRTF) focuses on longer term research issues related to the Internet while the parallel organization, Internet Engineering Task Force (IETF) focus on shorter term issues of engineering and standards making [26].

GSMA: Global System for Mobile Communications Association (GSMA) is a trade body that represents the interests of mobile network operators worldwide. Approximately 800 mobile operators are full GSMA members and a further 300 companies in the broader mobile ecosystem are associate members [27].

5.1 *Partners standardisation plans:*

ATOS

ISO/IEC JTC 1/SC 27 "Information Security, cybersecurity and privacy protection" is a subcommittee of the Joint Technical Committee ISO/IEC JTC1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). SC 27 aims at developing standards for the protection of information and ICT. Atos is involved in the committee ISO/ IEC JTC1/SC 27, and has participated particularly in the working group WG5 contributing to several standards as ISO 29003, 29115 (related to ARIES project), and also 27005 and 27010 (related to Cyberwiser and Concordia projects respectively).

Atos also takes part of the WG1 of ECSO, the European Cyber Security Organisation. This working group provides to ENISA with common priorities and industrial needs for definition of certification schemes on products, process and services. Atos may collaborate with this WG disseminating the standardization activities developed within the CAMEL consortium.

The Big Data Value Association (BDVA) is a non-profit organization under Belgian law with more than 200 industry partners from all over Europe. The BDVA is the private partner of the European Union Commission in implementing the Big Data Value PPP programme. The BDVA and the Big Data Value PPP programme have the common goal of positioning Europe as a world leader in creating Big Data Value. Contribution to standardization happens under Task Force 6, which has as main objective to identify applications in which big data technologies can create the biggest impact in Europe. As a matter of example of standards-related activities, BDVA has developed the following actions during 2018:

- Liaison with ISO/IEC JTC1/SC42: At the end of 2017 BDVA established an official liaison with the ISO/IEC JTC1/WG9 with the main objective of channelling European input (cPPP) into global standards.
- Organisation of 2 workshops (BDV CPPP Meetup and EBDVF 2018) and participation in 3 additional workshops (ITU-T FG-DPM meeting, CEN/CENELEC Trustworthy Artificial Intelligence: building a framework with standardization, World Standards Day conference⁶⁶ organised in Brussels on October 12th)
- Data Market Services project, CSA of the BDV cPPP including as one of its pillars standardisation support for SMEs, was selected for funding in 2018 and started in 2019.

Atos, as member of this task force, can disseminate the CAMEL activities related to standardization, and consider other type of actions if they fit with the CAMEL results.

6 Market Analysis, Business Models and Exploitation Strategy

This section provides the initial market analysis, business models and exploitation strategy, which define an appropriate exploitation for the CAMEL results. Market analysis, business models and exploitation strategy will be further expanded on the following standalone deliverables:

- D7.2 Market Analysis and Exploitation Potentials which is due on month 11 (M11).
- D7.5 Road mapping and Business Modelling Report on month 30 (M30).

6.1 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 [28] 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 [29], 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 17 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 17: Prediction on the number of connected cars

Such market trends are well aligned with CARMEL'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.

CARMEL 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 CARMEL's anti hacking solution, ML / AI based cyber-security threats detection and reaction tools. Figure 18 lists a SWOT analysis for the exploitation of CARMEL's proposed solution.

