E-CORRIDOR
Edge Enabled Privacy & Security Platform For Multi Modal Transport

D10.3

Progress Report Y1

WP10 Management

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multimodal Transport

Due date of deliverable: 30/05/2021

Actual submission date: 26/10/2021

26/09/2021

Version 1.2

Responsible partner: CNR

Editor: Fabio Martinelli (CNR)

E-mail address: fabio.martinelli@iit.cnr.it

Project co-funded by the European Union within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	**X**
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883135.

Authors: Fabio Martinelli (CNR), ALL WP leaders

Revision History

Version	Date	Name	Description
0.1	31/05/2021	Fabio Martinelli (CNR)	Table of Content (TOC)
1.0	22/06/2021	All WP leaders /and several partners contributed	Content
1.2	25/10/2021	All WP leaders /and several partners contributed	Revision for the comments: - Added for the events a column on feedbacks on the event table; - Finalized the effort/cost tables with all the requested info - Added a section on realized risks (in WP1) - Elaborated on the TRL at the end of the project in section 2.3 - Elaborated some countermeasures for partners not reporting on time financial information

Executive Summary

This document represents the technical periodic report for the 1st period of E-CORRIDOR (01/06/2020 – 31/05/2021)

Table of Contents

List of Figures

List of Tables

1. Explanation of the work carried out by the beneficiaries and Overview of the progress

1.1 Objectives and results

1.1.1 Objectives

E-CORRIDOR plans to develop a collaborative privacy aware and edge enabled information sharing, analysis and protection framework for cyber security in multimodal transport systems.

In this framework, often entities (either travellers or transport means) can be seen as *information prosumers*, i.e. producers and consumer of information. Information could be raw data as well as complex attack indicators that we may wish to share to enhance our security and safety or just to get a better service.

The sharing of the information is usually regulated by Data Sharing Agreements (DSAs) that can be used to express privacy preferences or contractual requirements for providing and consuming information (i.e. notification of data leakage). Often the information can be analysed either globally (in the cloud) or locally (in edge devices). Local analysis will increase privacy although global (with more information) could be more accurate. Our framework has the following key components:

- **Information sharing**: share information (including security ones) in a controlled manner, ensuring the respect of regulation and with confidentiality and integrity both in rest and in transit;
- **Information analytics**: advanced analytics functions and engines for data analytics and correlation identifying threats that hide themselves in the massive usage of services and related amount of logs
- **Mixture of technologies** to enable confidential and collaborative analysis of data: including homomorphic encryption: making computation in a confidential and distributed manner;
- **Advanced seamless access** mechanisms that that advantage of the analytics and sharing infrastructure to provide continuous authentication and authorization as well as privacy aware service as privacy aware data usage control.

E-CORRIDOR is pilot-driven and its main features have been designed to successfully cope with the pilots we identified in project proposal preparation.

The framework assumes federations of information *prosumers* aiming at sharing information to improve their cyber protections capabilities.

E-CORRIDOR will achieve the following objectives:

Objective 1: *E-CORRIDOR will build a flexible, confidential and privacy-preserving framework for managing **data sharing**, for several purposes, by different prosumers:*

The framework will allow a quick and effective deployment of contractual agreements among companies/entities that provide and consume data. This will be done in a confidential and privacy-preserving way, in respect of both the company data policies and the current legislation requirements on data privacy (i.e., the European data protection directive 95/46/EC and the forthcoming modifications). The framework will enforce continuous data usage control on data and data protection through encryption (in rest and transit).

Objective 2: *E-CORRIDOR will define edge enabled **data analytics and prediction** services in a collaborative, distributed and confidential way:*

The overall platform will offer data analytics as a service, in a confidential and collaborative way. Several technologies will be adopted for developing this data analytics service, also depending on the trust level the prosumers assume in the services, i.e. either trusted or not. The most appropriate data protection and analysis mechanisms will be implemented to trade-off

between several parameters, e.g. as privacy vs accuracy of the analysis. The framework will be efficient and secure and it will be an open platform with openAPI for easily integration and adoption of E-CORRIDOR framework.

Objective 3: *E-CORRIDOR will define a **secure and robust** platform in **holistic manner** to keep the communication platform safe from cyber-attacks and ensure service continuity:*

The growth in the Internet of Things and the increase in connected devices used by transportation operators in expanding networks will only increase the number of vulnerable points for unauthorized access. The E-CORRIDOR platform will offer a look at cyber-security in a holistic manner by addressing not only internet-connected systems, but also the "human element" factors by taking into account the fact that malicious passenger can easily provoke a physical cyber-attack from IoT devices equipped in the connected means of transport.

Objective 4: *E-CORRIDOR will improve, **mature** and **integrate** several existing tools provided by E-CORRIDOR partners and will tailor those to the specific needs of the E-CORRIDOR platform and Pilots:*

In particular, E-CORRIDOR considers tools for data analytics for security (including log and behavioural analysis), usage of homomorphic computing for selected data analytics functions, anonymization techniques for data sanitization, visualization tools for data analytics as well as managed security services.

Objective 5: *E-CORRIDOR will provide mechanisms for **seamless access** to multimodal transport.*

In particular, E-CORRIDOR considers seamless access to multimodal transport as a key ingredient of the project. It will have continuous authentication and privacy aware mechanisms. It will allow privacy aware authentication and authorization services.

Objective 6: *the framework and the services developed will be used to deliver three **pilot products** for:*

1. Centre of information sharing for multimodal transport (ISAC);
2. Airport and integrated train transport (AT);
3. Car sharing in smart cities (S2C);

These Pilots have been carefully chosen to show the variety of possible applications of the framework, considering relevance and coverage of the public/private sectors in the field of information sharing for cyber protection.

Objective 7: *E-CORRIDOR will be promoted and ease the **exploitation, communication, standardization, dissemination and early adoption** of its results.*

E-CORRIDOR partners are fully committed to maximize the impact of their innovation activities, in particular exploitation and commercialization. Specific attention has been devoted in consortium preparation, involving leading industry partners and end-users associations. Through an extensive advisory board (made of several associations in the transport and cyber security sectors) we plan to maximize the impact.

Success criteria: This objective will be realised through the deliverables of WP 9. Full achievement of the objective will require the achievements of the KPI for communication as well as for the proper implementation of the exploitation, communication, standardization and communication plans.

1.1.2 First year results.

All the planned milestones have been achieved and these are the main results in the first year:

- All the management activities have been carried out, including financial distribution. More than 6 plenary project (virtual) meetings were organized by the partners;
- All the requirements from the pilots have been collected and elaborated;
- The main E-CORRIDOR architectural features have been defined using the previous requirements;
- All the pilots have their own architecture and embed the E-CORRIDOR main architectural components;
- Several publications were produced in the topics of the project;
- Several stakeholders has been contacted and initial exploitation plans defined.

1.2 Explanation of the work carried per WP

1.2.1 WP1 Ethics

All the ethics deliverables has been provided and the ethics advisor appointed.

1.2.2 WP2 Airport and Train (AT) Pilot

Leading partner: ADP

Start month: 1, **End month**: 36

Participant partners: ADP, UTRC, SNCF, PEC, FhG, HPE, CEA

This WP is devoted to the implementation of the airport and train pilot. Its two main objectives are: (i) requirement identification and deployment of the AT pilot, (ii) validation of the E-CORRIDOR core framework through its instantiation in a running pilot system. The WP is composed by three Tasks, two of which are related to this reporting period and their progresses are detailed in the following.

The main results achieved in WP2 in this reporting period, with the active contribution of all the participant partners, are:

- Milestone 1 (M1) “Elicitation of E-CORRIDOR requirements”
- Submission of D2.1 “Requirements for the AT Pilot”
- Submission of D2.2 “Design and Architecture for the AT pilot”
- Contribution to M2 with a first version of the AT pilot instantiation of the E-CORRIDOR architecture

All the results have been achieved on time in accordance to the DoA with a collective efforts of the WP partners and with interactions with other WPs, in particular with the WP3 ISAC pilot for some security aspects, WP5 and WP6 for the E-CORRIDOR core framework and WP7 and WP8 for the analytics and advanced security services.

The WPs activities are organized through recurring bi-weekly meetings (plus additional ones when needed for finalizing the deliverables) whose meeting minutes are archived in the internal project repository.

