D7.4

Report of Standardisation, Dissemination, Communication and Digital Presence

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	M33
Actual Delivery Date	M33
Contributing WP	WP7
Project Start Date	01/10/2019
Project Duration	33 Months
Dissemination Level	Public
Editor	AVL, Capgemini (Altran)

Document History		
Version	**Date**	**Remarks**
0.1.0	15.02.2022	Initial TOC was created
0.2.0	31.03.2022	Preliminary content from partners was added to the document
0.3.0	19.05.2022	The first draft of the document was ready
0.4.0	31.05.2022	Review comments were received by UCY and Capgemini
0.5.0	02.06.2022	Review comments were addressed and ready for the SAB submission
0.6.0	27.06.2022	Added latest updates to the relevant sections

DISCLAIMER OF WARRANTIES

This document has been prepared by CARAMEL 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 CARAMEL Project Consortium Agreement, nor any person acting on behalf of any of them:

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

CARAMEL has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement (GA) 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 CARAMEL External Security Advisory Board as well as the Ethics and Data Management Committee (EDC) of the project. Hereby, it is confirmed that it does not contain any sensitive security, ethical or data privacy issues."

Table of Contents

1. List of Acronyms

API	Application Programming Interfaces
BSW	Basic software of contents
CA	Consortium Agreement
DoA	Description of Action
EC	European Commission
EAB	External and advisory board
ECSO	European Cyber Security Organisation
ECU	Electronic Control Unit
EDC	Ethics and data management committee
GA	Grant Agreement
PC	Project Coordinator
PO	Project Officer
POPD	Processing of Personal Data
PSO	Project Security Officer
RTE	Runtime environment Board
ToC	Table of contents
5GAA	5G Automotive Association

2. List of Figures

3. List of Tables

4. Executive Summary

The purpose of the Deliverable D7.4 Report of Standardisation, Dissemination, Communication and Digital Presence is to present the final results of the standardisation, dissemination and communication activities of the project carried out up to M32 with the aim of positioning the project among its stakeholders.

For a better understanding of the activities carried out, D7.4 has been structured into two main areas:

1. Standardization approach addressed in the chapter 2
2. Dissemination and communication activities covered by the chapters 3, 4 and 5.

In relation to the standardization and stakeholder engagement approach followed in the project, this document presents an overview about how the partners in CARAMEL are involved and participating in relevant standards bodies including ISO/SAE21434, AUTOSAR, 5GAAA and the IEEE-SA P2020 working group. Furthermore, the partners are also collaborating with open-source communities and other industrial initiatives such as ECSO or CSIRT.

In relation to the dissemination and communication channels, and despite to the current COVID-19 crisis, CARAMEL has participated in several international conference events in which at least 19 papers and 15 oral presentations have been presented (AI & Big Data Congress (AIBIGDATA) , 93rd Vehicular Technology Conference 2021 (VTC2021-Fall) , 23rd International workshop on Multimedia Signal Processing (IEEE MMSP), ITS International World Congress Hamburg (ITS Hamburg)). During the project implementation time, the consortium organised a couple of tailor-made workshops for the OEMs in order to introduce the project and to present the most important outcomes achieved by the outstanding research of the consortium members (First and second OEM workshop, Joint Standardisation workshops).

Furthermore, the website has been refactored and populated with new contents and social media accounts have been animated providing information about CARAMEL activities and progress. Statistics and information about the key performance indicators are given to measure the impact of these communication and dissemination actions.

1 Purpose and Scope

1.1 *Purpose of the document*

This document, entitled "*Report of Standardisation, Dissemination, Communication and Digital Presence*" is Deliverable D7.4 of the CARAMEL Project within work package WP7 "Dissemination, Communication and Exploitation of Results", and is more specifically related to *T7.1 Dissemination and Maximisation of Project Impact* and *T7.4 Interaction with Relevant Stakeholders, Standardisation*. The main purpose of the document is to detail the various activities that took place during the last phase of the project' regarding communication and dissemination of the CARAMEL project as well the standardization approach followed.

This execution of the dissemination, communication and standardization activities has been based on the plans provided on deliverable *D7.1 Dissemination, Communication and Exploitation Plan* [1] for dissemination & communication of projects results as well as for the outcomes of the standardization actions and links.

1.2 *Structure of the document*

This document is structured in 6 chapters:

- **Chapter 2 Standardisation Approach** introduces the Impact creation through the standardization activities in CARAMEL. Activities which are being carried out in the respective standardisation groups where the partners are actively involved.
- **Chapter 3 Dissemination and Communication channels** provides information about the different dissemination and communications channels utilized to generate awareness about the project and its outcomes. Some channels include the Website, Social Networks like Twitter, Linkedin, etc. and events, among many others.
- **Chapter 4 Dissemination and communication formats** reports all the communication material created in this 1st half of the project to be used in publications, events and digital media.
- **Chapter 5 Monitoring and Evaluation of dissemination & communication activities** presents the methodology for the monitoring and evaluation of dissemination and communication activities, along with the related performance indicators.

  Additionally, **Chapter 1** introduces the overall structure of the document meanwhile **Chapter 6** summarizes the main conclusions of the document.

2 Standardisation Approach

A predefined structure and workflow play a major role in defining the use of software and hardware components. To build any complex environment and system architecture an organized and reliable reference is needed and this is obtained by observing a uniform structure and interfaces in any product development. All these factors resulted for the need of standardization whose focus is to address the challenges in any product development.

In the present scenario, there are several standardization bodies which are active at National, International, and Industrial level. This chapter presents an overview about how the partners in CARAMEL are involved and participating in observing the standards that are relevant to the project. Furthermore, the partners also collaborate with open-source communities and other industrial initiatives. There are many organizations who have published many standards related to cybersecurity, automotive, electrical, electronic and other technologies. To name few organizations and committees.

1. **International Organization for Standardization (ISO)**: An international association for worldwide proprietary, industrial and commercial standards.

2. **European Telecommunications Standards Institute (ETSI)**: An International association for information and communication technologies (ICT) standards.

3. **International Electrotechnical Commission (IEC)**: An international association for electrical, electronic, and related technologies.

4. **Society of Automotive Engineers (SAE**): An international association for automotive standards.

5. **AUTomotive Open System ARchitecture (AUTOSAR):** is a worldwide development partnership to standardize software framework for intelligent mobility.

6. **5G Automotive Association (5GAA**): An international association which contribute to developing the frameworks, practical aspects, required standards, and business cases for 5G and the future application of connected mobility solutions.

7. **IEEE P2020 Standard:** An international working group on automotive imaging standards.

Any committee or organization which deals with standards has technical committees (TC) and subcommittees (SC) to construct suitable standards and supporting documentation. In ISO, there are six defined stages [8].

Stage	**Corresponding docs**
Preliminary	Preliminary work item (PWI)
Proposal	New work item proposal (NP or NWIP)
Preparatory	Working draft (WD)
Committee	Committee draft (CD)
Enquiry	Enquiry draft or Draft International Standard (DIS)

Approval	Final draft (Final Draft International Standard -FDIS)
Publication	International Standard (ISO)

Table 1 Stages and relevant documents to define standards

By following these predefined steps, a suitable standard is developed which can be applied/followed to improve engineering methods or operation of an organization to unify a way of working.

2.1 *Standardisation bodies*

2.1.1 ISO / SAE

In 2021 the UN Regulation No. 155 and an Interpretation document regarding the regulation have been published. The Regulation No. 155 defines requirements for approval of vehicles with regards to cybersecurity and for a so-called cyber security management system (CSMS) (Figure 1).

Also in 2021, the international standard ISO/SAE 21434 was released. This international standard defines requirements for the cybersecurity engineering and defines a framework for the CSMS implementation.

This international standard is accompanied by the publicly available specification ISO PAS 5112 that defines guidelines for the auditing of cybersecurity engineering. The ISO PAS 5112 was published in March 2022.

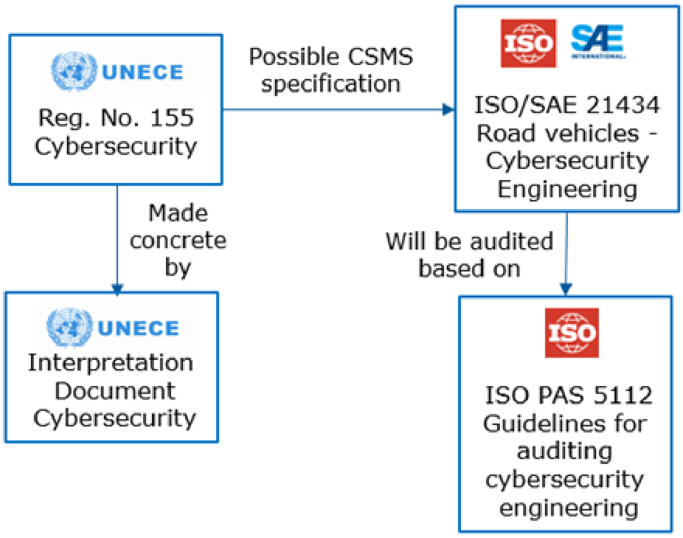

UNECE
Reg. No. 155 Cybersecurity
Possible CSMS specification
ISO SAE
ISO/SAE 21434 Road vehicles - Cybersecurity Engineering
Made concrete by
UNECE
Interpretation Document Cybersecurity
Will be audited based on
ISO
ISO PAS 5112 Guidelines for auditing cybersecurity engineering

Figure 1 Cybersecurity Regulations & Standards [14]

Next to the cybersecurity regulations and standards the topic software updates has been addressed recently. In 2021 the UN Regulation No. 156 and the corresponding Interpretation document have been released (as shown in figure 2). This regulation defines uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (SUMS). A large part of the standard is reflecting the topic of over the air (OTA) software updates.

Like in the UN Regulation No. 155, the UN Regulation No. 156 is also accompanied by a corresponding international standard (Include name of the standard before explain it in the next paragraph). The ISO 24089 defines requirements for software update engineering and the framework for a SUMS implementation. The draft version (DIS) is already available for purchase. The final version should be released end of 2022 the timeline is shown in Figure 3.

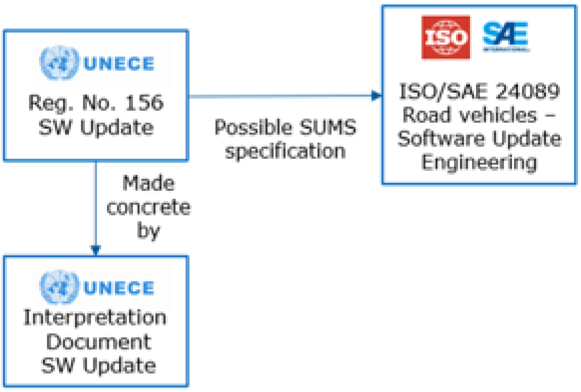


Figure 2 Software Update Regulations & Standards [14]

Security standards often have more varied origins and usually the relevant standards are published by more diverse standardization organizations. Among several of those standards one of the most noteworthy ones include the security management standards ISO/IEC 27000 series, the industrial automation and control systems IEC 62443, and the security certification standard ISO/IEC 15408

The CARAMEL project team includes active members (AVL, PANA, DT-sec) of the ISO/SAE working group. The participation of partners in the relevant standard group meetings ensured that the relevant controls regarding cybersecurity of the standards were considered in the project activities. Relevant project results will be used to propose refinements of relevant controls, if applicable.

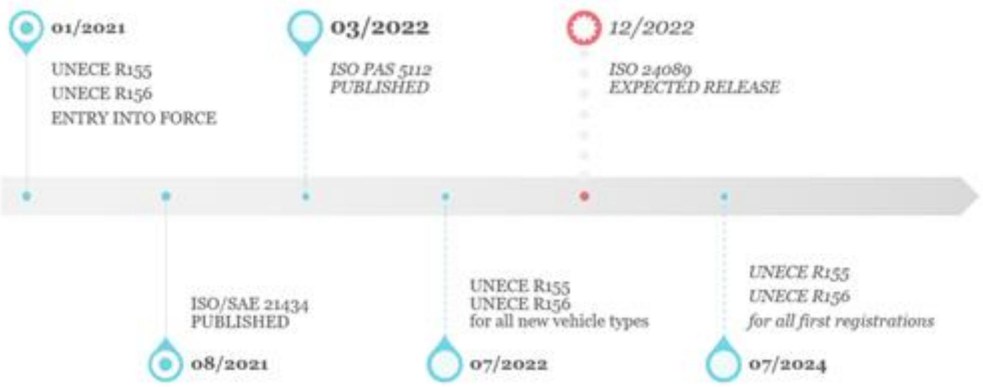


Figure 3 The following picture shows the timeline of the different standards and regulations [14]

2.1.2 ISO/TC 22/SC 32/WG 11

ISO/SAE 21434

The international standard ISO/SAE 21434 addresses cybersecurity in the engineering of E/E systems within road vehicles. The aim of the standard is to cover the different phases of the vehicle development and specify requirements that must be fulfilled in order to ensure an appropriate cybersecurity level.

The standard defines different requirements, recommendations and work products / deliverables that must be created before, during and after the product development. The whole standard is based on a risk-oriented approach as shown in figure 4:

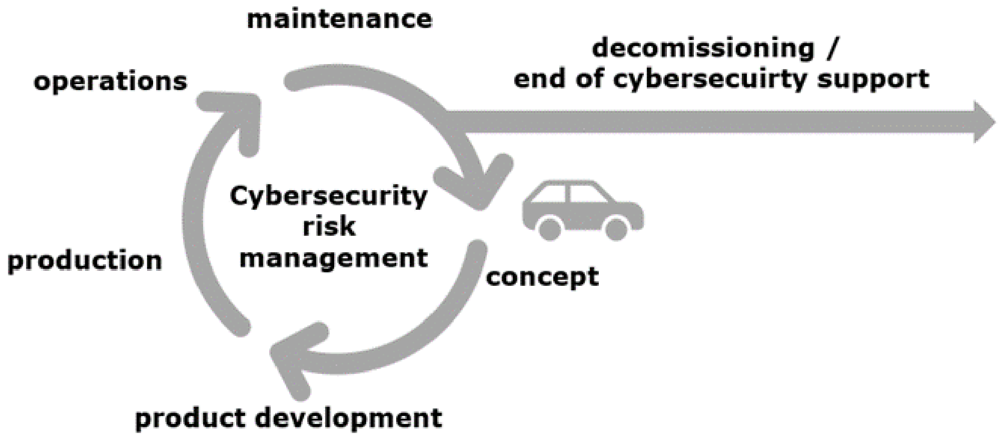


Figure 4 Overall cybersecurity risk management according to ISO/SAE 21434 [14]

The standard is divided into different sections. It consists of the following main areas:

- Organizational cybersecurity management
- Project dependent cybersecurity management
- Distributed cybersecurity activities
- Continual cybersecurity activities
- Concept phase
- Product development phase
- Post-development phase
- Threat analysis and risk assessment methods

ISO PAS 5112

The ISO PAS 5112 Road vehicles – Guidelines for auditing cybersecurity engineering is related to ISO/SAE 21434 and extends ISO 19011 - Guidelines for auditing management systems, to the automotive domain. It is aimed for all organizations within the automotive domains that must conduct audits at the organizational level. The project and product level are not in the focus of ISO PAS 5112.

The ISO PAS 5112 covers the management of an audit programme, the planning and conducting of management system audits and the needed competences of an audit team. It includes a set of audit criteria that are based on the objectives of ISO/SAE 21434. The ISO PAS 5112 also includes an example questionnaire that can be adapted.

According to ISO PAS 5112 the audit team should have specific knowledge and skills in different areas, especially related to road vehicle cybersecurity. The required knowledge and skills are:

- automotive technologies
- road vehicle cybersecurity processes and risk management
- cyber security management systems
- ISO/SAE 21434

The informative questionnaire in Annex A of ISO PAS 5112 covers objectives of ISO/SAE 21434 and can be used by the audit team as a reference. It can also be extended, if needed. The questionnaire includes the following sections:

- Cybersecurity Management (4 questions)
- Continual Cybersecurity Activities (4 questions)
- Risk Assessment and Methods (3 questions)
- Concept and Product development Phase (3 questions)
- Post-development Phase (6 questions)
- Distributed Cybersecurity Activities (1 question)

Each question includes the following topics:

- The question itself
- ISO/SAE 21434 Objectives
- Guidelines for the auditor (Topics that the auditor should verify)
- Evidence examples (e.g., ISO/SAE 21434 work products)

ISO/SAE 21434 and ISO PAS 5112 in CARAMEL context

The recently released automotive cybersecurity ISO standards require capabilities for the monitoring of cybersecurity events and incidents. This should enable fast reaction times in case of newly discovered vulnerabilities and attacks. In order to achieve these monitoring capabilities, it would also be required to implement some kind of security monitoring and intrusion detection within the fleet. At this point the results of CARAMEL can be very useful for achieving the requirements. Partners like AVL are actively involved in following and developing these standards for its compliance in their work.

2.1.3 ISO/TC 22/SC 32/WG 12

ISO 24089 (DIS)

ISO 24089 specifies requirements and recommendations for software update engineering in road vehicles on the organizational and on the project level. The requirements and recommendations apply to the vehicles XCUs and to software updates after the original development. It also defined requirements for the deployment of software updates to road vehicles.

The standard defined requirements and recommendations structured in the following areas:

- Organization level software update requirements
- Project level software update requirements
- Infrastructure design and development
- Vehicle and vehicle systems design and development
- Software update package development
- Software update campaign operations

In addition to the requirements and recommendations the standard ISO 24089 also defines different work products and deliverable, that must be created. The requirements defined here makes sure that the OEMs could follow security logging and intrusion detection system in the cars with which they are working. Partners like AVL is actively involved in following these standards for its compliance in their work.

ISO 24089 in CARAMEL context

The ISO standard 24089 regarding software update engineering goes along with the requirements of the cybersecurity management standards (ISO/SAE 24089 and ISO PAS 5112). The reason is that usually newly discovered vulnerabilities and attacks will require a very fast incident response. In many cases this response will include some kind of software update that has to be implemented in the vehicles, either in the workshop or over the air. Therefore, monitoring and intrusion detection capabilities are needed on the one side, for the discovery of new vulnerabilities and attacks and on the other side, it is also required to monitor the update procedures themselves. The reason is that also updates could be potentially misused by an attacker by implementing own, harmful software updates. Partners like AVL are actively involved in following and developing these standards for its compliance in their work.

2.1.4 *AUTOSAR*

AUTOSAR (AUTomotive Open System ARchitecture) is a worldwide development partnership of vehicle manufacturers, suppliers, service providers and companies from the automotive electronics, semiconductor and software industry.

The primary goal of the AUTOSAR development partnership is the standardization of basic system functions and functional interfaces as shown in figure 5.

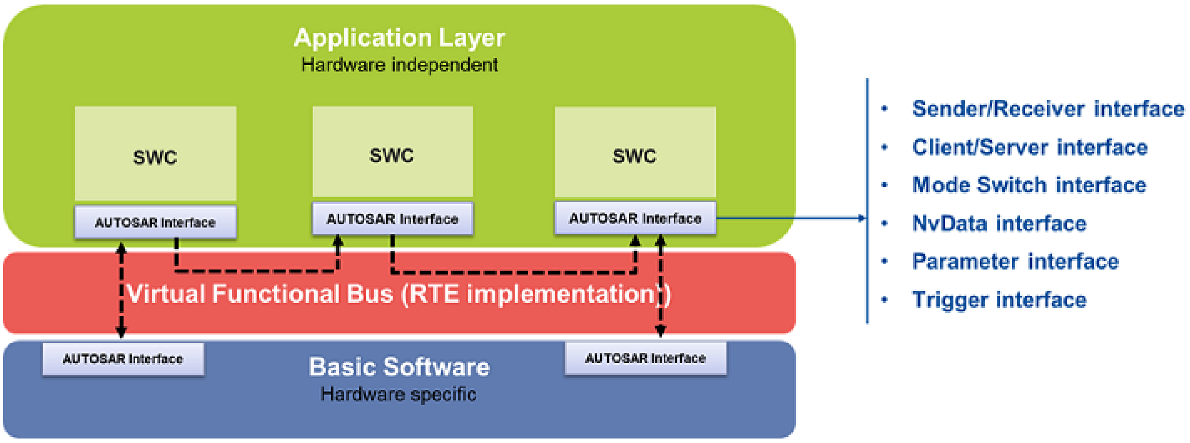


Figure 5 AUTOSAR basic system functions and functional interfaces [15]

Application interfaces:

AUTOSAR standardized a large set of application interfaces in terms of syntax and semantics for the following six vehicle domains: Body and Comfort, Powertrain Engine, Powertrain Transmission, Chassis Control, Occupant and Pedestrian Safety as well as HMI, Multimedia and Telematics.

The focus is on interface specifications of well-established applications in order to emphasize software reuse and exchange, which is considered as one of the main requirements of AUTOSAR. The deployment of standardized application interfaces is a key factor for the reuse of applications.

The application interface descriptions contain a richness of data standardized by experts of all partners. These standardized interfaces allow software designers and developers in case of expanding or reusing software components independent of a specific hardware and/or Electronic Control Unit (ECU).

In general, applications are the competitive edge of an ECU. AUTOSAR is not going to standardize the functional internal behaviour of an application, but the content exchanged between applications. Typical examples of applications are electronic stability control (ESC), steering, electric parking brake, park distance control, exterior light, anti-theft systems, remote keyless entry and so on.

AUTOSAR Classic Platform:

The AUTOSAR Classic Platform design separates three software layers that run on a microcontroller at the highest abstraction level: application, runtime environment (RTE), and basic software (BSW). As seen in the Figure 5, the AUTOSAR specifies a three-layer architecture and they are,

Basic Software (BSW): can be characterized as a standardized software module that provides numerous services required to run the top software layer's functional portion. The ECU-specific modules, as well as the generic AUTOSAR modules, make up this layer.

The BSW is further divided into three sub layers namely, Service layer, Electronic Control Unit (ECU) abstraction layer and the Microcontroller Abstraction Layer (MCAL). The MCAL is a software module that abstracts all of the Microcontroller's highest levels (the application layer and the BSW). As a result, MCAL aids in the independence of the top layers from the low-level hardware platform.

Runtime Environment (RTE): Between the AUTOSAR application layer and the lower levels, this layer works as a middleware. Essentially, the RTE layer is responsible for inter- and intra-ECU communication between application layer components, as well as communication between the BSW and the application layer.

Application layer: The AUTOSAR application layer consists of a number of application-specific software components that are meant to carry out a certain set of functions, depending on the use-case.

AUTOSAR in CARAMEL context:

PANASONIC will provide a state-of-the-art test vehicle equipped with all modern AUTOSAR compatible ADAS components. In case of incompatibilities or missing functionalities, AVL can provide also with an alternative test vehicle platform for the purposes of CARAMEL.

Capgemini, Altran’s parent organization, is premium member of the AUTOSAR consortium, a role we intend to exploit to drive new features, Application Programming Interfaces (APIs), functional and non-functional properties as developed in CARAMEL. The regular AUTOSAR conference also provides the ideal venue to reach the entire Automotive Industry.

2.1.5 *5GAA*

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of companies from the automotive, technology, and telecommunications industries (ICT), working together to develop end-to-end solutions for future mobility and transportation services.

Created on September 2016, the 5GAA unites a large member base, including 8 founding members: AUDI AG, BMW Group, Daimler AG, Ericsson, Huawei, Intel, Nokia, and Qualcomm Incorporated.

Since its inception, 5GAA has rapidly expanded to include key players with a global footprint in the automotive, technology and telecommunications industries. This includes automotive manufacturers, tier-1 suppliers, chipset/communication system providers, mobile operators, and infrastructure vendors. More than 130 companies have now joined 5GAA [3].

As the “5G” in the name implies, the 5GAA strives to promote the use of a single, forward-looking V2X standard based on 5G technology for the communication between vehicles and other vehicles, the roadside infrastructure, and central services.

DT-Sec’s parent company Deutsche Telekom is a member of the 5GAA, Joachim Springer from Deutsche Telekom’s subsidiary T-Systems International GmbH is the current Director General of the 5GAA.

DT-Sec is actively engaged in working on the Misbehaviour detection work item in 5GAA Security working group (WG7). As a result, the 5GAA has published a white paper on misbehaviour detection in the V2X area that includes results from pillar 2 of the CARAMEL project.

2.1.6 *IEEE P2020 Standard*

The IEEE-SA P2020 working group on automotive imaging standards was established to address the considerable ambiguity in measurement of image quality of automotive imaging systems, both human and computer vision based. The white paper, IEEE P2020 Automotive Imaging, outlines the goals, achievements, rationale and plans of the subgroup, which has started to work on development of a new standard.

Image quality plays a crucial role for both automotive viewing and automotive computer vision applications and today's image evaluation approaches do not necessarily meet the needs of such applications. Currently there is not a consistent approach within the industry to measure automotive image quality.The IEEE P2020 working group is attempting to remedy these deficiencies by connecting people in the field, identifying gaps in existing standards, and working to address these by creating a coherent set of key performance indicators by which camera systems and components may be evaluated in a manner that is consistent with their intended use. Panasonic Automotive is leading one of the sections of the Standard addressing the introduction of image quality metrics that are relevant to the accuracy degradation of Computer Vision Algorithms.

Video-based environmental modelling is expected to be one of the major components of an advanced driver assistance system (ADAS) or automated driving system. The process of environmental sensing in ADAS is the result of a complex effect chain consisting of which starts from a light source and ends with the final image stored in memory. In this information transfer chain, the signal could suffer from a variety of intermediate disturbances and Cyber-physical attacks, thus degradation of the signal quality will always take place to some extent. It is important that the system is designed so that enough relevant information about the world is still preserved in the chain. Hence, it is evident that meaningful KPIs need to be defined. Because the tasks of computer vision are so diverse and are solved in many and constantly evolving ways, existing standards such as EMVA 1288 [9], are typically restricted to component-level characterization. However, to cover special automotive use cases, the complete system along the imaging chain must be considered. Existing international standards for image quality, while application based, almost exclusively focus on the case of digital imaging for human consumption. The machine vision use cases of automotive imaging are so diverse, and the penalty for failure so severe in critical cases, that existing standards are inadequate for computer vision automotive application. What might lead to merely acceptable image quality degradation for human consumption may lead to sudden unacceptable failure for a computer vision system.

Traditionally, the evaluation and characterization of components in the imaging chain were covered by specific expertise in the field of each component. For example, optics KPIs such as Modulation Transfer Function (MTF) and such as the quantization of various effects of scattered light in the optical system are not directly compatible with image sensor KPIs like signal-to-noise (SNR) and dynamic range (DR). The overlapping effects between components often do not have a common unified evaluation standard across the component chain. The definition of the components requirements for an ADAS system is a complex procedure. A particular effect observed in the intermediate data flow is not necessarily isolated and it requires a complex analysis of the complete information transfer flow. This means it is necessary to analyse the chain from optical level down to electronic signal level (see Figure 6), and this must be done considering the use cases in which the system is expected to operate. Therefore, it is essential that components are not just characterized as isolated elements, but rather all effects in the chain are well covered under a single framework so that the total system can be appropriately characterized. A signal disturbance, such as the reduced contrast or quality distortion, could still be detected by an image sensor with sufficient contrast detection ability and consequently the Image Signal Processor (ISP) may reconstruct an image that allows detecting the car even in the left-hand side image with a still sufficient detection probability.

