

## D7.1

# Plan for Dissemination and Exploitation incl. Communication

Project number	101069688
Project acronym	CONNECT
Project title	Continuous and Efficient Cooperative Trust Management for Resilient CCAM
Start date of the project	1 <sup>st</sup> September 2022
Duration	36 months
Call	HORIZON-CL5-2021-D6-01-04

Deliverable type	R
Deliverable reference number	D6-01-04/ D7.1/ V1.1
Work package contributing to the deliverable	WP7
Due date	Feb 2023 – M06
Actual submission date	28 <sup>th</sup> February 2023

Responsible organisation	TEC
Editor	Nicole Mitsche
Dissemination level	PU
Revision	1.1 (disclaimer updated)

Abstract	This deliverable presents the CONNECT communication kit including the project's visual identity as well as communication and dissemination material to be used within the project. Furthermore, a detailed standardization plan is documented constituting a guideline for the liaison and further dissemination of the CONNECT project to external target groups and related standardization working groups. A timeline of short- and long-term dissemination activities is presented.
Keywords	Communication Kit, Collaborative Tools, Infrastructure, Website, Homepage, Internal Communication, Standardization, Liaisons, Stakeholders

## Document Revision History

Version	Date	Description of change	List of contributors
V0.1	12.12.2022	ToC was created.	Nicole Mitsche (TEC)
V0.2	15.12.2022	First draft, outline of dissemination and communication aspects	Nicole Mitsche (TEC)
V0.3	20.12.2022	Detailed outline on standardisation and exploitation chapters, including lead responsibilities	Nicole Mitsche (TEC)
V0.4	12.01.2023	First draft on standardisation and exploitation	Thanassis Giannetsos, Dimitris Karras (UBITECH) Ioannis Krontiris (HUAWAI) Antonio Kung (TRIALOG) Peter Schmitting (FSCOM) Francesca Bassi (IRTSX) Panagiotis Pantazopoulos (ICCS) Chris Newton, Liqun Chen (SURREY) Alexander Kiening (DENSO)
V0.5	26.01.2023	Finalised draft ready for review	Nicole Mitsche (TEC)
V0.5	02.02.2023	First internal reviews	Barbara Gaggl, Martina Truskaller (TEC)
V0.6	27.02.2023	Reviewed documents	Thanassis Giannetsos (UBITECH) Konstantinos Latanis (SUITE5)
V1.0	28.02.2023	Final version	Nicole Mitsche (TEC) Thanassis Giannetsos (UBITECH)
V1.1	03.04.2024	Disclaimer updated	Lisa Burgstaller-Hochenwarter (TEC)

**Editor**

Nicole Mitsche (TEC)

**Contributors** (ordered according to beneficiary numbers)

Barbara Gaggl, Martina Truskaller (TEC)

Thanassis Giannetsos, Dimitris Karras (UBITECH)

Ioannis Krontiris (HUAWEI)

Antonio Kung (TRIALOG)

Peter Schmitting (FSCOM)

Francesca Bassi (IRTSX)

Panagiotis Pantazopoulos (ICCS)

Chris Newton, Liqun Chen (SURREY)

Alexander Kiening (DENSO)

**Disclaimer**

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability

## Executive Summary

This Deliverable aims to provide a clear update on the **initial communication, dissemination and standardization plan**, of the CONNECT project. **Dissemination and communication activities that took place in the first six months of the project are explained and further plans are summarized.** Updates on the dissemination report will be provided in the upcoming periodic reports as well as in D7.2 “Dissemination, Communication, Clustering and Exploitation activities” in M18 and D7.3 “Dissemination, Communication, Clustering activities including concrete exploitation measures” in M36.

After the introductory chapter, Chapter 2 depicts the mission of CONNECT and the fundamental aspects of the dissemination and communication plan, including the main objectives and the planning of the envisioned activities. Chapter 3 then proceeds with the description of the KPIs (metrics for the evaluation of the dissemination and communication activities) already defined for a successful dissemination plan to the specified target audiences. Chapter 4 presents the various types of dissemination activities and tools – such as the project’s website, that will be used in order to support the project’s dissemination and communication activities. Chapter 5 and Chapter 6 put forth detailed lists of already performed communication activities and a series of workshops and events that CONNECT is planning to attend and contribute in the near future (short-term activities). This list is a live document that will be updated through the lifecycle of the project. Chapter 7 focuses on activities related the collaboration with relevant initiatives and the standardization plan. Chapter 8 sets the baseline for the exploitation plan that will be created later in the project by documenting the methodology to be followed (putting forth the envisioned Open-Source Development Plan to be employed) for the list of exploitable assets already identified. Finally, Chapter 9 concludes the document.

# Table of Contents

<b>Chapter 1</b>	<b>Introduction</b>	<b>1</b>
1.1	Purpose of the Document	1
<b>Chapter 2</b>	<b>Dissemination &amp; Communication Strategy</b>	<b>4</b>
2.1	CONNECT Mission	4
2.2	Visual Identity of the Project	5
2.2.1	Project Logo	5
2.2.2	Project Templates	6
2.3	CONNECT Advisory Board	7
2.4	Sustainable Dissemination and Communication Approach	8
<b>Chapter 3</b>	<b>Dissemination &amp; Communication Targets</b>	<b>9</b>
3.1	Dissemination KPIs	9
3.2	CONNECT Stakeholders	10
<b>Chapter 4</b>	<b>Dissemination and Communication Kit</b>	<b>12</b>
4.1	CONNECT Project Web Site	12
4.2	CONNECT Announcement Letter	14
4.3	CONNECT Leaflet	14
4.4	CONNECT Videos	15
4.5	CONNECT Social Media	16
4.6	CONNECT Newsletter	17
4.7	CONNECT Collaborative Tools	17
4.7.1	Project Internal	17
4.7.2	Mailing List Server	18
4.7.3	Online Conference Calls	18
4.8	CONNECT Events and Workshops	18
4.8.1	Innovation Workshops	19
4.8.2	Internal and External Training	19
4.8.3	Scientific Workshops	20
4.8.4	End-User Workshops	20
<b>Chapter 5</b>	<b>Past dissemination and communication activities</b>	<b>21</b>
<b>Chapter 6</b>	<b>Planned Dissemination and Communication Activities</b>	<b>25</b>
<b>Chapter 7</b>	<b>Relevant Initiatives and Standardization</b>	<b>28</b>
7.1	Liaison with Relevant Initiatives	28
7.1.1	Automotive Associations and Initiatives	29
7.1.2	5GAA	30

7.1.3	Open-Source Communities .....	31
7.1.4	Building Trust and Resilience in CCAM .....	31
7.2	Standardisation Activity Plan.....	31
7.2.1	Research and Standardization Communities .....	31
7.2.2	Standardization Bodies & CONNECT Road-Map.....	32
<b>Chapter 8</b>	<b>Exploitation Plan .....</b>	<b>39</b>
8.1	Exploitable Artefacts .....	39
8.2	Open-Source Development Plan.....	41
<b>Chapter 9</b>	<b>Summary and Conclusion .....</b>	<b>44</b>
<b>Chapter 10</b>	<b>List of Abbreviations.....</b>	<b>45</b>
<b>Chapter 11</b>	<b>References .....</b>	<b>46</b>

## List of Figures

Figure 1: Dissemination & Communication phases .....	1
Figure 2: The CONNECT Dissemination & Communication strategy.....	4
Figure 3: CONNECT Logo .....	6
Figure 4: CONNECT Power Point Template .....	6
Figure 5: The main page of the CONNECT website.....	12
Figure 6: CONNECT Blog .....	13
Figure 7: CONNECT project leaflet .....	14
Figure 8: CONNECT Video example.....	15
Figure 9: CONNECT 15 seconds video.....	16
Figure 10: CONNECT Short-Term Standardization Activities Plan.....	33
Figure 11: CONNECT Implementation of OSD Plan .....	42

## List of Tables

Table 1: Key performance indicators for dissemination and communication activities .....	9
Table 2: CONNECT Stakeholders.....	10
Table 3: CONNECT Mailing Lists.....	18
Table 4: Past dissemination and communication activities .....	21
Table 4: Planned dissemination and communication activities .....	25
Table 6: CONNECT Technology-related Associations and Initiatives.....	29
Table 7: Research and Standardization Communities.....	32
Table 8: Standardisation Bodies and CONNECT Road-Map.....	33
Table 9: Overview of CONNECT members participation in relevant clusters/associations associated to CONNECT outcomes .....	35
Table 10: CONNECT High-Level Summary of Exploitable Assets.....	40

# Chapter 1 Introduction

## 1.1 Purpose of the Document

This deliverable provides an overview of the **CONNECT communication, dissemination and exploitation plan** as well as a first report on activities, which includes communication and dissemination material that are created and used within the project. As thoroughly described in our initial plan of dissemination (D), communication (C) and exploitation (E) activities (DoA – Section 2.2), our activities are clustered into three main phases, illustrated in Figure 1.

**Dissemination activities ensure the visibility and awareness of the project and support the widest adoption of its results among potential users.** Our dissemination and communication plan prepares the way for successful exploitation by facilitating internal communication within the project from the outset. Dissemination and communication activities will be actively pursued from the beginning to the end of the project – engaging continuously with both internal and external audiences. The activities have been clustered into three main phases.

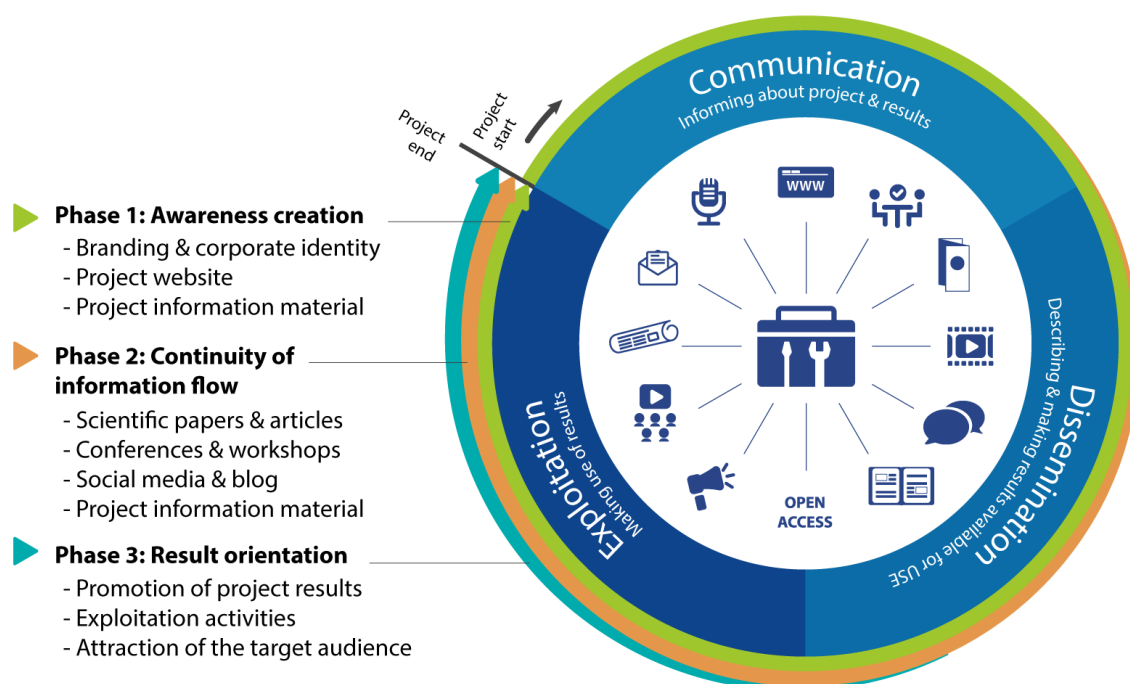


Figure 1: Dissemination & Communication phases

**The first phase is called “Awareness Creation”** and consists of building up the CONNECT branding and corporate identity, as well as establishing the CONNECT website and additional project information material, such as standard templates for project documents and presentations.

**In the second phase, the consortium partners will work on scientific papers to be submitted to conferences and journals to discuss the scientific results of the project.** This will give the consortium the opportunity to make presentations at conferences and workshops as to further raise awareness among the scientific and industrial stakeholders. This will facilitate lively discussions on project’s topics at these events by providing new insights and feedback on the project’s progress to project partners. This feedback will contribute to the project’s success and possibly also follow-up research activities. Furthermore, scientific publications and a selection of deliverables (those that are public) will be published on the project website to keep interested parties informed about the



latest progress. Twitter/LinkedIn and Blog associated with the project will be constantly updated to reach a wider and diverse audience and increase their interest. Besides that, newsletters, press releases, posters, information about workshops, conferences, videos and interviews, among others, are an integral part of this dissemination phase to enable a highly interactive communication within and outside the consortium. Finally, we expect to publish additional press releases and newsletters as soon as significant milestones are reached or for specific project events.

**In the third phase, dissemination activities will feed into exploitation**, which means using the results for commercial purposes or in public policymaking. There will still be some ongoing dissemination activities after the project has ended to promote the project results (e.g., the project website will be online for further five years, and similarly, social media, and cooperation activities with other projects, talks at conferences and follow-up projects, will be kept alive), and the main focus will be to exploit them and attract the target audience group.

In this context, WP7 focuses on identifying the relevant stakeholders that have to be contacted in order to reach the right supporters at the right time. It also involves preparation of the promotional materials and organizing activities to create an open, secure, decentralized, user- and OEM-oriented and highly engaged CONNECT community. The purpose of this deliverable is, therefore, to outline an inclusive dissemination and communication plan for the realization of the above stated goals and in particular to:

- ➔ Identify target audiences, including a broad range of stakeholders (i.e., OEMs, automotive vendors, security specialists) in the context of connected cars and autonomous driving;
- ➔ Present the strategy put in place for the dissemination and communication of knowledge and results;
- ➔ Describe CONNECT website architecture and present the initial results;
- ➔ Depict the methods, tools and promotional material that will be used in the project's dissemination and communication;
- ➔ Provide a complete overview of the planned activities, as well as list potential liaison opportunities with relevant standardization working groups and other related EU project initiatives (i.e., CCAM Partnership<sup>1</sup>);
- ➔ Describe the envisaged events and training activities as well as introduce the standardization plan specifying the type of working groups CONNECT will be trying to establish liaison with towards pushing its trust assessment artefacts and protocols as part of the ongoing specification formulation;
- ➔ Define the rules and procedures that will be applied to implement, monitor and evaluate all the communication and engagement activities;
- ➔ This is a "living" document, able to accommodate any required customization. The dissemination planning will, thus, be constantly evaluated and revised in the course of the project. Major updates will be included in the periodic reports and the subsequent versions of this deliverable (D7.2 and D7.3).

Overall, this deliverable constitutes the first essential communication kit regarding the CONNECT project's activities, including a narrative text, photographs, slides and any other suitable communication material, complemented with copyright licences for the European Commission. This kit will be updated in (D7.2) "*Dissemination, Communication, Clustering and Exploitation activities*" and (D7.3) "*Dissemination, Communication, Clustering Activities including Concrete Exploitation Measures*". The external IT communication infrastructure constitutes a guideline for presenting the CONNECT project to external target groups including conferences, dissemination and communication channels. Furthermore, this deliverable constitutes the formal launch of the internal CONNECT communication infrastructure including the establishment of mailing lists, the repository, and the CONNECT website.

Aside from the project website, a whole set of tools fosters the cooperation within the project and enables the dissemination of project results to the general public. TECHNIKON has developed a

<sup>1</sup> <https://www.ccam.eu/>

system, called “**Trusted-Knowledge-Suite**” (TKS), for distributed project collaboration in recent years. This trusted collaborative toolbox was awarded an Austrian ICT innovation prize<sup>2</sup> for its security and completeness. The toolbox was incorporated into the architecture initiated and configured for CONNECT. The main components of the knowledge management infrastructure include the following:

- *GitLab*: A project repository is available for shared documents and collaborative editing for deliverables. All data is versioned which prevents loss of data and allows precise logging of activities.
- *Mailing List Service*: Internal communication will primarily be handled by a mailing list server. For efficient communication there will be several lists, e.g. administrative, technical, financial, but also for external stakeholders.
- *Chat Service*: A real time chat system (Mattermost) is also incorporated in the TKS to allow instant messaging for quick and informal communication with the team.
- *Public Website*: A public dissemination website running on the WordPress content management system (CMS).