1.2.2.1 Task 2.1 Airport and Train Pilot Requirements (M1-M6)

This task was focused on the collection of functional and non-functional requirements, whose input contributed to the definition of the E-CORRIDOR platform requirements. In particular, as leader of the Task 5.1 "requirements for E-CORRIDOR platform", HPE provided templates, guidelines and suggestions for gathering the requirements expressed by the expert of the airport domain ADP. UTRC contributed to the requirement collection through interactions with the sister company Collins Aerospace. By actively participating to the bi-weekly web calls organized by ADP, all the technical partners in the project (UTRC, PEC, CEA, FhG, HPE) contributed to the requirement elicitation process. In particular, the collective effort of FhG and CEA mainly focused on the requirements of the security solutions, UTRC and PEC on the identification and authentication solutions, and HPE considered the point of view of the E-CORRIDOR platform by coordinating the collection requirements activities of all the three project pilots.

Deliverable D2.1 reporting on the outcome of Task 2.1 was submitted at the end of M6 as planned.

1.2.2.2 Task 2.2 Pilot Design and Integration (M6-M34)

This task is focused on design and implementation of the AT pilot architecture and set the basis for performing implementation, integration and subsequent validation of the E-CORRIDOR framework instantiated in the AT pilot. As this reporting period covers the first six months of execution of the T2.2, the effort has been mainly devoted to the design of the AT pilot architecture. ADP has led the design work by exploiting the requirement collection effort performed in T2.1 and through the continuous exchange of feedback with the parallel activities carried out by all the partners involved in WP5 on the definition of the platform architecture. To fulfil all the requirements expressed in Task 2.1, the features of the E-CORRIDOR core framework, the analytics and security components and their customizations have been identified thanks to the joint effort of FhG (on the security aspects), and UTRC and PEC (respectively on the identification, authentication and contextual analysis). Data, security and deployment models have been considered during the architecture design. Moreover, some interactions with the ISAC pilot (WP4) have been used to cope with the requirements on the sharing of threat information.

Deliverable D2.2 reporting on the first results of T2.2 was submitted on time at the end of M12.

1.2.2.3 Deviation from DoA

No technical deviation from the DoA to report.

1.2.3 WP3 Car Sharing Pilot (S2C)

Leading partner: CLEM'

Start month: 1**, End month:** 36

Participant partners: CLEM', HPE, CEA, PLD, FhG, WIT, FC, AMTU

The Car Sharing Pilot represents the application of E-CORRIDOR framework and the added-value that secure data-sharing brings to multimodal transportation. The objectives are identifying the requirements of the S2C Pilot and the integration and validation of E-CORRIDOR framework and the eWallet. Also, the integration of the S2C Pilot with the analytics services and the security infrastructure through the framework.

Overall,

- Milestone MS1 was achieved thanks to the participation of all E-CORRIDOR partners, especially the pilots. The work towards MS3 (Setup of running pilots) is in progress.
- Deliverables D3.1 Requirements for the S2C Pilot and D3.2 Design and Architecture for the S2C Pilot were submitted.

Results were achieved in accordance with the DoA.

1.2.3.1 Task 3.1 S2C Pilot requirements (M1-M6)

This task is about identifying the Pilot stakeholders, understanding their needs, and eliciting the requirements. The D3.1 deliverable is the report of the requirements of the Pilot.

During the period covering the 3 first months, a description of the pilot and the roles of the partners during the kick-off meeting was presented, and recurrent WP3 meetings were planned and fixed.

The partners bringing their expertise from different fields and perspectives shared their understanding of the needs of the listed stakeholders and their needs and how the E-CORRIDOR framework could solve their problems.

CEA Participated at gathering the requirements for this pilot. In particular, the requirements were collected through the definition of user-stories and the use-cases.

HPE As driver of the Task 5.1 “Requirements for E-Corridor Platform”, collecting input from the three Pilots, HPE has been following the activities of T3.1 giving templates and suggestion on how to fill up specific sections due for D5.1

HPE presented and provided the table of contents and guidelines for writing and presenting the requirements in the deliverable documents, so all E-CORRIDOR partners communicate and write in a more standardized way.

FACTUAL was in charge of the requirements definition for the microsubsidies use case and made contributions to D3.1.

FhG has joined the bi-weekly conference calls to jointly develop requirements with the respective partners for the security solutions of tasks T7.5 and T8.5 and contributed to the according deliverable D3.1.

Meetings and exchanges between partners within the WP3 and other exchanges with WP7 and WP8 leaders to establish a clearer understanding of the interactions resulting of their objectives.

A brainstorming for ideas of other ways for demonstrating the value of E-CORRIDOR within our work package especially leveraging the analytics services and security infrastructure of E-CORRIDOR.

The preparation of the D3.1 report took the following steps:

- WP3 partners clarified objectives in term of what is needed as High-level functions and started defining the workflows and the needed data sharing. Exchanges that result in a progress in the writing of the draft of the requirements (the first deliverable)

- Definition of the requirements for the Pilot and the use cases:
- Discussions with the WP3 partners about the functioning of the data sharing workflow and the usage of the data.
- Discussions between WP3 and WP5 WP7 WP8 WP6 for the integration of different WPs' use cases and WP3 use cases and the WP3 generated/shared data.
- Definitions of user stories use cases and their acceptance tests.
- Elaboration and submittal of the first deliverable.

1.2.3.2 Task 3.2 S2C Pilot Design and Integration (M6-M34)

This task spans over 28 months, representing the design, development, maturation, and integration of the Pilot. Therefore, it has 4 relevant milestones MS3, MS4, MS5 and MS6. From the first setup of the running pilots to the final version of the integrated infrastructure of the pilots. During this task, two deliverables are expected, D3.2 Design and Architecture for the S2C Pilot and D3.3 First implementation, test, and validation of the pilot. The first is a report and the second is an architecture with a running pilot.

Being in M12 now, the D3.2 was submitted on time. Some demonstrations of Pilot functions are being developed as a first step towards the setup of the running pilots Milestone.

Definitions of Pilot specific DSAs using the CNL, presenting the current functioning of the different partners' systems to understand our current internal architectures and the available data and its format related to the Project. Defining the basis on which we will define the Pilot architecture and components. Defining the workflows and underlying the first drafts of the architecture.

During the period, the following tasks were done:

• Brainstorming and devising a strategy for using the E-CORRIDOR framework and components for fulfilling the Pilot's multimodality requirements.

• Definition of the eWallet concept and architecture, as well as listing the features to be demonstrated in the pilot and the interactions in a global scenario from the point of view of the traveler.

• Design of the high-level architecture, synchronizing the work, the terminology, the color code, and the graph formats. With WP5 and the other partners.

• Study of the different authentication mechanisms and their scalability and potential for the eWallet. More In-depth discussions about the functioning of the eWallet

• Study of the authorization mechanisms of the DSA Lifecycle Infrastructure and their integration with the eWallet and the other components of the pilot.

• Design of the components using FMC Modeling language's Block diagrams, definition of the workflows of the features and their concerned components.

• Study of the security model: Reflection about the cyberthreats to the pilot, the E-CORRIDOR Framework and the eWallet's security model to mitigate these risks,

• Study and choice of the most convenient deployment model for the pilot.

• Definition of the analytics workflows (Multi-modal micro-subsidies and the privacy-preserving interest-based sharing).

• Preparation of the requirements for the integration of partner's information systems and E-CORRIDOR framework's components.

- First elaboration of the FHEncryption use-case (privacy-preserving interest-based sharing) : API development and development server's deployment.
- Preparation and submittal of the second deliverable.
- Internal reviews of deliverables.
- Preparation for the review meeting.
- Preparation of the demos.

FhG being involved with the eWallet authentication mechanism contributed significantly to this task:

- FhG has joined the bi-weekly conference calls to jointly develop requirements with the respective partners for the security solutions of tasks T7.5 and T8.5.
- FhG has contributed a concept for instantiation of the Trusted Service Manager component to secure the eWallet sharing. It secures the communication between eWallet platform and service providers and protects the contents of the eWallet against unauthorized access.
- FhG's input has been contributed to the according deliverable D3.2.
- From FhG's point of view, all objectives could be accomplished
- From FhG's point of view, no deviations from Annex 1 occurred.
- From FhG's point of view, no deviations from planned resources occurred.
- From FhG's point of view, no corrective actions are required.

1.2.3.3 Deviation from DoA

There is no technical deviations from DoA to report.

1.2.4 WP4 Information Sharing and Analytics Centre Pilot (ISAC)

The first objective of the WP4 is to produce a prototype of an Information Sharing and Analytic Center integrating E-CORRIDOR technology to allow controlled sharing/pooling of security data belonging to different prosumers.