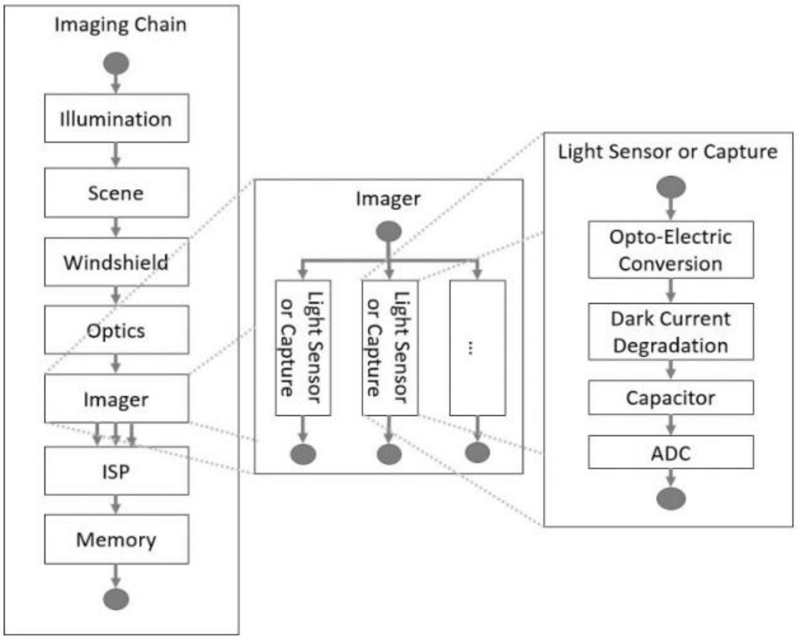


Figure 6 Example flow diagram of an imaging chain [19]

In order to design robust systems for the automotive industry, IEEE P2020 subgroup 3 (Image Quality for Computer Vision on System and Component Level) aims to develop consistent metrics that both describe various degradations and give bounds on their confidence. We will explore the probabilistic approach of distinguishability, such as the contrast detection probability (CDP). This helps to visualize the overall signal chain and aims to improve the cross-domain barrier. CDP is a metric designed to specifically measure this fundamental aspect, using a framework well founded in theory (Geese et al. [10]). Moreover, CDP has the ability to be applied to each element of the imaging system chain, so that the original task can be described at each step in the imaging chain. The P2020 standardization committee has come up with the final document of the standard, which addresses all the fundamental attributes that contribute to image quality for automotive applications. As well as identifying existing metrics and other information relating to these attributes, it defines a standardized suite of objective test methods for measuring automotive camera image quality and key performance indicators designed to assess the severity of signal degradation due to noise introduced through the electronic pipelines and potential cyber attacks. Moreover, it provides baseline test methods and relevant information about tools available to facilitate standards-based communication and comparison of performance among vehicle manufacturers, system integrators, and component vendors regarding automotive image quality 20).

2.1.7 *ITS TC204 adversity group 1*

ITS (Intelligent Transport Systems) is a technology that uses communication technologies to link people, infrastructure, and vehicles to improve road traffic safety, efficiency, and comfort while also contributing significantly to energy and environmental conservation through traffic flow facilitation, such as the elimination of traffic jams.

ITS has the potential to develop new sectors and markets due to its large range of associated technologies and its ability to dramatically alter social and economic structures. ISO/TC 204 is in charge of the overall system and infrastructure aspects of ITS, as well as the coordination of the overall ISO work program in this field, including the standards development schedule, considering the work of existing international standardization bodies. After organising several discussions rounds according to resolution 1489, ISO TC204 was officially resolved to disband its AG1 (Big data and AI) since last 59th ISO TC204 plenary meeting in April. Therefore, unfortunately, there are no more action available for the ISO TC204 regarding CARAMEL.

2.2 *Stakeholder Engagement*

2.2.1 *ECSO*

ECSO (European Cyber Security Organisation) [4] is (was) the partner of the European Commission (EC) for the implementation of the Cybersecurity Public-Private Partnership (PPP). ECSO managed the research, work and recommendations in the area of cybersecurity from both public and private stakeholders, including large companies, SMEs, research centres, universities, operators, end-users, etc. from European Member States and H2020 Programme associated countries.

The main objective of ECSO was to develop the European cybersecurity ecosystem and the advancement of European digital sovereignty. In order to achieve this objective, the organization is composed of different working groups, each of them focusing on different aspects:

- **WG1 standardization, certification and supply chain management** focus on cybersecurity standardization activities and certification.
- **WG2 market deployment, investments and international collaboration** supports activities for market deployment, investments, and collaboration with external European Member States.
- ***WG3 sectoral demand and users committee*** focuses on the needs of different technical and non-technical sectors of Europe in the field of cybersecurity
- **WG4 support to SMEs, coordination with countries and regions** focuses on support and work with SMEs across Europe, obtaining information about their needs and creating taskforces to increase their cybersecurity workforce and collaboration.
- **WG5 education, training, awareness, and cyber ranges addresses the specific education and training activities**. This is a very important aspect of cybersecurity together with the technical one, so the education covers from the universities to learning tools for organizations.
- **WG6 SRIA and cyber security technologies** works on the compilation of needs of different sectors and working groups in order to create an agenda of cybersecurity challenges that is provided to the EC in order to support them for the identification of next objectives in the research and innovation area.

As detailed above, there are different activities and working groups that could be aimed for collaboration in ECSO, specially WG6 (cybersecurity challenges). CARAMEL partners aim at having a close interaction with them and use their results for guiding cybersecurity work in CARAMEL and, on the other hand, provide ECSO with results of the project that can hence be used to enhance their work with real use cases.

2.2.2 *CSIRT*

The EU NIS Directive establishes in Article 12 the CSIRTs Network “to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation” (Full text of the NIS Directive). The NIS Directive, adopted on 6th of July 2016, represents the first EU-wide rules on cybersecurity. The objective of the Directive is to achieve a high common level of security of network and information systems within the EU, by means of improved cybersecurity capabilities at national level, increased EU-level cooperation and risk management, incident reporting obligations for operators of essential services and digital service providers. The NIS Directive is a major milestone towards building cybersecurity resilience on the European level and the Directive entered into force in August 2016.

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 [5].

The Deutsche Telekom CERT has the status “certified” in the ENISA CSIRT inventory and is also an actively contributing member of the FIRST (Forum of Incident Response and Security Teams) [6].

The Deutsche Telekom CERT is an integral part of DT-Sec, since all group-wide security-related activities and projects are centralized in this new company. Therefore, all results from the CARAMEL project will automatically be part of any current and future Deutsche Telekom CERT activities. To this end, DT-Sec feeds project results into the Deutsche Telekom knowledge management system and participates in internal workshops and events to promote re-use of CARAMEL project results.

Since Deutsche Telekom CERT is in turn a certified ENISA CSIRT and member of FIRST, Deutsche Telekom CERT will integrate all relevant CARAMEL results (especially the work done on Backend/SOC integration in the project) into standardization activities in these CSIRT communities where Deutsche Telekom CERT actively participates.

3 Dissemination and Communication channels

Communication channels are the means (online, traditional) through which the CARAMEL consortium keeps informing the interested audience about the project's results and outcomes. This conveyance of information is being carried out through the project's website, social networks and participation at events.

3.1 *Project website*

The website was created to share relevant information to all members of society but specifically at the sector of the population interested in the topics of cybersecurity, machine learning, autonomous mobility, and connected vehicles, which are some of the main topics that CARAMEL focuses on raising awareness. The project website has served as a helpful tool to communicate and disseminate the outcomes being developed in CARAMEL successfully. Interested audience can access the CARAMEL's website through the following link: https://www.h2020caramel.eu/

The CARAMEL website was developed to provide the most straightforward possible navigation by including six main themes accessible and navigable from the homepage: Posts, Consortium, the project, Resources, Upcoming events, and contact us.

- **Posts:** This website constantly publishes the latest news related to the Project in the form of short posts, which usually include a summary of the activity carried out. It is also used to promote upcoming events slightly more detailed than the information contained in social media posts.
- **Consortium:** This section includes a summary and the respective logo of each of the 18-member companies of the CARAMEL consortium. They are constituted by 18 companies located in 9 different countries of the Europe-Asia region.
- **The project:** The Project section has a more general function as it includes Project information such as Project runtime, expected impact, external advisory board, and objectives.
  - **CARAMEL's runtime:** Includes a timeline with the most important events carried out by CARAMEL from month 1 to its last month 33.
  - **Expected Impact:** Includes a short introduction to why cybersecurity became an emerging issue, with information dating back to 2018. It also presents some of the desired results at the end of the project.
  - **External advisory board:** This section introduces the group of experts heading the advisory board in CARAMEL.
  - **Objectives:** The objectives pursued by CARAMEL are presented by listing a set of 8 specific goals.
- **Resources:** The resources section is presented as the most detailed section as it includes a series of multimedia files that can be accessed or downloaded directly from the website or includes an access link in the case of the project's publications.
  - **Automotive Threat modelling:** This page presents a tutorial created by one of the consortium partners, which aims to inform new users about the necessary steps to carry out a threat analysis using the Microsoft Threat Modelling Tool.
  - **Brochure:** The CARAMEL flyer includes relevant information about the project in a summarised way to inform users about the scope and challenges that CARAMEL addresses.
  - **Deliverables:** this page lists all CARAMEL deliverables planned by CARAMEL. Also, in case they have been completed and approved, some of them with the public label are available for direct download.
  - **Multimedia:** As part of the dissemination activities, CARAMEL has created a series of videos that allow you to learn about the project objectives in an informative video. It

also includes the series of demonstration videos that CARAMEL currently has. All videos are embedded directly from the project's official YouTube channel.

- **Publications:** During the project's lifetime, the CARAMEL consortium has produced several publications, which are listed on this page, including a reference link to the original publication.
- **Webinar:** On this page, you will find the Webinars in video format in which the consortium has participated.
- **Workshop:** On this page, you will find the OEM Workshops that CARAMEL has organised to present the results to various OEMs.

- **Upcoming events:** This page presents the scheduled events in which CARAMEL will participate.
- **Contact us:** It includes a contact us form to communicate with the CARAMEL's project and technical coordinator.

It can be highlighted that the website's tree diagram showing the website's organisation was slightly modified compared to the one presented in deliverable 7.1 and 7.3. Figure 7 shows an updated view of the structural tree of the website.

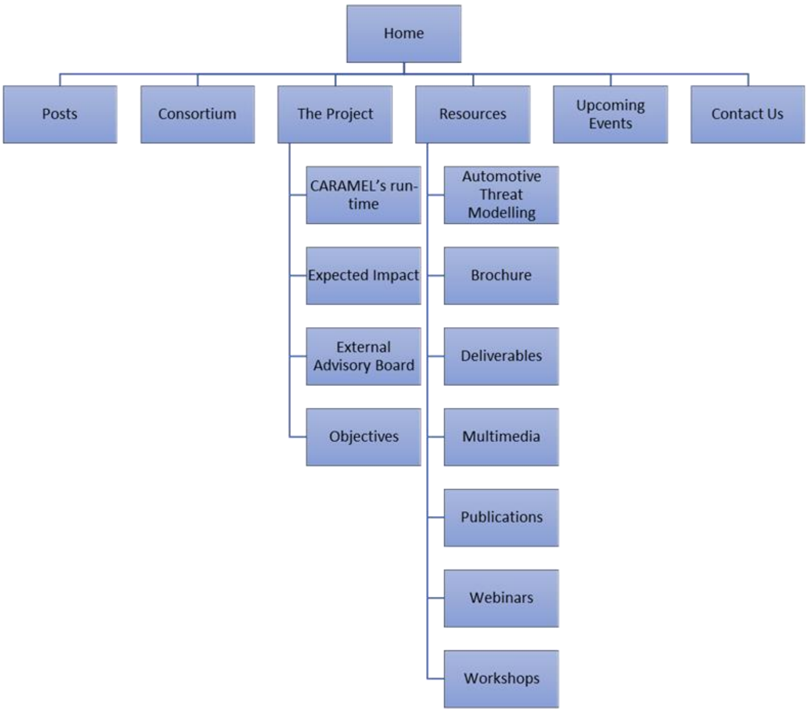
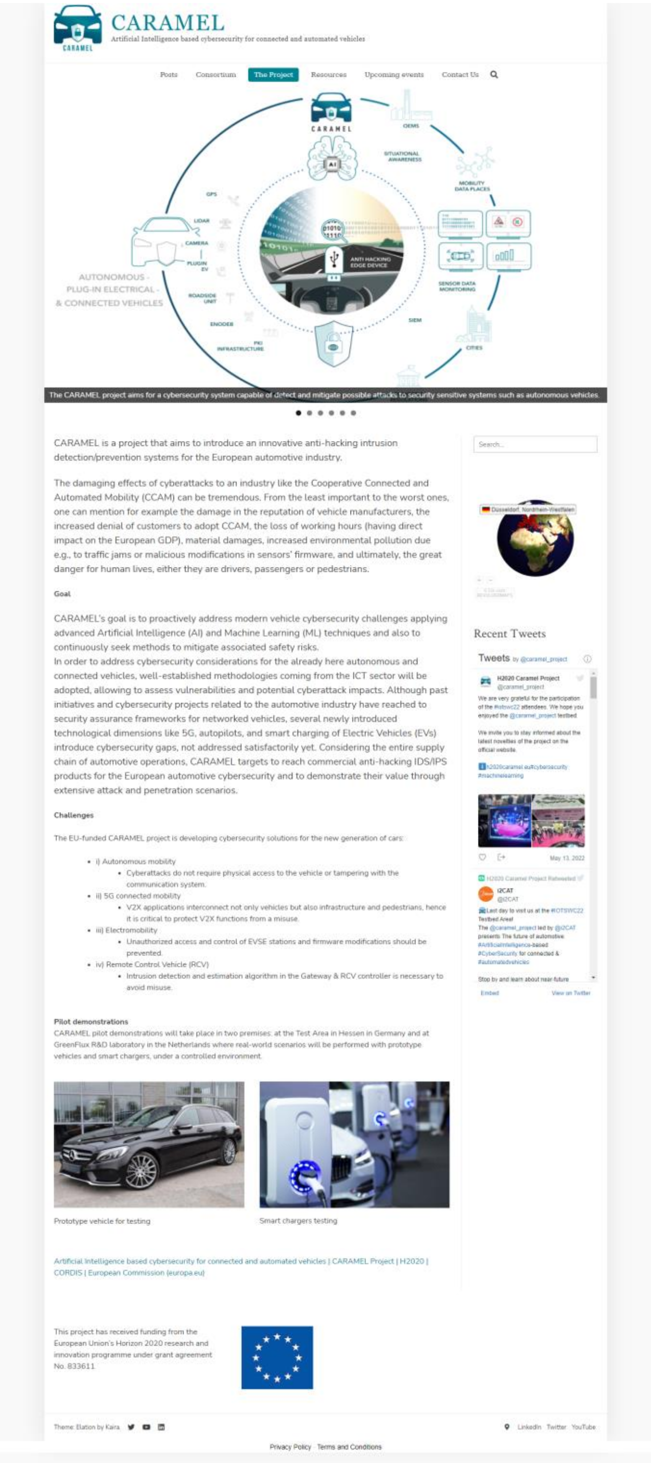


Figure 7 Website Structure Tree

As part of the changes made to the website, among the most relevant the consortium can highlight is a group of new functionalities which allow an intuitive web navigation, such as:

1. Sliding set of new images on the CARAMEL home page.
2. Added subtabs on Resources tab to include Deliverables, Publications and Webinars
3. New section to present the latest events
4. Integration of Bibsonomy to track all the published papers.
5. All public deliverables were uploaded to CARAMEL's website for easier consult.



The CARAMEL project aims for a cybersecurity system capable of detect and mitigate possible attacks to security sensitive systems such as autonomous vehicles.

CARAMEL is a project that aims to introduce an innovative anti-hacking intrusion detection/prevention systems for the European automotive industry.

The damaging effects of cyberattacks to an industry like the Cooperative Connected and Automated Mobility (CCAM) can be tremendous. From the least important to the worst ones, one can mention for example the damage in the reputation of vehicle manufacturers, the increased denial of customers to adopt CCAM, the loss of working hours (having direct impact on the European GDP), material damages, increased environmental pollution due e.g., to traffic jams or malicious modifications in sensors' firmware, and ultimately, the great danger for human lives, either they are drivers, passengers or pedestrians.

Goal

CARAMEL's goal is to proactively address modern vehicle cybersecurity challenges applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques and also to continuously seek methods to mitigate associated safety risks.
In order to address cybersecurity considerations for the already here autonomous and connected vehicles, well-established methodologies coming from the ICT sector will be adopted, allowing to assess vulnerabilities and potential cyberattack impacts. Although past initiatives and cybersecurity projects related to the automotive industry have reached to security assurance frameworks for networked vehicles, several newly introduced technological dimensions like 5G, autopilots, and smart charging of Electric Vehicles (EVs) introduce cybersecurity gaps, not addressed satisfactorily yet. Considering the entire supply chain of automotive operations, CARAMEL targets to reach commercial anti-hacking IDS/IPS products for the European automotive cybersecurity and to demonstrate their value through extensive attack and penetration scenarios.

Challenges

The EU-funded CARAMEL project is developing cybersecurity solutions for the new generation of cars:

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

Pilot demonstrations
CARAMEL pilot demonstrations will take place in two premises: at the Test Area in Hessen in Germany and at GreenFlux R&D laboratory in the Netherlands where real-world scenarios will be performed with prototype vehicles and smart chargers, under a controlled environment.

Prototype vehicle for testing

Smart chargers testing

Artificial Intelligence based cybersecurity for connected and automated vehicles | CARAMEL Project | H2020 | CORDIS | European Commission (europa.eu)

Recent Tweets

Tweets by @caramel_project

H2020 Caramel Project
@caramel_project
We are very grateful for the participation of the #iotswc22 attendees. We hope you enjoyed the @caramel_project testbed

We invite you to stay informed about the latest novelties of the project on the official website.

ℹ h2020caramel.eu#cybersecurity #machinelearning

May 13, 2022

H2020 Caramel Project Retweeted
i2CAT
@i2CAT
Last day to visit us at the #IOTSWC22 Testbed Area!
The @caramel_project led by @i2CAT presents The future of automotive #ArtificialIntelligence-based #CyberSecurity for connected & #automatedvehicles

Stop by and learn about near-future

Embed View on Twitter

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

Theme: Elation by Kaira.

LinkedIn Twitter YouTube

Privacy Policy · Terms and Conditions

Figure 8 CARAMEL website screenshot taken on May 2022

3.1.1 *Website statistics*

The website statistics are helpful to analyse from which part of the world visits were made or which are the most visited sections of the website. For this purpose, interesting data has been collected by using the APIs provided by google analytics and revolver maps. Both are used under a free license.

The website's success can also be analysed by comparing the number of visits the website has had within the second half of the project. It can be said that until May 2022, there have been visits from 100 different countries located on all the habited continents around the world. Figure 9 shows a top view showing the various locations worldwide that have visited the website during the first 32 months of the project.

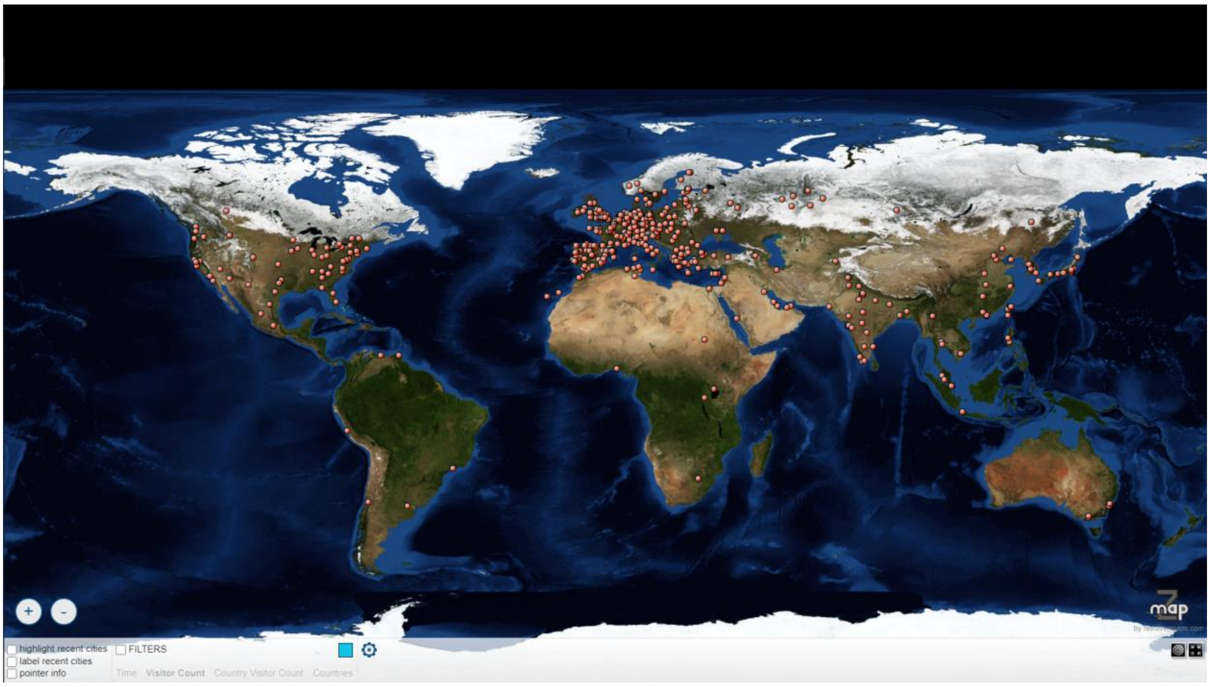
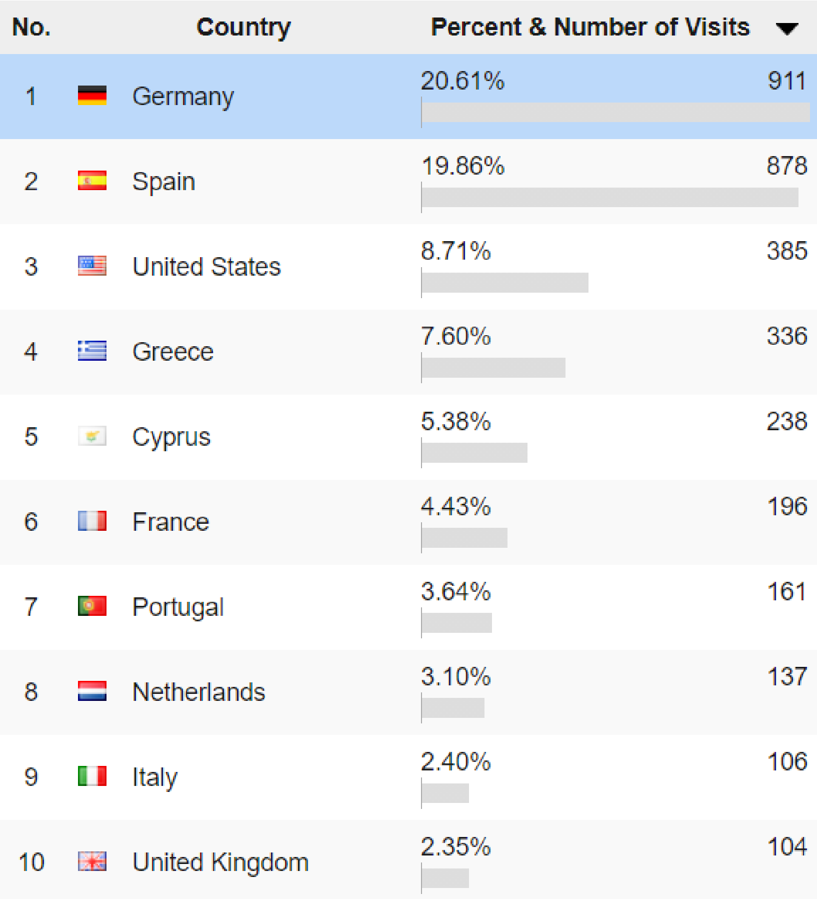


Figure 9 Top View visualizing sessions around the globe

1st half of the Project

It is important to note that despite having achieved a great interest in different parts of the world, the most significant number of visits are concentrated in a few countries, representing 69.8% of the visits, those website's visits correspond to Spain, Germany, USA, Greece, Cyprus, France and Netherlands. From the top ten list of the countries with more visits, it can be seen that the United States is the only country not a member of the European Union. Figure 10 shows the ten countries that provide the highest cumulative number of visits to the website.

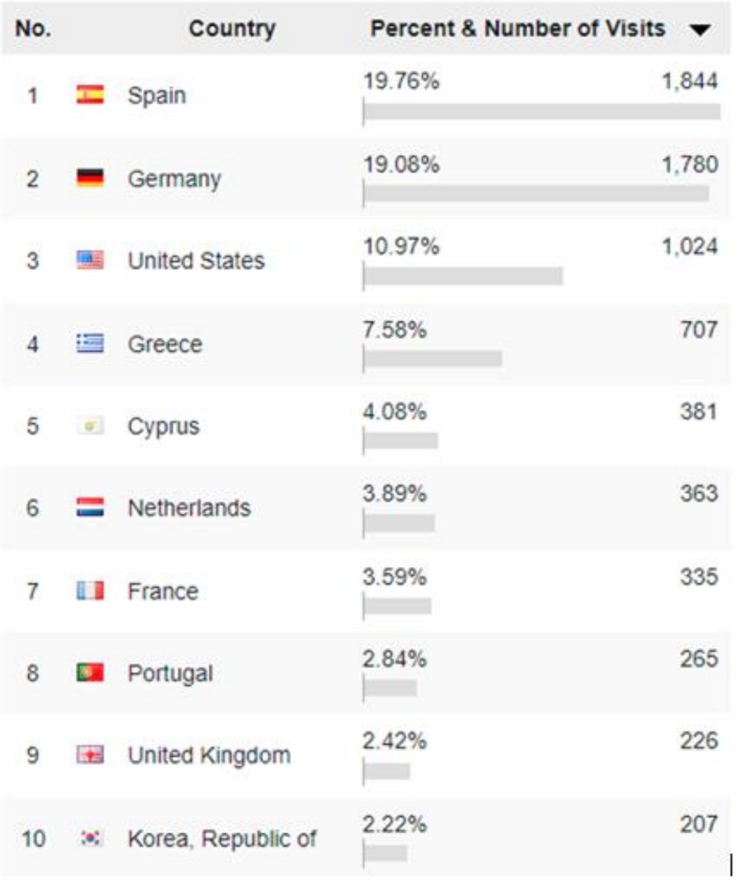


No.	Country	Percent & Number of Visits ▼	
1	Germany	20.61%	911
2	Spain	19.86%	878
3	United States	8.71%	385
4	Greece	7.60%	336
5	Cyprus	5.38%	238
6	France	4.43%	196
7	Portugal	3.64%	161
8	Netherlands	3.10%	137
9	Italy	2.40%	106
10	United Kingdom	2.35%	104

Figure 10 Top 10 countries with most registered visits during the first half of the project

2nd Half of the project

On the other hand, it is interesting to note that during the second half of the execution of the project, the percentage of visits per country has remained stable, with the exception of the visitors from the Netherlands who have increased their interest by surpassing Portugal and France with the number of visits. The list with the most significant number of visits is concentrated in a few countries, representing 68.95% of the visits, these visits to the website correspond to Spain, Germany, USA, Greece, Cyprus, Netherlands and France. Figure 11 shows the ten countries that provide the highest cumulative number of visits to the website during the second half of the project.



No.	Country	Percent & Number of Visits	
1	Spain	19.76%	1,844
2	Germany	19.08%	1,780
3	United States	10.97%	1,024
4	Greece	7.58%	707
5	Cyprus	4.08%	381
6	Netherlands	3.89%	363
7	France	3.59%	335
8	Portugal	2.84%	265
9	United Kingdom	2.42%	226
10	Korea, Republic of	2.22%	207

Figure 11 Top 10 countries with most registered visits during the second half of the project

CARAMEL's website referrals

1st half of the Project

From the referrals to CARAMEL's website, it can be highlighted the percentage of sessions initiated directly from the CARAMELs website link with 46% of the total number of sessions. It is also important that at least 37% of the sessions are accessed through referrals from external search engines, including but are not limited to Google, Bing, etc. Less than 10% of the sessions on the website correspond to links provided through social channels. The visits from social media suggest that a more prominent social channels campaign promoting the CARAMEL's outcomes might substantially increase the users base informed about the latest project activities. For the rest of the visits, 8% correspond to references to the CARAMEL website using direct links from third party websites. Figure 12 shows the percentage of referrals to CARAMEL's website.