GitLab and the instant messaging system (for example Mattermost) use encrypted communication paths and can be configured to work through corporate firewalls that allow encrypted web traffic (SSL<sup>3</sup>).

---

<sup>2</sup> [https://www.ots.at/presseaussendung/OTS\\_20061117\\_OTS0035/ausgezeichnete-innovation-in-kaernten](https://www.ots.at/presseaussendung/OTS_20061117_OTS0035/ausgezeichnete-innovation-in-kaernten)

<sup>3</sup> Secure Sockets Layer – Protocol for a secure connection

## Chapter 2 Dissemination & Communication Strategy

A clear communication and dissemination strategy is essential and a forerunner for the execution of a dissemination and communication plan. Therefore, the **CONNECT project has set out a clear strategy for dissemination and communication** (Figure 2). The strategy defines the **audiences the project aims to target and defines why such audiences should be targeted and by which means**.

While talking about communication the goal is to highlight the benefits of the CONNECT project for society, e.g., by showing the public society and media the impact of our project on everyday lives. When it comes to dissemination the goal is to transfer knowledge and make project results available to an audience that may take an interest.

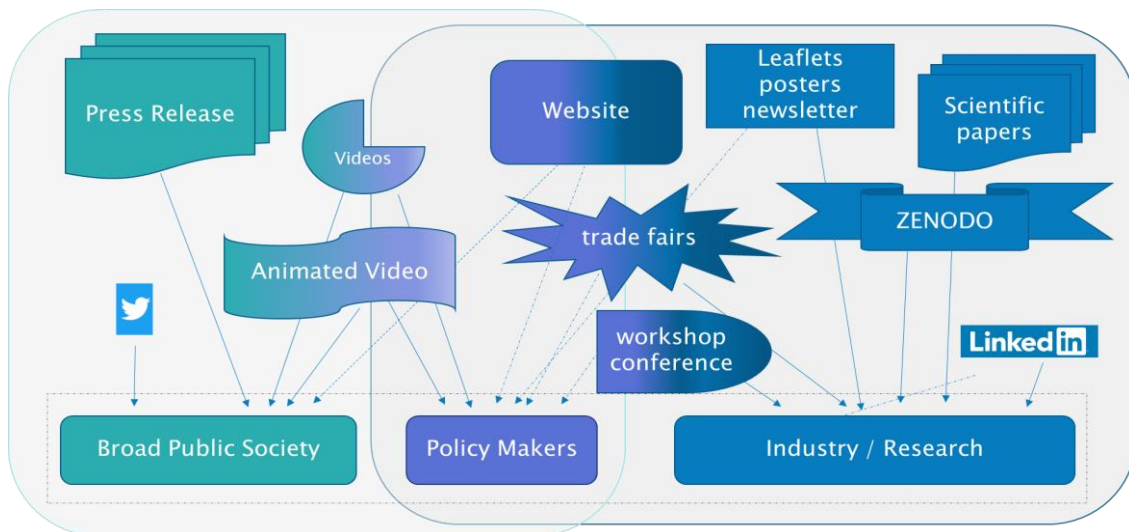


Figure 2: The CONNECT Dissemination & Communication strategy

Within the CONNECT project, three main audience groups can be defined:

- (A) **Broad public Society**
- (B) **Policy Makers**
- (C) **Industry/Research**

The link between named audiences using various channels can be seen in Figure 2. The channels and forms of their application are described in the following sections.

### 2.1 CONNECT Mission

The vision of CONNECT is to address the **convergence of security and safety in CCAM by assessing dynamic trust relationships and defining a trust model and trust reasoning framework based on which entities can establish trust for cooperatively executing safety-critical functions**. In this context, modern vehicles are no longer mere mechanical devices; they comprise dozens of digital computing platforms coordinated by an in-vehicle network, and have the potential to significantly enhance the digital life of individuals on the road. While this transformation has driven major advancements in road safety and transportation efficiency, significant work remains to be done to capture the strict security, privacy, and trust requirements of all involved stakeholders. For instance, driving on the road requires trust in others and the environment, but in reality, we never completely trust - not us, not other drivers or what is ahead of us. Therefore, *how can we be sure*

*about the data integrity and level of trust in connected cars that cooperatively need to execute a safety-critical function?*

This is where CONNECT envisions to close the gap by facilitating a **holistic trust assessment framework capable of modelling all complex trust relationships of future CCAM environments** comprising both the vehicles but also services running as part of the Mobile Edge Computing (MEC) infrastructure. **Edge Computing is an important enabler of V2X scenarios and services since it can accommodate the required guarantees of low latency and high reliability.** However, this additional layer, in the overall CCAM deployment architecture, introduces a **three-tier paradigm shift** [1] by considering an intermediate element at the network edge. This results in a new deployment model with an increased set of security, privacy and trust requirements for been able to safeguard the security profiles of both vehicles and drivers.

CONNECT's trust assessment model will enable both a) **cyber-secure data sharing** between data sources in the CCAM ecosystem that had no or insufficient pre-existing trust relationship, and b) **outsourcing tasks to the MEC and cloud in a trustworthy way.** Beyond the needs of functional safety, trustworthiness management needs to be included in CCAM's security functionality solution for verifying trustworthiness of transmitting stations and infrastructure. CONNECT will build upon and expand the **Zero Trust concept to tackle the issue of how to bootstrap vertical trust** from the application, the execution environment and device hardware from the vehicle up to MEC and cloud environments. This includes measuring the system when instantiating network functions and determining the integrity and origin of executed CCAM functionalities, aiming at:

- ✓ **Trust assessment and establishment** between all actors in the CCAM environment; i.e., capturing all modes of operations including V2V, V2I and in general Vehicle-to-Everything communication models.
- ✓ Providing strong **system integrity and operational assurance** (through advanced property-based attestation mechanisms) of Vehicle On-board Units (OBUs) towards the support of safety-critical services (such as collision avoidance, manoeuvre planning, etc.) with sound statements on their security properties.
- ✓ **Accountable sharing of such security claims** between vehicles and with the MEC towards the creation of a "chain of trust" with verifiable evidence on the Actual Trust Level (ATL) of each entity/component of this chain. This will enable the establishment of hierarchical compositions of CCAM architectures (considering vehicles as "Systems-of-Systems") with federated trust.
- ✓ **Extending the standalone vehicle domain to safe and security solutions distributed from vehicles to MEC and Cloud facilities** (three-tier paradigm shift) for securing and ensuring trust in the data exchanged.

CONNECT relies on these pillars (i.e., remote attestation, dynamic trust assessment based on the use of Subjective Logic, and enforcement of self-learning adaptable policies) to establish a secured baseline, as a trust domain, for guiding CCAM operation based on trust indicators that are commensurate to the traditional concepts of confidentiality, integrity and availability.

## 2.2 Visual Identity of the Project

The creation of a corporate visual identity plays a significant role in the way the CONNECT project presents itself to both internal and external stakeholders. A corporate visual identity expresses the values and ambitions of our project and its characteristics. Our corporate visual identity provides the project with visibility and "recognisability". It is of great importance that people are aware of the project and remember its name and core objectives at the right time. The following subchapters present the actions which were taken to create a visual identity of the project.

### 2.2.1 Project Logo

To improve its visibility, the CONNECT project has adopted a project logo. Technikon and UBITECH were the main partners responsible for the design of the project logo, including the colours, fonts

and icons. The consortium was involved in the designing process of the logo and supported with ideas. This logo will be used in all dissemination tools from internal documents and reporting templates to external communication tools such as the website, presentations and brochures. This consistent graphical identity will support effective communication and recognizable dissemination activities. The two versions of the logo, in horizontal and vertical format, are shown in Figure 3.



Figure 3: CONNECT Logo

### 2.2.2 Project Templates

The project identity is reflected in all documents created by the consortium for internal as well as for external use. The project management team established templates for different formats as MS-Word, MS-Excel, MS-Power Point, and Latex. The templates for documents and presentations are accessible to all project members. The templates are important to ensure a coherent theme and a consistent visual appearance of the project. An example of a template is shown in Figure 4 below showing the CONNECT presentation template.

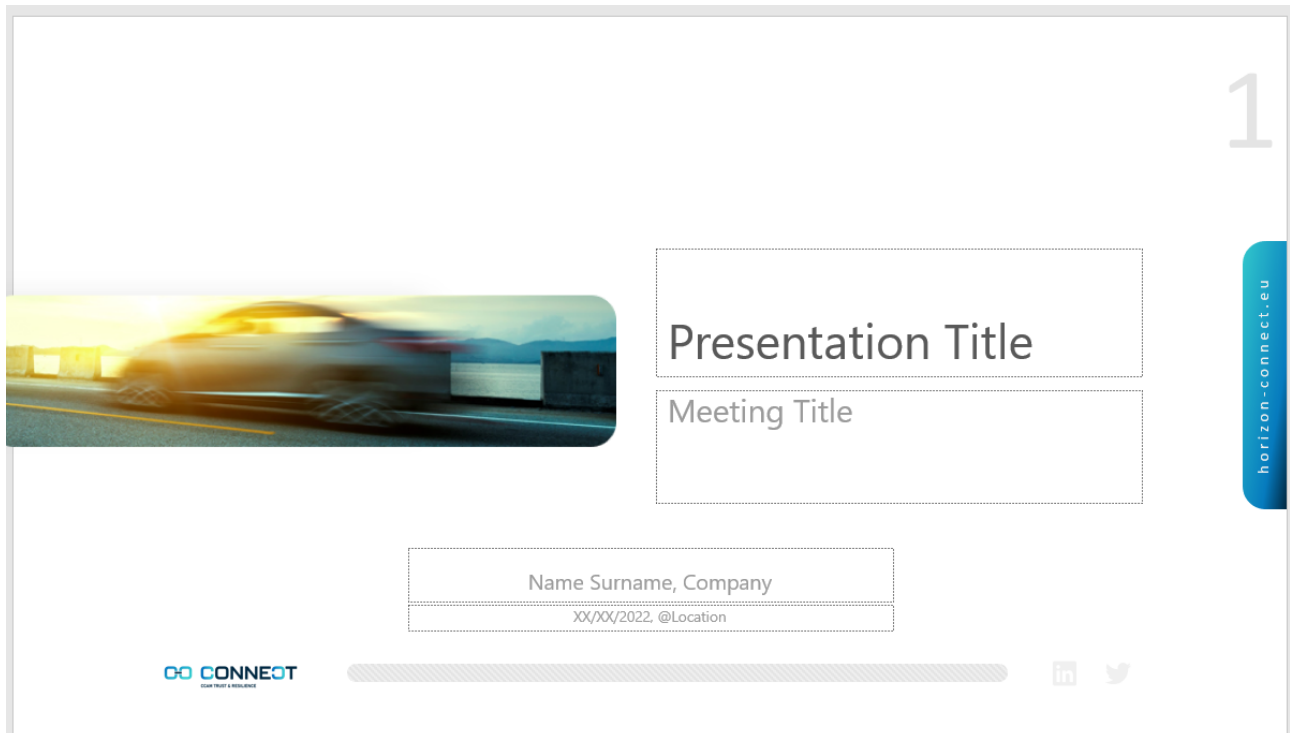


Figure 4: CONNECT Power Point Template

## 2.3 CONNECT Advisory Board

In order for the innovation developed within the CONNECT project to have any value, it is essential to show it and its applicability to industry needs. Within the industry, a large potential of stakeholders can be found which will eventually enhance the general exploitation of the innovation, thus also benefitting the global European economy. The CONNECT project foresees several ways to reach the industry and in particular the target audience listed in Table 2. Whereas the main channel is the attendance of trade fairs (such as the ESCAR<sup>4</sup> event focusing on Embedded Security in Cars), the industry is also reached by attending conferences, workshops and further by publishing newsletters and keeping the website up to date. In this context, the CONNECT consortium has also initiated the process for the establishment of an Advisory Board with outside experts in order to provide valuable feedback on the core research artefacts of the project from both an academic, scientific and industrial standpoint.

The CONNECT Advisory Board is a group of experts who will meet periodically with the CONNECT consortium throughout the project. They will provide technical guidance, input, and feedback on the CONNECT technology roadmap, advise on links with relevant interest groups (outside CONNECT), propose and assist potential interactions of the project with other projects, initiatives, activities and standardization bodies. In addition, the Advisory Board will critically evaluate project proceedings and the technological and scientific outcomes, give feedback to the dissemination and clustering exercises, and thus provide an external review of project actions. The AB members will document their experiences when it comes to the developments of the project and their feedback will be fed into all modelling actions and into the improvement of the final outcomes and deliverables.

In this direction, the Advisory Board will consist of a partner-nominated group of external senior academic, business, industry and standards-associated advisors who will assist in reviewing the project's development and progress from the very first steps of the project until its completion. During the construction of the AB, particular focus will be given on approaching experts with exposure on the international cybersecurity regulations and standards covering both regional (EU) and international (US and Japan) initiatives. This is of paramount importance so as to make sure that not only CONNECT is aligned with the latest security specifications but also participate (and possibly contributing) in the discussions towards the design of new cybersecurity management and risk assessment mechanisms enabling the long-term resilience of modern vehicles. Prominent regulatory and standards bodies include the ISO 26262 on "Functional Safety of Road Vehicles" [2]; ISO/SAE 21434 on "Cyber-Security Engineering of Road Vehicles" [3]; and the UNECE (United Nations Regulation) that recently published the WP.29 Cybersecurity and Cybersecurity Management System (CSMS) detailing the deployment model of the Public Key Infrastructure (PKI) needed for supporting the security and privacy of the entire lifecycle of road vehicles [4]. In this direction, CONNECT has already established relationships with international experts and representatives dealing with CCAM and Cyber-Security and will continue to try to liaise with organizations participating in the specification of such regulations to consolidate their findings and strengthen the international cooperation in automotive security.

Given the above, the consortium will liaise with numerous external, independent experts at different disciplines that will cover the following research/technology axes and impact categories of the CONNECT project:

- Tier-1 and Tier-2 OEMs of the automotive supply chain;
- Automotive Cyber-Security and Risk Management;
- Mobile Edge Computing (MEC) Architecture;
- Trusted Computing Technologies and Hardware-Software Remote Attestation;
- Lightweight Cryptography;

---

<sup>4</sup> There are various events organized throughout Europe, USA and Asia. For more information please refer to <https://www.escar.info/>

- Security and Functional Safety of Vertical Application Domains;
- Certifiability of Automotive Security as required by regulatory organizations such as ISO, UNECE, ENISA, etc.

Currently, the CONNECT consortium has initiated the process for inviting experts, from the following organizations and research institutes, to participate as members in the envisioned AB: Qualcomm, University of Dresden, Toyota, Volkswagen, University of Luxemburg, 5GAA, Bosch, Yokohama National University, Korea Transport Institute.

## 2.4 Sustainable Dissemination and Communication Approach

The CONNECT dissemination and communication approach considers the sustainability principles for the organization of events and the production of communication materials. For this purpose, the partners will:

- Organize virtual meetings and workshops instead of face-to-face events;
- Avoid using material resources where possible (avoiding printing flyers when unnecessary and promote the online download, producing promotional materials using recycled materials and avoiding single-use products, for example);
- Encourage the reduction of emissions through sustainable mobility practices (e.g., recommending bicycle use, public transport at CONNECT events and rewarding these actions);
- Work with suppliers (printers, caterers, etc.) that use sustainable products and materials;
- Try to measure the carbon footprint and compensation of emissions of partners' traveling to dissemination events.

## Chapter 3 Dissemination & Communication Targets

During the proposal phase of CONNECT, an initial communication and dissemination and exploitation plan was already set up, stating different audiences, what the objective of reaching the audience would be and what the impact of reaching them will be. This plan is the basis for D7.1 and can be found in Section 2.2 of the DoA (Description of Action).