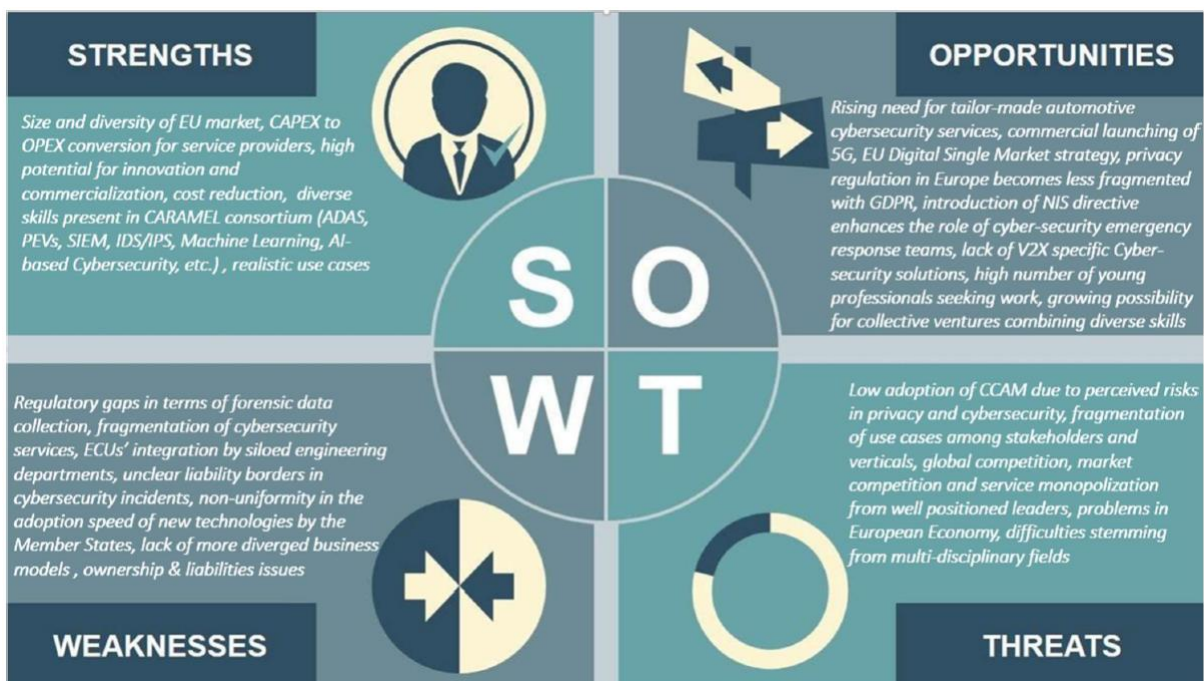


Figure 18: SWOT analysis

6.2 Business plan

The Business Plan is a key enabler for the success of this project and will be developed in Task 7.2 led by 8BELLS. The current section presents a draft plan of the common grounds for the business plan for the main CARMEL outputs. Market positioning the automotive domain and smart transportation in general is a key industrial sector for Europe [30], 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 [31], reduction of traffic fatalities [32], or increased mobility for an ageing population. These societal challenges are strongly supported by the following main technology trends:

- Vehicle electrification [33], 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 [34]], 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) [35] 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 19.



Figure 19: Business model canvas for CAMEL

6.3 Exploitation Action Plan

A brief outline of the envisioned activities to ensure a successful exploitation plan for all CAMEL assets by the end of the project and their market uptake in all corresponding pillars is presented in the Table 18. These activities are covered by WP7.

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 CAMEL 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 18: CAMEL 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 CAMEL results, while trying different models that will be evaluated by the EIB increasing their chances of successful implementation beyond the project timing. CAMEL 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 CAMEL activities.

6.3.1 ***Liaison with open source community***

CARMEL aims at delivering an innovative solution enabling more secure future V2X applications, e.g., CARMEL PKI / AAA manager which can be presented as a security extension to bigger open source initiatives, like ETSI Open Source MANO or open-source tools to simulate CARMEL cyber-attacks. Moreover, CARMEL threat analysis, attack surface modelling, etc. are good candidates to be pushed on MISP. In this way the project outcomes, beyond being exploited by the single project's partners, are disseminated and validated by several interested parties. The outcome of such a R&I interaction might be relevant for EU research and innovation community and open source initiatives. CARMEL will assign, for each of the identified key bodies and open source community, a person in charge of monitoring activities and identify potential collaborations and contributions. On the open source front, CARMEL will try to transfer the gained knowledge and experience to potential open source communities. To do so, in line with its innovation strategy, CARMEL fosters the adoption of open source licenses (e.g., Apache 2.0 [36]) for the developed software solutions within the project. The work on open source implementations will be instrumental to transfer CARMEL lessons learned to external audiences. In this way, the project ensures that the chosen approach on the reference architectures, attack surface models, etc. is relevant to the targeted stakeholders. It also guarantees the long-term adoption of CARMEL solutions.

7 Conclusion

The Deliverable 7.1 “Communication, Dissemination and Exploitation Plan” describes tasks performed and to be performed during the whole project lifetime. It aims to purposefully spread the gathered knowledge and produced results among both general and specialized audiences. D7.1 provides a set of guidelines to be used/followed by CARMEL members.

The task shall be performed consistently to reach not only the expected outcome as proposed by CARMEL but to spread widely the technological achievement in the addressed sectors. The strategy must be carried out not only by digital means but also by participating physically in a variety of events that involve the public from all sectors.

This document will be updated during the lifetime of the project.