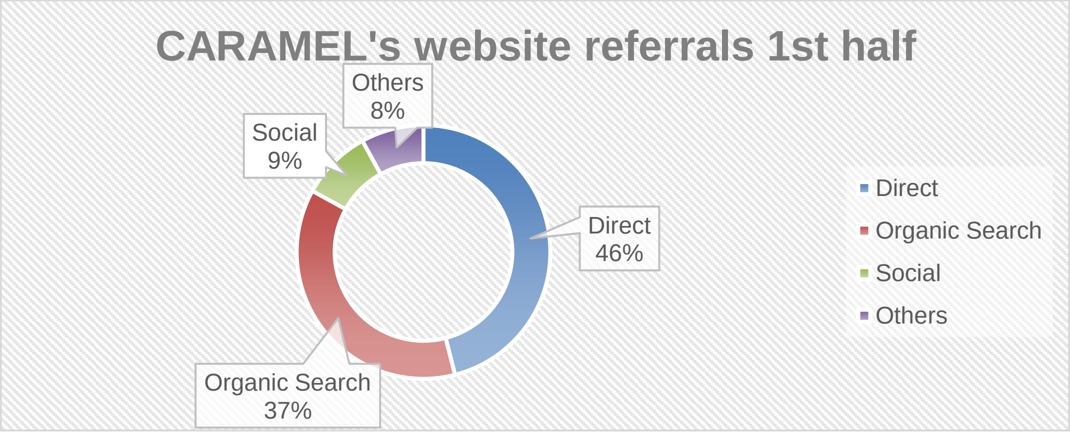
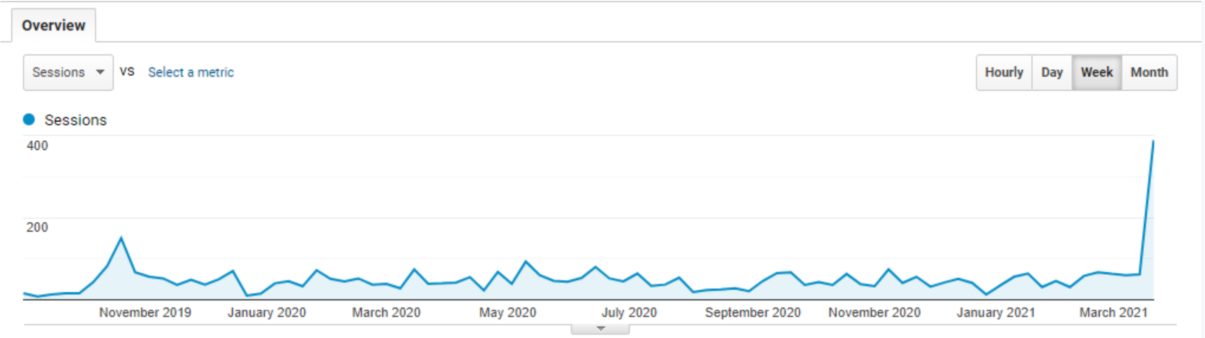
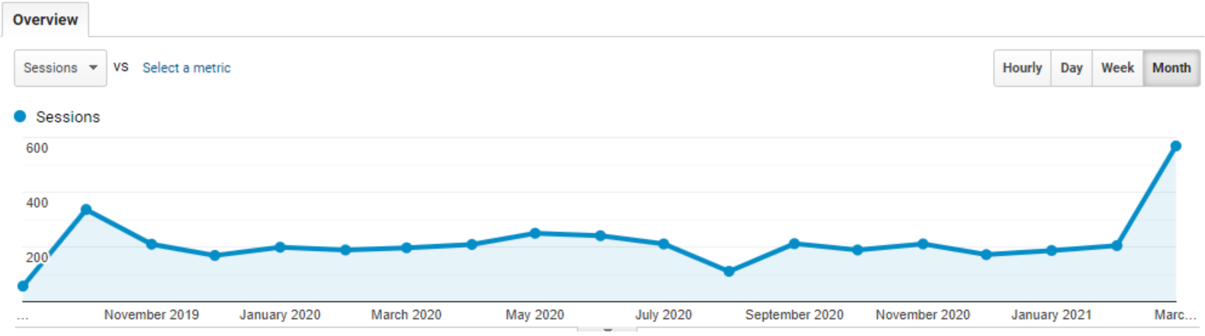


Figure 12 Number of referrals made to the CARAMEL website in 2021

During the project's runtime, different events have taken place in which some project members have participated by presenting papers or holding workshops. It is interesting to distinguish the highest peaks representing an increase in the number of visits to the website. In October 2019, during the starting phase, we can observe a substantial increase in the number of visits to the website, reaching a peak of 337 visits to the project website, as can be observed from the monthly basis analysis in Figure 13.



a) Weekly basis

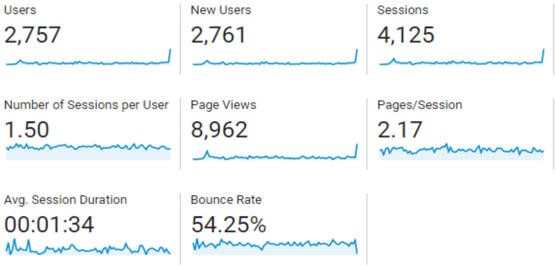


b) Monthly basis

Figure 13 CARAMEL website sessions statistics

The number visitors on the CARAMEL's website have remained constant without notable changes, with an average of 200 users per month. In the months June & July, a slight increase in the website visits is observed coinciding with the participation in the conferences EuCNC, ICTON and ISVLSI. After the second week of July, a small decrease in the weekly number of visits is observed. A second notable increase occurred during September when EWGT and ITSC were held, after which the numbers of visits remain constant until March 2021, one month after the first CARAMEL review.

According to Google Analytics tool as of March 2021. A total of 2761 users have visited the website, which represents 4125 visits to the website. Within this total number of visits, 8962-page views were registered, averaging a total of 2.17 pages visited per user. Figure 14 shows the most relevant website statistics as provided by Google Analytics



Users
2,757

New Users
2,761

Sessions
4,125

Number of Sessions per User
1.50

Page Views
8,962

Pages/Session
2.17

Avg. Session Duration
00:01:34

Bounce Rate
54.25%

Figure 14 CARAMEL website statistics

2nd half of the Project

When analysing the number of visits to the CARAMEL website during the second half of the project, we can observe a reduction in the number of visits to the website through direct access to the website with a reduction of 7% compared to the same segment during the first half of the project to 39% of the total, similarly access through search engines is reduced by 7% to a total of 29% of the total number of visits to the website. The amount of access via social media remains stable at 8%, resulting in an increase in referrals to the website via external websites, which increases by 15% to 23%. Figure 15 shows the percentage of referrals to CARAMEL's website during the second half of the project.

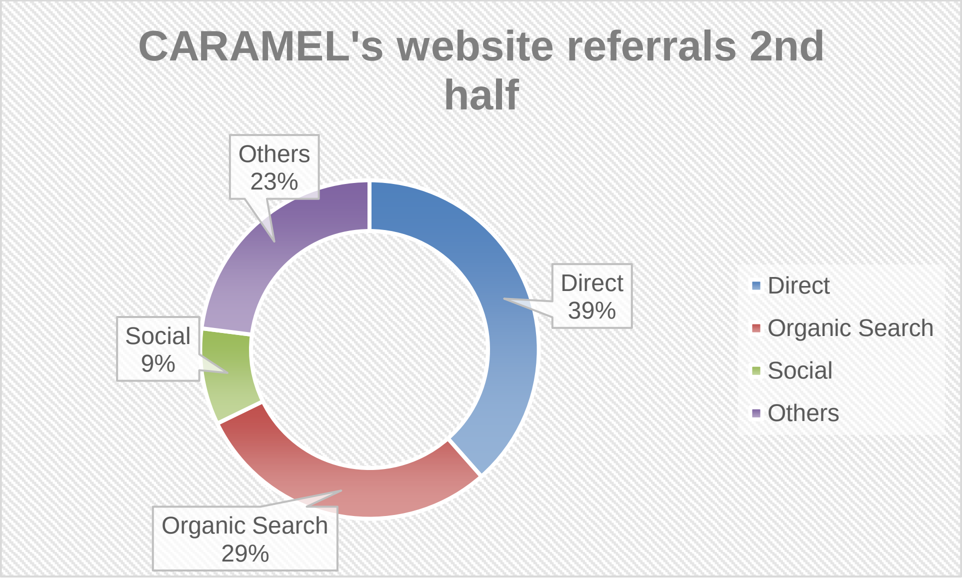
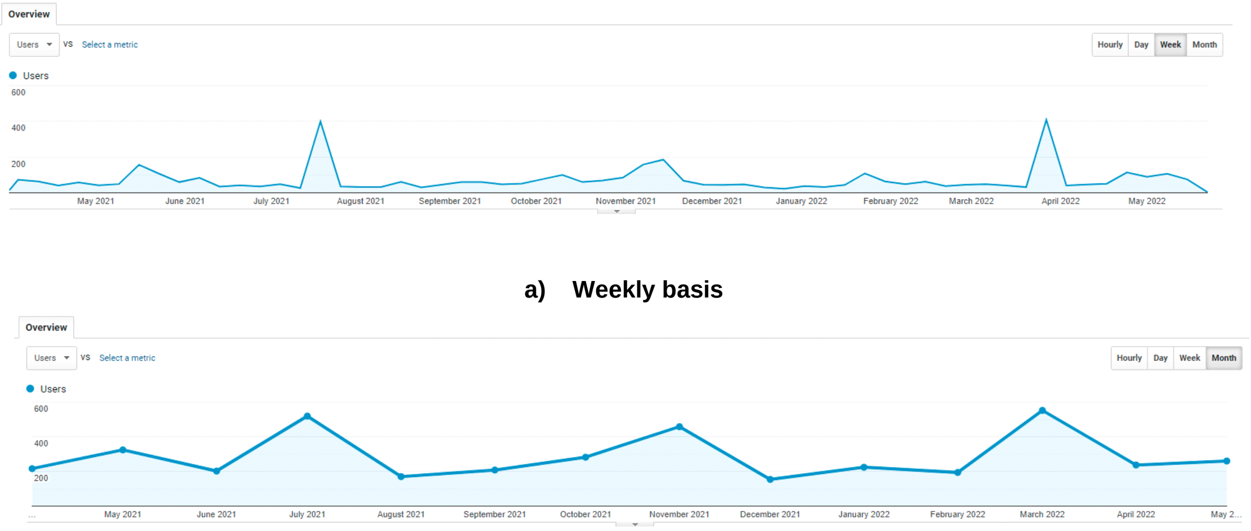


Figure 15 Number of referrals made to the CARAMEL website during the second half of the project

During the second half of the project, events have been held which have had a direct impact on the number of users visiting the project. During the last week of May, we can see an increase of about 40 in the number of visitors to the website which coincides with the event. On the other hand, during July we can observe an increase of 300% in weekly accumulated visits which corresponds to 550 visitors in the same month. Similarly, an increase is observed in the last months of 2021 in which an average number of visits of 430 users per month is registered, which corresponds to an increase of 100% in registered weekly user visits. The last major peak of visits is recorded during March 2022, with around 600 visits per month, but represents an increase of almost 400% compared to the weekly visits during March 2022. Figure 16 shows the monthly and weekly average of visits registered during the second half of the project.

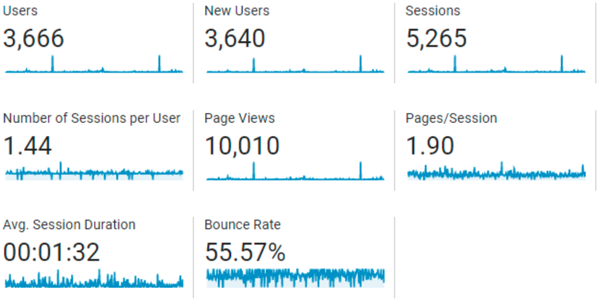
During most of the time of the second half of the project's life a stable number of visitors of approximately 200 visits per month is registered. However, certain months stand out due to the high number of visitors to the CARAMEL website due to the importance of the events disseminated through the social networks. The first example of this increase in users pertains to the dissemination of the first workshop for OEMs which took place during May. In the final weeks of July, a campaign to disseminate the results achieved was carried out through the creation of a series of demonstration videos presenting the most outstanding results of the CARAMEL project. It is important to highlight that the next increase of users interested in the project happened during the promotion of the 2nd OEM workshop organised by the CARAMEL consortium and which aimed to present the results of the project to potential OEMs, an event that took place during the second half of November 2021. The last major peak of users was registered during March 2022, coinciding with the participation in the proactive dissemination of the project through the activities of the DATE2022 conference, in which the project participated in a panel session planned to discuss research directions in Europe.



a) Weekly basis

Figure 16 CARAMEL website sessions statistics during second half of the project

From the information extracted from the analysis of visits during the second half of the project (Google analytics), it can be seen that a total of 3666 users were interested in the project, reaching around 10k views of the various sections of the website, representing a total of 1.9 pages per session. Figure 17 shows the most relevant website statistics during the the second half of the project as provided by Google Analytics.


Users 3,666

New Users 3,640

Sessions 5,265

Number of Sessions per User 1.44

Page Views 10,010

Pages/Session 1.90

Avg. Session Duration 00:01:32

Bounce Rate 55.57%

Figure 17 CARAMEL website statistics during second half of the project

3.2 *Social Networks*

Besides the CARAMEL website, social media channels are also being updated, such as Twitter and LinkedIn, enabling a direct communication with possible stakeholders about the addressed project's topics. It can be said that the social media channels had facilitated effective and fast communication to spread the latest project outcomes. This interaction helped us to reach an audience from all the habited continents around the world.

As a fundamental part of analysing the project's engagement with social network users, statistics collected within the social networks are analysed for each social media.

3.2.1 *Twitter statistics*

1st half of the Project

As of March 2021, the project has made a total of 70 tweets, which corresponds to an average of 4 tweets per month. So far in the project, the interaction on Twitter has achieved an average of 5400 impressions per month, which means the number of post's views produced through the social network. Figure 18 shows the accumulated number of impressions made through Twitter, during the project's lifetime.

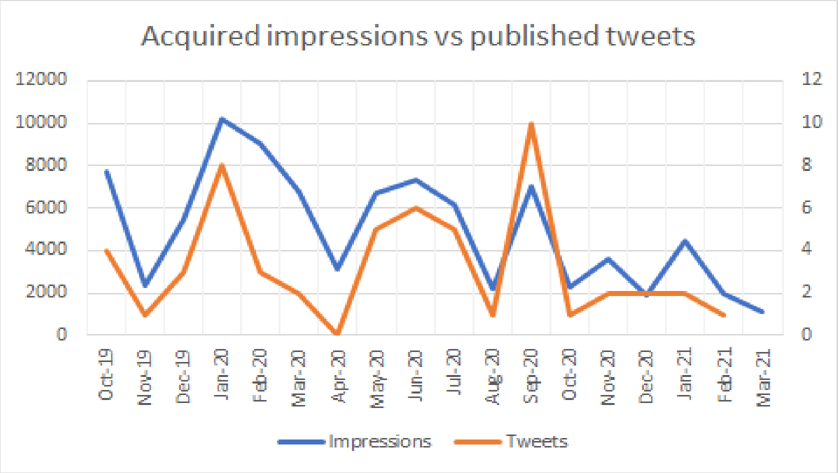


Figure 18 Monthly CARAMEL's Twitter impression during the first half of the project

In Figure 18 we can see the number of users reached through the use of tweets in more detail. A set of points representing the most achieved impressions can be highlighted, especially in October 2019, which marks the beginning of the project's life. January 2019 was the date on which the most significant number of tweets were made. June and September were the dates in which many events were held and promoted through the Twitter social network. Similar behaviour can be observed to the results presented in Figure 9, which showed a slight increase in visits in the same months. The aforementioned data suggest that a social network campaign considerably increases the dissemination activities.

As of 24 March 2021, the project's official Twitter account has been followed by 184 different users, suggesting that the project is relevant to a large community sector that encompasses other projects and individual users interested in the topic addressed by CARAMEL. As part of the analysis of the information shared on Twitter, a cloud tag analysis is added that visualises the most used words in the tweets made. It can be seen in Figure 19 that connected, mobility, workshop, project, cybersecurity and caramel are the most used words.

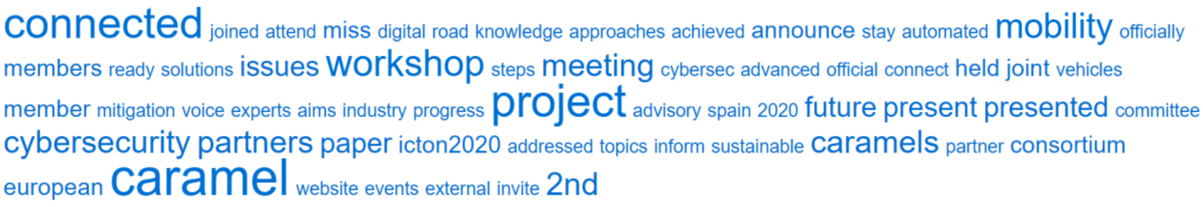

connected joined attend miss digital road knowledge approaches achieved announce stay automated mobility officially
members ready solutions issues workshop steps meeting cybersec advanced official connect held joint vehicles
member mitigation voice experts aims industry progress project advisory spain 2020 future present presented committee
cybersecurity partners paper icton2020 addressed topics inform sustainable caramels partner consortium
european caramel website events external invite 2nd

Figure 19 CARAMEL's Twitter cloud tag

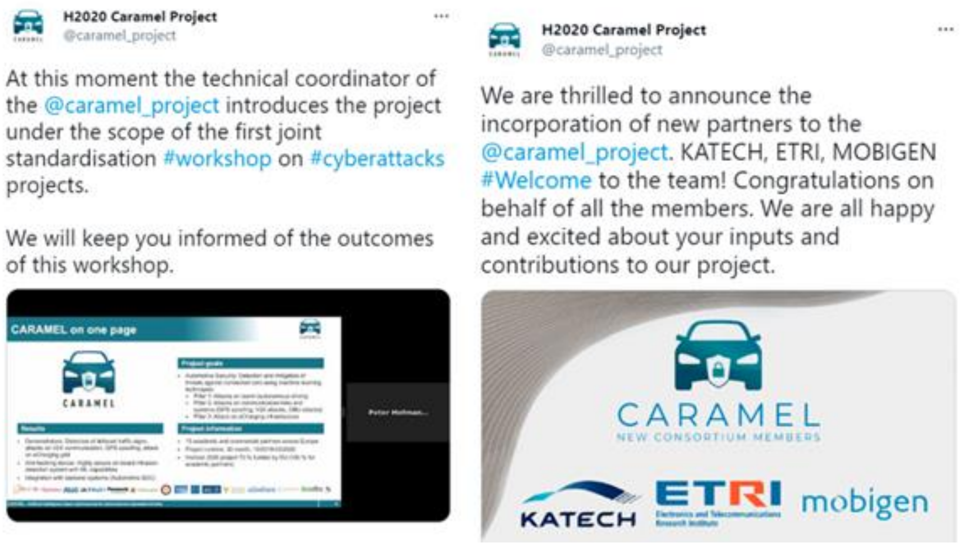
To have an effective social media communication, the CARAMEL Twitter account used a set of relevant hashtags aiming for maximum diffusion. This strategy used a diverse group of hashtags aiming to connect with an already interested audience, always trying to maintain the central core addressed by the project. Examples of the hashtags used by CARAMEL on all of its posts can be seen in Table 1.

#cybersecurity	#mobility	#webinar	#5g
#ai	#eu	#ccam	#future
#h2020	#road	#taxonomy	#cyber
#risk	#safety	#greener	#connectivity

Table 2 CARAMEL Hashtags

In Table 1, a slight deviation can be observed from the hashtags proposed in deliverable 7.1. However, it is still consistent with the central theme addressed by the project.

As part of our ongoing activities in the dissemination strategy, CARAMEL identified the most exciting tweets for the past six months, which achieved many engagements. Some of CARAMEL top tweets can be seen below in Figure 20



H2020 Caramel Project
@caramel_project

At this moment the technical coordinator of the @caramel_project introduces the project under the scope of the first joint standardisation #workshop on #cyberattacks projects.

We will keep you informed of the outcomes of this workshop.

H2020 Caramel Project
@caramel_project

We are thrilled to announce the incorporation of new partners to the @caramel_project. KATECH, ETRI, MOBIGEN #Welcome to the team! Congratulations on behalf of all the members. We are all happy and excited about your inputs and contributions to our project.

Figure 20 CARAMEL twitter from 22 Jan 2021 (Left) CARAMEL twitter from 10 Nov 2021 (Right)

The Twitter post from Figure 20 (left) shows the most impactful tweet, which achieved 2470 impressions with 79 engagements.

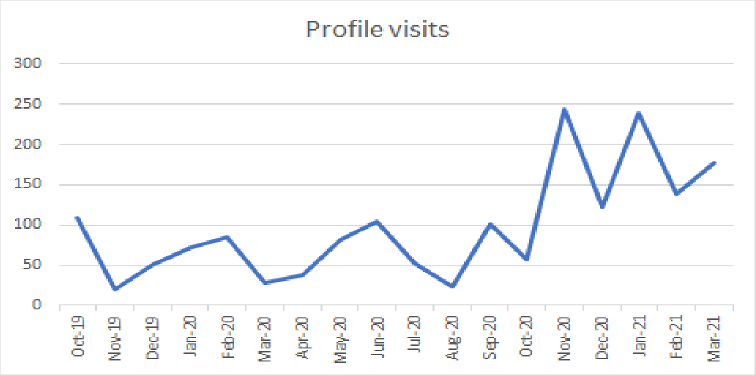


Figure 21 Monthly CARAMEL's profile visits

It is interesting to summarise that the communication strategy through tweeting has managed to reach a large audience. It is pleasing to note that the number of users visiting CARAMEL's profile has increased as the project has progressed. As shown in the Figure 21 in the last three months, there have been many users interested in the project.

2nd half of the Project

As of May 2022, the project has made a total of 133 tweets, which corresponds to an average of 4 tweets per month. So far in the project, during the second half of the project the interaction on Twitter has achieved an average of 3100 impressions per month, which means the number of post's views produced through the social network. Figure 22 shows the accumulated number of impressions made through Twitter during the second half of the project.

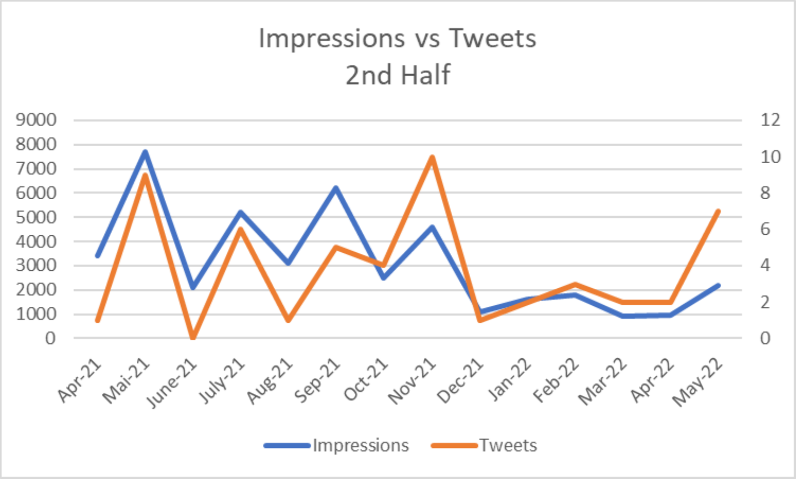
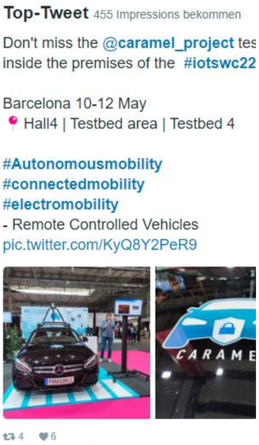


Figure 22 Monthly CARAMEL's Twitter impression during the second half of the project

The Figure 23 shows a summary of the twitter posts with the highest number of impressions, which coincide with some of the most important activities of the CARAMEL project. Such as the participation in the IoTS WC, AI&BigData congress, the publishing of the demo videos, and some of the organised workshops.



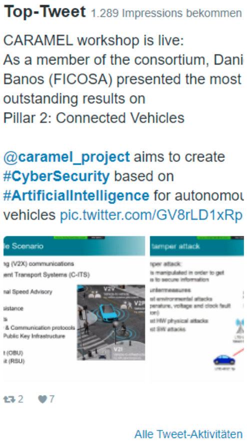
Top-Tweet 455 Impressions bekommen

Don't miss the @caramel_project tes
inside the premises of the #iotswc22

Barcelona 10-12 May
📍 Hall4 | Testbed area | Testbed 4

#Autonomousmobility
#connectedmobility
#electromobility
- Remote Controlled Vehicles
pic.twitter.com/KyQ8Y2PeR9

4 ♥ 6



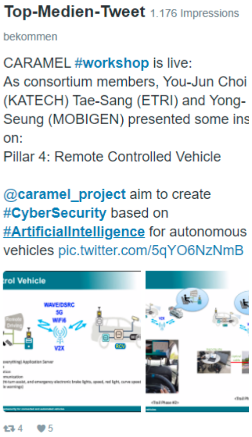
Top-Tweet 1.289 Impressions bekommen

CARAMEL workshop is live:
As a member of the consortium, Dani
Banos (FICOSA) presented the most
outstanding results on
Pillar 2: Connected Vehicles

@caramel_project aims to create
#CyberSecurity based on
#ArtificialIntelligence for autonomou
vehicles pic.twitter.com/GV8rLD1xRp

2 ♥ 7

Alle Tweet-Aktivitäten

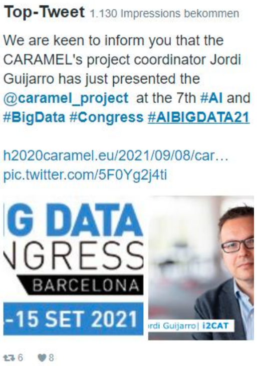


Top-Medien-Tweet 1.176 Impressions bekommen

CARAMEL #workshop is live:
As consortium members, You-Jun Choi
(KATECH) Tae-Sang (ETRI) and Yong-
Seung (MOBIGEN) presented some ins
on:
Pillar 4: Remote Controlled Vehicle

@caramel_project aim to create
#CyberSecurity based on
#ArtificialIntelligence for autonomous
vehicles pic.twitter.com/5qYO6NzNmB

4 ♥ 5

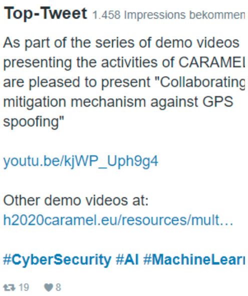


Top-Tweet 1.130 Impressions bekommen

We are keen to inform you that the
CARAMEL's project coordinator Jordi
Guijarro has just presented the
@caramel_project at the 7th #AI and
#BigData #Congress #AIBIGDATA21

h2020caramel.eu/2021/09/08/car…
pic.twitter.com/5F0Yg2j4ti

6 ♥ 8



Top-Tweet 1.458 Impressions bekommen

As part of the series of demo videos
presenting the activities of CARAMEl
are pleased to present "Collaborating
mitigation mechanism against GPS
spoofing"

youtu.be/kjWP_Uph9g4

Other demo videos at:
h2020caramel.eu/resources/mult…

#CyberSecurity #AI #MachineLearı

19 ♥ 8

Figure 23 Top Tweets during the second half of the project

As of 24 May 2022, the project's official Twitter account has been followed by 230 different users, suggesting that the project is relevant to a large community, mostly interested in the topics listed in Table 2. In the context of the analysis of information shared on Twitter, a cloud tag analysis is added which visualizes the words most used in the tweets made. Figure 24 shows that the words 'project', 'caramel', 'workshop', '2nd OEM are the most frequently used keywords.

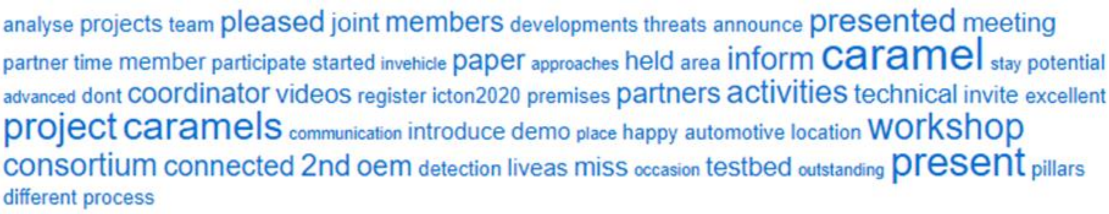


Figure 24 Cloud tag analysis until May 2022

#workshop	#cybersecurity	#iotswc	#5g
#mobility	#itshamburg2021	#ccam	#ai
#cyberattacks	#aiwe	#autonomousdriving	#future
#icton2020	#electricvehicles	#autonomousvehicles	#futuremobility
#evehicles	#v2x	#artificialintelligence	

Table 3 CARAMEL hashtags until May 2022

3.2.2 *LinkedIn statistics*

While some social networking sites focus on attracting a casual audience, Linked, **https://www.linkedin.com/in/caramel-project-3974a617b/**, focuses on connecting users in a more formal way. That said, it is possible to analyse not only the number of users visiting the site but also to identify the most common job position of the users attracted by the topics investigated by CARAMEL, their experience, the country from which the connection is made and the type of industry to which the users are related.