In the first period of the project have been successful completed the objectives related to the following task 4.1 (ISAC Pilot Requirements) and the design and architecture part of task 4.2 (Design and Architecture for the ISAC Pilot). The details of the two tasks are reported in the following:

1.2.4.1 Task 4.1: ISAC Pilot Requirements

Within task 4.1, MISE, CNR, DIG, CEA, and FhG collaborated on the definition of the pilot requirements by identifying the main stakeholders, defining the use cases, and identifying the functional and non-functional requirements that the system has to present to collect, share, analyze and dispatch the information.

MISE played the role of coordination of the WP. CNR handled the biweekly calls, the definition of the requirements and use cases, and the deliverable editing.

CEA has collaborated to define the ISAC cybersecurity notification service as pilot-specific analytic during the requirements definition.

During the use case definition phase, DIG organized a meeting with the Italian National Railway stakeholder to define an additional use case for the railway sector.

FhG has joined the bi-weekly conference calls to jointly develop requirements with the respective partners for the security solutions of tasks T7.5 and T8.5.

1.2.4.2 Task 4.2: ISAC Pilot Design and Integration

Within the WP4 task 4.2, MISE, CNR, HPE, FhG collaborated to define the pilot's architecture. To this end have been defined the architecture components to collect, analyze and dispatch cyber-threat information and the pilot-specific analytics. Finally, with the collaboration of AT and S2C pilot have been defined information to share with the ISAC pilot to increase the knowledge on cyber-threat.

HPE has been involved in the definition of the structure of the ISAC architecture.

FhG has evaluated various message formats for intrusion information sharing on their suitability for the information sharing and analytics component and integrated the STIX (Structured Threat Information eXpression) format with existing IDS solutions.

MISE played the role of coordination of the WP. CNR handled the biweekly calls, the definition of the architecture, and the editing of the deliverable.

1.2.4.3 Deviation from DoA

There is no technical deviations from DoA to report.

1.2.5 WP5 E-CORRIDOR platform: Requirements / Architecture / Implementation and integration

Leading partner: HPE

Start month: 1, **End month**: 36

Participant partners: HPE, CNR, MISE, ADP, PLD, UTRC, FhG, WIT, DIG

This work package has several goals related to the definition of the E-CORRIDOR platform, starting from the collection of the requirements, to the definition of the architecture, to its overall coordination via the implementation and integration efforts.

The requirements were collected from the Pilots WP2-WP4, which helped to achieve a consistent set of needs to proceed with a pilot-driven definition of the E-CORRIDOR reference

architecture. In fact we initially delivered the set of requirements that assisted the design of the first version of the E-CORRIDOR architecture (M12) with the definition of its major subsystems and components. The Information Sharing Infrastructure (ISI) is used to deliver the data sharing capabilities regulated by policy rules that we call Data Sharing Agreements (DSAs). The DSA Lifecycle Infrastructure is the subsystem aimed at providing the "instruments" to create such DSA rules in an easy and effective way, in particular through the DSA Editor component. The Information Analytics Infrastructure (IAI) outlines the mechanisms we provide to express data analytics capabilities over the collected data by the ISI subsystem; the IAI provides a plug-in based way to develop analytics services that can obey to the DSA rules, including those services defined in WP7. The Advanced Security Infrastructure (ASI) provides a set of complex services that leverages the capabilities defined in particular by the ISI and IAI subsystem, as discussed in the activities of WP8. Finally a set of Common Security Services (CSI) define cross-subsystems security capabilities (like Identity Management) that permit to concentrate of the core of the E-CORRIDOR framework services while at the same time leverage off-the-shelf components present at the enterprise.

1.2.5.1 Task 5.1 Requirements for E-CORRIDOR platform

The first 6 months of the reporting period (M1-M6) have been spent to collect the requirements in Task 5.1. It was a joint collaboration with the pilots' work packages (WP2, WP3, and WP4) that were also assisted by WP5 team members in order to deliver a consistent set of needs and deliverables to feed the WP5 activities. It was a challenge, considering that pilots' work packages were expected to deliver at M6 as it was for Task 5.1. This required to work in parallel between pilots' WPs and WP5 with a strong discipline to arrive at M6 with the output of activities that resulted in D5.1.

D5.1 is a pilot-driven deliverable, which includes the list of requirements and its mapping to each pilot, with the purpose to achieve an overall consistent set of needs to model the E-CORRIDOR architecture (i.e., Task 5.2).

WP5 also took time to outline the definition of the setup of the Development, Testing and Integration, and Production environments where the E-CORRIDOR implementation will be conducted.

1.2.5.2 Task 5.2 E-CORRIDOR platform architecture

Task 5.2 was a joint collaboration amongst all the consortium partners participating to WP5. The result at M12 was deliverable D5.2 that provides the first version of the E-CORRIDOR architecture that will be implemented to address the pilots' needs. In addition to defining the E-CORRIDOR subsystems (briefly discussed at the beginning of this WP5 chapter), we also defined how these subsystems can be accommodated in different "deployment models" to address the different pilots scenarios and partners' needs, i.e. from the edge to the cloud.

1.2.5.3 Task 5.3 E-CORRIDOR Platform vulnerability protection measures

E-CORRIDOR framework has been designed with great care of its internal security characteristics and capabilities. Focusing on the secure data exchange, Task 5.3 supported the discussion on how to create a secure data container (we called Data Bundle) that provides anti-tampering features like digital signature (for integrity) and encryption (for confidentiality). Also the DSA rules allow defining access and usage control to further protect not only the

information sharing, but also how such information can be used when we need to perform data analytics over it (i.e., control over data analytics execution).

1.2.5.4 Task 5.4 E-CORRIDOR platform implementation, integration and test bed

Even if activities till M12 were mostly related to E-CORRIDOR framework definition and design, we started to develop Task 5.4 related to the definition of the environments where the E-CORRIDOR platform will be implemented. As reported in D5.2, we setup a bunch of tools to support the continuous integration and deployment chain, and be ready to start for the next development activities that will result in the implementation of the first version of the E-CORRIDOR platform and test bed.

1.2.5.5 Task 5.5 Exploiting synergies among the Pilots and easing the integration of the Platform within the Pilots

In Task 5.5 we strongly support the collaboration with the pilots to decline or instantiate the conceived E-CORRIDOR architecture in each pilots' scenario and modelled the framework to address their necessities. That is why in D5.2 we also worked on described how the 3 pilots can use the E-CORRIDOR subsystems in what we called as "deployment models".

1.2.5.6 Deviation from DoA

No technical deviation from DoA.

1.2.6 WP6 Information Sharing and analytics infrastructures

Leading partner: CNR

Start month: 1, **End month**: 34

Participant partners: CNR, HPE, CEA, FHG

The main goal of WP6 is the definition and the development of the technologies that will be used in the E-CORRIDOR framework for supporting the privacy preserving sharing of information among users and the execution of collaborative analytics on such information. These functionalities will be provided by two distinct subsystems of the E-CORRIDOR framework that will be the output of this WP: the Information Sharing Infrastructure (ISI) and the Information Analytics Infrastructure (IAI). The ISI regulates the data sharing among different parties enforcing the usage control policies paired with such data, called Data Sharing Agreements (DSA), in order to protect data privacy. The IAI allows E-CORRIDOR users to execute data analytics functions exploiting the data shared through the ISI, obeying to the sharing and analytics constraints expressed in the DSAs paired with such data. Moreover, this WP also involves the design and development of a third subsystem, called DSA Lifecycle Infrastructure (DLI), which manages the life cycle of DSAs, from their creation to their deletion. The aforementioned subsystems are designed starting from the results of the C3ISP project (H2020-DS-2015-1, Collaborative and Confidential Information Sharing and Analysis for Cyber Protection, C3ISP, GA#700294).

The first activity we conducted in WP6, involving all the Tasks of the WP, concerns the analysis of the E-CORRIDOR reference scenario and of the use cases defined by the pilots in order to understand the maturation that is required to the architecture proposed in C3ISP to support the E-CORRIDOR data sharing and collaborative analytics model and pilots. A relevant input we used to perform this analysis are the requirements for the E-CORRIDOR platform collected from the pilots in WP5. Moreover, WP6 interacted with the WPs of the pilots (i.e., WP2, WP3, and WP4), mainly during the bi-weekly WP6 conference calls, in order to study more in details their security and privacy requirements. As result, we identified a number of reference DSAs for each pilot, i.e., the security and privacy policies that the pilots would like to enforce on the data that are shared in their scenarios. More in details, we identified the attributes that will be used by the Pilots to describe the features subjects, the data and the execution environment, and the preliminary operations that must be executed on the data before they are shared to perform the collaborative analytics, called Data Manipulation Operations (DMO), e.g., anonymization operations.