8 References

- [1] European Commision, "Glossary," 2018. [Online]. Available: <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/support/glossary>.
- [2] European Commision, "Communication toolkit," Mar 2020. [Online]. Available: <https://ec.europa.eu/easme/en/section/communication-toolkit>.
- [3] European Union, "European Union," Mar 2020. [Online]. Available: https://europa.eu/european-union/about-eu/symbols/flag_en.
- [4] Wordpress, "Wordpress," May 2019. [Online]. Available: <https://wordpress.org>.
- [5] S. Sinek, "TED," Sep 2009. [Online]. Available: https://www.ted.com/talks/simon_sinek_how_great_leaders_inspire_action.
- [6] Twitter, Inc., "Twitter," Mar 2020. [Online]. Available: https://about.twitter.com/en_us/company/brand-resources.html.
- [7] LinkedIn Corporation, Mar 2020. [Online]. Available: <https://brand.linkedin.com/downloads>.
- [8] Youtube, "Youtube," Mar 2020. [Online]. Available: <https://www.youtube.com/about/brand-resources/#logos-icons-colors>.
- [9] V. Beal, "webopedia," Mar 2020. [Online]. Available: <https://www.webopedia.com/TERM/W/Webinar.html>.
- [10] Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels, 18 Dic 2019. [Online]. Available: <https://eetac.upc.edu/ca/noticies/masteam-matt-talks-dr-pouria-sayyad-khodashenas-i2cat-protecting-the-new-generation-of-cars-from-cybercriminals>.
- [11] ERTICO, "ERTICO," Feb 2020. [Online]. Available: <https://ertico.com/>.
- [12] ENISA, "About," Feb 2020. [Online]. Available: <https://www.enisa.europa.eu/about-enisa>.
- [13] COMSOC, "About," Feb 2020. [Online]. Available: <https://www.comsoc.org/about>.
- [14] ECSO, "ECSO," Feb 2020. [Online]. Available: <https://ecs-org.eu/>.
- [15] 5GPPP, "About us," Feb 2020. [Online]. Available: <https://5g-ppp.eu/>.
- [16] Autosar, [Online]. Available: <https://www.autosar.org/>. [Accessed Mar 2020].
- [17] CEN CENELEC, [Online]. Available: <https://www.cencenelec.eu/Pages/default.aspx>. [Accessed Mar 2020].
- [18] ENISA, "CSIRTs Network," [Online]. Available: <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network>.
- [19] ARCADE, "Supporting the CAD initiative," [Online]. Available: <https://connectedautomateddriving.eu/about/arcade-project/>.
- [20] Cyberwatching.eu, "About us," [Online]. Available: <https://cyberwatching.eu/about-us>.

- [21] 3GPPP, "About-3GPP," [Online]. Available: <https://www.3gpp.org/about-3gpp>.
- [22] ETSI, "About us," [Online]. Available: <https://www.etsi.org/about>. [Accessed Mar 2020].
- [23] ISO Technical committees, "ITS Standardization activities of ISO/TC 204," 2019. [Online]. Available: <https://isotc.iso.org/livelink/livelink/Open/19964169>.
- [24] 5GAA, "About us," [Online]. Available: <https://5gaa.org/about-5gaa/about-us/>. [Accessed April 2020].
- [25] CAR 2 CAR Communication Consortium, "Mission & Objectives," [Online]. Available: <https://www.car-2-car.org/about-us/>. [Accessed April 2020].
- [26] Internet research task force, "Overview," [Online]. Available: <https://irtf.org/>. [Accessed April 2020].
- [27] GSMA, "About us," [Online]. Available: <https://www.gsma.com/aboutus/>. [Accessed April 2020].
- [28] BBC, "Fiat Chrysler recalls 1.4 million cars after Jeep hack," Jul 2015. [Online]. Available: <https://www.bbc.com/news/technology-33650491>.
- [29] Mordor Intelligence, "Cybersecurity Market For Cars - Segmented by Solution (Software Based, Hardware Based, Professional Services), Type of Security (Network, Application, Cloud), and Region - Growth, Trends and Forecasts (2018 - 2023)," March 2018. [Online]. Available: <https://www.mordorintelligence.com/industry-reports/global-market-for-cyber-security-of-cars-industry>.
- [30] ACEA, "Automobile Industry Pocket Guide 2016 - 2017," 2016. [Online]. Available: <https://www.acea.be/publications/article/acea-pocket-guide>.
- [31] European Commission, "The Paris Protocol – A blueprint for tackling global climate change beyond 2020," 2015. [Online]. Available: https://ec.europa.eu/clima/sites/clima/files/international/paris_protocol/docs/com_2015_81_en.pdf.
- [32] European Commission, "Road Safety in the European Union," Mar 2015. [Online]. Available: https://ec.europa.eu/transport/sites/transport/files/road_safety/pdf/vademecum_2015.pdf.
- [33] ERTRAC Working Group, "European Roadmap Electrification of Road Transport," Jun 2017. [Online]. Available: http://www.ertrac.org/uploads/documentsearch/id50/ERTRAC_ElectrificationRoadmap2017.pdf.
- [34] ERTRAC Working Group, "Automated Driving Roadmap," May 2017. [Online]. Available: http://www.ertrac.org/uploads/documentsearch/id48/ERTRAC_Automated_Driving_2017.pdf.
- [35] European Factories of the Future Research Association, "Factories 4.0 and Beyond," Sep 2016. [Online]. Available: https://www.effra.eu/sites/default/files/factories40_beyond_v31_public.pdf.
- [36] Apache Software Foundation, "Apache License, Version 2.0," [Online]. Available: <https://www.apache.org/licenses/LICENSE-2.0>.