1st Half of the project

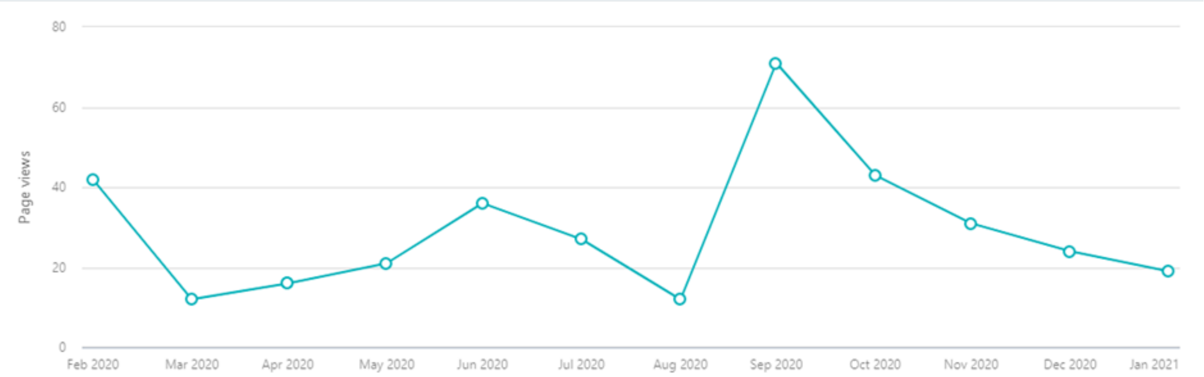


Figure 25 Visits made on CARAMEL´s LinkedIn account

Figure 25 shows the number of visits registered on LinkedIn from Feb2020 until Jan2021. Overall, it can be seen that during September it reaches its highest numbers of accumulated visitors in a month and coincides with the events carried out in Cyprus, on where our colleagues made an event EWGT2020.

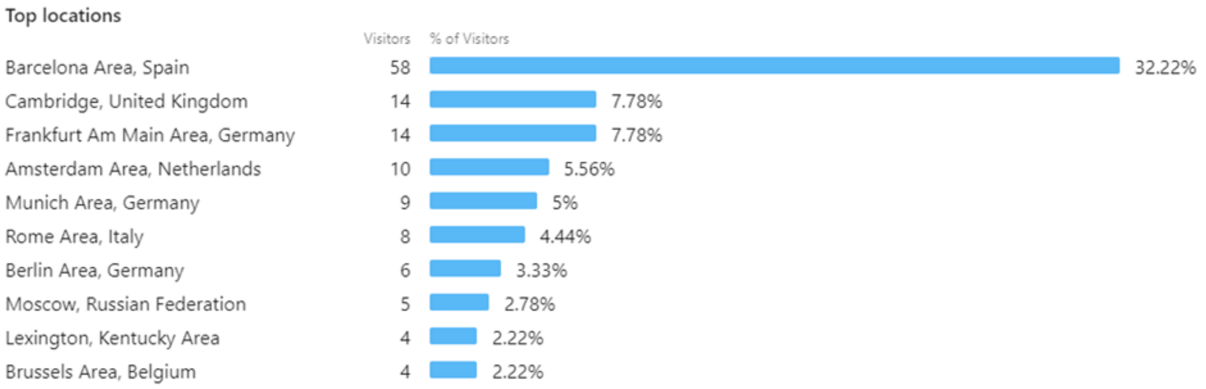


Figure 26 Top 10 Countries visiting CARAMEL's LinkedIn account

The bar chart in Figure 26 highlights the countries with the most visits to the LinkedIn website. A comparative analysis of the different visits to the CARAMEL website shows that Spain is the country with the highest number of visits, followed by Germany. It is important to note that the United States does not appear among the countries with the most visits to the site. Still, the UK, the Netherlands and Moscow are among the most visited countries even when they do not contribute to the same extent in the number of visits to the website as shown in Figure 27.

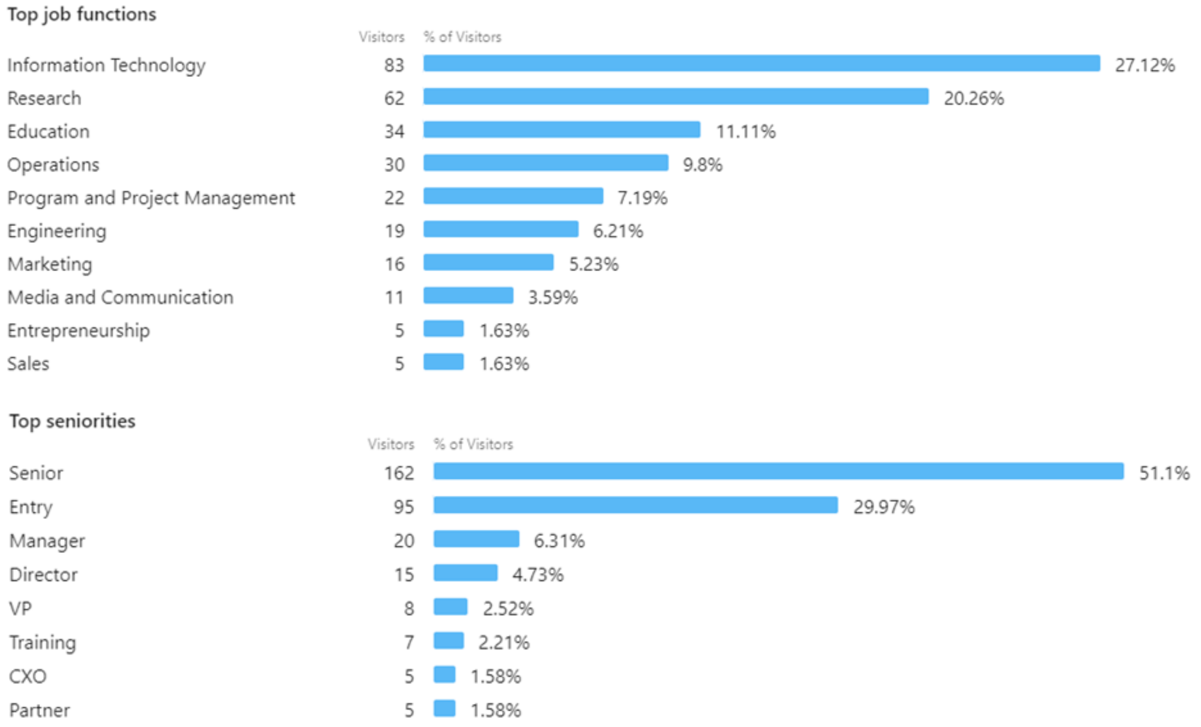
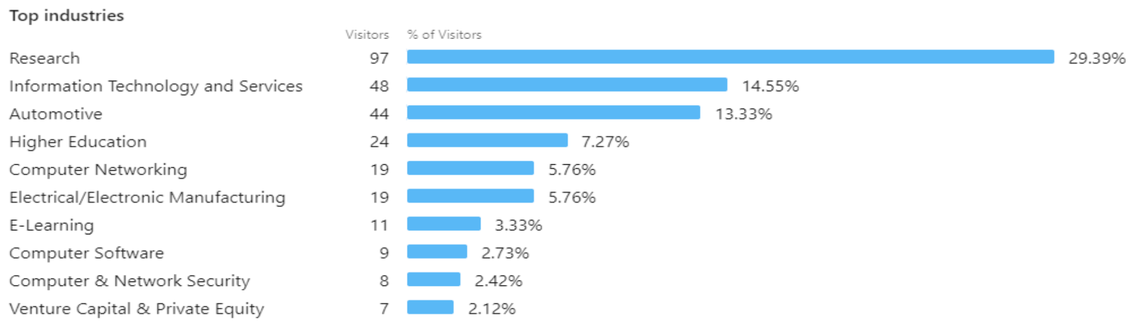


Figure 27 Top 10 visitor's job functions and seniority visiting CARAMEL's LinkedIn account



Top industries

	Visitors	% of Visitors
Research	97	29.39%
Information Technology and Services	48	14.55%
Automotive	44	13.33%
Higher Education	24	7.27%
Computer Networking	19	5.76%
Electrical/Electronic Manufacturing	19	5.76%
E-Learning	11	3.33%
Computer Software	9	2.73%
Computer & Network Security	8	2.42%
Venture Capital & Private Equity	7	2.12%

Figure 28 Top 10 industries visiting CARAMEL's LinkedIn account

Figure 28 shows the associations of visitors to a given industry. It can be seen that almost 30% of the registered visits come from a research association that is useful for disseminating results. There is a remarked fall in the percentage of visitors from Information and Technology industries with slightly less than 15%, closely followed by the automotive industry with 13% of the total number of visitors. The information, as noted above, is handy because it represents the project's subject matter audience from different sectors.

2nd Half of the project

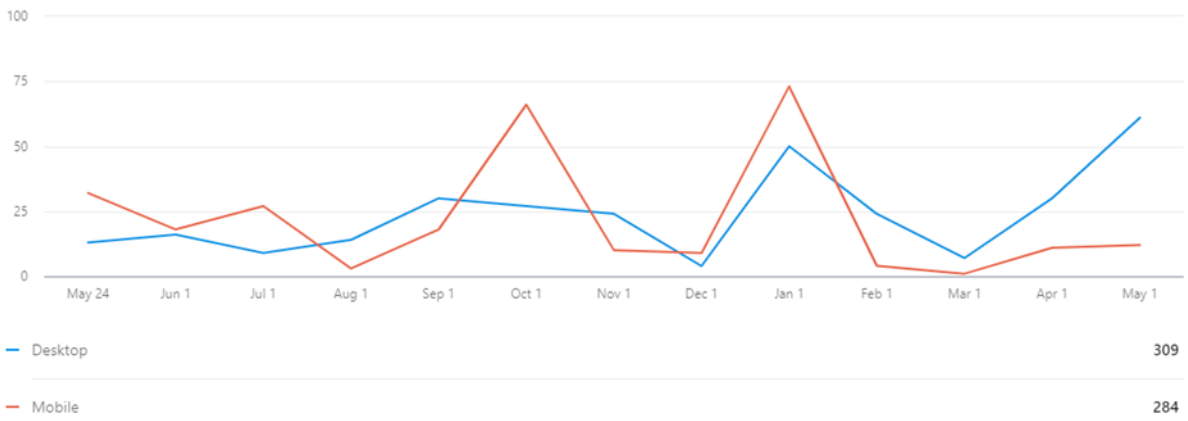


Figure 29 Visits made on CARAMEL's LinkedIn account

Figure 29 shows the number of visits registered on the official CARAMEL LinkedIn page from May 2021 to May 2022. Large peaks in the number of visitors using mobile devices can be observed during October and January 2021, which coincide with CARAMEL's participation in ITSHamburg2021 and the CARAMEL technical meeting, respectively. It is worth noting the number of users who visited the project profile, regardless of the device used, as we can see a peak of 90 and 125 visits to the CARAMEL profile for the months of October and January, respectively. Another notable event is the IoTS WC which took place in May 2022, and produced an increase in visitors during that month, reaching almost seventy visitors.

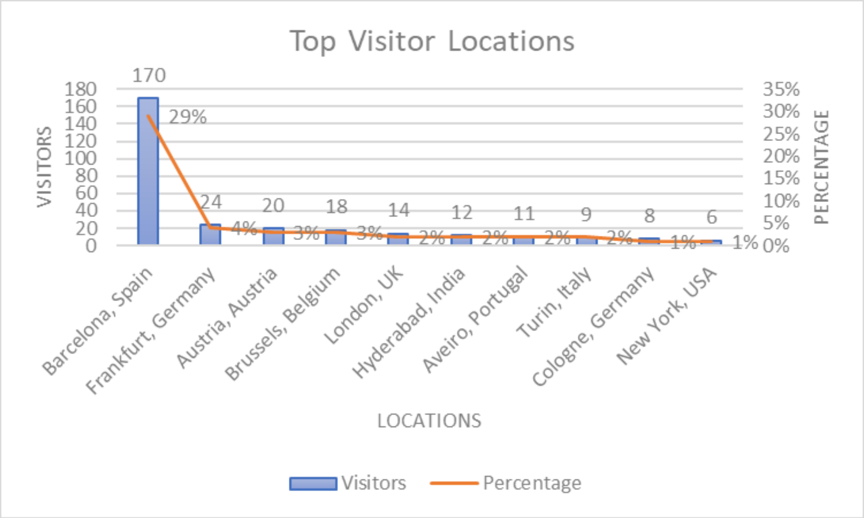


Figure 30 Top 10 Countries visiting CARAMEL's LinkedIn account

Figure 30 highlights the top ten countries with the highest traffic to CARAMEL's LinkedIn profile. It can be clearly seen that Barcelona is the location with the highest interest, with 29% of the total number of visits, followed by Frankfurt with 4%, slightly behind Austria, and Brussels, with 3% of the total visits each. It is interesting to point out a small interest from non-EU countries such as the UK, India and the USA which are in the top ten locations with more registered visits.

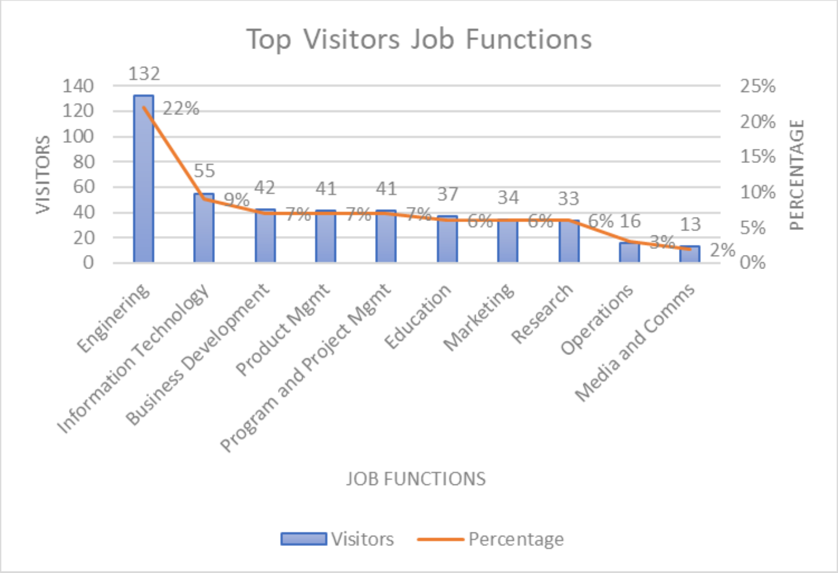


Figure 31 Top 10 visitor's job functions visiting CARAMEL's LinkedIn account

Figure 31 shows the percentage of visitors' roles in a company visiting the LinkedIn account, it can be observed that the role of engineering is the top job role representing 22% of the total visits in the analysed period, followed by Information technology roles with 9%, business development and management roles which reaches 7% each. This data suggests that within the analysed period in the second half of the project LinkedIn is an excellent way to connect with applied science and business stakeholders.

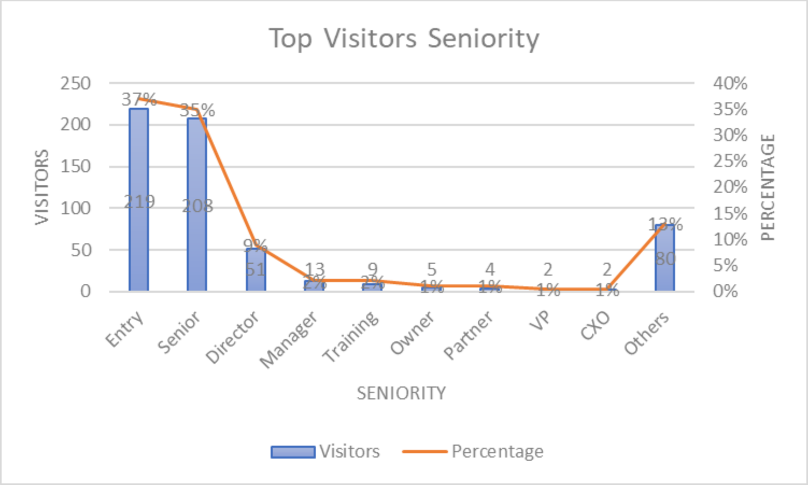


Figure 32 Top 10 visitor's seniority visiting CARAMEL's LinkedIn account

Regarding the experience of visitors to the CARAMEL profile presented in Figure 32, it can be seen that juniors and seniors are the most active groups on the CARAMEL profile on the LinkedIn social network, with visits representing 37% and 35% respectively. All the following roles correspond to positions with a percentage of visits of less than 3%, which does not allow us to have a representative sample. Concerning other experiences associated with the visiting users, it can be observed that directors and managers only represent 9% and 2%, respectively. Important to highlight that such positions typically are less common than other roles in a company, suggesting a highly interested audience in the topics addressed by the project.

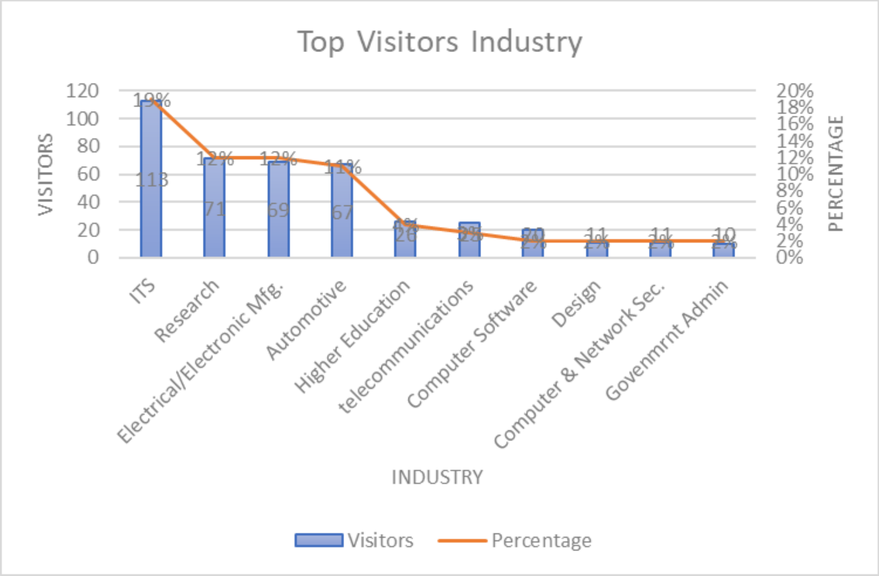


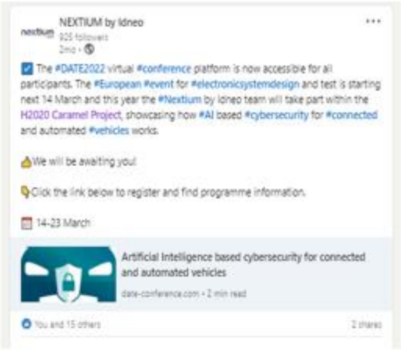
Figure 33 Top 10 industries visiting CARAMEL's LinkedIn account

Figure 33 shows the associations of visitors to a given industry. It can be seen that 19% of the visitors belong to the Information Technology and Services industry, followed by research and electrical manufacturing with 12% of visitors in both cases. In the fourth position, the automotive industry can be highlighted, which reaches an interest of 11% with respect to the industries with the highest interest in the topics of the project.

The information, as noted above, is handy because it represents the project's subject matter audience from different sectors. In regard to the dissemination, we managed together our MKT team to disseminate some events in our LinkedIn company profile.

Tweets by Nextium

Below are the screenshots (Figure 34 and 35) of few of the tweets made by Nextium to promote the CARAMEL project as part of dissemination activity and communication activity.



NEXTIUM by Idneo
925 followers
2mo •

☑ The #DATE2022 virtual #conference platform is now accessible for all participants. The #European #event for #electronicsystemdesign and test is starting next 14 March and this year the #Nextium by Idneo team will take part within the H2020 Caramel Project, showcasing how #AI based #cybersecurity for #connected and automated #vehicles works.

👍We will be awaiting you!

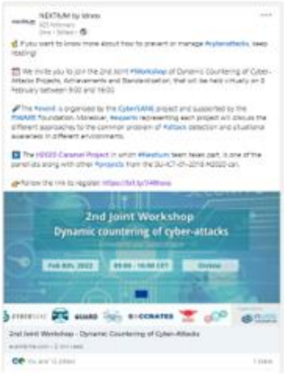
👇Click the link below to register and find programme information.

📅 14-23 March

Artificial Intelligence based cybersecurity for connected and automated vehicles
date-conference.com • 2 min read

You and 15 others 2 shares

Virtual Conference platform



NEXTIUM by Idneo
925 followers
5mo • Edited •

☝ If you want to know more about how to prevent or manage #cyberattacks, keep reading!

📅 We invite you to join the 2nd Joint #Workshop of Dynamic Countering of Cyber-Attacks Projects, Achievements and Standardisation, that will be held virtually on 8 February between 9:00 and 16:00.

🖊 The #event is organized by the CyberSANE project and supported by the [illegible] Foundation. Moreover, #experts representing each project will discuss the different approaches to the common problem of #attack detection and situational awareness in different environments.

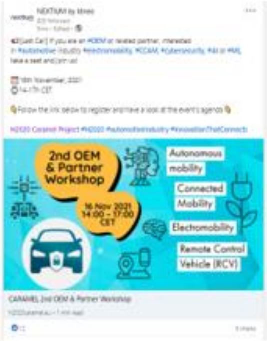
The H2020 Caramel Project in which #Nextium team takes part, is one of the panelists along with other #projects from the SU-ICT-01-2018 H2020 call.

👉Follow the link to register: https://bit.ly/[illegible]

2nd Joint Workshop - Dynamic Countering of Cyber-Attacks
eventbrite.com • 2 min read

You and 12 others 1 share

Dynamic countering of cyber-attacks



NEXTIUM by Idneo
925 followers
5mo • Edited •

📢[Last Call] If you are an #OEM or related partner, interested in #automotive industry #electromobility #CCAM #cybersecurity #AI or #ML take a seat and join us!

📅 16th November, 2021
⏱ 14-17h CET

👇Follow the link below to register and have a look at the event's agenda👇

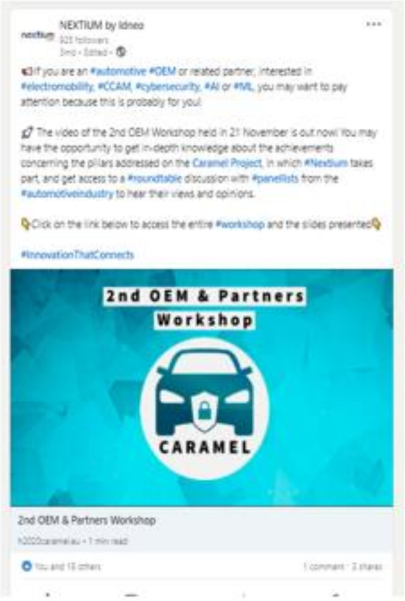
H2020 Caramel Project #H2020 #automotiveindustry #InnovationThatConnects

CARAMEL 2nd OEM & Partner Workshop
h2020caramel.eu • 1 min read

12 5 shares

2nd OEM & Partner Workshop

Figure 34 Screenshots of tweets by Nextium -1



NEXTIUM by Idneo
923 followers
3mo • Edited •

📢If you are an #automotive #OEM or related partner, interested in #electromobility, #CCAM, #cybersecurity, #AI or #ML, you may want to pay attention because this is probably for you!

🎝 The video of the 2nd OEM Workshop held in 21 November is out now! You may have the opportunity to get in-depth knowledge about the achievements concerning the pillars addressed on the Caramel Project, in which #Nextium takes part, and get access to a #roundtable discussion with #panellists from the #automotiveindustry to hear their views and opinions.

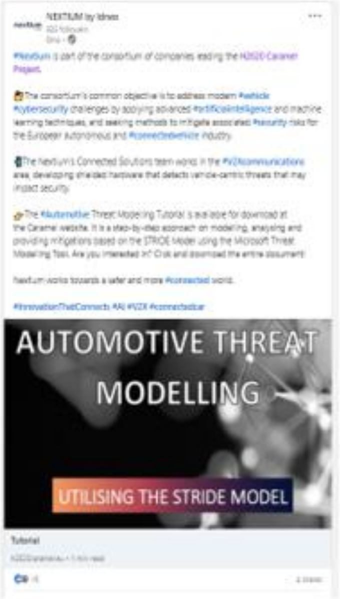
👇Click on the link below to access the entire #workshop and the slides presented👇

#InnovationThatConnects

2nd OEM & Partners Workshop
h2020caramel.eu • 1 min read

You and 18 others · 1 comment · 2 shares

OEM & Partners Workshop



NEXTIUM by Idneo
923 followers
3mo •

#Nextium is part of the consortium of companies leading the H2020 Caramel Project.

The consortium's common objective is to address modern #vehicle #cybersecurity challenges by applying advanced #artificialintelligence and machine learning techniques, and seeking methods to mitigate associated #security risks for the European autonomous and #connectedvehicle industry.

The Nextium's Connected Solutions team works in the #V2Xcommunications area, developing shielded hardware that detects vehicle-centric threats that may impact security.

👉The #Automotive Threat Modeling Tutorial is available for download at the Caramel website. It is a step-by-step approach on modelling, analysing and providing mitigations based on the STRIDE Model using the Microsoft Threat Modelling Tool. Are you interested in? Click and download the entire document!

Nextium works towards a safer and more #connected world.

#InnovationThatConnects #AI #V2X #connectedcar

Tutorial
h2020caramel.eu • 1 min read

16 · 2 shares

Automotive Threat Modelling

Figure 35 Screenshots of tweets by Nextium - 2

3.3 *Liaison with other Projects or Initiatives*

As part of the engagement with other peer projects, CARAMEL has established several collaboration lines, as described in Table 3:

Project	**Collaboration established**	**Lead partner**
Cyberwatching	Project added to cyberwatching database.	i2CAT, 8Bells, Atos
ARCADE	Project added to arcade database.	i2CAT
5GCroCo	Common Partner	i2CAT
5GMED	Common Partner	i2CAT
cyberwiser	Stakeholders Expert Board	i2CAT, Atos
nIoVe	Workshop Co-organization	ucy
Inspire 5GPlus	Common Partner	i2CAT
EUCCAM	Book contribution	i2CAT
5GAA	Standardization activities	DT-sec
IEEE P2020 WG3	Standardisation activities	Panasonic
ITS TC204 AG1		
BDV	i2CAT participates on BDV	i2CAT
Jump2Digital	speaker	i2CAT
CONCORDIA	Paper contribution	UCY, UPAT
C-AVOID	Book contribution	UCY
ECSO	Book contribution	i2CAT, Atos
5GCity	Paper contribution	I2CAT
ONOFRE-2	Paper contribution	i2CAT
TRUE5G	Paper contribution	i2CAT
CPSoSaware	Paper contribution	UPAT, Panasonic
SANCUS	Paper contribution	8Bells

Table 4 Liaisons

3.4 *Events*

The project has been able to share the progress of the activities with an international audience, through the presentation of papers at conferences, talks to which the project was invited as a special guest. Besides previous participation in events, there has been a couple of them which were organised by members of the CARAMEL consortium, making them even more valuable for reporting purposes. A small description of the event and the purpose of the participation are being included in the following section.

3.4.1 *Workshops*

CARAMEL as a consortium has contributed to certain events that provide the completion of the proposed dissemination goals through workshops, webinars, and conference stands. These events are presented below.