CONNECT's dissemination and communication activities are overarching throughout the whole duration of the project and aim to ensure a broad promotion and effective showcasing of the developed concepts, technologies, use cases and results. In terms of communication and marketing, this ambition translates into the following main objectives:

- Ensure broad visibility and raise awareness about CONNECT, spreading knowledge about the project and its results, establishing a distinctive and recognizable identity that will support marketing efforts;
- Reach, stimulate and engage a critical mass of relevant stakeholders to ensure that the results of the project are effectively showcased, leading to validation, improvement and possibly further adoption of the developed technologies and concepts, especially towards the secure deployment of connected cars enabling the vision of (Day-3) V2X services fostering vehicle automated functions that rely on collective perception and shared knowledge with the other vehicles' intentions, trajectories and maneuvers;
- Facilitate exploitation of project's outcomes and promote the development of innovative solutions based on the CONNECT technologies and architectures;
- Foster impactful contribution to relevant standardization bodies as appropriate and relevant to planned exploitation plans and the project's outcomes;
- Ensure close coordination with relevant H2020 projects and EC bodies, while establishing liaisons with related initiatives in research and innovation domains such as CCAM Partnership, ETSI, C2C-CC, TCG, AIOTI, etc. (more information can be found in Section 7.2).

### 3.1 Dissemination KPIs

In order to assess the effect of the dissemination and communication activities on the target audience, a number of Key Performance Indicators (KPI) have been selected, allowing to measure progress towards fixed goals for dissemination activities. These KPIs are repeatedly referenced in the document. The following table collects the selected KPI:

Table 1: Key performance indicators for dissemination and communication activities

Dissemination activity/ channel	KPI
CONNECT website	<ul style="list-style-type: none"> <li>✓ Number of visits</li> <li>✓ Number of new and returning visitors</li> </ul>
Newsletter	<ul style="list-style-type: none"> <li>✓ Number of contacts</li> <li>✓ Number of downloads</li> </ul>
Social Media	<ul style="list-style-type: none"> <li>✓ Number of postings</li> <li>✓ Number of follower/contacts</li> <li>✓ Engagement rate</li> </ul>
Scientific journals and conferences	<ul style="list-style-type: none"> <li>✓ Number of publications per year</li> <li>✓ Number of views per publication</li> <li>✓ Number of attendees</li> <li>✓ Number of citations</li> <li>✓ Feedback received</li> </ul>
Presentation/ workshops	<ul style="list-style-type: none"> <li>✓ Number of attendees</li> <li>✓ Number of events</li> </ul>



### 3.2 CONNECT Stakeholders

All the aforementioned communication and dissemination activities aim at reaching out at several different target groups with specific messages based on relevant interests' areas. The following table provides the detailed CONNECT impact and benefit for each target.

Table 2: CONNECT Stakeholders

Target Stakeholder Group	Benefits
<b>Automotive Vendors &amp; Tier 1/Tier 2 OEMs</b>	These include the primary contractors of CONNECT security services towards enhancing the <b>operational assurance and functional safety of road vehicles</b> . These include automotive vendors and vehicle manufacturers (e.g., FIAT, BMW, Volkswagen, Toyota, etc.), as well as on-board unit technology providers such as DENSO, Bosch, etc. <b>affiliated with the idea of cooperative road traffic based on secure V2V and supported by V2I communications</b> . Their primary interest is on CONNECT security artefacts and roadmap towards the deployment of Day-3 CCAM services [5] with high level of assurance capable of converging security with safety. Day-3 applications and services can take advantage from CONNECT newly introduced security and trust models (integrating also the MEC layer) extended to provide high integrity guarantees on the trustworthiness of both exchanged data but also the data sources.
<b>Service Providers</b>	They are the direct customers of CONNECT. These can again be automotive vendors and other service providers supporting a wide gamut of C-V2X applications; i.e., from In-Vehicle Entertainment services to software updates and other safety-critical services such as Intersection Movement Assistance, Manoeuvre Guidance, Collision Avoidance, etc. Such services might also require the processing of large amounts of data, thus, they can also benefit from the use of the secure MEC deployments supported by CONNECT.
<b>Security Solution Providers Vendors/Professionals</b>	They can acquire the CONNECT building blocks/services and utilize them in scenarios that are addressed to their cyber-security needs. One of the visions of CONNECT is to also enable the migration and integration of such security enablers to other safety-critical application domains with overlapping security and privacy requirements beyond the automotive: Including smart cities, smart aerospace, unmanned aerial vehicles, etc.
<b>Industry Associations &amp; Technology Clusters</b>	Includes project's results to collaborative research activities (roadmap, white papers, position papers) within the consortium, liaison with similar projects (i.e., SELFY, PODIUM, etc.) and the bilateral participation in events for knowledge exchange.
<b>Cybersecurity Engineers &amp; Architects</b>	Partners will be informed about Publication & Notices at least 45 days before publication according to Article 16 GA (Annex 5)
<b>Academia, Research Institutes, PhD Students</b>	Includes universities, engineering schools, research centers, industrial R&D departments, etc. They perform state-of-the-art research & innovation and disseminate their efforts, procedures and results to the wider community. They aim at the continuation of the research & innovation results and they may also exploit results in <i>training and mentoring activities</i> . They are direct contributors and facilitators (also as part of the consortium) to the project outcomes.
<b>Policy Makers</b>	They include the European Commission (and corresponding agencies, e.g., ENISA, UNECE, ANSI), governmental and international ministries. They establish regulations, policies and recommendations with which the various initiatives need to comply. They directly influence the research activities,

Target Stakeholder Group	Benefits
	and benefit from the fast, direct and expanded adoption of these guidelines, which also facilitate and strengthen international collaborations.
<b>Standardization Bodies</b>	They include standardization bodies that focus on <b>automotive cybersecurity regulation specification considering both in-vehicle cyber-security engineering as well as “Vehicle-to-Everything” trust management</b> . The most prominent standardization efforts are driven by organizations including ISO 26262 on “Functional Safety of Road Vehicles”; ISO/SAE 21434 on “Cyber-Security Engineering of Road Vehicles” [3]; UNECE; Car-to-Car Consortium (C2C-CC); Trusted Computing Group (TCG), 5GAA, etc. They can solidify their efforts through the adoption and dissemination of the standards from the project, as well as further expand these standards with contributions for the project. They provide input to the project, as well as receive input and benefit from the project innovations. CONNECT has already defined a detailed roadmap of envisioned activities and collaborations with standardization consortia as described in Chapter 7.
<b>General Public</b>	These constitute the end users that consume - and are affected - by the envisioned CCAM services. They can span from the <b>drivers of the vehicles to the pedestrians</b> that are the focal point of the infrastructure in order to ensure their safety by exchanging information so as to let receiving vehicles detect the occurrence of risky situations associated to a pedestrian presence. While they are informed about the EC efforts in enhancing road safety, they also constitute one of the core target groups that need to exhibit <b>high acceptance of these services</b> with clear understanding of its benefits as well as <b>high service adoption due to explicit evidence of safeguarding their security and privacy</b> in the technical CCAM architecture.

## Chapter 4 Dissemination and Communication Kit

This chapter describes the CONNECT overall communication kit, which includes the project website as the major communication tool, as well as all communication and dissemination materials used within the project. All these materials are freely accessible for download on the project website. Additional materials, which will be created throughout the duration of the project, will be added in D7.3 “Dissemination, Communication, Clustering activities including concrete exploitation measures”.

In general, we grant open access to all communication and dissemination materials. If, in a certain case, other licence requirements have to be taken into consideration, this will be marked accordingly. All the project material will be marked with the following sentence:



Funded by the European Union under grant agreement no. 101069688. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

### 4.1 CONNECT Project Web Site

For a better visibility of CONNECT, the project website was launched in month 2 of the project. As already recalled, the project website constitutes the main communication tool, and will be used to disseminate most of the project information and dissemination materials. The website has been designed to provide a user-friendly and informative environment. It is based on the WordPress Content Management System, which has been configured to allow the site to be accessed by the main public.

The CONNECT project website is available on the following link: <https://horizon-connect.eu/>

The design of the website is based on the templates and colours of the CONNECT Logo to establish a strong project identity in all communication activities.

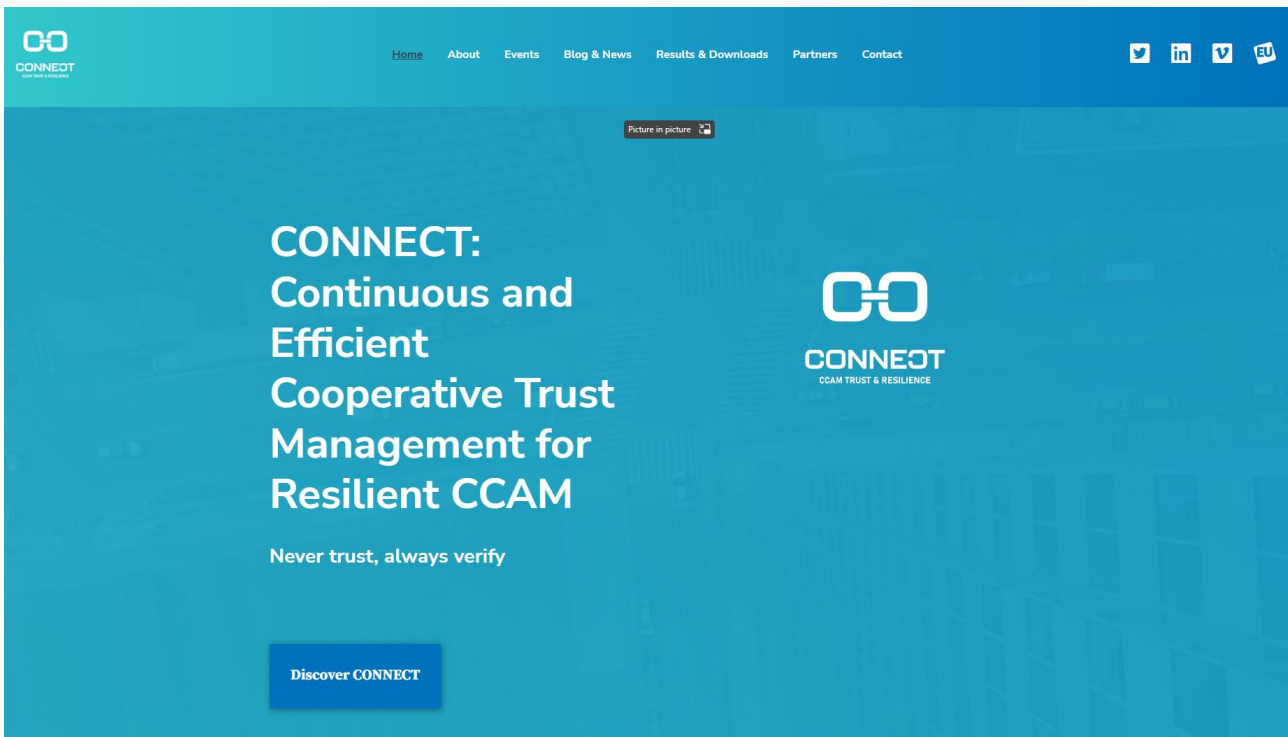


Figure 5: The main page of the CONNECT website

Figure 5: The main page of the CONNECT website (Figure 5) illustrates the start page of the CONNECT website. The main categories on the front page are: Home, About, Events, Blog, Results & Downloads, Partners and Contact.

- **Home**

In the first category, the visitor receives information about the project consortium and the contact persons. Furthermore, the most recent blog entries and upcoming events related to the project are shown as well as the 15 sec introduction video to CONNECT.

- **About**

In this area visitors can find an overview of the CONNECT project. This includes the project's vision, mission and key facts. It also provides an overview of the project's Motivation, mission & objectives and work packages.

- **Events**

This category shows past events the partners of the consortium participated in and upcoming events related to the CONNECT project.

- **Blog & News**

The consortium members can post relevant information on this blog, which includes a reflection on past events and activities partners participated in, call for papers, interviews with partners on events, as well as discussing recent publications or a brief discussion of the CONNECT Fact Sheets. As an example, Figure 4 shows one of the early project blog posts introducing CONNECT at the CCAM Multicluster Meeting. The blog will also feature an image gallery by which pictures of events can be presented.

- **Results & Downloads**

Here, visitors can see and download project publications, papers and public technical deliverables. For easy convenience the section is structured in scientific publications, public deliverables and dissemination & communication.

- **Partners**

This page presents an overview of the CONNECT project partners and their roles in the project.

- **Contact**

Using this page, website visitors can send an email directly to the coordinator of the CONNECT project, e.g. general feedback or questions regarding the project or website.



Figure 6: CONNECT Blog

Each page of the CONNECT website includes at the bottom the web site menu, the disclaimer, the legal notice, the privacy policy and the feedback form. The website can be viewed with a standard desktop web browser as well as on a smartphone and will be kept alive throughout the project period and a few years afterwards. The website has been successfully tested on several web browsers (e.g. Chrome, Firefox) in October 2022.

The website backend is updated by TECHNIKON on a regular basis, in particular as soon as major updates are made available by the developers of the WordPress CMS, with analytical statistics being available.

## 4.2 CONNECT Announcement Letter

On 16<sup>th</sup> August 2022 the official CONNECT announcement letter was published on the coordinator's website. This letter recalls the aims and objectives of the project and gives an overview about the participating partners, and lists the coordinator. The announcement letter can be found also on the project website: <https://horizon-connect.eu/dissemination-communication/>

## 4.3 CONNECT Leaflet

The CONNECT leaflet was made available to the consortium in M03 (see Figure 7). TECHNIKON was responsible for the content and design of it in cooperation with the technical lead UBITECH. It is an informative and graphically appealing A5 leaflet, highlighting the CONNECT vision, main goals, key technological aspects as well as background information and can be used for distribution at conferences or certain other dissemination events to provide further visibility to the CONNECT project. An electronic version of the leaflet is available on the project website: <https://horizon-connect.eu/dissemination-communication/>

In particular, the project leaflet covers the following aspects of the project:

- ✓ Project details, such as duration, funding and project number;
- ✓ Project vision;
- ✓ Project main goals;
- ✓ The consortium members and their country of origin;
- ✓ The project's contact person.



Figure 7: CONNECT project leaflet

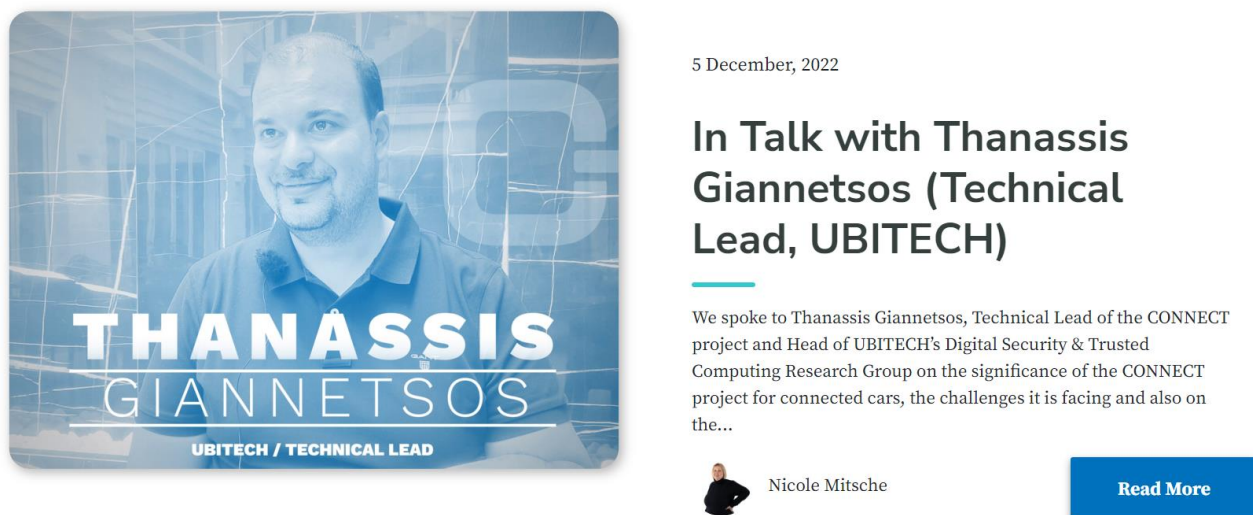
#### 4.4 CONNECT Videos

The CONNECT consortium will publish videos and interviews throughout the project. Video material with durations of up to 2 minutes and animated 2D/3D content will be produced by Technikon and published on Vimeo. There will be one promotional video, one video on the pilot and one video on the impacts.