Exploiting the E-CORRIDOR platform requirements and the feedbacks collected from the pilots we were able to identify a number of modifications to the language used for expressing DSAs, in order to enable it to write the security and privacy policies to be used in the pilots' use cases, and we re-designed the internal architectures of the three subsystems, ISI, IAI, and DLI, starting from the initial C3ISP design.

The work conducted in the reference period within WP6 has been described in deliverable D6.1 "Sharing and Analytics Infrastructure and Architecture", due at M12, which has been delivered on time.

1.2.6.1 Task 6.1 Data Sharing Agreement Infrastructure

This task is devoted to the definition of the format of the DSAs, the security and privacy policies that protect shared data, and of the infrastructure which manages its lifecycle, from its creation (through a graphical user interface called DSA editor) to its deletion or expiration.
In the reference period, exploiting the requirements for the E-CORRIDOR platform collected from the pilots described in D5.1, as well as the additional information and the reference DSAs resulting from the discussions held during the bi-weekly WP6 conference calls, we were able to identify the required modification to the DSA format. In particular, we identified a number of attributes that will be used in the DSAs to describe the features of subjects, of data and of the execution environment, and a number of operations that the Pilots want to specify in their DSAs to executed on the data to prepare them to be used in collaborative analytics (for instance, the anonymization of the email addresses present in the data). Consequently, we modified the DSA vocabulary in order to integrate the new terms required to express the reference DSAs, and we modify the graphical user interface of the DSA editor accordingly, as well as the DSA mapper, which is the component which translated human-readable DSAs into machine-enforceable ones.

1.2.6.2 Task 6.2 Data Collection and Enforcement

The data collection and usage enforcement functionalities of the E-CORRIDOR framework are implemented by the ISI subsystem. This component implements the confidential and privacy preserving data sharing by providing a flexible secure storage system along with the enforcement of the DSAs when data are used to perform analytics.

In the reference period, we exploited the requirements described in D5.1 for the E-CORRIDOR platform, and we discussed with the Pilots owners during the bi-weekly WP6 conference calls to re-design the architecture of this component to support the execution of the E-CORRIDOR use cases. With respect to the C3ISP platform, which was aimed at analysing Cyber Threat Information only, the E-CORRIDOR one aims at sharing and analysing any kind of data (also enabling analytics at the edge). As a matter of fact, the E-CORRIDOR pilots are focussed on multimodal transportation, and they take into account a very wide set of distinct data types. This required to introduction in the ISI architecture of the Obligation and DMO toolboxes, which are two components that can be easily configured to integrate any kind of obligations and DMOs, respectively, in order to satisfy the needs of all the E-CORRIDOR pilots.

1.2.6.3 Task 6.3 Analytics Infrastructure

The Information Analytics Infrastructure (IAI) is meant to support the execution of collaborative analytics on the data managed by the ISI.

In the reference period, from the analysis of the requirements described in D5.1 for the E-CORRIDOR platform, and from the discussion with the Pilots owners during the bi-weekly WP6 conference calls, we understood that a large (and possibly growing) number of different analytics are required by the E-CORRIDOR pilots. Hence, the IAI architecture has been maturated with respect to the C3ISP one by introducing the Analytics Toolbox, which is the component devoted to the execution of the analytics function, where new analytics can be easily integrated without disrupting the original IAI architecture. Moreover, since we found out that the E-CORRIDOR scenario also involves analytics that are implemented as composition of other analytics, the IAI architecture has been further maturated by introducing another component, the Analytics Orchestrator, which aims at managing the execution of composition of analytics.

1.2.6.4 Deviation from DoA

There is no deviation from DoA to report.

1.2.7 WP7 Data analytics techniques

Leading partner: UTRC

Start month: 1, **End month**: 34

Participant partners: UTRC, PEC, CEA, WIT, FhG, CNR

The main goal of WP7 is the design, development and maturation of the data analytics techniques part of the analytics toolbox of the Information Analytics Infrastructure (IAI). The components integrated in the toolbox encompass user identification, itinerary planning, privacy preserving security analytics, estimation of the carbon footprint consumption and intrusion detection technologies. The expected maturation efforts are oriented at improving the state of the art solutions and technologies with respect to accuracy, efficiency, privacy and ability to run on the edge.

As a complementary action to WP5 that has collected the requirements for the E-CORRIDOR platform from the pilots, and the pilot efforts (in WP2, WP3, and WP4), the WP7 activities (aligned with WP8) have matched the tasks in the analytics with the pilot use cases. The experience of the WP7 partners generated discussions on the potentiality of some analytics bringing interest to the pilots that have made some of the idea their own for the definition of the use cases. Also, important synergies among tasks within WP7 and with WP8 have been identified to satisfy some of the pilot requirements e.g., the orchestration of multiple components able to define advanced security services was required. The following activities will focus on the development of the components and their integration in the platform.

WP7 is composed by five Tasks, all of which are started at M1. In this reporting period, all the participant partners have focused their effort mainly on identifying requirements and designing the architecture for the proposed components.

- Contribution to M1 and M2 with the requirements of the analytics components
- Submission of D7.1 "Data Analytics techniques requirements and architecture"

A joint effort of all the WP partners allowed a timely achievement of the panned goals for the corresponding period.

Recurring bi-weekly meetings jointly held with WP8 to further exploit synergies have been organized by the WP7 leader UTRC. Additional meetings have been scheduled when needed for the finalization of the deliverable. Meeting minutes are archived in the internal project repository.

1.2.7.1 Task 7.1 Data analytics for driver identification

The original goal of this task was the exploitation of the sensor data available in the car (e.g., OBD readings, GPS, CAN bus messages) to identify the car's driver in the S2C pilot. By considering that even the AT pilot has requirements for identifying the user, this task has been extended to identify passengers from environmental sensors available in the transportation premises and personal devices (e.g., cameras, Bluetooth beacons, wearable and smartphone sensors).

The components identified by the partners so far are:

- Secure Routine for driver identification – Driver DNA (E-CORRIDOR-IAI-SR) [by CNR]
- Passenger location and flow optimization (E-CORRIDOR-IAI-PL) – [by UTRC]
- Passenger: Identification, Behaviour, Context (E-CORRIDOR-IAI-PBI) – [by UTRC]
- Gait analysis – passenger authentication (E-CORRIDOR-IAI-GA) – [by CNR]
- Face recognition – passenger authentication (E-CORRIDOR-IAI-FR) – [by PEC]
- Activity recognition – passenger authentication (E-CORRIDOR-IAI-AR) – [by PEC]

1.2.7.2 Task 7.2 Privacy preserving itinerary planning

Task T7.2 aims at the definition of analytics to infer or predict the best multi-modal travel itineraries for end-users. Activities in this task have focused on progressing in design and maturation of the itinerary planning tool. Thanks to interactions with WP partners and pilots, the key features to be implemented, maturated and integrated in the tool have been identified and prioritized. In particular, by working on the S2C pilot (WP3) use cases and user stories of the itinerary planning tool have been identified as well as the (input and output) data formats for

interfacing with the Clem' architecture. Moreover, potential synergies with Task 7.3 and 7.1 have been identified.

Multiple off-the-shelf multi-modal itinerary planning tools have been compared by WIT. The final choice fell on the OpenTripPlanner 2 (http://docs.opentripplanner.org/en/latest/) as the essential library for the development work. OpenTripPlanner (OTP) is an open-source multi-modal trip planner which has the advantages of good usability, flexibility and high performance. Its features will be improved and expanded to support for more modes of transport (car rental and on-demand bus), CO2 estimation, and micro-subsidy eligibility check.

- CO2-aware Trip Planning (E-CORRIDOR-IAI-MMIP) [by WIT]

1.2.7.3 Task 7.3 Privacy preserving (Security) analytics

It aims at defining a platform to integrate privacy preserving analytics on information shared on the Information Sharing Infrastructure (ISI) of the E-CORRIDOR platform. In this period, the technologies owned by CEA and CNR have been discussed considering requirements for using it in conjunction with the analytics proposed by the other partners. Being the privacy a crucial aspect of the project, different privacy preserving techniques have been considered (such as fully homomorphic encryption, differential privacy, and secure multiparty computation) with pros/cons for their application to the heterogeneous set of analytics required by the different tasks and use cases.