1. Cybersecurity of Connected and Automated Vehicles

On September 17th, 2020, UCY organized an Invited Session titled "Cybersecurity of Connected and Automated Vehicles" as part of the23rd Euro Working Group on Transportation (EWGT) conference that was held in hybrid format at Paphos, Cyprus, September 16-18, 2020. During this session, 5 peer-reviewed research papers were presented and around 15 participants attended the event online. https://easychair.org/smart-program/EWGT2020/

2. Advanced Cybersecurity Approaches for Connected, Automated and Electric Vehicles (CyberSec)

On September 20th, 2020, UCY, as a member of the CARAMEL consortium, organised, together with the nIoVe H2020 project, a workshop titled "Advanced Cybersecurity Approaches for Connected, Automated and Electric Vehicles (CyberSec)". The workshop was held online in conjuction with the 23rd IEEE International Conference on Intelligent Transportation Systems (ITSC) and covered topics such as: cybersecurity strategies, threat analysis, data communication, security in networked embedded systems, to mention just a few of the most relevant topics for CARAMEL.

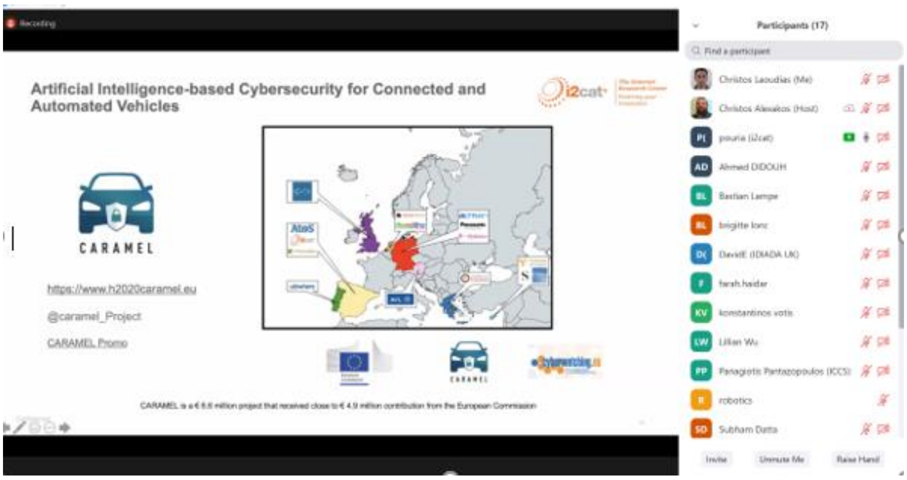
This workshop aimed to connect members from various sectors such as research and development, industry, component suppliers with activities related to autonomous vehicles, the internet of vehicles and electric charging stations. The program included 6 invited speakers and around 20 participants attended the event online. The event was held successfully and without complications of any kind. The official website of the workshop can be accessed via the following link. https://cybersec-itsc2020.isi.gr/

CyberSec

Advanced Cybersecurity Approaches for Connected, Automated and Electric Vehicles

on 23rd IEEE International Conference on Intelligent Transportation Systems
September 20 – 23, 2020, Rhodes, Greece

Figure 36 Main page of CARAMEL's co-organised workshop



Artificial Intelligence-based Cybersecurity for Connected and Automated Vehicles

CARAMEL

https://www.h2020caramel.eu

@caramel_Project

CARAMEL Promo

CARAMEL is a € 6.6 million project that received close to € 4.9 million contribution from the European Commission

Christos Laoudias (Me)
Christos Alexakos (Host)
pouria (i2cat)
Ahmed DIDOUH
Bastian Lampe
brigitte lonc
DavidE (IDIADA UK)
farah haider
konstantinos votis
Lilian Wu
Panagiotis Pantazopoulos (ICCS)
robotics
Subham Datta

Figure 37 Screenshot of the CyberSec online workshop

3. IoTI4 Anomaly Detection and Cyber Attack Detection Competition

Our team participated at the 17th International Conference on Distributed Computing in Sensor Systems (DCOSS) and presented a paper with title 'Synthetic Traffic Signs Dataset for Traffic Sign Detection & Recognition in Distributed Smart Systems' as part of the IoTi4 workshop and competition. The conference participation helped us to disseminate our work on traffic sign anomaly detection and promote the novel contributions including a novel traffic sign recognition (TSR) dataset that includes multiple classes and image deterioration as anomalies to ensure model generalisation. Also offers an overview of the new developed deep learning model specifically for TSR and presents a robust system and a methodology to train and evaluate the proposed system. Additionally, the overall architecture was extended to a Federated Learning environment proving its utility to modern decentralised interconnected systems.

Furthermore, the conference gave the opportunity to discuss the CARAMEL project and the overall contributions, outcomes, and impact with other researchers from industry and academia with potential extensions to emended devices and possible collaborations either at research level or future projects. Additionally, the proposed competition process offered a system to allow a fair comparison of anomaly detection solutions for cyber security applications including environmental attacks on autonomous vehicles focusing on the recognition of modified traffic signs.

Finally, we followed the events and presentations of other organisations and researchers aiming to get new ideas and understand how their work could impact or improve our solutions especially for the client server architectures and the AI models integration into a server. Also papers and talks on emended IoT devices were presented that offered information on how to optimise and integrate our systems more efficiently. The conference was organised online due to COVID-19, but the sessions were also recorded and mechanisms to discuss the presented papers were available.

IOTI4 2021 banner

SDN-uSense CARAMEL collaboration logo

Figure 38 IOT14 banner and logo

4. CAST

Figure 39 CAST Forum logo

The CAST forum is an association of German organisations interested in developments in IT security. The goal of the CAST association. is to confront and further develop the growing importance of IT security in all sectors of industry and in all areas of public administration. As part of one such effort, the event CAST Workshop “Automotive Security” was organised in Darmstadt, Germany, on the 3rd of September 2020.In this event the partner DT-SEC presented the objectives and preliminary results of the CARAMEL project

5. CCAM [CARAMEL] Ethics WS

In the introductory session of the CCAM partnership event introduction of members from Industry, Industry association, agencies and work-related clusters was given. DT-Sec participated in Data and algorithm ethics subgroup in group A. DT-sec gave introduction about the company and the CARAMEL project. In the discussion DT-Sec proposed to go beyond the recommendations and recommendations and introduce them into standards and certification schemes for software development in the automotive sector. It also discussed on topics like technology in an early stage, need for the iterative approach, and the idea of introducing code of ethics for companies. In the Final round group moderators announced the results of subgroups and at the end of the event the event moderators summarised and shared their viewpoint on the topics which were discussed in the whole event.

Connected and Automated Vehicles (CAVs) have the potential to make transport:
SAFER
GREENER
MORE ACCESSIBLE

Figure 40 CCAM Event logo

6. VDI conference - Cyber Security for Vehicles

This workshop will be held 1 week after project ends

As part of the project's dissemination activities, the project has been actively seeking opportunities to expand the involvement not only of citizens but also of potential stakeholders to continue the efforts made in the CARAMEL project.

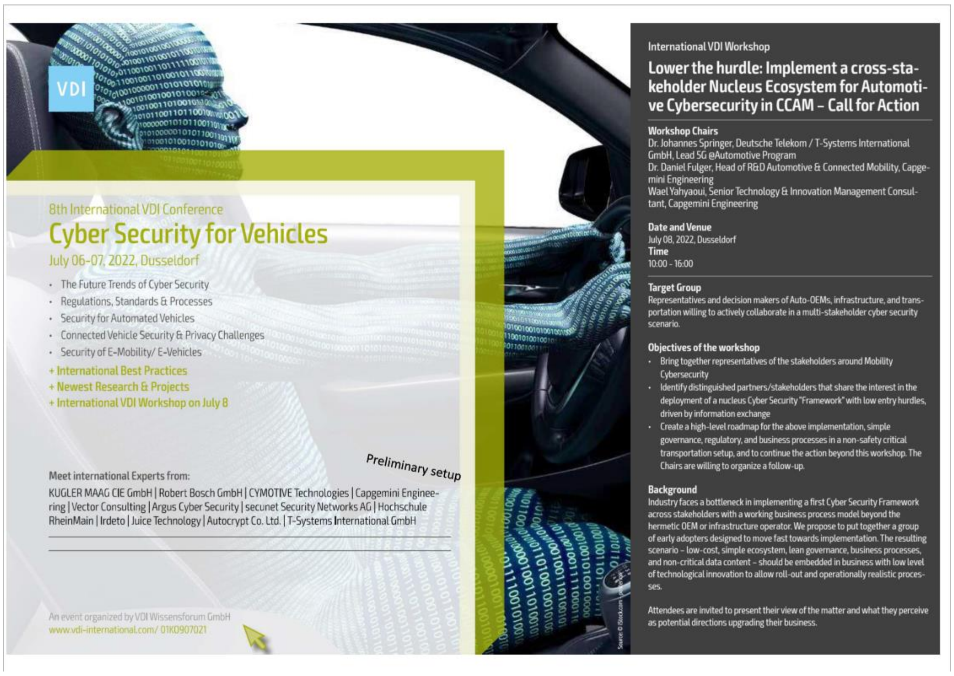
With that objective in mind, CARAMEL will participate in the international VDI conference which has as target users representative and decision-makers of Auto-OEMs, infrastructure and transportation industry who want to participate collaboratively in cybersecurity scenarios.

The VDI international conference will be held from June 6 to 7 in Düsseldorf, Germany and will focus on cybersecurity for vehicles.

During the conference activities, a talk will be given to present the CARAMEL project and its most outstanding results in automotive cybersecurity. One day later, a workshop will be offered.

Workshop objectives are:

- Bring together representatives of the stakeholders around Mobility Cybersecurity
- Identify distinguished partners/stakeholders that share the interest in the deployment of a nucleus Cyber Security “Framework” with low entry hurdles, driven by exchange information.
- Create a high-level roadmap for the above implementation, simple governance, regulatory, and business process in a non-safety critical transportation setup, and to continue the action beyond this workshop.



VDI
Preliminary setup
Source: © iStock.com

8th International VDI Conference

Cyber Security for Vehicles

July 06-07, 2022, Dusseldorf

- The Future Trends of Cyber Security
- Regulations, Standards & Processes
- Security for Automated Vehicles
- Connected Vehicle Security & Privacy Challenges
- Security of E-Mobility/ E-Vehicles

+ International Best Practices
+ Newest Research & Projects
+ International VDI Workshop on July 8

Meet international Experts from:

KUGLER MAAG CIE GmbH | Robert Bosch GmbH | CYMOTIVE Technologies | Capgemini Engineering | Vector Consulting | Argus Cyber Security | secunet Security Networks AG | Hochschule RheinMain | Irdeto | Juice Technology | Autocrypt Co. Ltd. | T-Systems International GmbH

An event organized by VDI Wissensforum GmbH
www.vdi-international.com/ 01K0907021

International VDI Workshop

Lower the hurdle: Implement a cross-stakeholder Nucleus Ecosystem for Automotive Cybersecurity in CCAM – Call for Action

Workshop Chairs
Dr. Johannes Springer, Deutsche Telekom / T-Systems International GmbH, Lead 5G @Automotive Program
Dr. Daniel Fulger, Head of R&D Automotive & Connected Mobility, Capgemini Engineering
Wael Yahyaoui, Senior Technology & Innovation Management Consultant, Capgemini Engineering

Date and Venue
July 08, 2022, Dusseldorf
Time
10:00 - 16:00

Target Group
Representatives and decision makers of Auto-OEMs, infrastructure, and transportation willing to actively collaborate in a multi-stakeholder cyber security scenario.

Objectives of the workshop

- Bring together representatives of the stakeholders around Mobility Cybersecurity
- Identify distinguished partners/stakeholders that share the interest in the deployment of a nucleus Cyber Security "Framework" with low entry hurdles, driven by information exchange
- Create a high-level roadmap for the above implementation, simple governance, regulatory, and business processes in a non-safety critical transportation setup, and to continue the action beyond this workshop. The Chairs are willing to organize a follow-up.

Background
Industry faces a bottleneck in implementing a first Cyber Security Framework across stakeholders with a working business process model beyond the hermetic OEM or infrastructure operator. We propose to put together a group of early adopters designed to move fast towards implementation. The resulting scenario – low-cost, simple ecosystem, lean governance, business processes, and non-critical data content – should be embedded in business with low level of technological innovation to allow roll-out and operationally realistic processes.

Attendees are invited to present their view of the matter and what they perceive as potential directions upgrading their business.

Figure 41 VDI workshop flyer - Cyber Security for Vehicles

3.4.2 *Workshops for OEM*

During the project implementation time, the consortium organised a couple of tailor-made workshops for the OEMs in order to introduce the project and to present the most important outcomes achieved by the outstanding research of the consortium members.

These workshops were held virtually due to the current conditions that increase the security of the participants.

1. First OEM & Partners Workshop

As part of the customised CARAMEL activities for OEM representatives on 27 May 2021 was held the first OEM workshop, it started at 09:00, a 2-hour virtual workshop. The CARAMEL project presented its activities to OEM representatives, increasing the visibility of CARAMEL and gathering advice on the topics addressed by CARAMEL.

The aim of the workshop was to highlight the results achieved in developing artificial intelligence-based cybersecurity for connected and automated vehicles.

Main Pillars of the project

Pillar 1: Autonomous Mobility

Pillar 2: Connected mobility

Pillar 3: Electromobility

Pillar 4: Remote Control Vehicle (RCV)

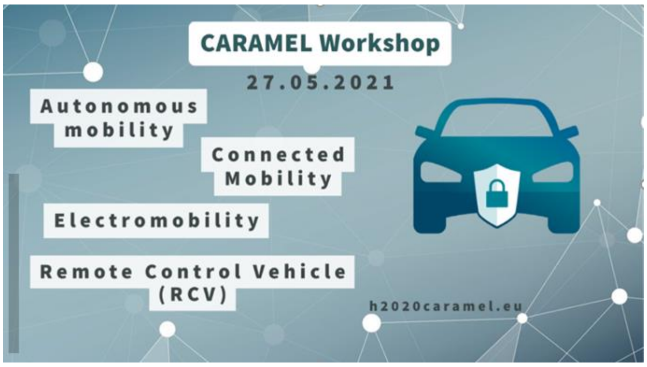


Figure 42 1st Caramel Workshop banner

2. Second OEM & Partners Workshop

The CARAMEL project organised the second OEM and Partners workshop on 16 November 2021 between 14:00 and 17:00. The objective of the workshop was to present the most remarkable results of the research and development carried out by the different members of the consortium. In addition, this workshop was also oriented towards OEM representatives, which could increase the visibility of the project and gather opinions on the subjects addressed by CARAMEL.

The purpose of the workshop was to highlight the results achieved for the development of AI-based cyber security for connected and automated vehicles. At the end of the workshop, it took place a round table style meeting to discuss and collect perspectives and views on the topics and solutions by different partners.

The CARAMEL project has four fundamental pillars for the safety of connected autonomous vehicles.

Some of the addressed topics in this OEM workshop are listed below:

Autonomous Mobility

- Taxonomy of the attacks.
- Cyber attacks Detection and Mitigation on Sensing and Navigation modalities.
- Elevation of Perception Engines as core modules for cyber-attack detection & mitigation engines.
- Towards robustifying D-CNNs to tackle adversarial attacks on the scene layer.
- Multimodality and Redundancy of Sensors beat malicious attacks on CAVs.
- Fall back actions to enhance safety.
- Key Performance Indicators for assessing Mitigation Performance.

Connected mobility

- Interoperability between radio technologies for V2X communications
- Secure V2X communications and related hardware

- GNSS, V2X and HW attack detection and response process
- Vehicle tracking using its signature certificates

Electromobility

- Communication architecture of an EV charging network

Remote Control Vehicle (RCV)

- ML-based traffic between 5G-RCV
- Control Center anomaly detection
- Prediction algorithm development

Figure 43 2nd OEM & Partner Workshop banner

The link to the event presentation is: https://www.h2020caramel.eu/2021/10/12/caramel-2nd-oem-partner-workshop/

Results

During both CARAMEL OEM workshops organised, approximately 110 users have registered, of which at least 70 users connected in both workshops. However, the most remarkable was the presence of representatives from 5 OEM companies.

The OEM workshops allowed us to present CARAMEL's developed technologies for a future with safer roads to the decision-makers of the auto-OEM companies.

3.4.3 *Joint Workshops*

This series of workshops aims to bring together projects called under the same action to create synergies and collaborate with each other to carry out standardization activities.

1. Joint Standardisation Workshop

Figure 44 Banner Workshop Dynamic countering of cyber-attacks projects

During this workshop organised by the CyberSane project, the European Commission's sister projects under the Horizon 2020 programme were presented. All the participating projects were called through the same call for innovation, including projects related to cybersecurity. CARAMEL presented its results to this specialised group in order to achieve a synergy that will allow to reach some of the project objectives.

2. 2nd Joint Standardisation Workshop

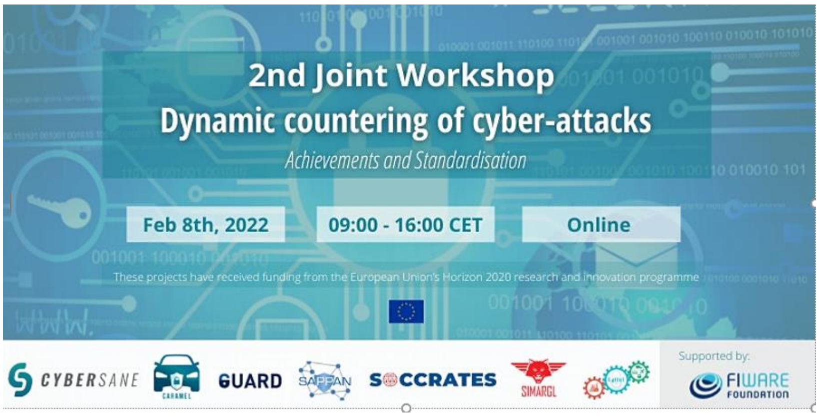

2nd Joint Workshop
Dynamic countering of cyber-attacks
Achievements and Standardisation
Feb 8th, 2022
09:00 - 16:00 CET
Online
These projects have received funding from the European Union's Horizon 2020 research and innovation programme
CYBERSANE
CARAMEL
GUARD
SAPPAN
SOCCRATES
SIMARGL
Supported by:
FIWARE FOUNDATION

Figure 45 2nd Joint Standardization Workshop

3.4.4 *Webinars*

1. Future Mobility

During the second week of May 2020 Ubiwhere as a member of the consortium organised a webinar for which the project coordinator was invited to introduce the CARAMEL project from a future mobility cyber security point of view. This webinar is part of a series of webinars organised by Ubiwhere. Various topics regarding the future of mobility were discussed. Also, the member produced an e-book with the most relevant information from this webinar series, which can be accessed via the following address **https://www.ubiwhere.com/en/news/ebook-future-mobility-webinar-series.**

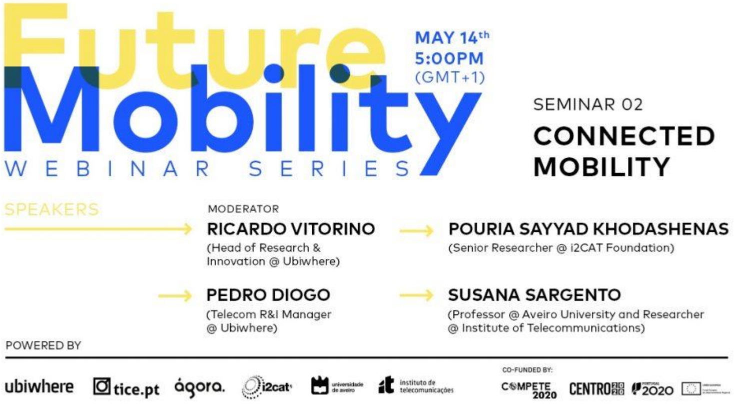

Future
Mobility
WEBINAR SERIES
MAY 14th
5:00PM
(GMT+1)
SEMINAR 02
CONNECTED MOBILITY
SPEAKERS
MODERATOR
RICARDO VITORINO
(Head of Research & Innovation @ Ubiwhere)
POURIA SAYYAD KHODASHENAS
(Senior Researcher @ i2CAT Foundation)
PEDRO DIOGO
(Telecom R&I Manager @ Ubiwhere)
SUSANA SARGENTO
(Professor @ Aveiro University and Researcher @ Institute of Telecommunications)
POWERED BY
ubiwhere
tice.pt
ágora.
i2cat
universidade de aveiro
instituto de telecomunicações
CO-FUNDED BY:
COMPETE 2020
CENTRO 2020
PORTUGAL 2020

Figure 46 Ubiwhere Future Mobility Webinar series

2. IoT Solutions World Congress

During the IoT Solutions World Congress 2022 CARAMEL partners organised a recorded a video webinar that explain some of the most important outcomes of the project.

In such Webinar the CARAMEL's project coordinator gave a small introduction to introduce the 4 main pillars addressed by the project, after which members of the project presented the innovations being demonstrated as part of the CARAMEL testbed.

This webinar is accessible from CARAMEL's YouTube channel.

https://youtu.be/7dfKLMbClIQ

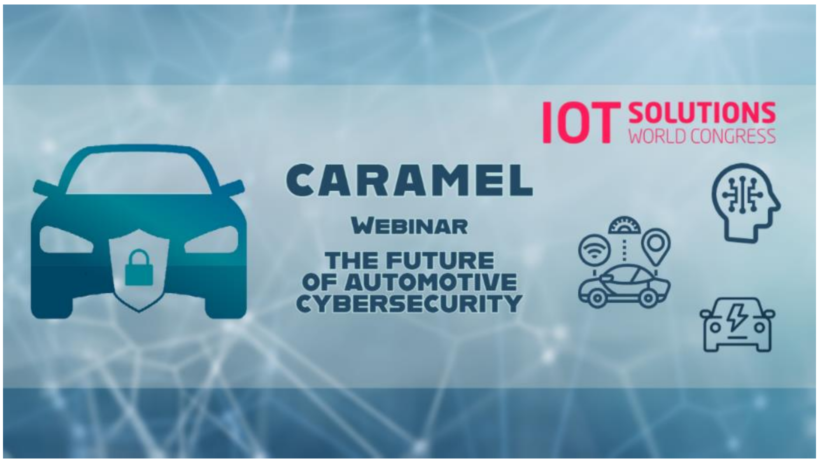


Figure 47 CARAMEL IoTS webinar banner

3. CARAMEL Webinar Series

After the final demonstration of the project, some of the consortium members offered to present the project results in the form of a webinar. For this purpose, the following videos were created and made accessible through the official CARAMEL channel on Youtube.

https://www.youtube.com/playlist?list=PLrjgPTVt9x3zg1e9KsaKSVs35bvwwnkO6

a. CARAMEL webinar - Holistic Situational Awareness with ML Application

Aims and Contributions

Exploring the recent progress in Artificial Intelligence (AI) and Machine Learning (ML) to provide holistic situational awareness and eliminate the effect of the adversarial attacks on the scene analysis modules.

b. Detection and Mitigation of Camera Sensors Attacks on Autonomous Vehicles

Aims and Contributions

DriveGuard - A lightweight Spatio-temporal autoencoder, which utilizes separable convolutions, as an image reconstruction tool for robustifying semantic segmentation for autonomous vehicle applications.

Investigate different architectures and loss function combinations, with the structural similarity index (SSIM) and mean square error (MSE), for better structure understanding and pixel-wise restoration respectively.

Constructed a more challenging dataset and deployed it to test a combination of traditional noise models and more targeted attacks comprised of realistic and synthetic data with diverse weather conditions generated from an autonomous driving simulator.

Figure 48 CARAMEL Webinar Series banner

3.4.5 *Participation in events*

CARAMEL has participated in several international conference events in which at least 18 papers and fifteen oral presentations have been presented. The venues for which CARAMEL made a presentation during its runtime, includes:

- European Conference on Networks and Communications (**EUCNC**),
- IEEE Computer Society Annual Symposium on VLSI (**ISVLSI**)
- International Conference on Transparent Optical Networks (**ICTON**)
- 16th European Conference on Computer Vision (**ECCV2020**)
- Euro Working Group on Transportation (**EWGT**)
- The 16th European Conference on Computer Vision (**ECCV**)
- Conference on intelligent transport systems (**IEEE ITSC**)
- Fifth Innovation and Entrepreneurship Forum (**IEF2020**)
- Winter Conference on Applications of Computer (**WACV**)
- International Conference on Distributed Computing in Sensor Systems (**DCOSS 2021**)
- AI & Big Data Congress (**AIBIGDATA**)
- 93rd Vehicular Technology Conference 2021 (**VTC2021**-Fall)
- 23rd International workshop on Multimedia Signal Processing (**IEEE MMSP 2021**)
- ITS International World Congress Hamburg (**ITSHamburg**)
- Barcelona Digital Talent (**Jump2Digital**)
- (RISE **2022**)
- Design, Automation and Test in Europe Conference and Exhibition (**DATE2022**)
- IoTS Solutions World Congress (**IoTSWC2022**)

EUCNC 2020

EUCNC
2020
June 15-18
European Conference on Networks and Communications | Dubrovnik, Croatia

Figure 49 EUCNC 2020 logo

In the second week of June 16-17, the European Conference on Networks and Communications took place in Dubronik Croatia. To bring together experts in cutting-edge research from both academic centres and world-renowned industries, the European Conference on Networks and Communications was held in Dubronik Croatia. EuCNC is a space to present the latest advances being researched, specifically by projects funded by the European Commision.

One **paper** was presented during this event:

1. The CARAMEL Project: a Secure Architecture for Connected and Autonomous Vehicles

As part of this conference a special compilation was created that includes the best papers presented which were allowed to create an extended version. These papers were selected for presenting quality research activities related to networks and systems beyond 5G, thus presenting the finest results in the evolution of research in mobile and wireless communications. *EURASIP Journal on Wireless Communications and Networking*.

One **paper** was presented during this event:

2. The CARAMEL Project: Results on a Secure Architecture for Connected and Autonomous Vehicles

ISVLSI 2020

Figure 50 ISVLSI 2020 logo

From 6 to the 8th of July 2020 the IEEE Computer Society Annual Symposium on VLSI was held in Limassol, Cyprus. This conference aimed to explore trends and new ideas in the field of VLSI. However, it had a special section on security, artificial intelligence and cyber-physical systems. It was possible to include CARAMEL's participation as a stimulus for new developments for VLSI developers.

One **paper** was presented during this event:

3. Towards Artificial-Intelligence-Based Cybersecurity for Robustifying Automated Driving Systems Against Camera Sensor Attacks

ICTON 2020

22nd
ICTON2020
International Conference on Transparent Optical Networks
July 19th - 23rd, 2020 | Bari, Italy

Figure 51 ICTON 2020 logo

The International Conference on Transparent Optical Networks will be held on July 19-23, 2020. This event was held virtually due to the impositions as a containment measure to the worldwide virus COVID-19. ICTON is a conference focused on applying optical technologies for telecommunications, measurement, computing and novel fields derived from the above topics.

Four **papers** were presented during this event:

4. Towards Artificial-Intelligence-Based Cybersecurity for Robustifying Automated Driving Systems Against Camera Sensor Attacks
5. Multi-Radio V2X Communications Interoperability Through a Multi-Access Edge Computing (MEC)
6. 5G Enabled Cooperative Localization of Connected and Semi-Autonomous Vehicles via Sparse Laplacian Processing
7. GNSS Location Verification in Connected and Autonomous Vehicles Using in-Vehicle Multimodal Sensor Data Fusion

ECCV2020

The 16th European Conference on Computer Vision (ECCV 2020) was held between 23rd - 28th August 2020. ECCV is a renowned and reputable conference for computer vision topics and our main aim to attend the conference was to gain insights and state-of-art knowledge within the field of computer vision. The knowledge gained from the attendance of this conference was useful for specifically our use case on traffic sign anomaly detection. During the conference we learned about various topics within the domain of deep learning and especially with a focus on newer types of model architecture design and their uses.