Technikon's media department will produce and record interviews at the project meetings or remotely and host them on the Vimeo platform. They will be then shared via <https://euvation.eu/>, Technikon's platform for research innovation.

The links to the videos and interviews will also be published on the different social media channels. These videos will then also be shared on the website and on the CONNECT Social Media accounts. The first two CONNECT interviews with the technical and scientific lead discussing the project's challenges and opportunities, including its relevance for the young can already be found on the CONNECT web site and Technikon's vimeo presence (see links below).


- In Talk with Thanassis Giannetsos (Technical Lead, UBITECH)  
<https://horizon-connect.eu/in-talk-with-thanassis-giannetsos-technical-lead-ubitech/>
- In Talk with Frank Kargl (Scientific Lead, UULM)  
<https://horizon-connect.eu/in-talk-with-frank-kargl/>



5 December, 2022

### In Talk with Thanassis Giannetsos (Technical Lead, UBITECH)

We spoke to Thanassis Giannetsos, Technical Lead of the CONNECT project and Head of UBITECH's Digital Security & Trusted Computing Research Group on the significance of the CONNECT project for connected cars, the challenges it is facing and also on the...

 Nicole Mitsche

[Read More](#)

Figure 8: CONNECT Video example

These are the first two interviews conducted by the project. In the dissemination plan the project anticipated 2-4 interviews.

The dissemination plan also outlines 1 promotional video, 1 pilot video and 1 further video. A promotional video 15 second video (see Figure 9) showing the three main objectives is already available on vimeo <https://vimeo.com/788936526/17a3c4a7e4> and has been integrated on the homepage of the CONNECT web site <https://horizon-connect.eu/>, as well as being distributed through social media.



Figure 9: CONNECT 15 seconds video

#### 4.5 CONNECT Social Media

The use of social media helps spreading project information to a large audience. Therefore, social media will be actively used during the third project period to disseminate the project's ideas and results. In particular, the project will use Twitter and LinkedIn to this end.

- ➔ *Twitter* is an online social networking service and micro blogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets". The CONNECT project is available on: [https://twitter.com/connect\\_horizon](https://twitter.com/connect_horizon)
- ➔ *LinkedIn* is a social networking site for people in professional occupations or simply a social network for business. The CONNECT project is available on: <https://www.linkedin.com/company/horizon-europe-connect-project-101069688/>
- ➔ Direct links to the CONNECT Twitter Account and the LinkedIn page can be found on the CONNECT website.

The social media plan is backbone is the dissemination and communication strategy outlined in the DoA Section 2.2.1. which is then mirrored and linked to the planned activities communicated by the CONNECT Consortium in the planned dissemination and communication activities outlined in (Chapter 6). A number of content-based posts such as partner introduction, interviews, videos, fact sheets or short facts are pre-planned with a regular posting plan, as well as in advance notice of conference presence by partners, publications or organisation of conferences/workshops.

Space within the posting schedule is left available to share more ad-hoc content from partners in the CONNECT consortium (such as success stories, insights in the project) as well as from close linked partner sites (e.g., CCAM, CINEA and our partner project SELFY).

## 4.6 CONNECT Newsletter

The CONNECT Consortium will publish a periodic newsletter, informing about the main outcome and results of the project. In fact, newsletters are an efficient communication channel to provide news on the project progress, and to discuss ongoing topics relevant to CONNECT for internal and external project partners, stakeholders and other interested bodies. In addition, publications and participation in conferences will be promoted in the newsletters. The newsletters can be found in section blog and news of the CONNECT website and are posted via the CONNECT Twitter and LinkedIn accounts to raise further public awareness.

## 4.7 CONNECT Collaborative Tools

A set of collaborative tools are provided by the coordinator to facilitate the cooperation within the project and to assist in the coordination work. These tools are:

- ➔ A project repository (GitLab) for shared documents and collaborative editing for technical and smaller deliverables
- ➔ A mailing list system for information exchange.
- ➔ MS Teams (for remote telephone conferences)
- ➔ Mattermost Chat (for an easy and fast communication within the project consortium)

### 4.7.1 Project Internal

**GitLab** is used as the repository for the CONNECT project. The repository is hosted at the main GitLab Server at the University of Ulm. GitLab allows easy synchronisation of documents between the server and the participants' local file storage. The system includes tools for retrieving older versions of a particular file, resolving conflicts between different versions of the same file.

Two main access tools are provided by the server. On the one hand, a client application provides the user both reading and editing rights on all documents through Tortoise Git. On the other hand, users can access GitLab directly using their web browsers and download and upload documents to the repository. Easy read access is provided in the web browser for .txt and .pdf files.

Some major advantages of the GitLab are:

- ➔ Offline availability of the data via GitLab Client (stored on user local hard disc).
- ➔ Read-only access via HTTPS (Web Browser).
- ➔ Synchronizing the data between Client/Server.
- ➔ All former versions of the file are available and reproducible.
- ➔ E-mail notification on activity (e.g., "commit" action).

For joint synchronous editing of larger deliverables which includes a large number of members the CONNECT team uses for the deliverable only Google Docs. The final deliverable is then moved to the GitLab repository during the document's review process.

The CONNECT team makes further use of the GitLab functionalities *GitLab Wiki* and the *Mattermost Chat* tool.

**GitLab Wiki** is used to distribute current dissemination and outreach opportunities to submit research activities to conferences, workshops, journal articles, special issues, working groups and standardization activities related to the CONNECT project. It is a page to promote potential opportunities internally, and highlight initiatives partners are involved in. Past opportunities will be moved to a parallel document for future reference to the team.



The **Mattermost Chat Tool** is an extension of the GitLab functionalities. Each work package has their own chat channel. The main purpose of the communication within Mattermost are discussions of specific topics team members of the work package are working on. Links to the GitLab server can be easily shared within Mattermost.

#### 4.7.2 Mailing List Server

Several mailing lists are available to the project members for easy communication with a set of participants. For subscriptions and other management tasks it is necessary to write an email to [coordination@horizon-connect.eu](mailto:coordination@horizon-connect.eu). Access is controlled by the coordinator to ensure the integrity of the lists. Transparency within the consortium is through the publication of the subscriptions to mailing lists as part of the CONNECT contact list on GitLab.

TECHNIKON uses the MS Teams mailing server with a wide range of different mailing lists, where all people who are responsible for the various sections are subscribed.

The different CONNECT mailing lists currently active are described in the following table:

Mailing List Name	Members
technical	For all technical correspondence & EB member discussions
ga	General Assembly members and deputies
financial	Personnel responsible for financial questions and tasks (financial reporting, reporting of PMs, payments etc.)
legal	Personnel responsible for legal questions and tasks
publication	Partners will be informed about Publication & Notices at least 45 days before publication according to Article 16 GA (Annex 5)
all	All personnel actively involved in the project
wp2	Members working on WP2
wp3	Members working on WP3
wp4	Members working on WP4
wp5	Members working on WP5
wp6	Members working on WP6
wp7	Members working on WP7

Table 3: CONNECT Mailing Lists

#### 4.7.3 Online Conference Calls

In addition to face-to-face meetings and due to the recent challenges (Covid-19; travel restrictions), online meetings for CONNECT will be held on a regular basis. A tool provided by the coordinator Technikon is available for all partners. This web conferencing tool MS Teams allows CONNECT partners to host online meetings.

### 4.8 CONNECT Events and Workshops

Awareness, Interaction and Promotion regarding CONNECT is expected to be impacted positively by the project representation in relevant events. Events are an important means for the consortium

to communicate and disseminate the aims, developments and results of its work. We distinguish among:

- ➔ Events organized by CONNECT;
- ➔ External events in which CONNECT will participate.

Events are often the only way of interesting mainstream press in EU affairs, to ensure a Press Release and organize interview opportunities with high-profile participants. The project will be supported by the relevant communication material produced, namely the Event Toolkit (brochure, banners, posters, flyers etc.). As the per Grant Agreement specifications, we expect to be involved in a variety of event formats, such as: Workshops, Demo Events, Scientific Conferences, industry Events, Fairs and Exhibitions, and Events of affiliated projects, clusters and communities.

The first three categories are currently being planned in collaboration with the consortium. Their exact targets and KPIs are presented in Section 3.1.

#### **4.8.1 Innovation Workshops**

The dissemination plan includes the organization of three (2) innovation workshops. The organization of these workshops will be managed by the entire CONNECT consortium, and the foreseen time schedule for their realization is before M30. Each of these will have a different scientific focus and will be targeted to the scientific and trusted computing research and industrial communities.

The organizing partners will work with the Dissemination and Communication Officer as well as with the Project Coordinator to further define their plans and begin their preparations for the workshop. These include main topic(s) definition; key participants and target audiences; scientific program and workshop agenda; promotional material and communication channels, time schedule, logistics and practical issues setup; documentation and reporting.

#### **4.8.2 Internal and External Training**

Training activities will be organized during the project involving both internal and external members of the project. One of the goals is to mitigate the gap that typically separates practitioners and theoreticians by providing a series of regular structured training events in the form of workshops and schools on topics relevant to the project. The meetings will ensure that practical aspects inform theoretical research, that developers benefit from proper theoretical foundations, and that the project fosters cross pollination of ideas. A second relevant aspect of the training activities within this project is the offering of this training element to external PhD students, post-docs and researchers and the possibility for external parties to participate in research exchanges, to visit project member's research lab, and to contribute to the schools and workshops. Such visits are extremely beneficial to foster strong scientific collaboration and to benefit from external knowledge relevant to the project.

Example training activities and events include:

- ➔ Teaching activities on trusted computing technologies and trust assessment on a number of MSc courses;
- ➔ Internal departmental seminars (organized by CONNECT consortium partners) for presenting the emerging trends in automotive cyber-security and also presenting the research avenues investigated within the CONNECT project.
- ➔ Supervision of MSc and PhD theses;
- ➔ PhD Summer or Winter Schools;

- ➔ Supervision of special project courses on topics related to the use of subjective logic towards enhanced trust management; remote attestation for assessing the integrity and operational assurance of a vehicle; in-vehicle key management systems, etc.

### 4.8.3 Scientific Workshops

Organization of numerous scientific workshops that will facilitate discussions between researchers, academia and industry on topics related to building trust and resilience in CCAM. CONNECT is envisioning to be affiliated with at least five (5) scientific workshops and has already taken the following actions towards the support of the following two workshops (further details on the outcomes will be documented in D7.2 [8]):

#### CONNECT Scientific Workshops

UULM and HUAWEI are two of the co-organizers of the **Dagstuhl Seminar: "Privacy Protection of Automated and Self-Driving Vehicles"**, which is going to take place on 11-16 June 2023. Participants of this Seminar will be around 30 world-wide security experts in the automotive domain that work in the next generation connected and automated vehicles. The participants are a mix of engineers, legal and policy experts. The output of the Seminar is going to be a roadmap to address the major road-blockers that the experts see in making progress on the way to deployment of privacy protection in Automated and Self-Driving Vehicles. This Seminar will be a venue for disseminating the CONNECT trust framework and elaborate on its usefulness and adoption by the automotive industry.

The CONNECT project will be organizing the 4<sup>th</sup> Edition of the CYSARM Workshop (4<sup>th</sup> Workshop on Cyber-Security Arms Race) co-located with the [ESORICS 2023](#) conference. The workshop will be held on September 2023. Cybersecurity is a complex ecosystem that is based on several contradicting requirements. For this reason, it is often defined as an **arms race between attackers and defenders**: for example, when a new security model or algorithm is devised, it could act as a double-edged sword since it might both enhance the security posture of a system and introduce additional vulnerabilities. The goal of **CYSARM workshop** is to foster collaboration and discussion among cyber-security researchers and practitioners to discuss the various facets and trade-offs of cybersecurity and how new security technologies and algorithms might impact the security of existing or future security models.

### 4.8.4 End-User Workshops

In the process of defining the concept of Trust, CONNECT puts emphasis also on how trust is perceived by end-users, i.e., road-side users or drivers participating in the system. For this analysis, CONNECT plans to organise a Workshop where it will invite end-users and collect their feedback on a number of aspects related to trust when using CCAM services. Our plan is to first make a series of short presentations to explain to them the concepts developed in CONNECT and then disseminate a questionnaire to them for answering some questions that will be later used in our analysis.

## Chapter 5 Past dissemination and communication activities

The first phase on dissemination and communication activities focused on “Awareness Creation” through the named activities in the DoA (Section 2.2.1) of the announcement letter, project web site and branding, audio and video material and social media. Appearances in Conferences and Workshop focused on creating awareness of the project presented the core concept of the CONNECT framework, as well as elements related to the overall concept.

Table 4: Past dissemination and communication activities

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Workshop	TRIALOG		SASSUR 2022 : 9th International Workshop on Next Generation of System Assurance Approaches for Critical Systems	09.06.2022	Online	Presentation of the main concept of CONNECT from TRIALOG – ( <a href="#">Link</a> )
Press Release	TEC	UBITECH	CONNECT Announcement letter	01.09.2022	Online	<a href="#">Link</a>
Organisation of a Workshop	TRIALOG		Member of SASSUR committee 9th International Workshop on Next Generation of System Assurance Approaches for Critical Systems <a href="https://sites.google.com/view/sassur2022/home">https://sites.google.com/view/sassur2022/home</a>	06.09.2022	Virtual	Dynamic assurance and measurement of trust Mentions UL4600 (ANSI standard) Standard for the safety of the evaluation of autonomous products ( <a href="#">Link</a> )
Website	TEC	ALL	CONNECT project web site & Dissemination of Branding	07.10.2022	Online	Official web site online: <a href="https://horizon-connect.eu/">https://horizon-connect.eu/</a>
Participation to a Conference	UULM		SIP-ADUS Conference 2023	11.- 13.10.2022	Kyoto, Japan	Cooperation and exchange with research and industry community in Japan. Presenting about trust modelling in the plenary
Social Media	TEC		CONNECT Twitter account	14.10.2022	Online	<a href="https://twitter.com/connect_horizon">https://twitter.com/connect_horizon</a>

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Social Media	TEC		CONNECT LinkedIn account	14.10.2022	Online	<a href="https://www.linkedin.com/company/horizon-europe-connect-project-101069688/">https://www.linkedin.com/company/horizon-europe-connect-project-101069688/</a>
Participation to other events	HUAWEI	UBITECH	CCAM Multicluster Meeting	26.10.2022	Brussels	CCAM Cooperation Meeting presenting CONNECT's goals and objectives
Workshop	HUAWEI	UBITECH, ICCS	Huawei System Security Workshop	02-04.11.2022	Online	Bring professors and experts from top universities, research institutions and corporations in Europe together to exchange and discuss the latest research in various security domains. Both UBITECH and ICCS presented the core concepts of the CONNECT project, especially as it pertains to the design of trust assessment models that can enable future CCAM ecosystems to operate in a Zero Trust security principle.
Participation to a Conference	UULM		ESCAR Europe	15.-16.11.2022	Berlin, Germany	Co-organizer, networking with community, discussions about trust modelling, advertising CONNECT project
Other	UBITECH	TEC	Meeting with SELFY Project Coordination	18.11.2022	Online	Meeting with SELFY Project Coordination initiated by PO. Discussion on collaborative actions for the periods of both projects.
Flyer	TEC	UBITECH	Project leaflet	21.11.2022	Online	<a href="https://horizon-connect.eu/dissemination-communication/">https://horizon-connect.eu/dissemination-communication/</a>
Organisation of a Workshop	TRIALOG		Digital twin standards (EDBVF <a href="https://european-big-data-value-forum.eu/">https://european-big-data-value-forum.eu/</a> )	21/11/2022	Prague	Presentation of a survey of digital twin standards

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Other	IRTSX	FSCOM	ISO technical report TR 12786 titled “Intelligent transport systems — Big data and artificial intelligence supporting intelligent transport systems — Use cases”	01/12/2022	Online	Contribution to this effort with a use case ‘Edge Misbehaviour Detection for V2X data reliability’ ( <a href="#">Link</a> )
Other	TEC	UBITECH	In Talk with Thanassis Giannetsos (Technical Lead)	05.12.2022	Online	Interview on the significance of the CONNECT project for connected cars, the challenges it is facing and also on the relevance of the project for younger generations.
Other	TEC	UULM	Interview with Frank Kargl (Scientific Lead)	04.01.2023	Online	Interview on the significance of the CONNECT project, the role of trustworthiness in connected cars and his role as a scientific lead in the project. He discusses the challenge of translating this into technical terms and the outlook within the project, as well as the relevance of it for younger generations.
Other	TEC	UBITECH	15 sec CONNECT Video	04.01.2023	Online	Introducing the main objectives of CONNECT through a short 15 sec video <a href="https://vimeo.com/788936526/17a3c4a7e4">https://vimeo.com/788936526/17a3c4a7e4</a>
Participation to a Workshop	POLITO		Multi-stack, open and plug & play On-Board Unit for on-field testing and retrofit with multiple V2X technologies	16.- 18.01.2023	Ponte di Legno, Italy	Presenting in the Italian Networking Workshop (INW) 2023, networking with community, discussions about V2X communications, advertising CONNECT project

Type of activities	Main Leader	Other partners	Title	Date	Place	Type and goal of the event / website
Participation to a Workshop	UBITECH		Joined workshop on SELFY project's requirements	07.02.2023	Virtual	Requirements and recommendations for the development of tools to increase cybersecurity in the mobility sector. Organised by SELFY Project
Social Media	TEC	All partners	The people behind each CONNECT partner - Social Media post	17.02.2023		Introducing partners background with group photo. The first post introduces the diversity of the consortium. A series of posts introduces each partner, the focus of their work in the CONNECT project and the people working in the team. The posts are scheduled on a weekly basis.