Requirements for integrating the CEA's OpenAPI for fully homomorphic encryption in the pilots have been discussed and the next effort will be focused on customization and implementation in the actual use cases of the three pilots. Moreover, CNR is working on a secure multi-party computation technique exploiting sensitive data of the driver.

- OpenAPI for Fully Homomorphic Encryption (FHE) (E-CORRIDOR-IAI-FHEC) [by CEA]
- Secure Multiparty-computation for Routine based authentication - Private Secure Routine (E-CORRIDOR-IAI-MPCSR) [by CNR]

1.2.7.4 Task 7.4 Carbon footprint analytics

This task aims at designing analytics for inferring by approximation the actual CO2 footprint in a multi-modal transport system. WIT has developed the initial carbon footprint calculator for multi-modal transport, prioritizing its efforts on the vehicles since road transportation generates more CO2 than other transport modes. In collaboration with the WP3 activities, within the tool, a vehicle CO2 emission database has been deployed to support distance-based CO2 estimation, and some APIs have been exposed for the end-users and other tools (such as the itinerary planning tool in T7.2). Future research and development efforts will be oriented at adding more metrics for CO2 estimation and designing more accurate algorithms able to consider vehicle emission test procedures (e.g., the worldwide harmonized light vehicles WLTP).

- CO2 Analytics (E-CORRIDOR-IAI-CFA) [by WIT]

1.2.7.5 Task 7.5 Intrusion detection technologies

It aims at designing machine learning approaches for intrusion detection systems and anomaly-based detection. Activities transversal to the three pilots AT (WP2), S2C (WP3), multi-modal

ISAC (WP4) have been identified. The identified approach foresees that AT and S2C can perform some security analysis at the edge (e.g., airport, car) and transfer some other data for further analysis or knowledge sharing through the ISI (WP6) to the multi-modal ISAC (e.g., running on the cloud) according to specific Data Sharing Agreements (DSAs).

Three main components have been identified and designed: an intrusion prevention system (developed by CNR) and two intrusion detection. Of the latter two, the first is tailored to the vehicular network (by FhG) and the second is more generic and exploits the fully homomorphic encryption (by CEA). The requirements of such components have been pinpointed as well as their application to the pilots. Notably, synergies among the intrusion prevention and the intrusion detection systems have been identified and will be exploited in the next months through a collaboration between CNR and FhG.

- Automotive Intrusion Detection (E-CORRIDOR-IAI-CANIDS) [by FhG]
- Fully Homomorphic Encryption-based intrusion detection (E-CORRIDOR-IAI-FHEIDS) [by CEA]
- Intrusion Protection System (IPS) – EARNEST (E-CORRIDOR-IAI-CANIPS) [by CNR]

The approach designed by FhG for the E-CORRIDOR-IAI-CANIDS component has the ability to track behaviour conformance and security compliance of a system, as well as to predict critical situations. A concept for a Predictive Security Analyzer (PSA) that combines FhG's previous IDS approaches and integrates their methodology into the context of the E-CORRIDOR project has been defined. Other than reported in D71, this research effort on the algorithms used within the PSA in order to automatically identify the inner structure of CAN message content has been published in:

- Florian Fenzl, Roland Rieke, Yannick Chevalier, Andreas Dominik, and Igor Kotenko, "Continuous fields: Enhanced in-vehicle anomaly detection using machine learning models", Simulation Modelling Practice and Theory 105 (2020), 102143, https://doi.org/10.1016/j.simpat.2020.102143
- Florian Fenzl, Roland Rieke, and Andreas Dominik: "In-vehicle detection of targeted CAN bus", ARES 2021.

1.2.7.6 Deviation from DoA

There is no deviation from DoA to report.

1.2.8 WP8 Advanced security services

The main objective of this work package is the integration of tools and technologies for the advanced security services to facility passengers' multi-factor authentication and authorisation while respecting privacy and security constraints.

The work package was also organised to achieve a sustainable technology and know-how transfer to the partners. From the technical point of view, the work package was organised around an open common platform and open APIs (RESTfull web services) based on standard micro-service architecture, able to integrate the various security software tools developed, and to support the three pilot operations in particular.

Tasks carried out during the first year
During the first year of project, the following tasks have been carried out:

- Identification of the pilot user stories and use-cases which can be supported by the security tasks described in WP8;
- Collection of the security requirements from three pilots;
- Identification of common security and privacy requirements;
- High level design of integration architecture for all the security technologies proposed by E-CORRDIOR partners;
- Selection and proposition of appropriate processing security algorithms with respect to privacy seamless multimodal authentication and autorisation.

To complete these tasks, during the first year of project, all the partners in WP8 were stressed to work on gathering security and privacy pilot's requirements. The conf-call meetings was organised every two weeks. CEA is leader of this WP, attended regularly in Pilots' meetings in order to keep up to date pilots requirements and to ensure information management across WPs.

1.2.8.1 Task 8.1 Privacy aware seamless multimodal authentication

This task lead by UTRC, the participants of this task proposed a mechanism for privacy-aware multi-factor authentication (MFA) by exploiting multi-biometric, behavioral, location and contextual information of the user. To enhance the security of the authentication mechanism, they need to collect data from multiple sources of information to identify and authenticate the users. More details of this approach the reader can refer to D8.1.

1.2.8.2 Task 8.2 Continuous behavioural authentication

This task lead by UTRC, the participants of this task proposed a "*continuous and token-based*" authentication in a multimodal transportation domain. A federated authentication approach based on eIDAS was offered to apply in E-CORRDIOR advanced security framework to perform a token-based authentication in a multi-stakeholder environment. More details of this approach the reader can refer to D8.1.

1.2.8.3 Task 8.3 Privacy aware interest-based service sharing

This task lead by CEA, the participants of this task proposed applying *fully homomorphic encryption* technology and *two-party computation* techniques. These two techniques consists of using profile matching to help customers from a country find the right service located in another country with similar attributes (e.g., interest, location, background, etc.). More details of this approach the reader can refer to D8.1.

1.2.8.4 Task 8.4 Privacy aware authorization

This task lead by CEA, the participants of this task proposed a "*federated model for attribute based encryption*", which allows sharing data without compromising actors' privacy, effectively, peers may share data based on their interests, and those ones will be matched without disclosing out the degree of interest. More precisely, they will develop a fine-grained access control for sharing data based on passenger's interests. More details of this approach the reader can refer to D8.1.

1.2.8.5 Task 8.5 Secure Identity Management

This task lead by FhG, the participants of this task proposed a secure identity management system for both eWallet digital token and the continuous authentication checking for the passenger and baggage. The main activities of this task focus to implement the secure distribution of credentials to establish strong identities in the participating entities. This approach includes the user identification with his token, backend systems like the E-CORRIDOR backend, car sharing, or airport backend systems as well as passengers and baggage tracking in the continuous authentication use case. More details of this approach the reader can refer to D8.1.

1.2.8.1 Deviation from DoA

There is no deviation from DoA to report.

1.2.9 WP9 Exploitation, Dissemination, Communication and Standardization

WP9 Exploitation, Dissemination, Communication and Standardisation corresponds to Objective 7 of the project, namely "E-CORRIDOR will be promoted and ease the exploitation, communication, standardisation, dissemination and early adoption of its results". The objective will be realised through the proper implementation of the exploitation, communication, standardisation and communication plans, the successful delivery of the WP9 deliverables, and the achievements of the key performance indicators for communication.

In the first project year, WP9 has defined its first Exploitation and Dissemination Plan in D9.1 *First exploitation and dissemination plan*, describing the set of strategies and approaches for enlarging ECORRIDOR's impacts. WP9 partners have conducted lots of dissemination and communication activities to achieve the targets set for this period. The progress in dissemination, communication, exploitation, and standardisation against the plan has been reported in D9.2 *First exploitation and dissemination report* and will be briefly explained in the following subsections.

Within WP9, there are four tasks, which are Task 9.1 *Exploitation and Innovation*, Task 9.2: *Standardization*, Task 9.3 *Dissemination and Communication*, and Task 9.4 *Data management Plan.* WP9 partners have made their contributions to these tasks, but since the project is at the beginning stage and focusing on defining the requirements and architecture for its solutions, more progress has been concentrated around Task 9.3. However, with the maturation of more technical tools and the E-CORRIDOR platform, more concrete achievements can be expected in the other tasks.