Figure 52 ECCV banner

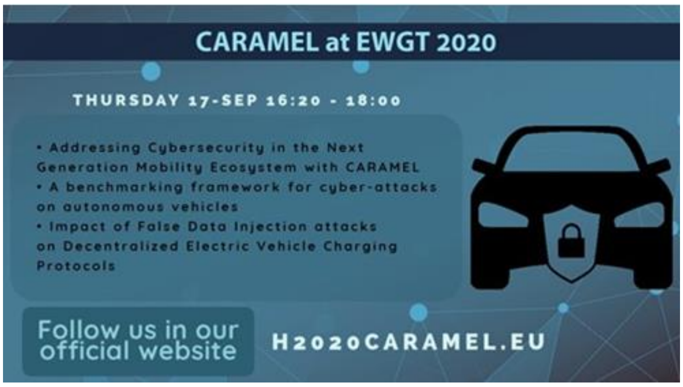
EWGT2020

Figure 53 EWGT 2020 logo

The 23rd Euro Working Group on Transportation was held from 16 to the 18th of September 2020 as a conference dedicated to presenting innovative projects related to transportation and addressed topics such as Modeling and Control, Economics and Policy Planning and operation, Connected and Automates Vehicles for naming a few. Like the other conferences, this one was held in a hybrid face-to-face/virtual way to contain the spread of the COVID19 virus which is stalking the whole world.

Three **papers** were presented during this event:

8. Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL
9. Impact of False Data Injection attacks on Decentralized Electric Vehicle Charging Protocols
10. A benchmarking framework for cyber-attacks on autonomous vehicles



CARAMEL at EWGT 2020

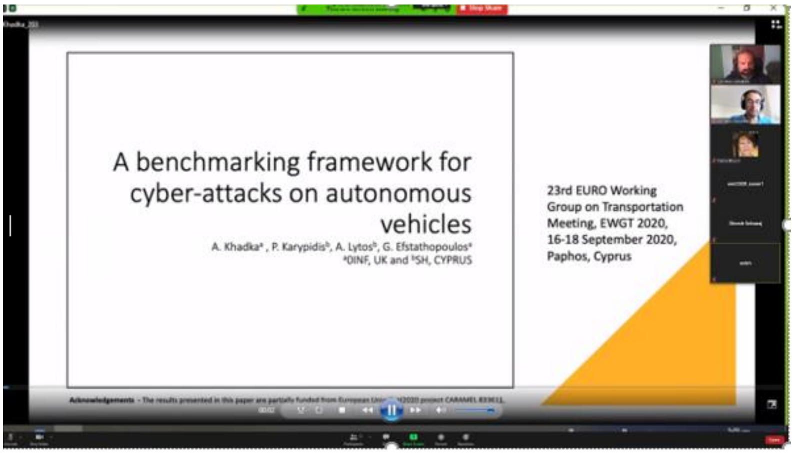
THURSDAY 17-SEP 16:20 - 18:00

- Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL
- A benchmarking framework for cyber-attacks on autonomous vehicles
- Impact of False Data Injection attacks on Decentralized Electric Vehicle Charging Protocols

Follow us in our official website

H2020CARAMEL.EU

Figure 54 EWGT event banner



A benchmarking framework for cyber-attacks on autonomous vehicles

A. Khadka[a] , P. Karypidis[b], A. Lytos[b], G. Efstathopoulos[a]
[a]OINF, UK and [b]SH, CYPRUS

23rd EURO Working Group on Transportation Meeting, EWGT 2020, 16-18 September 2020, Paphos, Cyprus

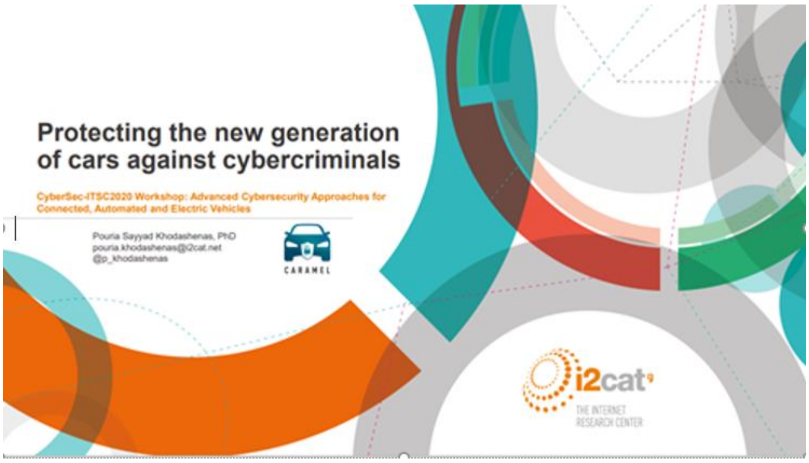
Acknowledgements – The results presented in this paper are partially funded from European Union's H2020 project CARAMEL 833611.

Figure 55 Screenshot of the CARAMEL Invited Session with peer-reviewed papers at EWGT 2020

IEEE ITSC

During the fourth week of September 2020, a virtual conference on intelligent transport systems was held in Rhodes, Greece; the international conference focused on gathering knowledge around the theory, analysis, simulation, modelling of intelligent transport systems.

In addition to the workshop organised in conjunction with the nIoVe project, there were some talks as part of the activities, and one of them was preceded by the project coordinator, Dr Pouria Sayaad Kodashenas, who presented a talk with the title “Protecting the new generation of cars against cybercriminals”. In this talk, Dr Pouria introduced the different levels of automation achieved and expected in autonomous vehicles and a short introduction to the European 5G providers for connected vehicles. Finally, some of the European projects aiming to develop solutions to the challenges imposed by the expected levels of automation in autonomous vehicles were presented.



Protecting the new generation of cars against cybercriminals

CyberSec-ITSC2020 Workshop: Advanced Cybersecurity Approaches for Connected, Automated and Electric Vehicles

Pouria Sayyad Khodashenas, PhD
pouria.khodashenas@i2cat.net
@p_khodashenas

CARAMEL
i2cat
THE INTERNET RESEARCH CENTER

Figure 56 Talk at the IEEE ITSC

IEF2020

In the third week of December, the fifth Innovation and Entrepreneurship Forum, organised annually by the University of Cyprus, took place. This event brings together experts in artificial intelligence from all levels to discuss the challenges of artificial intelligence and to answer the uncertainties facing the future of artificial intelligence and its impact on society, as well as economic and policy issues.

Thanks to the participation of the UCY, CARAMEL presented “A modular approach to detect GPS location spoofing attack in autonomous vehicles”.

A cost-effective and modular solution for the AVs to timely and reliably detect and mitigate the GPS spoofing attack was presented. Specifically, an in-vehicle detection scheme is being developed those leverages multi-sensor fusion coupled with Bayesian filtering to produce in real-time an alternative GPS-free location stream of the AV that is used to check the integrity of the GPS location stream.

Video link: https://youtu.be/dLS1gYhfTac

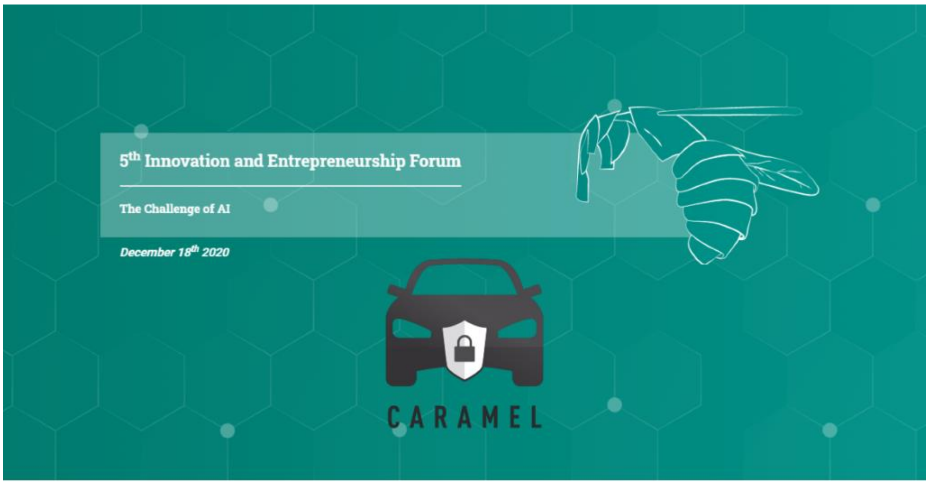
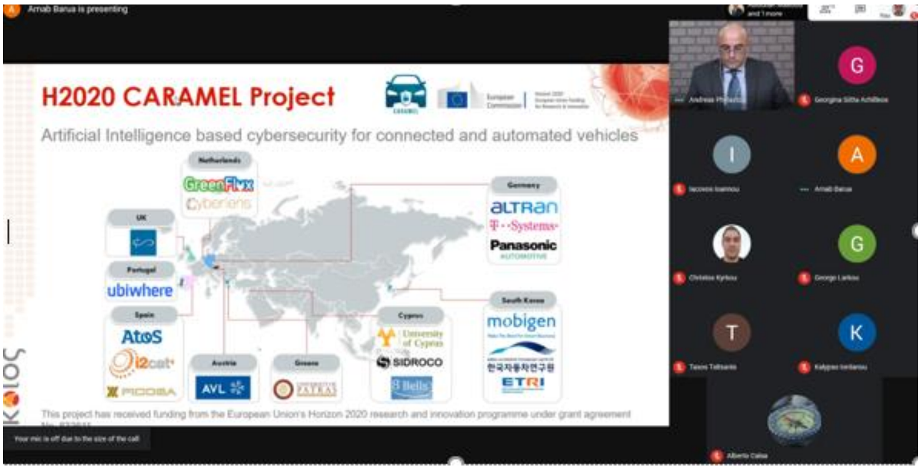


Figure 57 IEF2020 banner


Arnab Barua is presenting

H2020 CARAMEL Project

Artificial Intelligence based cybersecurity for connected and automated vehicles

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

Your mic is off due to the size of the call

Figure 58 Screenshot of the online session at IEF2020

WACV2021

Figure 59 WACV banner

The WACV conference is an international event focused on computational vision in which various lectures, tutorials and workshops take place. Mainly focused on being low-cost and therefore valuable. As usual last months this event was held as a virtual event due to the restrictions imposed to contain the spread of the COVID19.
One **paper** was presented during this event:

11. **DriveGuard: Robustification of Automated Driving Systems with Deep Spatio-Temporal Convolutional Autoencoder (https://dcoss.org/dcoss21/ https://ioti4-2021.web.uowm.gr/)**

IEEE DCOSS 2021

IEEE
DCOSS 2021
INTERNATIONAL CONFERENCE ON DISTRIBUTED
COMPUTING IN SENSOR SYSTEMS

Figure 60 DCOSS 2021 Logo

“The annual International Conference on Distributed Computing in Sensor Systems (DCOSS 2021) is intended to cover several aspects of distributed computing in sensor systems such as high-level abstractions and models, systematic design methodologies, signal and information processing, algorithms, analysis and applications”. However, a co-located workshop was held with DCOSS2021.
The 3rd International Workshop on IoT Applications and Industry 4.0 took place on 14-16 July 2021 and focused on promoting new ideas for the proliferation of applications in the IoT industry.

The area of the Internet of Things has been boosted in recent years due to the revolution in the potential of connected devices to impact everyday tasks as well as business processes. In this case the workshop focuses on the topic of the internet of things in industry.

Having said that, the CARAMEL Project was positioned as a project with enough qualities to present a **paper** in such venue.

12. **Synthetic Traffic Signs Dataset for Traffic Sign Detection & Recognition in Distributed Smart Systems**

AI & Big Data Congress 2021

Figure 61 AI & BIG DATA CONGRESS 2021 banner

On the 15th of September 2021, the AI & Big Data Congress took place at the AXA Auditorium in Barcelona. The congress was organised by the Innovation Centre for Information Technology and Artificial Intelligence. The event focused on providing a meeting point for professionals, suppliers, and companies carrying out projects in artificial intelligence and big data.

The 2021 event was marked by its emphasis on the challenging topics of artificial intelligence, technical innovations and their applications. Success stories were also presented in detail.

The CARAMEL project was presented within the congress activities by the project coordinator Jordi Guijarro. He explained the challenges in the four areas addressed by the CARAMEL project. Autonomous Mobility, Connected Mobility, Electromobility and Remote Controlled Vehicles.

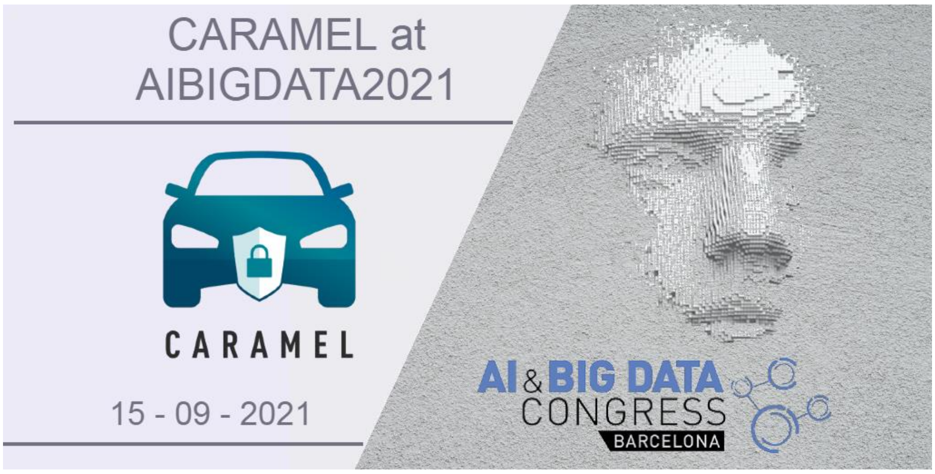


Figure 62 Dissemination of the AI and Big data congress

VTC2021-Fall

[93rd Vehicular Technology Conference 2021]

On 27-29 September, the IEEE 94th Vehicular Technology Conference: VTC2021-Fall was organised with the aim of bringing together academic experts, industry and government representatives to share ideas on wireless, mobile and automotive technology. To achieve this purpose, presenters were invited to offer tutorials, technical sessions or even applications, In one of the spaces provided by the conference, one of the CARAMEL members presented one of the results of the project in the form of a **paper:**

13. **GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles**

VTC2021-Fall

September 29 2021

13:00

Track:
AUTONOMOUS VEHICLES

GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles

WWW.H2020CARAMEL.EU

Figure 63 Dissemination of the VTC2021- Fall

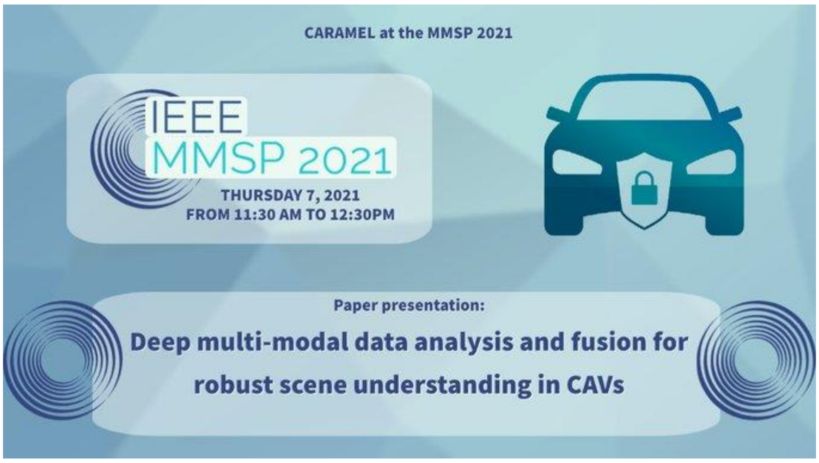
IEEE MMSP 2021 - 23rd International workshop on Multimedia Signal Processing

During the second week of October 2021, the 13th IEEE International Congress on Multimedia Signal Processing (MMSP) was held. This congress was for three days a meeting point for professionals developing in academic or working environments in multimedia signal processing to share knowledge, ideas and shape the future of future research.

As part of the CARAMEL activities, the University of Patras presented the paper “Deep multi-modal data analysis and fusion for robust scene understanding in CAVs” which addresses the challenges of artificial intelligence in the face of adversarial cyber-attacks by proposing a novel multi-modal approach against which achieve robustness to adversarial attacks, by appropriately modifying the analysis Neural Networks and by utilising late fusion methods

One **paper** was presented during this event:

14. **Deep multi-modal data analysis and fusion for robust scene understanding in CAVs**



CARAMEL at the MMSP 2021

IEEE MMSP 2021

THURSDAY 7, 2021
FROM 11:30 AM TO 12:30PM

Paper presentation:

Deep multi-modal data analysis and fusion for robust scene understanding in CAVs

Figure 64 IEEE MMSP

ITSHamburg 2021

From 11 to 15 October 2021, the largest international conference focused on intelligent mobility and digitisation of transportation, also known as the Hamburg ITS World Congress, took place.
As part of the activities of this congress, CARAMEL representatives had the opportunity to be present inside the venue, where they handed out information about the project either verbally or in the form of project information folders.

Figure 65 Dissemination of the CARAMEL participation at the ITSHamburg

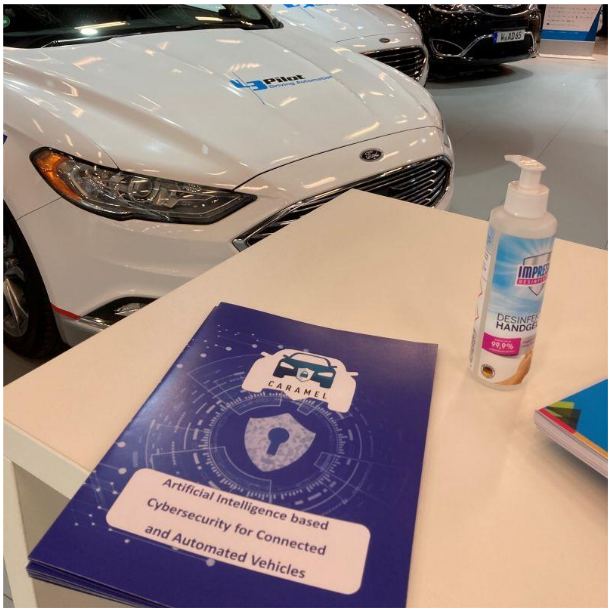


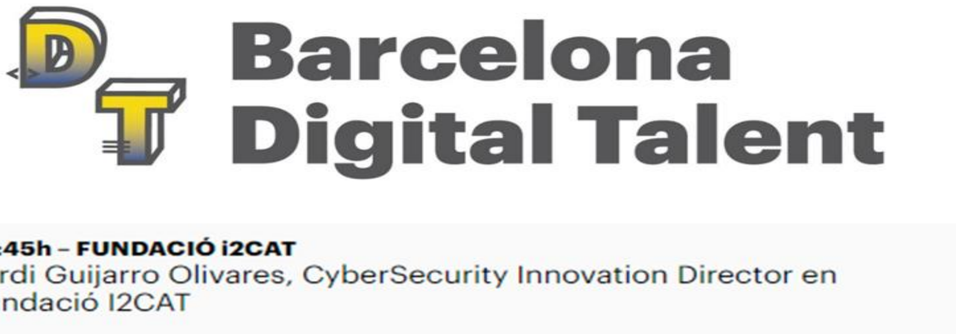
Figure 66 Dissemination of the CARAMEL participation at the ITSHamburg – CARAMEL Brochure

Jump2Digital

Barcelona Digital Talent is an event focused on motivating and incorporating new talent into Spain's productive sectors through the presentation of successful cases of professionals working in the digital business. Digital talent has become an important sector for Spain's economic competitiveness on a global scale.

In this context the Project Coordinator Jordi Guijarro gave a talk in which he presented CARAMEL as a use case of digital talent that allows to address one of the critical sectors in Europe. Especially now with the new times the industry has gone digital allowing remote work, and this is how CARAMEL addresses the need for cybersecurity from a remote work.

JUMP2DIGITAL | Barcelona Digital Talent



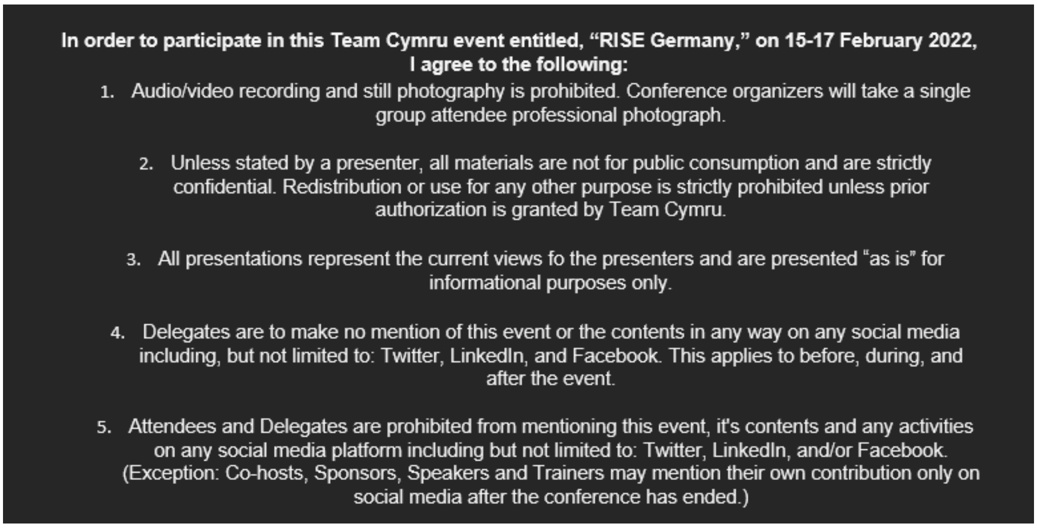
Barcelona Digital Talent

18:45h – FUNDACIÓ i2CAT
Jordi Guijarro Olivares, CyberSecurity Innovation Director en Fundació I2CAT

Figure 67 Barcelona Digital Talent

RISE 2022

During February 2022 the RISE 2022 conference took place in Bochum Germany. At this conference the main coordinators of the project presented the innovations of the project to a group of experts in the field of internet security and enforcement representatives. During the talk, the project was presented, and the pillars of the caramel project were explained. Due to the classification of the event (TLP-Red), no further information can be provided.



In order to participate in this Team Cymru event entitled, "RISE Germany," on 15-17 February 2022, I agree to the following:

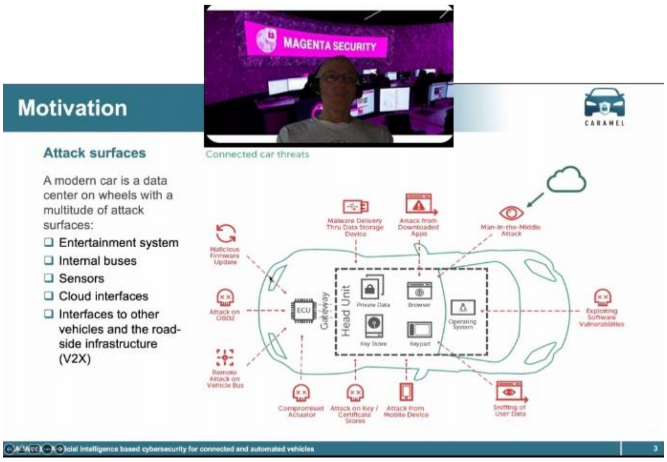
1. Audio/video recording and still photography is prohibited. Conference organizers will take a single group attendee professional photograph.
2. Unless stated by a presenter, all materials are not for public consumption and are strictly confidential. Redistribution or use for any other purpose is strictly prohibited unless prior authorization is granted by Team Cymru.
3. All presentations represent the current views fo the presenters and are presented "as is" for informational purposes only.
4. Delegates are to make no mention of this event or the contents in any way on any social media including, but not limited to: Twitter, LinkedIn, and Facebook. This applies to before, during, and after the event.
5. Attendees and Delegates are prohibited from mentioning this event, it's contents and any activities on any social media platform including but not limited to: Twitter, LinkedIn, and/or Facebook. (Exception: Co-hosts, Sponsors, Speakers and Trainers may mention their own contribution only on social media after the conference has ended.)

Figure 68 RISE Conference Rules and regulations for the participation

DATE 2022

As part of the dissemination activities of the project, it was decided to participate in the DATE2022 conference which aims to be a meeting point for researchers, software and hardware designers, electronic circuit manufacturers, among others, while focusing on technology and systems.

During this event the CARAMEL project participated in the discussion session dedicated to providing a platform for discussion of opportunities and collaborations for innovation and research in Europe, in which the project's technical coordinator Peter Hofmann took part in the important panel session "The Good, the Bad and the Trendy of Multi-Partner Research Projects in Europe". Although the conference was originally scheduled to be held in a face-to-face format, it had to be reorganised at short notice to an online format.



Motivation

Attack surfaces

A modern car is a data center on wheels with a multitude of attack surfaces:

- ❑ Entertainment system
- ❑ Internal buses
- ❑ Sensors
- ❑ Cloud interfaces
- ❑ Interfaces to other vehicles and the road-side infrastructure (V2X)

MAGENTA SECURITY
CARAMEL
Connected car threats
Malware Delivery Thru Data Storage Device
Attack from Downloaded Apps
Man-in-the-Middle Attack
Malicious Firmware Update
Attack on OBD2
Remote Attack on Vehicle Bus
ECU
Gateway
Head Unit
Private Data
Browser
Key Store
Keypad
Operating System
Exploiting Software Vulnerabilities
Compromised Actuator
Attack on Key / Certificate Stores
Attack from Mobile Device
Sniffing of User Data
icial Intelligence based cybersecurity for connected and automated vehicles
3

Figure 69 Presentation of the project as part of the panel session

The importance of the CARAMEL project for the DATE2022 conference community is summarised below.

What makes the project concept unique?
In the CARAMEL project, we strive to implement machine-learning based detection of attacks against the connected and/or autonomous vehicle by analysing sensor data, V2X data, and the status of embedded controllers like the OBU (on-board unit) in real time using a tamper-proof device that directly integrated into the car - the anti-hacking device (AHD). This architecture and concept are novel and innovative, and CARAMEL is the first project to implement and demonstrate this.

What project outcomes can be of use to the DATE 2022 community?
Even as CARAMEL implements its concepts and architectures in the automotive space, the key CARAMEL innovations are transferable to other IoT and Embedded applications domains as well, such as factory floors, building automation systems or others. Therefore, the CARAMEL presentation and presence of CARAMEL representatives during the conference would be of value to the DATE 2022 community.

What inputs (solutions) are expected from the DATE 2022 community?
In the CARAMEL project, several integration options for the anti-hacking device based on different IoT devices have been pursued already. However, for the concept to be commercially viable and cost-effective, the concept of a machine-learning-based intrusion device must be even better integrated into commercial offerings for the Automotive and IoT market. The DATE 2022 community could provide valuable input for that endeavour.

What new research topics and trends the project introduces?
CCAM and IoT both will face important security challenges in the future as bad actors discover these new areas for their activities. Since bad actors will use machine learning to subvert machine-learning based processes and algorithms in the CCAM and IoT world (e.g., using Generative Adversarial Networks (GAN)), a trend in the security industry is also to use machine learning to detect and counter these attacks. The CARAMEL project showcases this approach in the Automotive context.

It is also important to highlight the presentation of a paper within the activities of the caramel conference, which is entitled:

15. A Comprehensive Solution for Securing Connected and Autonomous Vehicles

Figure 70 Banner for the DATE2022 conference [17]

IoT Solutions World Congress

This conference is intended to be a meeting point to showcase the most innovative solutions and technologies being developed that have the potential to transform the IoT industry. It is also an excellent meeting point for leaders and organisations aiming to identify new technologies.

The CARAMEL Project was selected to present its innovations in the field of artificial intelligence-based cybersecurity solutions for the CCAM connected and automated mobility industry as part of the IoT Solutions World Congress activities.

The event was a great meeting point after 2 long years without face-to-face events where we could meet face-to-face not only the creators of these new technologies but also connect with the citizens by giving us the opportunity to present the latest project results.

The CARAMEL project had a successful participation in the activities of the IoTS WC, thanks to the participation of more than 400 people who were interested in the project and who were offered a personalised explanation, through the official project tours or individual conversations, to inform them about the most outstanding results of the project.

We highlight the participation of I2CAT, Capgemini, Panasonic, Atos and Nextium who had the opportunity to be in the testbed offering specific information about the project to each of the visitors to the CARAMEL testbed.