## Chapter 6 Planned Dissemination and Communication Activities

In the upcoming project months, the CONNECT team will continue to raise further awareness of the CONNECT project through its web site, blog and social media channels. A stronger focus in the upcoming month in this Phase 2 “Continuity of information flow is on press releases, blog posts, articles, whitepapers, interaction with policy makers, digital liaisons with related projects in particular with the CCAM’s Network and the SELFY project and standardization associations. A strong emphasis in this phase has been set on the participation in and publication of scientific papers in conferences and high impact factor journals with various partners presenting CONNECT concepts and first results from their work through scientific publications and presentations.

Table 5: Planned dissemination and communication activities

Type of activities	Main Leader	Other partners	Title	Start	Place	Type and goal of the event / website
Website	TEC	UULM, HUAWEI	Fact Sheet 1: Trust Assessment	02.03.2023	Online	Detailed information and animated graphic; as blog, pdf and via social media
Social Media	TEC	All partners	Women in Technology	08.03.2023	Online	International Women's Day: Celebrating the Women of the CONNECT project
Website	TEC	UBITECH, DENSO	Fact Sheet 2: Integration of trusted computing in vehicles	06.04.2023	Online	Detailed information and graphic; as blog, pdf and via social media
Website	TEC	Partners	Interviews	20.04.2023	Online	Topic based interviews with partners. Two further upcoming interviews are planned which will elaborate in the more technical aspects of the project.
Participation to a Conference	RHT		KubeCon / CloudNativeCon Europe 2023	17.-21.04.2023	Amsterdam, Netherlands	<a href="https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/program/cfp/">Paper submitted to https://events.linuxfoundation.org/kubecon-cloudnativecon-europe/program/cfp/</a>
Organization of a Conference	UULM	DENSO	IEEC Vehicular Networking Conference VNC	26.-28.04.2023	Istanbul, Turkey	Organization of conference by UULM, presentations by partners



Type of activities	Main Leader	Other partners	Title	Start	Place	Type and goal of the event / website
Panel Participation	UULM		Panel Discussion on “Privacy, Trust and Reputation Management in Internet of Vehicles (IoV)” to be published on the June (2023) issue of the IEEE IoT Magazine	05.2023	Online	Participation in a roundtable discussion on privacy, trust and reputation management in Internet of Vehicles (IoV). This discussion is organized as part of the NIST clustering activities.
Website	TEC	UTWENTE	Fact Sheet 3: Trust relationships	04.05.2023	Online	Detailed information and graphic; as blog, pdf and via social media
Participation to a workshop	UBITECH		TPM Development Community ( <a href="https://tpm.dev">TPM.dev</a> )	16.05.2023	Online	Keynote talk on the trusted computing related activities of CONNECT towards the creation of a chain of trust when exchanging in-vehicle data. Detailed presentation on CONNECT’s security claims that can be self-issued by each OBU (equipped with a Root-of-Trust such as a TPM or TEE) towards the provision of verifiable evidence on the integrity state of the control unit.
Panel Presentation	UBITECH, ICCS, HUAWEI		<a href="#">ITS European Congress 2023</a>	22-24.05.2023	Physical	Two panel sessions on “Trust in CCAM” and “Future of CCAM Services” have been proposed to the year’s ITS EU Congress by the CONNECT partners. Waiting on the outcome.
Participation to a Conference	UBITECH		ACM WiSec 2023	29.05.-01-06.2023	Guildford, Surrey, UK	<a href="https://wisec2023.surrey.ac.uk/">https://wisec2023.surrey.ac.uk/</a> ,
Organization of a Conference	SURREY		ACM WiSec 2023	29.05.-01-06.2023	Guildford, Surrey, UK	<a href="https://wisec2023.surrey.ac.uk/">https://wisec2023.surrey.ac.uk/</a> ,
Participation to a Conference	RHT	UBITECH	RHT Development Conference - EU Research Projects	15.06.2023	Brno, Czech Republic	<a href="https://www.devconf.info/cz/">https://www.devconf.info/cz/</a>

Type of activities	Main Leader	Other partners	Title	Start	Place	Type and goal of the event / website
Organization of Workshop	UULM, HUAWEI	UBITECH, DENSO, TRIALOG	Dagstuhl Seminar on “Privacy Protection of Automated and Self-Driving Vehicles”	11-16.06.2023	Physical	Organization of a Dagstuhl Seminar, affiliated to CONNECT, for discussing the current security and privacy-related issues that need to be resolved for enabling the future of connected cars (organized by UULM and HUAWEI).
Participation to a Conference	UULM		IEEE Vehicular Technology Conference VTC Spring	18.-21.06.2023	Florence, Italy	<a href="https://events.vtsociety.org/vtc2023-spring/">Paper submitted - https://events.vtsociety.org/vtc2023-spring/</a>
Participation to TCG Physical Meeting	UBITECH		Trusted Computing Group Annual Members Meeting	25.07.2023	Physical	Presentation of CONNECT’s attestation enablers and primitives to the TPM Working Group. Discussion also on the overall CONNECT architecture with the TPM Automotive Working Group.
Organisation of a Workshop	UBITECH	CONNECT Partners	4th Workshop on Cyber-Security Arms Race (CYSARM)	25.09.2023	The Hague, The Netherlands	ESORICS 2023 Workshop Proposal submitted, awaiting outcome
Participation to ETSI Security Week	FSCOM	ITRSX, UULM, UBITECH, HUAWEI, DENSO	ETSI Security Conference 2023 <sup>5</sup>	16-20.10.2023	Physical	Presentation of CONNECT’s vision and defined use cases in the context of Intersection Movement Assistance, Vulnerable Road User Protection and Slow Moving Traffic Detection.
Workshop	UBITECH	ALL	Internal workshop with SELFY project	TBC	Online	The focus of the workshop is to share requirement elements of both projects.

<sup>5</sup> <https://www.etsi.org/events/2155-etsi-security-conference-2023>

## Chapter 7 Relevant Initiatives and Standardization

### 7.1 Liaison with Relevant Initiatives

An important part of the dissemination activities includes the build-up of liaison with other projects and initiatives relevant to the fields of CONNECT. Through this connection, CONNECT will promote stakeholders clustering, focus on targeted engagement and perform cross-dissemination activities. The aim is to disseminate project's outcomes, ensure exchange of knowledge and best practices to the mutual benefit of all parties involved, and increase visibility of CONNECT within the market and potential future clients for its solutions.

Under this approach, CONNECT will seek developing liaison and collaborations with:

- Related projects and research initiatives;
- Industrial associations;
- Appropriate standardisation bodies and Working groups.

An initial list of receivers is the already established and rich portfolio of connections with related projects and initiatives by the members of the consortium. The strong and multi discipline partnership of CONNECT's consortium poses a wide network of synergies that will be exploited to engage with several market players and domain stakeholders. This list will further grow with the addition of relevant organizations and peers that will be identified during the project's lifetime.

In this direction, CONNECT has already established a liaison with the recently started PODIUM EU project ("*PDI Connectivity and Cooperation Enablers Building trust and Sustainability in CCAM*") towards building trust and sustainability for CCAM. Both project initiatives envision to address the challenges in road automation and telecommunications linked with low latency, cooperation, data management, security and resilience for the development of advanced CCAM solutions. **The vision is that combining connectivity, cooperative systems and automation will enable automated and fully orchestrated vehicle maneuvers, thus, bringing us closer to the overall CCAM vision.** CONNECT and PODIUM share a subset of use cases (especially in the context of **Intersection Movement Assistance and Corridor Management through Maneuver Assistance**) and discussions are already ongoing to investigate possibilities for common activities on setting up and investigating shared experiments. While PODIUM, for instance, investigates the use of Subjective Logic (SL) for enabling vehicles to self-assess their internal perception system, CONNECT leverages SL to assist vehicles in assessing the level of trust of their internal as well as the collaborative perception received from neighboring vehicles (or the MEC). The endmost goal is to ensure that the complementary results of both projects can be implemented, capitalized and evaluated in large-scale proof of concept environments.

Continuing on the same path, liaison with the other EU project funded in the same call towards "*Cyber Secure and Resilient CCAM*" has already been established. The SELFY project initiative focuses on enhancing the resilience of CCAM ecosystems through enabling **situational awareness and collaborative perception**: Obtain a comprehensive understanding of the environment based on the shared data, from all comprised CCAM vehicles and devices, towards allowing better decision making systems. To support this vision, SELFY also envisions to build a secure and trusted environments for data sharing between all actors in such decentralized environments. Thus, the two consortia will be collaborating to exchange views on the **common research topic of trust assessment and management** which can lead to new ideas, perspectives, and insights that can improve the research output. Sharing knowledge, research findings, and techniques will improve the overall understanding of trust in ITS systems and can lead to the development of more comprehensive and complete trust-building techniques and technologies that can be used in ITS systems. As trust building in ITS is a critical factor for the success and widespread acceptance of ITS, collaboration and liaison can help in addressing the trust issues and concerns that are preventing the widespread adoption of ITS.

For the latter, industrial associations are listed in Table 6 with actions foreseen by CONNECT partners. This list may further grow during the lifetime of the project depending on the involvement

of CONNECT representatives. CONNECT will aim at participating in the associations with CONNECT partners that are members with the objective of contributing with project results and working on various specification activities related to the key objectives of the CCAM Partnership [6]. This will make the project's work visible to the membership of the associations and make them part of the associations' publications which will further raise the awareness of the CONNECT work.

**Standardisation organisations and involved CONNECT partners are listed in Table 8 and Table 9.** The list is comprehensive and covers the technical areas in which CONNECT works comprehensively. CONNECT will adhere to existing standards and specifications; gaps and shortcomings may be found in the documents which will lead to feedback (e.g., change requests) to the SDOs that produced them. Furthermore, CONNECT will actively promote project results by participation of its partners in the SDO activities. This will include the presentation of the CONNECT work in standardisation workshops and by direct work in relevant working groups with the objective of contributing CONNECT results to existing and new standardisation working items (as the one that is already ongoing with the 5GAA Association as described in Table 8). It should be noted that at the time of writing the present deliverable, CONNECT had already contributed with one Use Case (Edge Misbehaviour Detection for V2X data reliability) to the work of ISO/TC204 WG20 which covers 'Big Data and Artificial Intelligence supporting ITS' and is currently developing the technical report - ISO TR 12786 "Intelligent transport systems — Big data and artificial intelligence supporting intelligent transport systems — Use cases".

The 5G Infrastructure Public Private Partnership (5G PPP, <https://5g-ppp.eu/>) is a joint initiative between the European Commission and European ICT industry (ICT manufacturers, telecommunications operators, service providers, SMEs and researcher Institutions). The 6G Smart Networks and Services Industry Association (6G-IA, <https://6g-ia.eu/>) represents the private side where in 5G-PPP, the European Commission represents the public side. Partners in Horizon Europe projects are encouraged to join the working groups to feed in their project results which makes it an ideal forum to liaise with other projects also participating in the different WGs.

Overall, WGs should be followed by the CONNECT partners to identify partners for collaborations. FSCOM, for example, is member of the Pre-Standardisation WG which identifies standardisation and regulatory bodies to align with e.g. ETSI, 3GPP, IEEE and other relevant standards bodies; FSCOM will (and has already in Q4 2022) contribute with CONNECT standardisation results to the quarterly SDO impact reports.

### 7.1.1 Automotive Associations and Initiatives

CONNECT is in the position to contribute to various technical specifications and initiatives on cyber-security and trust in CCAM due to the novelty of its solution, as well as on the fact that it tackles a domain that is currently under investigation for overcoming the security hurdles that will enable higher levels of vehicle automation and safety-critical services. Its envisioned security architecture will provide a flexible trust model that is applicable in various road environments including also the MEC layer for supporting high connectivity and low latency. Apart from the envisioned participation and contribution to various standardization bodies (detailed in Section 7.2), CONNECT aspires to also contribute to a series of open source communities, which are highlighted below:

Table 6: CONNECT Technology-related Associations and Initiatives

CCAM Industry Associations	
<b>Global Semiconductor Alliance</b>	<a href="#">GSA Trusted IoT Automotive Ecosystem Security (TIES)</a> is a collaborative group of companies in the automotive value chain focusing on promoting use cases and end-to-end solutions that minimize risks. They have extended work on secure "Chip-to-Cloud" assurance solutions for enabling trustworthy and resilient safety-critical automotive services such as autonomous driving, connected cars, shared mobility, intersection management, collision avoidance, etc. CONNECT envisions to contribute to the current specifications of how <b>trusted components can be deployed in the vehicles acting as a Root-of-Trust for enabling the establishment of trust relationships and trust calculations in next-generation CCAM.</b> UBITECH is already a member of GSA TIES.

CCAM Industry Associations	
<b>C2C Consortium (C2C-CC)</b>	C2C-CC aims at accident-free traffic (vision zero) at the earliest possible date by supporting the highest safety level at improved traffic efficiency anywhere, anytime at the lowest cost to the end user and the environment. The membership is made up of leading European and international vehicles manufacturers, equipment suppliers, engineering companies, road operators and research institutions. CONNECT will closely monitor The C2C-CC work and identify points of common interest to contribute with project results. DENSO and IRTSX are already members of the C2C-CC regularly participating in the technical meetings.
<b>Open Networking Forum (ONF)</b>	Has developed an SDN architecture that may be relevant for SDN and NFV concepts. ONF activities and groups that may be relevant include: the North Bound Interface (NBI), the Carrier Grade SDN WG and the Mobile WG. CONNECT aspires to monitor the advancements of these groups and explore the possibility of contributing to the open-source specifications related to optimal device resource allocation.
<b>ETSI OSG Open Source MANO (OSM)</b>	An open-source initiative whose objective is to create a production-quality NFV orchestrator based on open-source code that should become a reference implementation of the MANO stack. CONNECT aspires to closely monitor the developments of the OSM and contribute based upon the advancements of the development of the distributed attestation-enabled CPS orchestration for heterogeneous and high-density edge devices, leveraging the root of trust capabilities of the CONNECT remote attestation services and providing security and trust features at all levels of the VNF stack.
<b>IEEE SDN</b>	Abroad-based collaborative project focused on Software Defined Networks and Network Function Virtualization (NFV). Providing contributions to IEEE NFV regarding the dynamic resource allocation mechanisms that are going to be applied, exploiting the CONNECT collective threat intelligence analysis and forecasting engine.
<b>CCAM Partnership/ Association</b>	The CCAM (Connected Cooperative Automated Mobility) Partnership aligns all stakeholders' R&I efforts to accelerate through the introduction of a coherent and long-term research and innovation agenda the implementation of innovative CCAM technologies and services aiming to realise: increased safety, reduced environmental impacts, and inclusiveness in Europe. The Partnership develops and implements a shared, coherent and long-term R&I agenda by bringing together the complex cross-sectoral value chain actors sharing the vision of European leadership in safe and sustainable automated road transport. The CCAM Association, represents the innovation stakeholders in the CCAM Partnership, aims to gather (currently more than 150 members) all types of CCAM stakeholders, ranging from players of different industry sectors to research institutes and universities, associations, service providers, and national and local authorities. The CONNECT consortium, through its multi-stakeholder profile (i.e., research, SMEs, industry) will leverage (accordingly) the CCAM partnership/association channels to contribute to both the CCAM the Strategic Research and Innovation Agenda (SRIA) and also the innovation outreach (to the community and even broader audiences).