1.2.9.1 Task 9.1: Exploitation and Innovation

For Task 9.1, some foundational work has been conducted to support specific business modelling, development, and exploitation activities in subsequent phases. A 4-step exploitation approach has been identified to coordinate the exploitation activities within the project, which are **Discovery, Definition, Validation**, and **Go-To-Market Plans**. In Year 1, an exploitation survey has been distributed to all partners to help them identify the key exploitable results and make exploitation plans. The survey also contributes to a project-level exploitation plan, the advice from the Exploitation Board and the future internal exploitation workshops, since it will provide valuable insights into partners' exploitation interests and plans.

The IPR management of the project was also covered by D9.1. Since the exploitation activities will intensify in the final stages of the project and rely heavily on learnings and outcomes from the pilots, Year 1 of the project focuses more on defining an overall exploitation plan. The exploitation and innovation work can be further improved with more substantial resources.

WIT is the leader of WP9 and led the definition of the exploitation plan in D9.1. It has analysed the relevant business environment and strategies and identified the initial business plan by adopting analysis methods like Kotler's product level model and SWOT and analysing the exploitation surveys distributed to E-CORRIDOR partners.

UTRC, CNR, FhG, Factual and WIT have refined their target assets and individual exploitation strategies around their target assets in the internal exploitation surveys. Their inputs have significantly refined and complemented the project-level exploitation plan. Other partners in the consortium have revised their individual exploitation plans defined at the beginning of the project.

All partners have contributed to the two deliverables, D9.1 and D9.2, with some significant contribution from the following partners. WIT led most of the sections. UTRC, CNR, and FhG provided lots of constructive suggestions for exploitation, such as using the Horizon Results Platform of European Commission as an additional exploitation channel.

1.2.9.2 Task 9.2: Standardization

Task 9.2 is mainly led by CNR and FhG, since they have in-depth participation in several international standardisation organisations. The E-CORRIDOR standardisation activities have been reported in D9.2, and since E-CORRIDOR solutions will mature in Year 2-3, partners have been focusing on continuously monitoring, reporting the relevant standardisation landscape, and recommending E-CORRIDOR outputs when the opportunity comes in Year 1.

FhG is actively involved in standardisation activities in various standardisation bodies, in particular in ETSI, IETF, TCG, car-2-car communication consortium, DKE/VDE, and ISO TC 22. The progress in these activities has been shared with the project members to help them keep in pace with the latest trend for standardisation in the cybersecurity domain. Other partners keep monitoring the relevant standardisation landscape and seeking opportunities to provide contribution and recommendations.

1.2.9.3 Task 9.3: Dissemination and Communication

Task 9.3 aims at reaching the broadest spectrum of stakeholders from the scientific and industrial community and the general audience with the main results from E-CORRIDOR to ensure the maximum impact during and after the project.

This task has defined its first dissemination and communication plan in D9.1 with the contribution from all partners and decided to follow a four-phase communication plan to reach its audiences. The four phases are **Awareness, Consideration, Conversion** and **Advocacy**, and each phase corresponds to a specific communication objective at a stage that could shape audiences' mindsets around E-CORRIDOR. For instance, Year 1 corresponds to the Awareness phase, aiming at raising the awareness of E-CORRIDOR when the technical work packages are maturing their critical assets.

Specifically, some major achievements for dissemination and communication have been summarised as follows:

First, WP9 defined its first dissemination and communication plan in D9.1 to direct all the dissemination activities within the project. WIT has led the editing work of the plan and merged the inputs and opinions from partners to form this plan. Also, FhG, UTRC, CNR, Pildo, and DITECFER provided lots of concrete inputs into the work package deliverables, promoting their quality and contributing to the optimisation of dissemination and communication strategies.

Second, the WP leader WIT has prepared different promotional materials to be used by partners in their communication and dissemination activities, including E-CORRIDOR logos, flyers, leaflets, slide deck, spreadsheets for tracking dissemination activities, and website (https://e-corridor.eu/, online since November 2020). For the website, 1.6k individual users have visited the website, and 5 pieces of E-CORRIDOR news shared on the website (the target is 6k individual users for the website and 10 pieces of news published before the end of the project).

Third, WP9 has set up and running its social media since the beginning of the project, and the project has more than 500 connections for LinkedIn and over 1100 followers for Twitter and published 33 tweets from the account. Thus, by checking these numbers with our communication KPIs, we can conclude that these communication and dissemination channels run as expected and reach the communication targets for Year 1, indicating good progress achieved in setting up communication channels and generating dissemination materials.

Furthermore, for publication and events, CNR and FhG contributed to most of the research papers (9 conferences papers and 4 journal papers submitted/published) and events participated. UTRC and WIT also participated in some of the events to ensure the presence of E-CORRIDOR. To be specific, there are 3 workshops supported by E-CORRIDOR with project members (mainly CNR and FhG) serving as invited speakers and another 6 events attended to ensure the project presence. The project also started the cooperation in organizing cybersecurity-relevant events with other projects with similar interest, as SPARTA and CitySCAPE. All these dissemination activities have been recorded in some tracking spreadsheets (stored on the project SVN) and reported in D9.2.

Last, each WP9 partner revised their individual dissemination plan and utilised their own channels to promote the project. For instance, FACTUAL disseminated the news related to the car-sharing pilot and the prospects of the micro-subsidy tool through its social networks. DITECFER focuses on disseminating the information with regards to the ISAC pilot.

In all, partners have made reasonable efforts in Task 9.3 and achieved corresponding progress there. In the upcoming project year, partners should focus on continuing to promote the project through various communication channels and organising more E-CORRIDOR-centric events and workshops.

1.2.9.4 Task 9.4: Data management Plan

Task 9.4 *Data management Plan* is dedicated to managing data collection across research activities, and a Data Management Plan (DMP) has been delivered in D9.1. This DMP consolidated the procedures to be followed by project partners regarding the administration of all data that will be produced, collected, stored and shared both during and beyond the project lifecycle.

Most of the data generated within the project will be processed by the Information Sharing Infrastructure (ISI) and Information Analytics Infrastructure (IAI), and the generated results will be consumed by the prosumers defined in the DSAs attached to the data. HPE, CNR, UTRC, and CEA, as the WP5-8 leaders, have collected the protentional data types that need to be used by the pilots and the framework. As a result, Table 3 of Deliverable 5.1summarised all the initial data classes and contains information such as Data Type Class, Data Format, Standard, Pilot Use Case ID, and usage purposes (for sharing, for analysis, for performing a Data Manipulation Operation), serving as a good start point to manage all the project data. Then, a data management plan has been defined in D9.1 on top of the above work and also considered the ‘FAIR’ principles (making research data findable, accessible, interoperable and re-usable)

The Data Management Plan of E-CORRIDOR is intended to be a living document in which information can be made available on a finer level of granularity through updates as the implementation of the project progresses and when significant changes occur. The project will regularly check the requirements for data types from pilots and data analytics tool providers and reflect them in the DMP.

1.2.9.1 Deviation from DoA

There is no deviation from DoA to report.

1.2.10 WP 10 Management

1.2.10.1 Project coordination

This task devoted to the coordination of the project in order to ensure a harmonised approach to the handling of the tasks, the definition of the tasks outcomes, management of the issues that might arise and the successful application of the innovation management procedures.

All the project management bodies were set up as planned at the beginning of the project.

Regular monthly conf-calls have been set up among all the relevant bodies.

Several general meetings were set up (6) where all the partners participated and some bilateral project meetings were also organized when necessary.

The project is technically on track. There have been however issues w.r.t. pandemic that hindered the contributions of some partners.

1.2.10.2 Administrative and financial management

Risk management CNR properly managed all the administrative and financial issues related to the project. In particular, the pre-financing has been distributed as planned in the Consortium Agreement. A regular updated of partners' efforts have been carried on.

1.2.10.3 Risk management

CNR developed the risk management plan and organized all the activities in a manner to cope with possible risks. Deliverables at month 6 and month 12 are basically on time. A consideration of covid issues has been considered and several actions have been done.