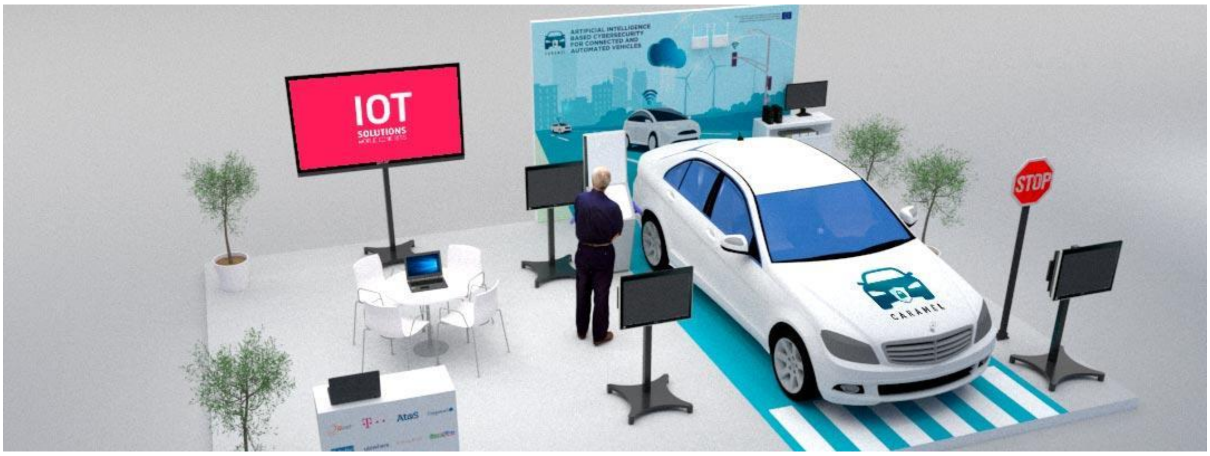

IOT
SOLUTIONS
ARTIFICIAL INTELLIGENCE BASED CYBERSECURITY FOR CONNECTED AND AUTOMATED VEHICLES
STOP
CARAMEL
Atos

Figure 71 Render of the CARAMEL's testbed

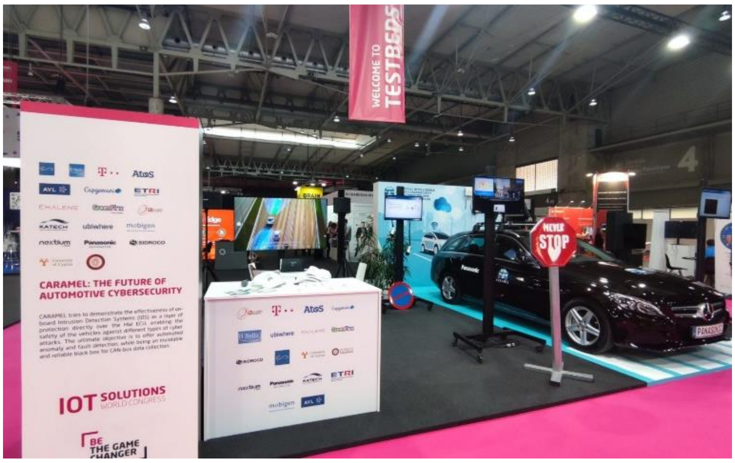

WELCOME TO TESTBEDS
Atos
ETRI
CARAMEL: THE FUTURE OF AUTOMOTIVE CYBERSECURITY
IOT SOLUTIONS WORLD CONGRESS
BE THE GAME CHANGER
STOP

Figure 72 The scenario of the testbed during the 3 days of IoTs

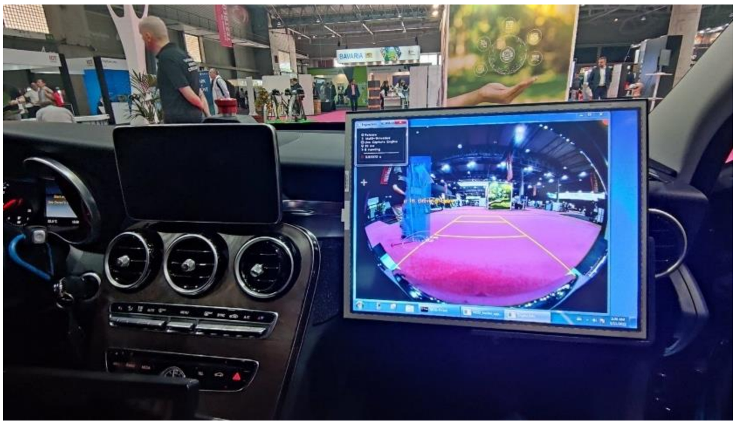


Figure 73 Interior of the autonomous vehicle in the IoTS WC

Figure 74 IoT Solutions Congress Banner

3.4.6 *CARAMEL events*

21st General Assembly

Figure 75 21st General assembly dissemination

On 28th April took place the CARAMELs 21st general assembly among all members of the consortium. After some months of reluctance to have these live conversations, finally happened a the first face-to-face meeting.

The meeting took place on the premises of the University of Cyprus, in the library “Stelios Ioannou” Aglantzia, Nicosia.

In this meeting, the project focused on organising the activities necessary to carry out the final demonstrations of the project, the participation of the IoTS WC as well as the final evaluation.

KIOS Seminar Series

Figure 76 KIOS Seminar banner

The University of Cyprus through the KIOS institute offered its educational facilities to the Korean partners of the consortium to give a seminar about the projects in which they are participating. For this reason, Dr You-Jun Choi and Dr Taesang Choi presented their collaboration in the projects listed below.

- 5G MOBIX (5G for cooperative & connected automated MOBIlity on X-border corridors) and standardization issue on infrastructure guidance Localized Service for urban connected automated mobility
    - In this presentation, the H2020 project called, 5G-MOBUX and ITS standardization issue on infrastructure guidance Localized Service for urban connected automated mobility will be discussed. 5G-MOBIX aims to showcase the added value of 5G technology for advanced Cooperative, Connected and Automated Mobility (CCAM) use cases and validate the viability of the technology to bring automated driving to the next level of vehicle automation (SAE L4 and above). The remote-control vehicle using mmWave communication which is the main use case of KR trail site. As an international standardization issues, Infrastructure guidance localized service to extend conventional ODD for connected automated mobility will be also briefly discussed.

- 5G AgiLe and fLexible integration of SaTellite And cellular (5G-AllStar)
    - In this presentation, we try to provide the results of KR-EU collaboration project called, 5G-AllStar to demonstrate multiple access technologies considering 5G cellular and 5G satellite to ensure high service availability and service continuity over a wide area and provide network reliability. Such heterogeneous multiaccess technology can provide reliable and high-quality for various future services, especially intelligent transportation services which require seamless network connectivity.

Technical Meeting

On 25th January the CARAMEL consortium started a technical meeting among all participants to synchronise the activities carried out to achieve the proposed goals and present the challenges related to the integration of the various research tasks carried out over the last months. The meeting was opened by Petros Kapsalas, who updated the activities carried out as part of Work Package 6.

Thus, the advantages of artificial intelligence as a mitigation technique to counter elaborate attacks were mentioned. Later, the consortium members were reminded about the used vehicle to demonstrate the project's outcomes in the final review.

Afterwards, each consortium member involved in activities related to each of the four pillars, presented their progress to synchronise efforts promptly.

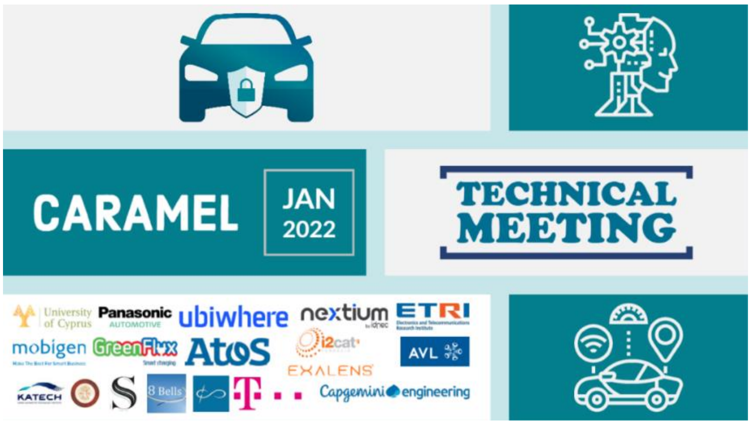


Figure 77 Technical meeting poster

Final Demonstration Preparation

As part of the final demonstration activities to be presented in Frankfurt prior to the final review. A series of preparation activities were carried out at the project's technical demonstration facilities.

During these 2 days different integration activities were carried out aiming to avoid or identify and mitigate any kind of adverse situation during the final demonstration. The antennas were integrated to provide interoperability between the different radio communication technologies targeted by the project. The OBU modules that contain the security mechanism against hardware modification were tested. Additionally, the project members integrated the communication from the anti-hacking device with the CARAMEL backend. This backend service communication has the ability to collect, analyse and inform other devices about threats detected previously by the connected vehicles. This whole ecosystem of technology allows strengthening the idea that would allow the future to achieve safe roads for connected vehicles.

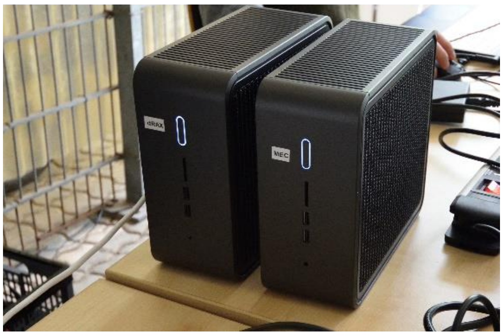


Figure 78 MEC and Road Side Unit Controller

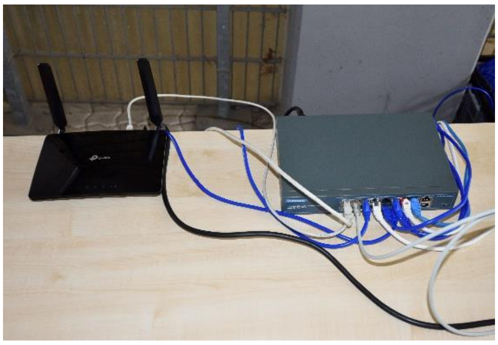


Figure 79 Radio communication enabler devices

Figure 80 CARAMEL's Final Demo Preparation Banner

3.4.7 *Other type of events*

Apart from the common activities planned. CARAMEL has been involved in unplanned events. An example is a presentation made for the students of the Universitat Politècnica de Catalunya (UPC) in Barcelona, Spain. This recurrent event is being organised by the university to keep in touch with professionals and master students of the program. During such activity, it was presented the CARAMEL project with the scope of protecting the new generation of cars from cybercriminals. Table 6 shows a summary of all events on which CARAMEL has participated.

Figure 81 CARAMEL at the Ametic event

3.4.8 *IoTS World congress*

As was well known, during much of the project's months of execution, the whole world went through a complicated situation, which made it impossible to hold large-scale, physical conferences in which to showcase the project's results to stakeholders. Despite the dissemination efforts made in virtual activities during 2019-2020, the user engagement impact of virtual events is not the same as for physically-based events. For this reason, and due to improvements to the disease contention rules, at the end of 2021, the project endeavoured to identify physical conferences that could be held before the end of the project identifying the following: DATE2022, TNC2022, IoTS World Congress.

It can be highlighted the participation in the IoTS World congress after the project applied in time and form for the possibility to get a free testbed inside the IoTS exhibition halls.

So it was that the CARAMEL project after the application was selected among more than 42 contending projects for one of the 10 testbeds offered for free by the organizers.

1. Application and outcomes to be presented

The project had as a consideration for the testbed how integrating different technologies helps to withstand certain autonomous vehicle’s cyberattacks.

The OBU is secured through a secure design called Point-of-Sale, in which in case of a box opening detection, active wire-meshes protect the susceptible signals and circuits. Furthermore, logical methods are also implemented to prevent firmware manipulation.

The Multi-Access Edge Computing (MEC) allows MEC applications into the AHD. However, MEC applications require constant communication, which might compromise the system due to two factors:

vehicles without V2X communications and incompatible interoperability between communication protocols.

The CARAMEL project has developed software packages to permit V2X communications via cellular interfaces, thus mitigating the first V2X communications issue. Nevertheless, cellular communications have unicast addressing, which is not suitable to broadcast V2X information by itself. Therefore, CARAMEL provides the required infrastructure, hosted in a MEC, which receives V2X messages transmitted over cellular networks and forwards them to all relevant vehicle neighbours.

The second problem arises because nowadays, there are incompatible mainstreams of V2X radio technologies: the IEEE 802.11p plus its evolution, the IEEE 802.11bd, and the 3GPP's LTE-V2X plus the recently published NR-V2X. In addition, we must consider those vehicles using V2X over cellular networks. CARAMEL uses a network of Road Side Units (RSUs) and access to cellular networks to receive all transmitted messages in a MEC, which forwards them to the required vehicles using their specific radio technology.

CARAMEL has also developed a threat detection showcase based on a backend that allows collecting, detecting, and analysing information on suspicious activities. Threats can come from any system deployed on the vehicle or infrastructure (Intrusion Detection Systems, MEC, anti-hacking device, etc.) and use the collective information gathered by previous vehicles to make other vehicles aware of threats in the surrounding areas.

2. Preparation and Assembly

The project underwent a long preparation to meet the safety requirements set by the organizers. Because originally it was planned to have an even bigger false wall that would allow the presentation of the autonomous vehicles factor in a graphical way inside the stand.

However, the false wall had by regulation a maximum height and could not cover a certain amount of square meters, the reason for which the booth design was modified, resulting in the rendering of the CARAMEL booth shown in Figure 82.

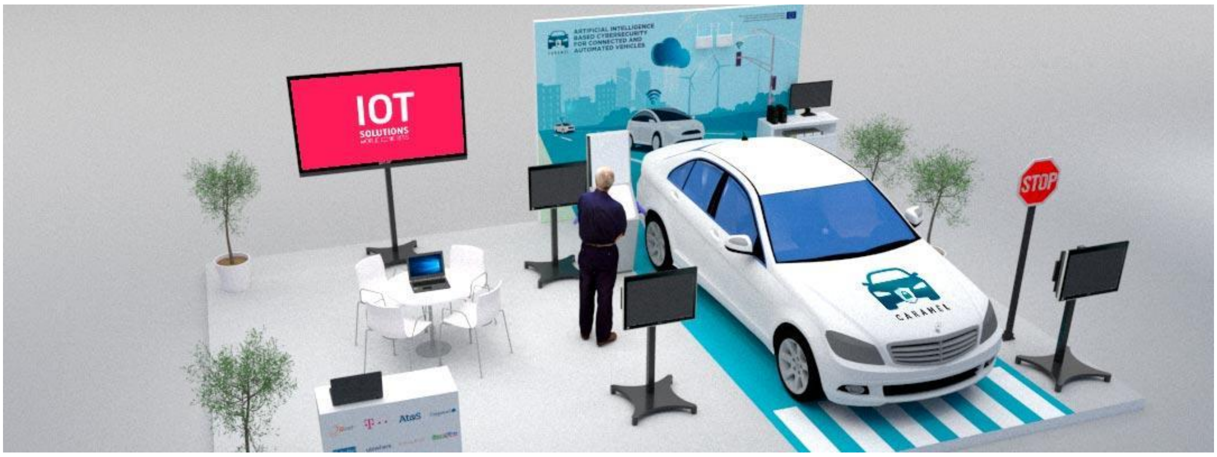

IOT
SOLUTIONS
ARTIFICIAL INTELLIGENCE BASED CYBERSECURITY FOR CONNECTED AND AUTOMATED VEHICLES
STOP
CARAMEL
AtoS

Figure 82 Render of the CARAMEL booth at the IoTS WC 2022

As shown in Figure 82 the rendering shows the devices necessary to carry out the technical demonstrations of the project which include the following devices.

HW requirements

- 1 LTE Small Cell
- 1 802.11p RSU
- 2 802.11p + LTE (OBUs)
- 1 Ethernet Switch
- 1 Vehicle

Frequency requirements

- GPS repeater

3. Execution

On the main screen was the CARAMEL introduction video which summarizes the contributions of the project in 3 minutes, is published on Youtube, and contains references to each of the demonstration videos created by the partners and which contain the results obtained.

In addition to the technologies originally planned to be demonstrated, demonstration videos were shown explaining the results of the project for each of the pillars addressed during the project.

Pillar 1:

On the screen on the front and right side of the vehicle, there were video demonstrations about:

- Detection and mitigation of physical attacks on traffic signs.
- Communication and operation of the backend for attack compilation.

Pillar 2:

On the screen on the left side of the vehicle there are video demonstrations about:

- OBU security
- V2X Interoperability
- Multi-Access Edge Computing

Pillar 3, 4:

On the screen on the back and right side of the vehicle there are video demonstrations about:

- Security of the charging stations
- Remote-controlled vehicles

During the three days of the exhibition, the project was presenting the technologies that will allow autonomous and connected vehicles to defend themselves against the possible cyberattacks addressed by the project.

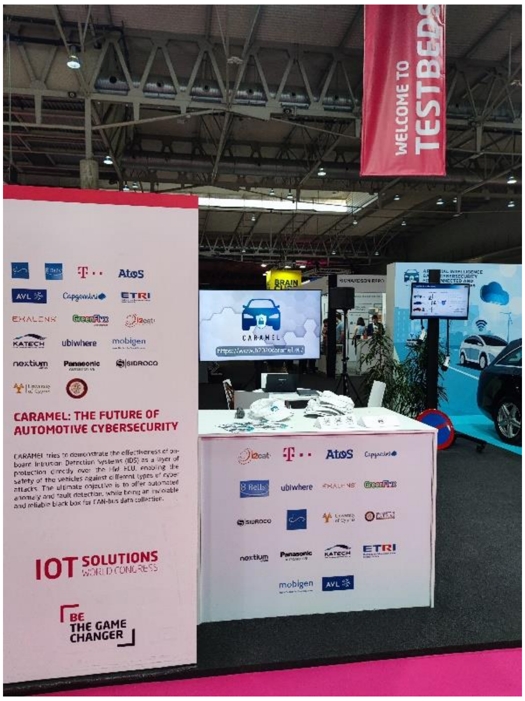

WELCOME TO
TESTBEDS
CARAMEL: THE FUTURE OF AUTOMOTIVE CYBERSECURITY
IOT SOLUTIONS WORLD CONGRESS
BE THE GAME CHANGER
CARAMEL

Figure 83 CARAMEL at the IoTS WC 2022

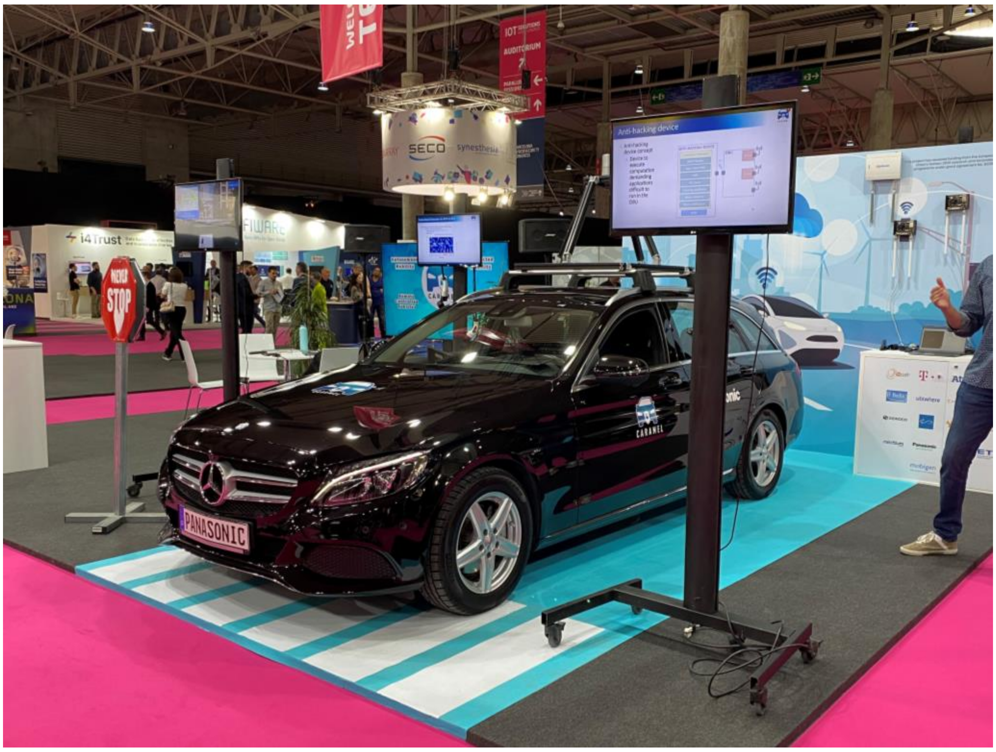


Figure 84 CARAMEL booth at the IoTS WC 2022

4. Results

It was incredible to witness the response of the visitors to the explanations of each of the members of the consortium since the visitors were always left with a smile for the incredible explanation.

The CARAMEL project had a successful participation in the activities of the IoTS WC, thanks to more than 400 visitors who were interested in knowing more about the project, to which the CARAMEL members offered them a personalised explanation to inform them about the most outstanding results of the project. The way in which these explanations were made was through official project tours or individual conversations.

According to the post-event analysis, it is estimated that up to 12,000 visitors [1] were present during the 3 days of the project exhibition, of which more than 400 were given detailed explanations, thus achieving wide dissemination of the results obtained by the project.

In addition to the detailed presentations offered, a percentage of the visitors were not only interested in the explanation but also approached CARAMEL to offer proposals of evolution and improvement oriented to a possible future of the project.

We highlight the participation of I2CAT, Capgemini, Panasonic, Atos and Nextium who had the opportunity to be in the testbed offering specific information about the project to each of the visitors to the CARAMEL testbed.

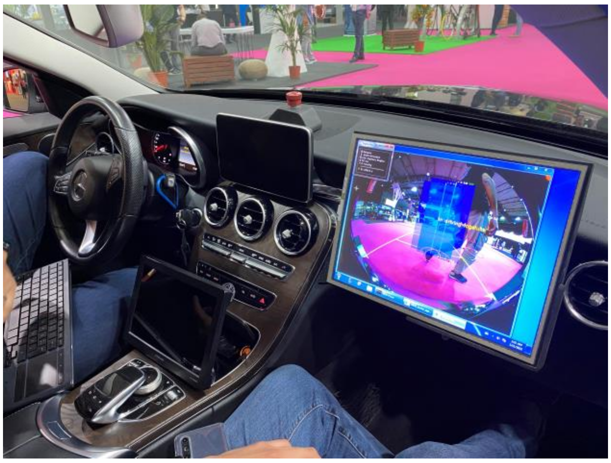


Figure 85 Interior of the vehicle used for the demonstration of CARAMEL

3.4.9 *Cancelled events*

It is important to mention the efforts made in planning for a couple of events that could not be carried out due to the pandemic that the entire world is facing.

It is the case of the mobile world congress, for which i2CAT would have a space available to promote the project activities. Among the planned activities, it was giving away flyers, and some videos about the project were about to be displayed on in-site screens. Besides, members of the consortium were going to be present to solve any doubt about the project. Sadly, due to the current pandemic, the event was cancelled, the official statement used to be in the following link. MWC | MWC Barcelona 2021. Alternatives press releases can also be found at the following link GSMA Statement on MWC Barcelona 2020 From John Hoffman, CEO GSMA Limited | Business Wire.

It was planned that during the ITS2020 congress to be held from 18 to the 20th of May 2020, Ubiwhere would be present at a stand. As members of the consortium, they would have the authority to distribute official brochures about the project. However, the restrictions imposed during that time prevent us from carrying out such activity. The official declaration of cancellation of the event can be found on the following website. Covid-19 Update - ITS in Europe (itseuropeancongress.com).

As part of the dissemination activities, a plan was organised to be conducted while attending ICT 2020, to be held from 1st to the 3rd of December 2020. There were plans to attend as one of the main exhibitors and to have a large participation of the members. CARAMEL as a consortium was about to showcase the initial results of the project with a set of interactive demos. However, once again, due to the actual situation, the event was cancelled. The official cancellation statement can be found at the following
link https://ec.europa.eu/digital-single-market/en/news/ict-2020-exhibitors-guide-event-cancelled.

3.4.10 *CARAMEL referrals*

During the time of running the CARAMEL project, several important results have been achieved, which are worthy of being presented or referred to by other websites. Table 5 presents a compilation of all the references to the objectives or results achieved by CARAMEL.

Referral ownership	Referral
Arcade Project	ARCADE database
Cyberwatching Project	Cyberwatching
Bavarian Research Alliance	Bavarian Research Alliance
Universitat Politecnica de Catalunya	MASTEAM-MATT
Altran	CARAMEL - Cybersicherheit für sicheren Straßenverkehr - Altran Deutschland
Atos	https://booklet.atosresearch.eu/project/caramel
Atos	https://booklet.atosresearch.eu/content/intelligence-based-cybersecurity-cooperative-connected-and-automated-mobility-ccam

Ficosa	https://www.ficosa.com/news/industrial-vehicle/european-commission-funded-project-caramel-cybersecurity-challenge-mobility/
i2CAT	https://i2cat.net/projects/caramel/
Greenflux	https://www.greenflux.com/greenflux-takes-part-in-h2020-cybersecurity-project-caramel/
8Bells	https://www.8bellsresearch.com/projects/h2020-caramel/
8Bells	https://www.8bellsresearch.com/our-projects/
Ubiwhere	https://www.ubiwhere.com/en/research-innovation/cybersecurity-caramel-tbd
Ubiwhere	https://www.ubiwhere.com/en/news/ubiwhere-integrates-cybersecurity-project-for-safer-connected-and-autonomous-mobility
University of Cyprus	https://www.kios.ucy.ac.cy/projects_kios/caramel-artificial-intelligence-based-cybersecurity-for-connected-and-automated-vehicles/
University of Cyprus	https://www.kios.ucy.ac.cy/kios-coe-develops-novel-solutions-for-detecting-cyber-attacks-against-vehicles/
Sidroco	https://sidroco.com/portfolio/sidroco_caramel_h2020_project/
Sidroco	https://sidroco.com/safer-roads-in-europe-the-h2020-project-caramel-kicks-off-in-barcelona/
CIT UPC	CARAMEL – Cybersecurity based on artificial intelligence for connected and automated vehicles - CIT UPC
i2CAT	CARAMEL keeps forging ahead on AI-based cybersecurity next-generation mobility - i2CAT
Cyberwatching	Korean Partners contribution plans to CARAMEL | Cyberwatching

Table 5 CARAMEL referrals

3.4.11 *CARAMEL press releases*

During project's runtime, different press articles have been published on local and international websites, which allow maximizing the dissemination of results at international level. Some of these publications were made during the presentation of the project at the international congress IoTSolutions. The congress was attended by about 12000 people and was covered by local and international news agencies. However, the intention of the CARAMEL project was from the beginning to be present at international congresses in order to have a higher visibility, unfortunately the pandemic suddenly changed some events.

Table 6 shows a compilation of the different press articles that have been published on different websites.

Lead member	Referral
i2CAT	About Intelligent Mobility For Energy Transition (IMET) | Smart Cities Marketplace (eu-smartcities.eu)
Sidroco	CARAMEL-SID-PRESS_RELEASE_09_2021.pdf (sidroco.com)
i2CAT	https://i2cat.net/i2cat-and-the-caramel-project-partners-present-innovative-anti-hacking-solutions-for-connected-and-automated-vehicles/
i2CAT	**https://i2cat.net/the-h2020-project-caramel-presents-innovative-anti-hacking-solutions-for-connected-and-automated-vehicles-at-iotswc-2022/**
La Vanguardia	El saló IOT repetirà l'aliança amb l'ISE per "reimaginar la digitalització" sumant les dues cites (lavanguardia.com)
inews24	[IOTSWC 2022] 자율주행차 해킹사고 어쩌나…EU ’카라멜' 철벽 사이버보안 (inews24.com)
La Vanguardia	Las empresas de ciberseguridad buscan profesionales en Barcelona (lavanguardia.com)

Table 6 Press release

3.4.12 *CARAMEL events participation*

The CARAMEL project has participated in a large number of events during the last 32 months of the project's life. These include a large number of presentations of papers at international congresses, participation in workshops with international attendance and of course in events organized by the project itself. Table 7 Compiles each of CARAMEl's participation in different events.