### 7.1.2 5GAA

The 5G Automotive Association (5GAA, <https://5gaa.org/>) 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. The main essence of 5GAA work is to bring together two main categories of stakeholders: First, telecommunication companies (like operators, neutral hosts, network technology providers, chip

makers, etc.) that are providing connectivity and networking systems, devices and technologies. Second, automotive players (like vehicle OEM manufacturers, OEM suppliers, system integrators, etc.) that work on vehicle platforms, hardware and software solutions. 5GAA has 119 industry members, including automotive manufacturers, tier-1 suppliers, chipset/communication system providers, mobile operators and infrastructure vendors.

**Trust in C-ITS becomes an increasingly important topic in 5GAA.** Several WIs have called for the need to establish trust in the use of MEC in C-ITS applications, as well as in the exchange of geolocation information between vehicles and other sensor sharing applications. However, establishing mutual trust has been discussed only in the context of Safety so far, while the discussion on technological innovation for trust only begins now. CONNECT is planning to drive these discussions and bring its solutions to the forefront for elaboration between 5GAA industrial participants and adoption by standards.

### 7.1.3 Open-Source Communities

The ECLIPSE foundation has transferred its headquarters to Europe in order to address the needs for open source in Europe. In particular ECLIPSE is a partner of the OpenContinuum support action that will support the various European research projects in creating impactful open-source projects. To this end, ECLIPSE, with the help of TRIALOG has defined an Open-Source Development plan guidance that is adapted to research project and that will be considered by CONNECT in its own open-source project.

Further the outcome of CONNECT in terms of secure data exchange building block in the continuum could be of interest in future data space initiatives (GAIA-X, IDSA connectors) and coordination will be sought to identify synergies. TRIALOG who is part of the standardisation advisory board of IDSA, the co-chair of the standardisation working group of AIOTI and the standardisation representative of BDVA will be involved in this liaison.

### 7.1.4 Building Trust and Resilience in CCAM

The following activities in standardization will also be taken into consideration by CONNECT for enabling **trustworthiness management to be included in CCAM's security functionality solutions for verifying the trustworthiness of transmitting stations and infrastructure.** The goal is to align the trust architecture and model to be constructed in CONNECT with the latest activities and trust considerations in the gMEC4AUTO Architecture [7]: CCAM deployments constitute a complex multi-vendor, multi-supplier, and multi-stakeholder ecosystem lacking a central entity that implements system-wide security assurances or accepts full liability if things go wrong. As a result, this brings to the surface the issue of mutual trust between stakeholders meaning that we cannot make assumptions about the trustworthiness of participating entities and we have to move to the discussion of what is needed to prove that an actor is trusted or not. A number of activities are currently ongoing in ISO towards the creation and adoption of a generic trust model defining the properties that need to be exhibited by the various actors for achieving specific Levels of Assurance.

- ➔ Adopting the concept, framework and architecture being worked out by ISO/IEC JTC1/WG13 (trustworthiness)
- ➔ Adopting the trustworthiness principles and views of ISO/IEC JTC1 SC41 (IoT and digital twins).
- ➔ Integrating and contributing to various security and privacy standards (ISO/IEC 27564 Privacy models - in particular using ITS use cases, ISO/IEC 27568 security and privacy of digital twins)
- ➔ Monitoring, integrating and contributing CEN-CENELEC JTC21 (WG4 on AI trustworthiness characterization, WG2 on AI conformity assessment)

## 7.2 Standardisation Activity Plan

### 7.2.1 Research and Standardization Communities

Reaching the **research and standardization communities** is crucial to innovation within the European Union: *in order for the CONNECT project to have a real impact in further research, and to*

help the standardization path, it is essential to reach and gain the interest of the communities, as aforementioned.

For the former, there are many channels through which the research community can be reached, and results of the project can be made available. First of all, it is necessary to publish in open access. CONNECT will provide open access to all published articles, on the ZENODO platform, and all publications will be made accessible on the project website, where they will be linked to their DOIs.

For the latter, standardisation is an utmost important aspect of the CONNECT project. CONNECT envisions to actively contribute to the security and interoperability efforts regarding futureproofing of CCAM ecosystems that the European Commission instruments, standardisation bodies and private organizations are pursuing. Towards this goal, the consortium will continuously analyse the standardisation potential of the project's key innovations and will map the key exploitable innovations to the standardisation objectives in order to continuously update the concrete plan, already put forth in Section 7.2, towards submitting contributions to relevant standardisation bodies.

CONNECT partners aspire to exceed instead of merely reaching the following list of Impact KPIs, concerning Standardization Activities in all parallel channels, as these are gathered from the relevant sections of the Grant Agreement and tracked through the plan presented in this deliverable.

**Note:** This list might be further enriched as the project progresses and the present plan is updated and refined accordingly (in M18 and M36 respectively).

Table 7: Research and Standardization Communities

Relevant Activities	Impact Metric – KPI	Target
Collaborations, Synergies, Liaisons, with projects clusters and initiatives	Synergies with Projects	$\geq 6$
	Joint Activities, Joint Dissemination, Joint presence in Events	$\geq 8$
Standardisation Bodies	Liaison with working groups	$\geq 3$
	Project presentation in standardisation meetings	$\geq 5$
	Contributions to technical specifications related to remote attestation, use case specification (e.g., Misbehavior Detection), trust management, etc.	$\geq 2$
	Participation in Committees (meetings)	$\geq 3$

### 7.2.2 Standardization Bodies & CONNECT Road-Map

As aforementioned, a key strategic objective of CONNECT is to contribute to standardization efforts at EU level with ISO/IEC, ETSI, 5GAA (among others). Planned outcomes of the project include the development of standardization proposal that push the state of the art in core areas (targeted by CONNECT) of trust assessment and management, remote attestation (and underlying trusted computing technologies), lightweight cryptography, and the secure and accountable exchange of collective perception data in CCAM environments.

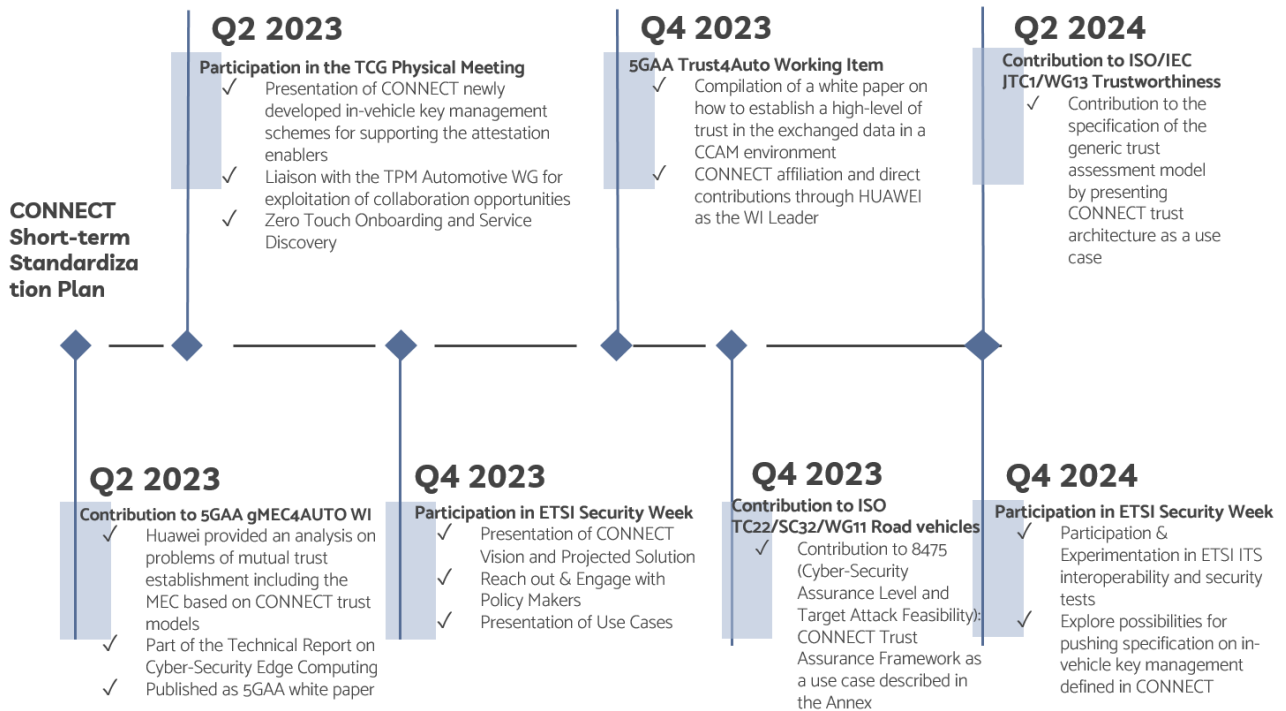


Figure 10: CONNECT Short-Term Standardization Activities Plan

Towards this direction, CONNECT will involve the technical committees of the relevant standardization bodies, as listed in the following table. A summarized version of the immediate standardization plan till fall 2024 is also depicted in Figure 10.

Table 8: Standardisation Bodies and CONNECT Road-Map

TCG
<p>UBITECH and SURREY have already established an Academic Liaison relationship with the Trusted Computing Group (TCG) and are aiming to disseminate the work conducted in the context of CONNECT WP4 towards novel property-based attestation mechanisms to the TCG. They participate in the following working groups: Trusted Platform Module (TPM), TPM Software Stack (TSS), Trusted Network Communications (TNC), the Internet of Things (IoTs), and DICE. In addition, SURREY is working on a new breed of Direct Anonymous Attestation schemes which are targeted for inclusion in a future TPM. Furthermore, UBITECH is planning to become a member of the C2C-CC for disseminating the work towards decentralized security and privacy-preserving architectures in the V2X domain (where trust is shifted from the infrastructure towards the edge) based on the use of advanced crypto primitives and especially Control-Flow Attestation.</p>
ETSI
<p>IRTSX and FSCOM are both active in ETSI TC ITS, namely in its WG5 which covers the security aspects. This ETSI TC meets 4 times per year with ETSI hosting the meetings in its premises in Sophia Antipolis, France. FSCOM has also for many years participated in ETSI STF (specialized Task Force) and TTF (Testing Task Force) groups for the development of test specifications and has also been actively involved in the organization and execution of ITS interoperability test events (ETSI Plugtests™) both including work on the ITS security aspects. Furthermore, FSCOM is following and contributing to work of several other ETSI groups (ISG MEC, ISG NFV, TC SmartM2M, TC INT, etc.).</p> <p>IRTSX is active in the WG5 of ETSI TC ITS, where it edits the TS 103 759 on the Misbehaviour Reporting Service. Publication of TS 103 759 is scheduled in Q1 2023. IRTSX will continue its activity in WG5, and plans to propose a new working item on Misbehaviour Reporting Service, to extend support to reporting misbehaviour on the Collective Perception Service, and to propose security solutions for the protection of the security and privacy of the misbehaviour reporting process.</p> <p>ETSI will be hosting the ETSI Security Conference 2023 during the week of 16 to 20 October, in ETSI, Sophia Antipolis, France. CONNECT has taken first contacts with the ETSI staff organizing this annual flagship event on Cyber Security with the aim of successfully submitting CONNECT papers to the</p>



conference. Presenting the CONNECT concepts at this important conference will be an important asset in raising awareness of the project and will be both a great dissemination and networking opportunity.

#### CEN-CENELEC

TRIALOG is active in JTC21 on AI trustworthiness characterization and AI conformity assessment, and in general standards that will address the AI act. TRIALOG also follows JTC13 on the standards related to the RED directive that started in the fall of 2022.

#### ISO Related Activities

FSCOM is participating in the meetings of ISO TC204 on ITS, namely in the working groups WG19 on Mobility integration, WG20 on Big Data and Artificial Intelligence supporting ITS and WG17 on Nomadic Devices in ITS Systems where FSCOM holds the chairmanship of sub-WG17.2 which aims at developing a series of international standards which define energy-based green ITS services providing urban transport management and smart city mobility applications on nomadic & mobile devices. During ISO WG plenary meetings which are held twice a year in a rotating venue scheme (Europe, Americas, Asia-Pacific) special time slots are reserved for workshops. It is planned to present the CONNECT project, its methodology and results at those workshops which draw an international (worldwide) audience with big delegations from China, Japan, Korea and the USA. This will be the perfect stage to disseminate knowledge of CONNECT beyond the European context.

An ISO WG may have additional meetings held between the plenary meetings. CONNECT has already submitted a use case description to ISO TR12786 which is currently developed by WG20. FSCOM will follow up on the further development of this technical report which will be the first concrete CONNECT contribution to an internationally recognized standard.

SURREY have already been involved in ISO/IEC JTC1 SC27/WG2, which specify cryptographic mechanisms. SURREY attend this working group's meetings regularly and have contributed to many existing standards, including entity authentication, digital signatures, anonymous digital signatures, direct anonymous attestation, hash functions etc. They are therefore in a good position to introduce any new requirements and the corresponding solutions from the CONNECT project to this working group.

TRIALOG is involved in ISO/IEC JTC1/AG8 in a guidance document on future reference architecture standards. TRIALOG is also involved, in ISO/IEC JTC1/SC41 on IoT and digital twin on the future IoT reference architecture, on the future Digital Twin reference architecture, on the future standard on interoperability, on the future guidance on use case, and on the future standards for data spaces. TRIALOG is involved in ISO PC317 and ISO/IEC JTC1 SC24 on standards related to cybersecurity assurance of systems of systems, security and privacy of digital twins, privacy models, data provenance, CPS, AI security and privacy.

#### 5GAA

Several partners of CONNECT are also members of 5GAA, i.e. HUAWEI, DENSO, Intel, and FIAT CNR (via Stellantis). HUAWEI is also the co-chair of 5GAA WG7 on Security and Privacy and it has already initiated the establishment of a Liaison of CONNECT to 5GAA. **HUAWEI provided an analysis on the problems of mutual trust establishment in using the MEC for C-ITS applications and recommendations on identifying the need of new solutions in the lines of CONNECT. This analysis was integrated into the report of WI qMEC4Auto and it will be published as part of an upcoming 5GAA white paper by April 2023.** At the same time HUAWEI has **initiated and will be leading a new WI (called Trust4Auto) in 5GAA WG7 dedicated to the topic of Trust for CCAM. The WI was approved by the 5GAA board in February 2023 and will last 9 months.** The work in this WI will be published as white paper and it will provide guidance on how to establish a high level of trust into exchanged data and MEC applications for enabling CCAM scenarios. This WI will create a bidirectional exchange between 5GAA and CONNECT, where industrial and academic partners will provide feedback and elaborate on the ideas from both groups.