Risks materialized and corrective actions:

#	Risk description	WPs	Prob	Impact	What happened	Response Actions
1	Key partners underperform or ….	10	L/M	H	Due to COVID several partners whose core business is transport like	The initial response action "*Redistribute the work among remaining*

					ADP/SNCF had serious staff issues, both in terms of personnel availability and of time for working. For instance ADP people could work in general a few days per week, and thus even less in the project.	*partners*" has been applied and other partners supported ADP/SNCF.
2	Actors involved in pilots do not perform as planned	2-4	L/M	H	Same ad before since the main affected partners were in the pilots (as end users)	The initial response action "*Reorganize or optimize the pilot planned task*" has been adopted and more will come through an amendment in the second year, already agreed with the PO.
6	Issues related to partners' communication.	10	L/M	M	Some partners that had less time to work and that were really concerned with pandemic, resulted less active.	As coordinator this communication aspects were raised during meetings and Management calls. WPs leaders were asked to make more continuous calls. When necessary direct phone calls to the partners not responding were done. Still certain partners failed to deliver on time relevant information for the consortium. Those were warned that there could be actions to remove those from the project. In the

						amendment, stricter conditions on reactions time will be inserted.

1.2.10.4 Collaboration with other projects

E-CORRIDOR started the cooperation with other projects with similar interest, as SPARTA and CITY SCAPE.

1.2.10.5 Deviation from DoA

There is no technical deviation from DoA to report.

Gender issues:

All E-CORRIDOR project's partners are aligned and fully agree with the EC objectives to promote gender equality and foster involvement of researchers of both sexes, whose recruitment is based solely on their qualifications and technical merit. Further, E-CORRIDOR project members agree to encourage the practices for a better work/life balance achievement (e.g. maternity and paternity leave) and flexible work planning (e.g. teleworking).

Several members of the E-CORRIDOR consortium teams are female and with relevant roles in their organizations.

2. Update of the plan for exploitation and dissemination of result (if applicable)

2.1 Communication and Dissemination

This section will report the dissemination and communication activities of the project in generating dissemination materials and conveying E-CORRIDOR messages to targeted audiences through different channels.

i. Promotional Materials

The primary dissemination and communication channels used by E-CORRIDOR are the websites and social media, and the individual channels owned by partners (such as their own Twitter channels and newsletters) complement these channels.

To support the dissemination and communication activities and create an impressive visual identity, E-CORRIDOR has designed and used the following promotional materials to engage with our target audiences.

1. E-CORRIDOR Logo

As outlined in Figure 1, the E-CORRIDOR logo symbolises the project, and it unifies and reinforces the branding. It should be used in all project materials such as project website, document templates, presentations, social media accounts, newsletters, posters and other distributed materials to ensure consistency.

This logo is based around a shield representing Security/Safe/Strong. The blue and green colours express a message of trust and security and correspond to the vision of the project to contribute to a secure, resilient and digital Europe by supplying E-CORRIDOR solutions. Also, the white dot in the centre is to also show the shield as a map marker/position, representing the transport domain. The blue line circling the shield with 3 lines through it is to represent an interconnected network. These lines represent Communication/Connection. These lines are also to represent a character E and match the exact size and spacing as the E in the E-CORRIDOR.

The logo is available in JPEG, PNG, and AI (original design files) formats and shared in both the project SVN repository and the project website. When not using the logo, E-CORRIDOR should be referred to in capital letters, just as it is used in Figure 1. A detailed brand guideline has also been provided to project partners to regulate the usage of colours, logos, fonts and images in various dissemination scenarios.

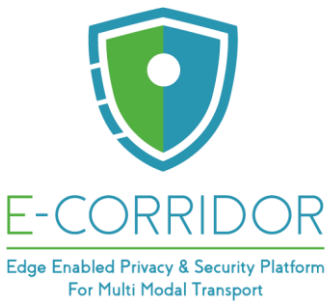

Figure 1. E-CORRIDOR logo (Left: with tagline; Right: without tagline).

2. Deliverables and Slides Templates

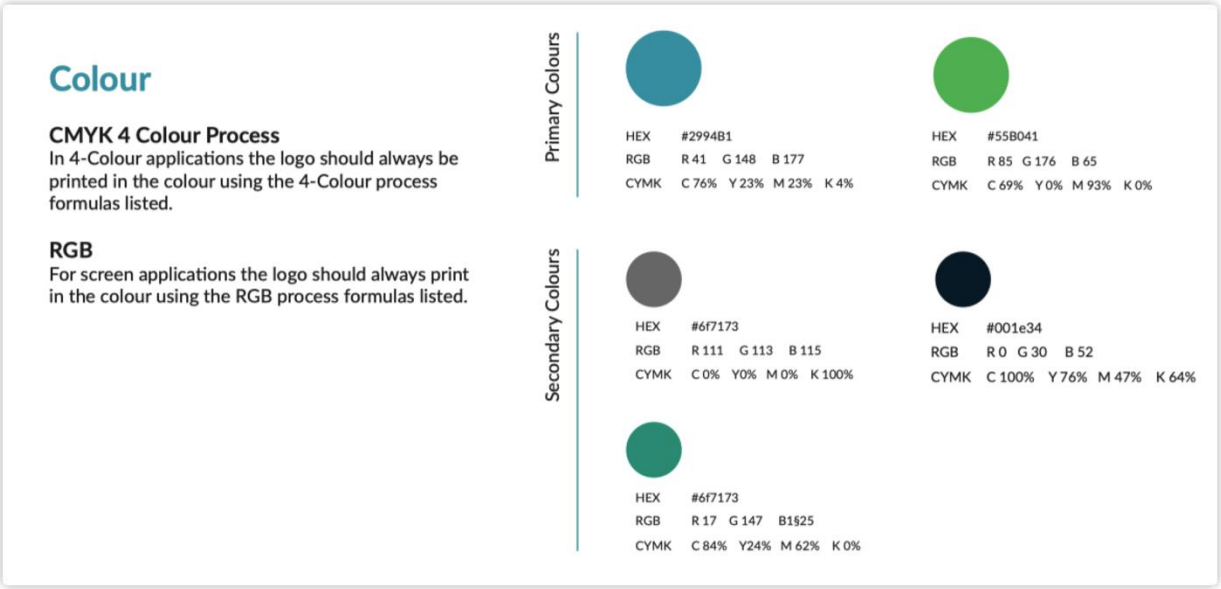

Figure 2. E-CORRIDOR colors in the project branding guideline.

The templates for deliverables and slides have been provided in Section 8 *Templates* of D10.1 *Project Quality Handbook*, and they provide a unified format for the two most important documents within the project.

3. Videos

E-CORRIDOR has planned to create a series of promotional or interview videos to promote the concepts and innovation of the project. This work has been scheduled to start in Month 13 when a clearer technical roadmap is in place for each work package.

The length of each online interview will be around 10 mins, and the interview introduces the expertise of partners and their contributions to E-CORRIDOR project. Each partner should finish at least 1 video interview to achieve the set targets for WP9. However, if the outputs from partners such as pilots and deliverables need to be disseminated, more interviews/ news can be arranged. The WP9 leader will make a timetable for the interviews, record the videos interviews with partners, edit the videos, and publish them on our websites and social media.

Some example questions are as follows, but partners can also bring their own questions highlighting their originations and innovative work in E-CORRIDOR.

- Your organization and its involvement/expertise in the E-CORRIDOR project?
- Please introduce the project/work package/task achievement to date.
- What is the main challenge for the project or your work package? For instance, COVID-19 and travel restrictions around the world.
- What are the expected outcomes from your WP/tasks?
- How will the industry and academia benefit from the outputs of E-CORRIDOR?

4. Flyer and Leaflet

Flyers and leaflets act as important dissemination materials for the E-CORRIDOR project to support partners in attending events, presentations and workshops. These materials condense the project profile into a one- or two- page visually appealing document.

If roller banners or posters are needed for future events, their design will be based on the flyer shown below to ensure design consistency. The content on the roller banners or posters will be adjusted based on their applications.