Event type	**Event name**	**Place**	**Dates**	Event/Material link
Workshop	Cybersecurity of Connected and Automated Vehicles	Online	17.09.2020	https://easychair.org/smart-program/EWGT2020/
Workshop	Advanced Cybersecurity Approaches for Connected, Automated and Electric vehicles	Online	20.09.2020	https://cybersec-itsc2020.isi.gr/
Invited to Workshop	IoTI4 Anomaly Detection and Cyber Attack Detection Competition	Online	15.07.2021	https://ioti4-2021.web.uowm.gr/program
Invited to workshop	CAST “Automotive Security”	Darmstadt,Germany (Online)	16.11.2020	https://cast-forum.de/workshops/programm/285?ts=1613392322057
Invited to workshop	CCAM Ethics WS	Online	26.10.2020	https://op.europa.eu/en/publication-detail/-/publication/b62d779f-f959-11ea-991b-01aa75ed71a1/language-en

OEM Workshop	1st OEM CARAMEL Workshop	Online	28.11.2020	https://www.h2020caramel.eu/2021/05/14/caramel-workshop/
OEM Workshop	2nd OEM CARAMEL Workshop	Online	13.12.2020	https://www.h2020caramel.eu/2021/10/12/caramel-2nd-oem-partner-workshop/
Joint Standarization Workshop	Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects	Online	19.11.2020	https://www.cybersane-project.eu/standardisation-workshop-2021/
Joint Standarization Workshop	2nd Joint Standardisation Workshop	Online	19.12.2020	https://www.eventbrite.com/e/2nd-joint-workshop-dynamic-countering-of-cyber-attacks-tickets-253095735157
Webinar	Future Mobility	Online	01.05.2020	https://www.ubiwhere.com/en/news/ebook-future-mobility-webinar-series
Webinar	IoTS	Barcelona	11.05.2022	https://youtu.be/7dfKLMbClIQ
Webinar	UCY,UPAT	Online	25.06.2022	https://www.youtube.com/playlist?list=PLrjgPTVt9x3zg1e9KsaKSVs35bvwwnkO6
Oral presentation	EuCNC2020	Dubrovnik, Croatia,	29.09.2020	https://zenodo.org/record/4441684#.YAl_mTmSlhF
Oral presentation	EuCNC2020	Dubrovnik, Croatia,	29.09.2020	10.1186/s13638-021-01980-w
Oral presentation	ISVLSI2020	Limassol, Cyprus,	02.10.2020	https://zenodo.org/record/3987790#.YAl_qjmSlhF
Oral presentation	ICTON2020	Bari, Italy,	05.10.2020	https://zenodo.org/record/4441693#.YAl9LDmSlhF
Oral presentation	ICTON2020	Bari, Italy,	08.10.2020	https://zenodo.org/record/4441739#.YAl_tzmSlhF
Oral presentation	ICTON2020	Bari, Italy,	11.10.2020	https://zenodo.org/record/4441754#.YAl_szmSlhF

Oral presentation	ICTON2020	Bari, Italy,	14.10.2020	https://zenodo.org/record/4441693#.YAl9LDmSlhF
Oral presentation	EWGT2020	Paphos, Cyprus	17.10.2020	https://www.sciencedirect.com/science/article/pii/S2352146521000685
Oral presentation	EWGT2020	Paphos, Cyprus	20.10.2020	https://www.sciencedirect.com/science/article/pii/S2352146521000715?via%3Dihub
Oral presentation	EWGT2020	Paphos, Cyprus	23.10.2020	https://www.sciencedirect.com/science/article/pii/S2352146521000703
Oral presentation	IEF2020	Online	04.11.2020	https://www.youtube.com/watch?v=dLS1gYhfTac
Oral presentation	WACV2021	Online	26.10.2020	https://zenodo.org/record/5647753#.YoywZ6hBxD8
Oral presentation	DCOSS 2021	Online	15.07.2021	https://zenodo.org/record/6598222#.YpccN6hBxD8
Oral presentation	VTC2021-Fall	Online	29.10.2020	https://zenodo.org/record/5791231#.YdXV6WhKhhE
Oral presentation	IEEE MMSP	Hybrid/Finland	04.12.2020	https://zenodo.org/record/6637704#.YqxJcKLP1D8
Oral presentation	DATE 2022	Online	18.03.2022	https://zenodo.org/record/6580784#.YqxI1KLP1D8 https://www.date-conference.com/project/caramel
Speaker	MASTEAM-MATT talk	Barcelona	10.11.2020	https://eetac.upc.edu/ca/noticies/masteam-matt-talks-dr-pouria-sayyad-khodashenas-i2cat-protecting-the-new-generation-of-cars-from-cybercriminals
Speaker	AI & Big Data	Barcelona	01.12.2020	https://www.h2020caramel.eu/2021/09/08/caramel-at-aibigdata21/
Speaker	IEEE ITSC	Online	01.09.2020	-
Speaker	JUMP2DIGITAL	Barcelona	01.11.2021	https://www.h2020caramel.eu/2021/05/14/caramel-workshop/
Speaker	Risk	-	-	Information can not be shared
Speaker	DATE2022	Online	01.11.2020	https://www.h2020caramel.eu/2022/03/22/caramel-at-the-date2022/

Conference Participation	ECCV 2020	Online	22.11.2020	https://eccv2020.eu/
Conference Participation	Cybersecurity Standardization Conference 2021	Online	25.11.2020	https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021
Congress Participation	ITS WC Hamburg 2022	Hamburg	07.12.2020	-
Congress participation	IoTSWC	Barcelona	12.05.2022	https://www.h2020caramel.eu/2022/05/17/caramel-at-the-iot-solutions-world-congress/
CARAMEL meeting	Project KickOff	Barcelona	22.10.2019	https://www.h2020caramel.eu/2019/10/22/intelligence-based-cybersecurity-for-cooperative-connected-and-automated-mobility-ccam/
CARAMEL meeting	2nd General Assembly	Aveiro	29.01.2020	https://www.h2020caramel.eu/2020/01/31/2nd-general-assembly-of-caramel-project/
CARAMEL meeting	Technical Meeting	Online	15.01.2022	https://www.h2020caramel.eu/2022/01/25/technical-meeting/
CARAMEL meeting	21st General Assembly	Cyprus	28.04.2022	https://www.h2020caramel.eu/2022/04/28/21st-ga-meeting/
CARAMEL meeting	Kios Seminar Series	Cyprus	28.04.2022	https://www.h2020caramel.eu/2022/04/28/21st-ga-meeting/
CARAMEL meeting	Demo Preparation	Frankfurt	08.06.2022	https://www.h2020caramel.eu/2022/06/10/final-demonstration-preparation/
CARAMEL meeting	Final Demo	Frankfurt	21.06.2022	https://www.h2020caramel.eu/2022/06/22/final-demonstration/

Table 7 List of events

4 Dissemination and communication formats

Dissemination and communication formats are understood to be any sort of means through which the CARAMEL project's main messages can be transmitted and communicated outside of the consortium.

4.1 *Communication material kit*

During the first half of the project, some audio-video media were created to enable communication and dissemination of relevant information. The files can be found in the following compilation table.

Demo Video Series

Figure 86 CARAMEL Demo Video Series Logo

As part of the effort to disseminate the results of the project, demonstration videos were created to explain in a general way the modules that contribute to the anti-hacking system developed by CARAMEL. Each of the videos is composed of an introduction to the developed system, followed by a general explanation of the system, and finally a presentation of the most outstanding results of the particular system. Within the scope of the developments presented, you can find systems developed for some of the pillars addressed by CARAMEL.

The titles of the videos are:

- RSU-OBU-TestBed
- Traffic sign anomaly detection and mitigation pipeline
- Detecting possible attacks on the camera sensor using a deep learning approach
- In-vehicle Location Spoofing Attack Detection
- Holistic Situational Awareness with ML Application
- Collaborating mitigation mechanism against GPS spoofing

Brochure	https://www.h2020caramel.eu/wp-content/uploads/2020/02/Caramel_flyer.pdf
Video	https://youtu.be/AAL1sk-vDYk Multimedia – CARAMEL (h2020caramel.eu)
Poster	https://www.h2020caramel.eu/wp-content/uploads/2021/03/CARAMEL_poster.png

Table 8 Audiovisual media compilation

4.2 *Automotive Threat Modelling Tutorial*

Figure 87 Automotive threat modelling logo

Have you ever wondered how to perform a detailed analysis to identify threats in autonomous vehicles?

CARAMEL's members created a tutorial that explains how to develop and analyse an automotive threat model using Microsoft's Threat Modelling tool through the STRIDE technique.

The tutorial focuses on providing step-by-step information to develop and analyse a threat model for Automotive using the Microsoft Threat Modeling Tool and STRIDE threat modelling approach, which utilises a data flow diagram of a process or system to identify relevant threats.

The STRIDE technique tries to identify as many threats as possible in the system by decomposing a more extensive system into its most relevant components.

The STRIDE technique was named after the threats, it can identify.

Spoofing
Tampering
Repudiation
Information disclosure
Denial of service
Elevation of privilege

After reading the tutorial you will be able to:

- Install the Microsoft Threat Modelling Tool
- Create a threat model
- Design a data flow
- Identify threats using a STRIDE model
- Identify mitigation actions

The automotive threat tutorial has been published on the official website of the project to present a collection of open knowledge around the use of the Microsoft Threat Modelling Tool application.

The tutorial was completed and published on the website in August 2021, since then the tutorial has been downloaded a total of 521 times according to the statistics collected by the website.

4.3 *Publications*

During past 32 months, CARAMEL has developed several papers, developed as a result of the project's research outcomes. Some of those papers have been presented to a wider audience by means of different international conferences. The full list of accepted CARAMEL papers can be found in Table 8.

4.3.1 Open Access

Open access (OA) refers to making research publications openly available so that anybody can read and use it. Open access can mean more than just making research available for reading; it can also mean allowing others to reuse it. Allowing content to be analysed via text mining1 or utilized for commercial purposes, for example. Open access to research data and books is becoming more common. Open access is part of a larger "open" movement that promotes the free exchange of knowledge and resources to increase access and foster creativity. Several benefits like wider economy and society make sure that everybody could benefit from the ongoing research rather than only the people who can afford it. Open access has made it possible in improving the reach of the research work, the reputation of the research institutions and their hosts because of the increased number of the citation, and at the end, open access has greatly impacted improving the quality of the research as it is more open transparent and reproducible [13]. A similar workflow or the idea behind the open science and open access is being adapted in the Caramel project in order to facilitate the ongoing research in the field of sensor technology, V2X communication, electromobility, etc. Partners who are coming from an academic background are very keen to follow these methodologies as it helps in building the research community in a more transparent way since the research of any topic is a collaborative effort. The papers published by the partners of the project are made easily accessible to all, for instance, the Caramel project has a community that includes open access versions of all publications on Zenodo and all the partners are vocal towards creating a collaborative and supportive research community by adhering the idea of open science and open access.

As part of the dissemination activities of the project some of the papers already published have been added to a public collection within the Zenodo platform. The aim of this collection is to compile each of the papers done by CARAMEL in an open access repository.

The link to access the CARAMEL community on Zenodo's homepage is:

https://zenodo.org/communities/caramel_h2020

Type	Name	Authors	Publisher	Link
1	The CARAMEL Project: a Secure Architecture for Connected and Autonomous Vehicles	Vitale, C.; Piperigkos, N.; Laoudias, C. ; Ellinas, G. Casademont, J.; Khodashenas, S.P.; Kloukiniotis, A.; Lalos, A. S.; Moustakas, K.; Barrientos Lobato, P.; Moreno Castillo, J.; Kapsalas, P.;Hofmann, K. P	IEEE	10.1109/EuCNC48522.2020.9200945
2	Towards Artificial-Intelligence-Based Cybersecurity for Robustifying Automated Driving Systems Against Camera Sensor Attacks	Kyrkou, Christos; Papachristodoulou, Andreas; Kloukiniotis, Andreas; Papandreou, Andreas; Lalos, Aris S. Moustakas, K.; Theocharides, T.	IEEE	10.1109/ISVLSI49217.2020.00-11
3	GNSS Location Verification in Connected and Autonomous Vehicles Using in-Vehicle Multimodal Sensor Data Fusion	Souli, N.; Laoudias, C. ; Kolios, P. ; Vitale, C. ; Ellinas, G. ;Lalos, A. ; Casademont, J. ; Khodashenas, P. S. ; Kapsalas, P.;	IEEE	10.1109/ICTON51198.2020.9203087
4	Multi-Radio V2X Communications Interoperability Through a Multi-Access Edge Computing (MEC)	Casademont, J.; Cordero, B. ;Camps-Mur, D. ; da Conceição, L. A. M. ; Lalos, A. ; Vitale, C. ; Laoudias, C. ; Khodashenas, P. S.;	IEEE	10.1109/ICTON51198.2020.9203495
5	5G Enabled Cooperative Localization of Connected and Semi-Autonomous Vehicles via Sparse Laplacian Processing	Piperigkos, N. ; Lalos, A. S. ; Berberidis, K. ; Laoudias, C. ; Moustakas, K.;	IEEE	10.1109/ICTON51198.2020.9203314
6	Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL	Argyropoulos, N; Khodashenas, P. S; Orestis, M.; Eirini, K.; Anastasios, L.;Karypidis, P.A.; Hofmann, P.	Elsevier	10.1016/j.trpro.2021.01.036

7	Impact of False Data Injection attacks on Decentralized Electric Vehicle Charging Protocols	Piperigkos, N.; Lalos, A. S.	Elsevier	10.1016/j.trpro.2021.01.039
8	A benchmarking framework for cyber-attacks on autonomous vehicles	Khadka, A; Efstathopoulos, G.; Karypidis, P; Lytos, A	Elsevier	10.1016/j.trpro.2021.01.038
9	Exploring Adversarial Attacks and Defences for Fake Twitter Account Detection	Panagiotis, K.; Nikolaos, P.; Pitropakis, Nikolaos Mylonas, Alexios Kylilis, Nicolas	MDPI	10.3390/technologies8040064
10	CARAMEL: results on a secure architecture for connected and autonomous vehicles detecting GPS spoofing attacks	Vitale, C.; Piperigkos, N.; Laoudias, C.; Ellinas, G.; Casademont, J.; Escrig, J.; Kloukiniotis, A.; Lalos, A.S.; Moustakas, K.; Diaz, R.; Baños, D.; Roqueta G.; Hofmann, P.; Khodashenas, P. S. ; Kapsalas, P.	Springer Open	10.1186/s13638-021-01971-x
11	DriveGuard: Robustification of Automated Driving Systems with Spatio-Temporal Convolutional Autoencoder	Andreas Papachristodoulou, A.; Kyrkou, C.; Theocharides, T.	IEEE	10.1109/WACVW52041.2021.00016
12	Deep multi-modal data analysis and fusion for robust scene understanding in CAVs	Papandreou, Andreas; Kloukiniotis, Andreas; Lalos, Aris; Moustakas, Konstantinos	IEEE	10.1109/MMSP53017.2021.9733604

13	**GPS Location Spoofing Attack Detection for Enhancing the Security of Autonomous Vehicles**	**Kamal, Mohsin; Barua, Arnab; Vitale, Christian; Laoudias, Christos; Ellinas, George**	**IEEE**	**10.1109/VTC2021-Fall52928.2021.9625567**
14	**A Comprehensive Solution for Securing Connected and Autonomous Vehicles**	**Kamal, Mohsin; Kyrkou, Christos; Piperigkos, Nikos; Papandreou, Andreas; Kloukiniotis, Andreas; Casademont, Jordi; Porras Mateu, Natalia; Banos Castillo, Daniel; Diaz Rodriguez, Rodrigo; Durante, Nicola Gregorio** **Hofmann, Peter; Kapsalas, Petros; Lalos, Aris** **Moustakas, Konstantinos; Laoudias, Christos** **Theocharides, Theocharis; Ellinas, Georgios**	**IEEE**	**10.23919/DATE54114.2022.9774594**
15	**Synthetic Traffic Signs Dataset for Traffic Sign Detection & Recognition In Distributed Smart Systems**	**Ilias Siniosoglou, Panagiotis Sarigiannidis, Yannis Spyridis, Anish Khadka, Georgios Efstathopoulos, Thomas Lagkas**	**IEEE**	10.1109/DCOSS52077.2021.00056
16	Validation and Benchmarking of CNFs in OSM for pure Cloud Native applications in 5G and beyond	Adrian Pino, Pouria Khodashenas, Xavier Hesselbachz, Estefanıa Coronado, Shuaib Siddiqui	**IEEE**	10.1109/ICCCN52240.2021.9522356
17	Countering adversarial attacks on autonomous vehicles using denoising techniques: A Review	Andreas Kloukiniotis, Andreas Papandreou, Aris Lalos; Petros Kapsalas; Duongvan Nguyen, Konstantinos Moustakas	**IEEE**	10.1109/OJITS.2022.3142612
18	CarlaScenes: A synthetic dataset for odometry in autonomous driving	Andreas Kloukiniotis, Andreas Papandreou , Christos Anagnostopoulos, Aris Lalos, Petros Kapsalas , Duongvan Nguyen, Konstantinos Moustakas,	**CVPR**	**Not released yet (15.06.2022)**

19	Automotive and 5G Network Threats	**Konstantinos Kaltakis, Emmanouil Kafetzakis, Ioannis Giannoulakis**	**-**	Automotive and 5G Network Threats

Table 9 List of Publications

5 Monitoring and Evaluation of dissemination & communication activities

5.1 *Methodology for Evaluation*

The work performed under T7.1 "Dissemination, Communication and Exploitation of Results" of CARAMEL project will be closely monitored and coordinated by the task leader. To measure the impact of the conducted activities and to be able to adjust/fine-tune the dissemination and communication strategy for achieving the expected outcomes and maximising visibility, a set of initial metrics has been developed. Such metrics (Performance Indicators hereafter) will allow having a constant view of the quantitative amount and the qualitative effectiveness of the dissemination and communication activities conducted.

5.2 *Related Performance Indicators*

Course	Student	Title	Partner
PhD 1	Nicolas Souli	Robust Localization and Navigation of Autonomous Vehicles using Signal of Opportunity	UCY
PhD 2	Andreas Papachristodoulou	Multi-task learning for scene understanding with Graph Neural Networks	UCY
Master 1	Roser Batlle Roca	Implementation of a virtual environment to perform driving test in static	I2CAT
Master 2	Carlos García Manrique (VIU)	Connected Car: V2X Threat Modelling analysis	I2CAT
Master 3	Cesar Manuel Ymaya (VIU)	Connected Car: V2X Threat Modelling analysis	I2CAT
Master 4	Eduardo Cervantes Duenas	Resilience of Edge-optimized CNNs to Adversarial Attacks	Capgemini Engineering

Table 10 Academic related collaboration

As a way of tracking CARAMEL's activities, a compilation of the project's performance indicators can be seen in the following table.

KPI	Description	Target description	Status/Target
CARAMEL website “Yearly visits”	Disseminate the project and its achieved goals to a wider audience	200 visits to the website each month.	9384/6600 (31 May 2022)
Conferences	Participation on conferences	3 oral presentations per year	15/9
Industrial fairs	Participate in exhibitions	8 participations per year	39/24
Training “Tutorial”	Tutorial package for threat analysis and cyber-threats	File should be downloaded at least 500 times.	512/500 20 May 2022
Training “Supervision of students”	Supervision or co-supervision of students	At least 2 Phd and 4 M.Sc	2/2 PhD 4/4 M.Sc
Workshop seminars	Organise 3 workshops at academia and industry.	3 Workshops	4/3

Webinars	Offer 3 Webinars	3 Webinars	2/3 1 Webinar in progress
White papers	Contribute with: 2 CARAMEL white papers 5 joint white papers	CARAMEL white papers are planned based on the topics of WP2, WP3, WP4.	2/2 CARAMEL WP 5/5 Joint WP
Standard contributions	Creation of 2 standard contributions	Standardisation KPIs was slightly modified	This KPI was modified (Table 12)
Workshops to “potential clients”	Introduce the outcomes of CARAMEL to potential clients	More than 110 users were registered for the planned workshops, to which at least 5 participants were representing an OEM	5
CARAMEL website “File downloads”	Provide an open-source publications collection	30 monthly downloads of any uploaded document.	6564 total downloads from all the papers published by the CARAMEL consortium

		900	
CARAMEL website “external link”	Track references from external websites	Increasing Trend	18 (Table 5)
Press releases	Press releases in tech and magazines	2 references per year in any tech magazine or website	4 internal press releases 3 external press releases (Table 6)
Market events Presence	Professional presence 3 presences per year.		10/9 (Table 7)

Table 11 CARAMEL dissemination and communication KPI

5.3 *KPI's for Standardization Activities*

The new KPIs represent measurable, concrete indicators for the efforts invested by CARAMEL partners into standards contribution (supported by calendar entries as well as internals documents and deliverables). Additionally, the KPIs measure the impact of the standards and standards organization by looking at geographical reach and industry support (measured by countries and companies involved). Since the standardisation activity is a long-term activity in CARAMEL project the goal of the KPI's related to standardisation has been divided into several activities carried out by the partners. In the below table the partners have tried to summarise the ongoing activities in the respective standardisation bodies. DT-Sec one of the partners from CARAMEL has actively involved and contributed to a work item on 5G-Automotive association; WG7; Misbehaviour Detection.

Horizon Standardisation booster initiative is giving the standardisation support for Horizon Europe and H2020 R&I projects and hence helping to increase valorise project results by contributing to the creation or revision of standards. To increase the European impact on (international) Standardisation and strengthen European competitiveness, HSbooster.eu facilitates and streamlines the dialogue between Horizon 2020 and Horizon Europe Research & Innovation projects with the Standardisation landscape and its main actors, namely corresponding Standards Developing Organizations (SDOs). CARAMEL project has applied for the initiative as an interested project and is awaiting to evaluate the first open call at the consortium level. This is a good opportunity for the consortium and specially for the main partners involved actively in standardisation activities going forward following EC specific programmes in this important field

Sl No	KPI Description	Targets	PASEU	PASEU	AVL	AVL	5GAA Misbehaviour detection
1	Number of Working Groups (WG) Involved	3	ADASIS	IEEE P2020/ WG3	ISO/TC22/ SC32/WG11	ISO/TC22/ SC32/WG12	1 WG
2	Importance of Standardization group - International reach (e.g., number of countries involved)	100	22	20	33	33	20
3	Importance of standardization group - Number of members in the committee	10	234	200	234	107	10
4	Number of meetings attended during the CARAMEL runtime	50	12 (20.08.2020)	12 since July 2016	12 (since 01.10.2020)	14 (since 01.10.2020)	85
5	Number of contributions (verbal or written) to standardization (e.g., verbal contribution to a meeting, mail to a mailing list)	20	10	8	10	2	10

Table 12 Standardization KPIs

5.4 *Overview of dissemination and communication channels and formats*

Items	Type of Activity	Amount
Publications (current reporting period)		
1	Publications (books, magazines, journals)	20
TOTAL (1)		**20**
Events (current reporting period)		
2	Participations in events	34
3	CARAMEL events	7
4	CARAMEL workshop	4
TOTAL (2-4)		**45**
Digital presence (current reporting period)		
5	Twitter Posts	135
6	Linked Posts	100
7	CARAMEL website posts	33
TOTAL (5-7)		**268**
Other activities (current reporting period)		
8	Liaison projects and initiatives	11
TOTAL (8)		**11**
Formats (current reporting period)		
9	Brochure	1
10	Press release	7
11	Video	7
	TOTAL (9-11)	**15**

Table 13 Overview of dissemination and communication actions

6 Conclusions

According to the work plan of CARAMEL the main objective of the task T7.3 and report D7.4 is to coordinate the process of dissemination, communication, Standardization, and interaction with the stakeholders. In the first reporting period, main preference was given to defining a suitable work plan and progress in the defined direction. Whereas in the last period of the project the discussions were made as how to address or collaborate with the target stakeholders and hence events like OEM workshops were organised. With these events the CARAMEL consortium was able to reach out to wide variety of audiences and establish a relation with innovation bodies and organize more events to connect with the audience from all possible fields.

This final report is vital for the effective Dissemination and Communication strategy therefore this document has elaborated on the status of Standardization, Dissemination, Communication and Digital Presence. Several Standardization bodies are involved in cybersecurity ISOs (e.g., ISO/SAE DIS 21434, ISO PAS 5112) and worldwide development partnerships of vehicle manufacturers such as AUTOSAR (AUTomotive Open System ARchitecture). With regards to the activities related to standardisation the ISO standard 21434 and ISO/PAS 5112 are finally published and now available to be applied or followed. ITS TC204 adversity group1 was dissolved in April and all the activities related to it has been halted. To this end, the release of these standards is a big milestone regarding the standardization of cybersecurity engineering in the automotive sector as OEMs are now obliged to follow security logging and intrusion detection technologies to protect the vehicle against any attacks or security events.

The Dissemination and Communication channels were elaborated in detail covering an array of channels including websites, Social Networks, Liaison with other projects and initiatives and organization and participation in events related to the automotive and cybersecurity context. To ensure the dissemination process qualitatively and quantitatively, a monitoring and evaluation procedure was established including several key performance indicators that were defined. It is important to build up on the consortium strengths and its shared views towards dissemination and communication for CARAMEL to achieve maximum visibility and create an impact within the business and scientific community in order to accelerate faster adoption of the research and innovation outputs.

The following actions were performed during the last phase of the project.

- Creation and launch of various press releases
- disseminate results through social networks and other public platforms
- Keep the website up to date
- Create Tutorial package for threat analysis and cyber-threats
- Maintain and create new partnerships with other projects
- Keep participating in events

Given the above, the current deliverable covers all the relevant activities which are carried out by the CARAMEL partners as part of the task 7.3 and WP7.

7 References

1) Dissemination, Communication and Exploitation Plan, CARAMEL consortium, April 2020

2) ISO, https://www.iso.org/stages-and-resources-for-standards-development.html (last time retrieved March 2022)

3) 5GAA, https://5gaa.org/about-5gaa/about-us/ (last time retrieved April 2022)

4) ECSO (European Cyber Security Organisation), https://ecs-org.eu/ (last time retrieved March 2022)

5) CSIRTs, https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network (last time retrieved March 2022)

6) Deutsche Telekom CERT, FIRST (Forum of Incident Response and Security Teams). https://www.first.org (last time retrieved April 2022)

7) P2020,https://www.image-engineering.de/content/library/white_paper/P2020_white_paper.pdf

8) ISO, Stages, and resources for standards development https://www.iso.org/stages-and-resources-for-standards-development.html (last time retrieved March 2022)

9) https://www.btc-es.de/en/blog/autosar-what-every-function-developer-should-know.html (last time retrieved April 2022)

10) https://standards.iteh.ai/catalog/tc/iso/22b5a80b-91bd-410c-8c5f-edca3509638c/iso-tc-204 (last time retrieved April 2022)

11) https://open-science-training-handbook.gitbook.io/book/open-science-basics/open-concepts-and-principles (last time retrieved April 2022)

12) https://blog.theopenscholar.com/en/open-science-purpose-benefits (last time retrieved May 2022)

13) https://www.jisc.ac.uk/guides/an-introduction-to-open-access (last time retrieved May 2022)

14) Cybersecurity Regulations and Standards in the Automotive Domain, Thomas Schober, Gerhard Griessnig, AVL List GmbH

15) https://www.btc-es.de/en/blog/autosar-what-every-function-developer-should-know.html (last time retrieved May 2022)

16) https://www.btc-es.de/en/blog/autosar-what-every-function-developer-should-know.html (last time retrieved May 2022)

17) https://www.date-conference.com/project/caramel (last time retrieved May 2022)

18) https://www.embitel.com/blog/embedded-blog/decoding-the-component-concept-of-the-application-layer-in-autosar (last time retrieved May 2022)

19) IEEE Standards Association, IEEE P2020 Automotive Imaging White Paper, Authored by Members of the IEEE P2020 Working Group, October, 2019 https://www.image-engineering.de/content/library/white_paper/P2020_white_paper.pdf

20) P2020™/D2 1 “Draft Standard for Automotive System Image Quality”, Developed by the Members of the IEEE P2020 Working Group, June 2022 (submitted to IEEE SA Standards board)