Table 9: Overview of CONNECT members participation in relevant clusters/associations associated to CONNECT outcomes

Group	Company	Role of involvement	Description of involvement
ISO/IEC JTC1/AG8 Metareference architecture for system integration	TRIALOG	French delegate	Responsible for task force patterns, and contribution to guidelines standards development on reference architecture, based on ISO/IEC/IEEE 42010 architecture description. Connect will take into account those guidelines to facilitate contribution of standards
ISO/IEC JTC1/WG13 Trustworthiness	TRIALOG	Liaison officer from SC41	Contributions to 5957 (Trustworthiness reference architecture); 9814 (Trustworthiness concepts), 18149 (Trustworthiness ontology). Connect will take into account WG13
ISO/IEC JTC1/SC27 Information security, cybersecurity and privacy protection.	TRIALOG	French delegate Liaison officer from PRIPARE (EC project)	Editor of 27563 (security and privacy in AI use cases – best practices), 27568 Security and privacy of digital twins, 5986 Cybersecurity assurance of systems and SoS, 27564 Privacy models, 27091 AI systems privacy protection (under ballot). Contribution to 5888 (Security requirements and evaluation activities for connected vehicle devices) Contributions from Connect are expected
ISO/IEC JTC1/SC41 IoT and digital twins	TRIALOG	French delegate Liaison officer from AIOTI	Contributor to 30141 (IoT reference architecture, PWI digital twin reference architecture). Editor of 30149 (IoT Trustworthiness principles), 21823-5 (Behavioral and policy interoperability). PWI Guidance on IoT and digital twin use cases. Chair of AG25 (use cases), AhG30 (CPS), AG31 (impact of other standards on SC41) Connect will take into account SC41
ISO/IEC JTC1/SC42 Artificial intelligence	TRIALOG	French delegate	Contributor to 5392 (Knowledge engineering reference architecture). Connect will take into account SC42
ISO PC317 Privacy-by- design for consumer goods and services	TRIALOG	Liaison officer from PDP4E (EC project)	Contributor to 31700-1 (high-level requirements) Editor to 31700-2 (use cases)

Group	Company	Role of involvement	Description of involvement
ISO TC22/SC32/WG11 Road vehicles	TRIALOG	French delegate	Contributor to 8475 (Cybersecurity assurance level and Target attack feasibility), 8477 (Cybersecurity verification and validation),
CEN-CENELEC JTC21 Artificial intelligence	TRIALOG	French delegate	Contributor to WG2 AI conformity assessment (task force on automotive domain), to WG4 AI trustworthiness characterisation
ETSI TC ITS WG5	TRIALOG	Delegate	Following the WG to ensure alignment with ISO 21434 (road vehicles cybersecurity) as well as privacy protection (e.g. impact of PKI model)
IEC TC1	Technikon	TC 1 Advisory Group	Providing advice on IEC terminology work
ISO TC204	FSCOM	Convenor SWG17.2, delegate in other groups	Active in WG17, 19 20
ETSI TC ITS WG5	IRTSX	Delegate	Rapporteur TS 103 759 (misbehaviour reporting service)
ETSI TC ITS	FSCOM	Meeting delegate STF/TTF member Member of ETSI Plugtests™ team	All WGs Development of test specifications, active testing during Plugtests
ETSI ISG MEC	FSCOM	Meeting delegate STF/TTF member Member of ETSI Plugtests™ team	Development of test specifications, active testing during Plugtests
5G-PPP/6G-IA	FSCOM	Project representant for 5G-IANA, 5G-LOGINNOV, 5GMETA and CONNECT	Pre-Standardisation and Trials WG
5GAA	Stellantis (CRF)	Board member	Currently not actively contributing in Security Topics
5GAA	DENSO	Board member	Currently not actively contributing in Security Topics
5GAA	HUAWEI	Board member, WG7 co-chair	Leading WI “Trust4Auto - Creating Trust in Connected Automated Vehicles” in WG7 bringing contribution from CONNECT into 5GAA. Also contributing to WI “gMEC4Auto - Technical Report on Cybersecurity for Edge Computing” on Trust considerations for the use of MEC in CCAM from the CONNECT perspective.

Group	Company	Role of involvement	Description of involvement
5GAA	Intel	Board member	Leading the WI “gMEC4Auto - Technical Report on Cybersecurity for Edge Computing”
CCAM Partnership			HUAWEI represented CONNECT project in the Multi-Cluster meeting in Brussels in October 2022, making sure that the project’s mission and results are well aligned with the CCAM Strategic Research and Innovation Agenda.
ERTICO (public-private partnership)	ICCS	Full partner	Participation in the ERTICO innovation & deployment activities ICCS is member of the ERTICO Supervisory Board acting as the ERTICO Chairman
AIOTI	INTEL	WG Research and Collaborations co-chair	steering AIOTI SRIA, ensuring proper impact of AIOTI work in the European ecosystem
	TRIALOG	WG Standardisation chair	Ensuring proper contribution of AIOTI work to standardisation, in particular on data spaces and digital twins Participation to high-level architecture and semantic interoperability groups.
6G IA	ICCS	Full member	WGs not started yet; 5G-PPP WGs still in action. ICCS participates in 5G4CAM and TMV WGs, while it also participated in the 5G-PPP Technical Board
C-ROADS platform (Joint initiative of European Member States and road operators)	ICCS	Implementing body	Technical member in C-ROADS Greece. Development of the PKI system.
ETSI MEC Industry Specification Group (ISG)	ICCS	Participant	Monitoring developments
ETSI Zero Touch network & Service Management (ZSM)	ICCS	Participant	Monitoring developments
ETSI Network Functions Virtualisation - ISG	ICCS	Participant	Monitoring developments

Group	Company	Role of involvement	Description of involvement
ETSI Experiential Networked Intelligence (ENI) WG.	ICCS	Participant	Monitoring developments
6G IA	INTEL	WG Trials / Stream "5G and towards 6G Verticals" Lead	Driving the discussion in 6G-Ia on new use cases and potential new vertical sectors 6G will bring
AIOTI	INTEL	WG Research and Collaborations co-chair	steering AIOTI SRIA, ensuring proper impact of AIOTI work in the European ecosystem
GSA TIES	UBITECH	Member of WG-02, WG-05, and WG-17 on Secure and Trusted Computing Functionalities for Decentralized Automotive Services	Monitoring Developments & Participation in Specifications related to the design of new attestation enablers.
Trusted Computing Group	UBITECH	Invited Expert to TPM WG	Monitoring Developments & Participate in Discussions/Specification Construction
SSI eSSIF	UBITECH	Member of eSSIF Ecosystems	Monitoring Developments
ISO/IEC JTC1 SC27 WG2	SURREY	Member of WG02	Monitoring the specification of lightweight crypto protocols
ETSI TC ITS	UULM	Member	We are member but currently not actively involved in any activities. We could get active if we have to contribute something.
C2C-CC	IRTSX, DENSO, UULM	Member	IRTSX and DENSO are full members of the C2C-CC and they plan to monitor the discussions on CCAM services and applications definition for Day-3 by participating in the technical meetings.

## Chapter 8 Exploitation Plan

Besides dissemination and standardization activities, another important aspect of CONNECT's activities pertain to the exploitation opportunities of the various technical artefacts and security enablers to be designed and implemented. The main objective of an efficient exploitation strategy is to ensure that the results and benefits of the developed project outputs are attractive and well-known in the industry. As such, the objectives of the CONNECT exploitation plan are to:

- Establish and maintain mechanisms for effective exploitation,
- Inform stakeholders of the project development and encourage interactions/networking,
- Coordinate all levels and types of exploitation of the knowledge produced by the project,
- Ensure that information is shared with appropriate audiences in a timely manner and by the most effective means and medium.

Alongside the dissemination of the project results, exploitation of the achievements of CONNECT is of crucial importance and is recognized as one of the key elements for the success of CONNECT as underpinned by its significant industrial participation. **Our common goal is to create knowledge, research new solutions and pave the way for successful commercial product innovation.** Individual exploitation plans, as well as a common project exploitation roadmap, will be documented in D7.2 [8] and will be finalized in D7.3 [9] at the end of the project activities where all technical artefacts will have been finalized. However, a detailed list of such expected exploitable artefacts is listed in the following section and Table 10.

Another crucial objective of CONNECT is its vision to **share most of its artefacts and components as open-source so as to better facilitate the endmost goal of securing next-generation CCAM ecosystems: By allowing all stakeholders in the automotive supply chain to be able to leverage CONNECT's security enablers as building blocks in their own deployments.** Compounding this issue, CONNECT has already identified an open-source development plan (as specified in Section 8.2) with the vision to engage with the standardized ECLIPSE WG.

While the main goal of CONNECT is the specification and design of a dynamic trust assessment framework for complex CCAM ecosystems, through the conversion of vehicles into security "hardened" tokens equipped with a new breed of trusted computing enablers, the results of the project are valid beyond that and therefore can be exploited to a broader range of products. These include Hardware Security Modules (HSM), Trusted Execution Environments as defined by the GlobalPlatform, the ARM TrustZone, Intel's SGX, to name but a few. All of these will need 1) new algorithms and protocols that can leverage them for producing strong security claims on the level of trustworthiness of a device, and 2) none of them have a comprehensive security model and analysis. Thus, the CONNECT aims to exploit its results also in the context of all of these stakeholders.

### 8.1 Exploitable Artefacts

In the following, we aim to identify and present the **core technologies of CONNECT**, as well as the **exploitable assets**, which are essentially the innovations and **value propositions of CONNECT** in terms of marketability, and will set the scene for its market positioning taking into consideration the novel features it offers compared to its competitors, in terms of both the CONNECT framework as a whole, as well as its individual modules. In order to be able to later perform an analysis of the market trends and exploitation possibilities that covers the widest possible range of industry viewpoints (to be included as part of D7.2 [8] and D7.3 [9]), an extensive research framework will be employed. A mixture of different approaches will be followed in order to gain valuable knowledge and a complete understanding of the target markets. Specifically, three insight perspectives will be used in CONNECT:

- **Market insights:** Involves researching and studying publicly available industry and monetary reports in order to identify long term and emerging market trends, including estimates about market size evolution, challenges, and opportunities.

- **Competition insights:** Involves listing key competitors and their product offerings with emphasis on existing or planned features, their placement in the market, as well as their strengths and weaknesses. It should be noted that, due the nature of the market, a large volume of information about existing products and services is not available to the general public.
- **Client insights:** Involves identifying the key activities and main points of importance from the perspective of a potential customer. This includes the value proposition and its importance to the aforementioned customers, and aims to identify the customer base of CONNECT and assist in performing customer segmentation.

Taking into consideration the above, the purpose and ultimate goal of the exploitation analysis and plan is to align and fine-tune the development of CONNECT with the expectations and needs of the market. Additionally, it seeks to determine the most effective exploitation tactics with an appropriate business model for the system. As previously mentioned, CONNECT is focused on enhancing the operational assurance and trust model of the entire automotive supply chain and service graph chain. In this context, several technological domains will be employed and integrated into the CONNECT framework, including **Trust Assessment, Trusted Computing, Attestation and Integrity Conformance, HW-based Trust Anchors, Blockchain technologies, and Risk Assessment.**

Each of the aforementioned technologies will be explored in CONNECT in a modular manner, and each one corresponds to a concrete **exploitable asset** that will be designed in. In what follows, we provide a high-level specification of the envisioned CONNECT assets that will be considered in the later exploitation planning and will be part of the overall open-source development roadmap. It must be noted that this is a live process that will go through several iterations in the life cycle of the project and will be updated dynamically. The final reporting of this process will be performed in D7.3 [9].

Table 10: CONNECT High-Level Summary of Exploitable Assets

CONNECT Asset	Description
<b>Trust Assessment Framework</b>	CONNECT will define a trust architecture capturing the trust model and trust relationships of the next generation CCAM systems. This will enable vehicles to continuously assess the level of trust they can place on the Edge server to make calculations on their behalf or the level of trust they can place on the input from other vehicles. To address the dynamic nature of CCAM systems, the safety-critical nature of the services and the presence of multiple actors (multi-MNO and multi-OEM), we place the Zero Trust concept at the base of CONNECT’s trust architecture: trust on any entity is initially zero and needs to be established through suitable mechanisms. The framework consists of two related elements: on the one hand, an <b>automated, real-time risk assessment mechanism</b> that will enable a vehicle to calculate the required trust level (RTL) needed to cooperatively execute a certain CCAM function addressing the identified risks. On the other hand, a <b>reasoning mechanism</b> to infer the actual trust level (ATL) that can be placed into a remotely executed function or externally received data. Only if the actual trust exceeds the required trust can this function be executed safely; otherwise, the system may resort to fallback mechanisms. At the core of this framework, trust is expressed in a formal verifiable manner ( <b>security claims</b> ) to be offered by the CONNECT Attestation Enablers.
<b>Risk Assessment Engine</b>	Based on the threat landscape to be defined for the entire CCAM ecosystem, CONNECT will employ risk assessment methodologies for developing a tool that is capable of reasoning on the Required Trust Level (RTL) of a vehicle. This essentially will provide the necessary trust policies that will govern the entire lifecycle of a road vehicle and will dictate the type of evidence that it needs to provide prior to be allowed to establish a communication channel with another entity. Appropriate risk quantification methodologies will be employed leveraging the latest advancements in the ISO/SAE 21434 on automotive

CONNECT Asset	Description
	cyber-security engineering [3] – in particular the Attack Potential risk quantification approach.
<b>Attestation Enablers</b>	The attestation toolkit of CONNECT will provide the mechanisms for assessing the configuration integrity and operational correctness of a CCAM actor (can be the MEC, a Vehicle or a specific vehicle OBU) prior to allowing the establishment of secure relationships between only attested actors. This is envisioned in the context of secure “Chip-to-Cloud” assurance solutions for enablement of trustworthy and resilient safety-critical automotive services such as Autonomous Driving, Connected Cars, Shared Mobility, Intersection Management, Collision Avoidance, etc. More specifically, CONNECT will define and leverage <b>attestation mechanisms and secure offloading protocols to enable the establishment of trust relationships and trust calculations in next generation CCAM</b> . This includes the integration of TEE technologies that enable highly secure, trusted, and verifiable remote computing capabilities, which can offer guarantees and assurances for the establishment of trust through the required proofs/claims. Such proofs can provide verifiable evidence on their correctness and functional safety, from their trusted launch and configuration to the runtime attestation of both behavioral and low-level concrete execution properties.
<b>Cryptographic Primitives</b>	In order to guarantee the integrity and confidentiality (where needed) of the data exchanged in the V2X realm, appropriate crypto primitives need to be employed. While there is a wide set of crypto protocols and schemes been defined in the CCAM latest security architecture (based on the use of PKIs), CONNECT envisions to employ the use of Trusted Execution Environments (TEEs) for enabling establishment of hardware-based keys towards the protection of messages exchanged. Appropriate <b>in-vehicle key management and key restriction usage policies</b> will be designed while also the use of advanced attestation schemes (including Direct Anonymous Attestation (DAA)) will be investigated for the construction of verifiable security claims that can disclose those system properties needed for evaluating the Actual Level of Trust (ATL) of a vehicle (or other CCAM actor).
<b>Runtime Tracer</b>	Employs different algorithms to identify OBU system traces efficiently and correctly, towards providing runtime properties that can be used as indicators on the level of trust of the target CCAM actor. This can include configuration integrity tracing and control-flow tracing of CCAM functions running as part of the in-vehicle service landscape.
<b>Misbehavior Detection</b>	Assess the trust level in the nodes (vehicles) concerning their ability of distributing genuine V2X data. This is done based on data sent by all vehicles to the MEC (misbehaviour reports, containing V2X data received by the reporter). The MEC distributes the result of the trust evaluation back to the vehicular layer. The result is the level of trust in the CONNECT Trust Assessment framework.

## 8.2 Open-Source Development Plan

Some of the artefacts that CONNECT is considering for exploitation will be open-source. Since the practice of open-source requires a good understanding of the specific needs and a preparation, CONNECT will undertake work towards: (1) the identification of open-source exploitable artefacts (i.e., Trust Assessment, Attestation Enablers, Crypto Primitives and Misbehaviour Detection), and (2) the implementation of an open-source development plan.



Because open-source development plan requires experience and guidance, CONNECT will use an Open-source Development (OSD) plan template that is being developed in the frame of the OpenContinuum support action. TRIALOG is working on this template with ECLIPSE, so it will be able to provide support to CONNECT. The template (a version of which is put forth in Appendix A) includes:

- Information on stakeholders behind the plan;
- Context information describing the business intention;
- Strategy information (open-source business canvas, licensing, community approach, governance);
- Engagement information (stakeholders, in-bound and outbound activities);
- Project development (environment, development and release approach, support, evaluation);
- Approval and commitment.

The OSD plan is specific to collaborative projects as it makes the difference between activities carried out within the project and those carried out beyond the project (exploitation), currently one or two years after the project. Furthermore, it ensures interactions between partners on the preparation of the plan and its executions, through internal workshops.

The CONNECT OSD was constructed by TRIALOG, and then validated by ECLIPSE in the OpenContinuum project. It assumes a collaboration scheme with OpenContinuum which is described in the figure below (Figure 11), towards the identification the definition an appropriate OSD plan based on the nature of the technical activities of each project. For CONNECT, it is expected that the OpenContinuum project will be able to provide support in the definition of its open-source development plan, according to the timeline shown in Figure 11.

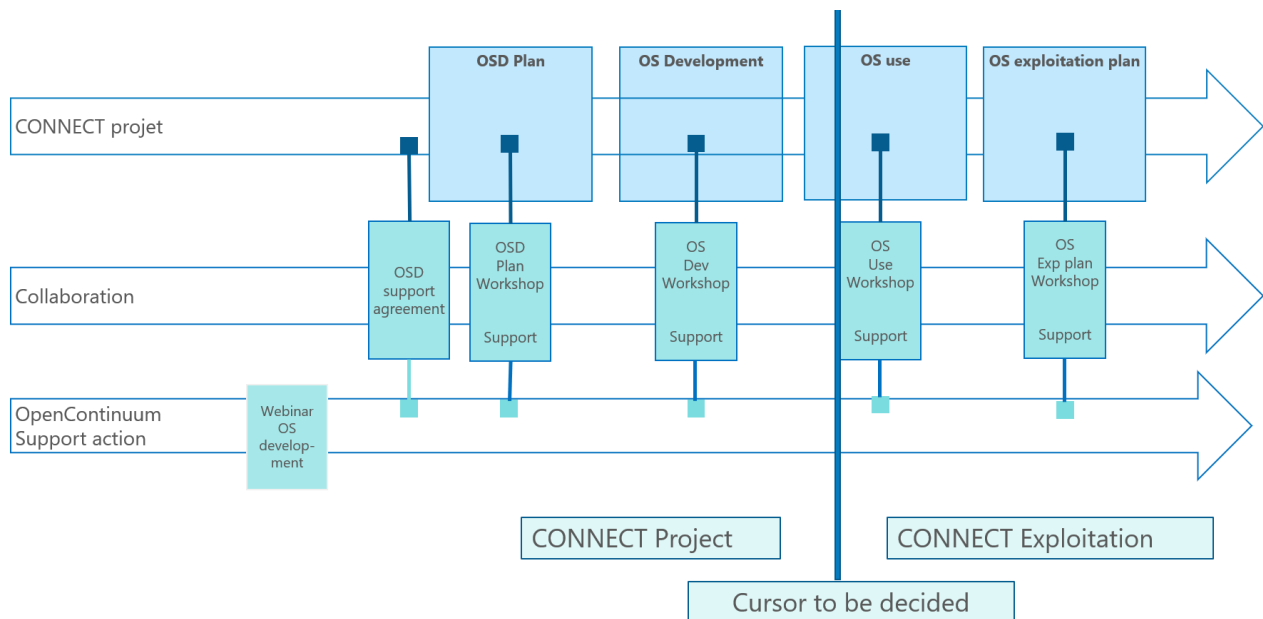


Figure 11: CONNECT Implementation of OSD Plan

The support will consist of:

- ✓ Webinar explaining the questionnaire and the OSD plan template;
- ✓ An agreement for support provided by OpenContinuum;
- ✓ Up to four supporting sessions

The envisioned benefits of this collaboration are the following:

- ✓ **CONNECT:** Good practice and Awareness on potential collaboration with the continuum open source initiatives (e.g. meta OS);
- ✓ **OpenContinuum:** Insight on an OSD plan template that can be used for future European projects and Insight on the CONNECT building block as a potential solution in the continuum.

The OSD template (see Appendix A) collects and reflects on the CONNECT's project (1) Open-source plan info, (2) Context, (3) Strategy including Business, Open-source licensing and IPR, Community approach and Governance, (4) Engagement of stakeholders and activities, (5) Project development encompassing environment, development and release approach, support, and evaluation.

## Chapter 9 Summary and Conclusion

This document provides an initial documentation of the CONNECT communication infrastructure as well as IT-related infrastructure.

First, a presentation of the visual identity of the CONNECT project, including the project logo and project templates, is given. A corporate visual identity expresses the values and ambitions of the CONNECT project and its characteristics. The visual identity provides the project with visibility and "recognisability".

The CONNECT communication kit consists of the project website as the major communication tool, the announcement letter, an overall PowerPoint presentation, giving an overview about the key facts of CONNECT, the project leaflet, as well as social media channels and the CONNECT newsletter.

The website is divided into different sections, which will be updated on a regular basis. It was reviewed by several management and research employees of Technikon and very useful feedback has been received by the partners.

Through publishing all relevant public information of the project on the official CONNECT website, the website will be kept lively, and external visitors will immediately see the current news and activities. Further, this allows more interaction and communication within and outside the CONNECT Consortium. In general, we grant open access to all communication and dissemination materials published on the project website. If in a certain case, other licence requirements have to be taken into consideration, this will be marked accordingly.

The CONNECT communication kit and IT infrastructure provides an essential benefit for all project partners. All project partners are able to access all project relevant information and documents. Further, the communication environment, including the announcement letter and leaflet, the website, social media and the newsletter, but also the different mailing lists, and conference call systems, help to distribute relevant information and create transparent efficient working conditions.

Finally, this deliverable also put forth the details of the exploitation plan that will be further refined in the coming months. The identification of the core exploitable assets was performed, based on the technologies investigated in CONNECT, so as to identify those mechanisms that can be further disseminated and advertised in the community. CONNECT envisions to create an open-source community, hence, most of these assets will be considered as part of the Open-Source Development (OSD) plan that has already been sketched and will further be detailed and validated with the support of ECLIPSE, as the most prominent standards on the creation of International Data Spaces.

## Chapter 10 List of Abbreviations


Abbreviation	Translation
5GAA	5G Automotive Association
ATL	Actual Trust Level
C-V2X	Cellular Vehicle-to-Everything
CMS	Content Management System
DoA	Description of Action
DAA	Direct Anonymous Attestation
ECU	Electronic Control Unit
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standard
HTTPS	Hypertext Transfer Protocol Secure (used for a secure connection between Browser and Web server)
MEC	Mobile Edge Computing
OBU	On-board Unit
OSD	Open Source Development Plan
RTL	Required Trust Level
SDOs	Standards Developments Organizations
SL	Subjective Logic
SSL	Secure Sockets Layer
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TKS	Trusted Knowledge Suite
TPM	Trusted Platform Module







## Chapter 11 References

- [1] 5GAA Automotive Associate, “MEC for Automotive in Multi-Operator Scenarios”, Technical Report, 2012, [Available Online: <https://5gaa.org/mec-for-automotive-in-multi-operator-scenarios/>] “D7.6: Project Impact Assessment.” *The ASSURED Consortium*, July 2022.
- [2] ISO 26262:2018, “Road Vehicles Functional Safety Standards”, 2018, [Available Online: <https://blog.ansi.org/2019/02/iso-26262-2018-road-vehicle-functional-safety/>].
- [3] ISO/SAE 21434:2021, “Road Vehicles – Cyber-Security Engineering”, 2021, [Available Online: <https://www.iso.org/standard/70918.html>].
- [4] WP.29 Cybersecurity and Cybersecurity Management System (CSMS), “UN Regulations on Uniform Provisions Concerning the Approval of Vehicles with regards to Cyber-Security and of their Cyber-Security Management Systems”, 2020, [Available Online: <https://unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>]
- [5] Car 2 Car Communication Consortium, “Guidance for Day 2 and Beyond Roadmap”, 2019, [Available Online: [https://www.car2car.org/fileadmin/documents/General\\_Documents/C2CCC\\_WP\\_2072\\_RoadmapDay2AndBeyond.pdf](https://www.car2car.org/fileadmin/documents/General_Documents/C2CCC_WP_2072_RoadmapDay2AndBeyond.pdf)]
- [6] CCAM Partnership, “CCAM Strategic Research and Innovation Agenda”, 2021, [Available Online: <https://eraportal.sk/wp-content/uploads/2021/12/CCAM-Partnership-SRIA-FINAL-2021.pdf>]
- [7] 5GAA Automotive Association, “Working Item MEC4Auto – Technical Report on Use Cases and Initial Test Specifications Review”, 2020, [Available Online: <https://5gaa.org/mec4auto-use-cases-and-initial-test-specifications-review/>]
- [8] CONNECT Consortium, “Dissemination, Communication, Clustering and exploitation Activities – Initial Version”, February 2024.
- [9] CONNECT Consortium, “Dissemination, Communication, Clustering and exploitation Activities – Initial Version”, September 2025.

## Appendix A OSD Template

1 Open-source plan info		
Authors name and e-mail	<i>CONNECT persons in charge of providing and maintaining the plan. Can involve different partners.</i>	
History	<i>The open-source plan can be updated several times, depending on how the status of its execution. Examples are:</i> <ul style="list-style-type: none"> <li>- <i>Change of strategy (e.g., modification of KER objective, merging with another KER)</i></li> <li>- <i>Change in licencing approach</i></li> <li>- <i>Change in community approach</i></li> <li>- <i>Change in infrastructure use (e.g. Gitlab to Github)</i></li> </ul>	
	Date	
	Version	
	Description of modification	
Confidentiality	<i>You may wish to have up to three versions of the plan:</i> <ul style="list-style-type: none"> <li>- <i>Confidential at partner level (not provided to consortium) – However experience shows that it does not run</i></li> <li>- <i>Confidential at consortium and EC level (needed for deliverable)</i></li> <li>- <i>Public (needed for engagement)</i></li> </ul>	

2 Context	
Initial Key exploitation result name	<i>Mention if you have modified your plans with respect to the grant agreement.</i>
Initial description	<i>Mention if you have modified your plans with respect to the grant agreement</i>
Key exploitation result name	
Description	<i>Provide a rationale for the change if you have modified your plans</i>
Category of building block	 <i>How do you position your key exploitation results with respect to the 12 building blocks (OpenDei design principles for data spaces?)</i>

3	Strategy	
3.1	Business	
Open source canvas	<p><i>Option 1: Major open-source initiative</i> Provide a first version of the open-source canvas. <a href="https://opensource.com/article/16/12/open-source-canvas">https://opensource.com/article/16/12/open-source-canvas</a></p>  <p><i>The other options are identified by ECLIPSE</i></p> <p><i>Option 2: Leveraged service business model</i></p>  <p><i>Option 3: Technology specialist</i></p>  <p><i>Option 4 Open source foundation</i></p>  <p><i>Option 5 Co-creation of open-source extendible platforms</i></p>  <p><i>Option 6 e-Pure service business model</i></p> 	
Assessment within project	Describe tasks to be carried out on business within the project	
Assessment beyond project	Describe tasks that will be carried out on business beyond the project, make recommendations for a roadmap	
3.2	Open-source licensing and IPR	
Current licensing and IPR status	<p>Explain the current status (e.g., the selected licensing plan) and the dependencies. See <a href="https://opensource.org/licenses">https://opensource.org/licenses</a></p> <p>Describe decisions to be made on licensing and IPR within the project</p>	
Analysis	Provide an analysis of how you plan to enforce business-friendly licenses	
Decisions within project	Describe decisions to be made on licensing and IPR within the project, justify when you do not select a well-accepted licensing scheme	
Decisions beyond project	Describe decisions to be made on licensing and IPR beyond the project, justify when you do not select a well-accepted licensing scheme	
3.3	Community approach	
Community	<p>Assess the intended community approach. Some references (<a href="https://opensource.org/community">https://opensource.org/community</a>, <a href="https://en.wikiversity.org/wiki/Open_community_approach">https://en.wikiversity.org/wiki/Open_community_approach</a>, <a href="https://www.linuxfoundation.org/resources/open-source-guides/participating-in-open-source-communities">https://www.linuxfoundation.org/resources/open-source-guides/participating-in-open-source-communities</a>, <a href="https://www.eclipse.org/collaborations/">https://www.eclipse.org/collaborations/</a>)</p>	

	<p><i>Example of community:</i></p> <ul style="list-style-type: none"> <li>- Governance: single organisation, Development: single organisation</li> <li>- Governance: single organisation, Development: community</li> <li>- Governance: open-source organisation, Development: community</li> </ul>	
	Current status of KER	TRL
		Community
	Intended status at the end of project	TRL
		Community
Intended status beyond project	TRL	
	Community	
Decisions within project	Describe decisions to be made on community approach within the project	
Decisions beyond project	Describe decisions to be made on community approach beyond the project	
<b>3.4</b>	<b>Governance</b>	
Governance	Select the agreed open-source governance approach (see <a href="https://opensource.com/article/20/5/open-source-governance">https://opensource.com/article/20/5/open-source-governance</a> )	
Decisions within project	Describe decisions to be made on community approach within the project	
Decisions beyond project	Describe decisions to be made on community approach beyond the project	

<b>4</b>	<b>Engagement</b>	
<b>4.1</b>	<b>Stakeholders</b>	
Developers	Current team	List developers and their roles . Is the team involving several partners?
	Team evolution during project	Explain if the team will evolve during project



	Team evolution beyond project	<i>Explain if the team will expand externally beyond the project, and how engagement will take place</i>
Users	Intended users	<i>List users (pilots) and their needs</i>
	External users during project	<i>Explain if there will be external users during project, and how they will be engaged</i>
Other stakeholders	<i>List potential stakeholders that can have an interest to the project and need to be engaged</i> <ul style="list-style-type: none"> <li>- Other open-source communities</li> <li>- Platform / data space stakeholders</li> <li>- Domain specific stakeholders (Consumers, local communities, data energy cooperatives)</li> <li>- Energy and non-energy business stakeholders (finance, healthcare, water, mobility, etc.)</li> <li>- Regulated operators</li> <li>- Standardisation bodies</li> </ul>	
4.2	Activities	
Activities within project	<i>Inbound activities: liaison with other projects (through Int-Net, DSCC, OpenContinuum, and other Horizon projects), presentation to data space events (IoT, BDVA, BRIDGE, ...), conferences, blogs, ...</i> <i>Outbound activities: if any</i>	
Activities beyond project	<i>Inbound activities</i> <i>Outbound activities</i>	

5	Project development	
5.1	Environment	
Platform	<i>List platforms and dependencies on other products or components</i>	
Development environment	<i>Explain development environment used to develop open-source project (e.g. Yocto)</i>	
Decisions during project	<i>Describe decisions to be made on environment during project</i>	

Decisions beyond project	<i>Describe decisions to be made on environment beyond project</i>
<b>5.2</b>	<b>Development and release approach</b>
Development lifecycle	<i>Explain lifecycle approach (development, verification et validation) and approach (e.g. DevOps) including tools to be used</i>
Development lifecycle security assurance	<i>Explain measures for development lifecycle security assurance</i>
Release building approach	<i>Explain approach including tools to be used</i>
Decisions during project	<i>Describe decisions to be made on development and release during project</i>
Decisions beyond project	<i>Describe decisions to be made on development and release beyond project</i>
<b>5.3</b>	<b>Support</b>
Pilots involved	
Contact points pilot	
Contact points KER	
Training material	
Training schedule	
<b>5.4</b>	<b>Evaluation</b>
Schedule	<i>Provide schedule for questionnaire to pilots, questionnaire to developers and evaluation report</i>

6 Evaluation and approval of plan	
Project manager name	
Approval date	
Exploitation manager name	
Approval date	