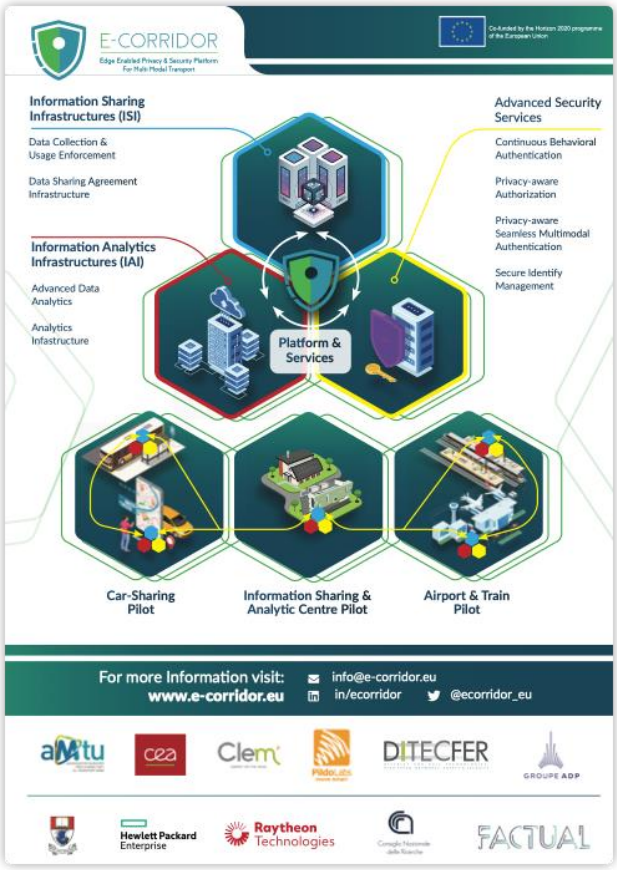

Figure 3. E-CORRIDOR flyer.

Figure 4. E-CORRIDOR leaflet.

5. Slide Deck

In some cases, the target audience of E-CORRIDOR may want to learn more in-depth information about the project, where the flyer and poster could not meet the demand due to the limited space. Thus, E-CORRIDOR has created a 12-page slide deck with more project details provided. It is shared at the link https://e-corridor.eu/resources/ under the tab "BRANDING & LOGOS". The slide deck also functions as a project brochure, providing information on the project objectives, consortium, methodology, and pilots. Besides, the content of the slide deck will be regularly updated to reflect the latest information and outputs of the project.

Figure 5. E-CORRIDOR slide deck.

ii. Website

The E-CORRIDOR website (https://e-corridor.eu/) is the primary dissemination channel to share project information with the world. The website (shown in Figure 6) was designed and developed by the Creative Design Unit (CDU) at TSSG/WIT over the course of several months and has been online since November 2020.

A wealth of information to introduce the project and the project's progress has been provided across different sections of the website. Besides, it has been continuously monitored and updated to facilitate better dissemination, outreach and project operation.

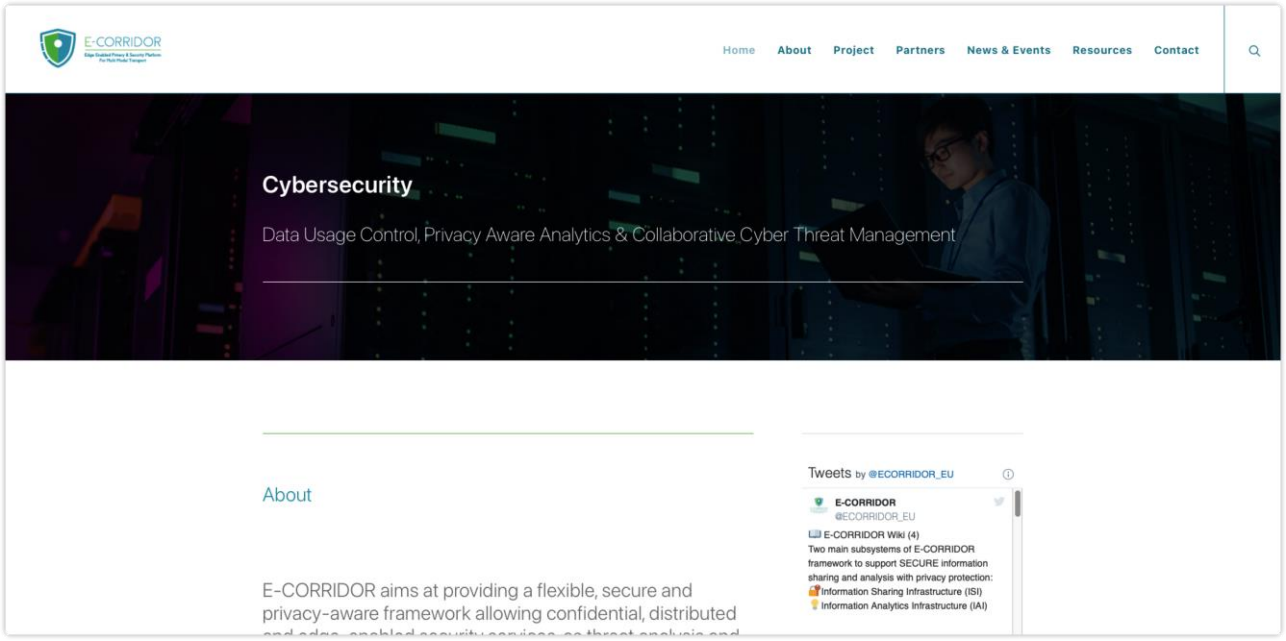

Figure 6. E-CORRIDOR website homepage.

Figure 7. E-CORRIDOR website - news page.

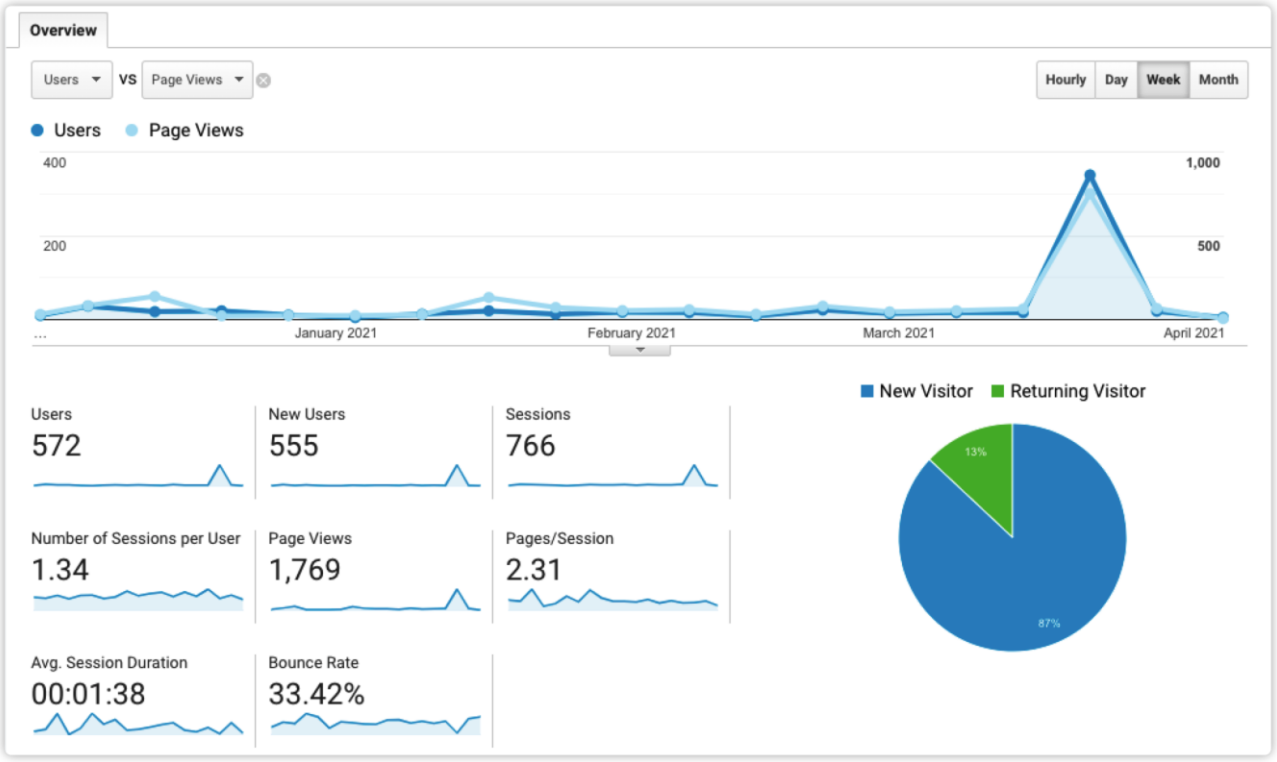

Figure 8. E-CORRIDOR website audience overview.

In this section, we will present the viewing trends of the E-CORRIDOR website (obtained through Google Analytics [1]), along with some relevant analysis in accordance with the presented data.

Figure 8 presents an overview of the E-CORRIDOR website audience and statistics between December 1st, 2020 and April 7th, 2021. The website has attracted 555 new (unique) users during this period and has a total of 1769 page views. For a project in its first year of operation and with a sparsity of concrete results due to development being in its early stages, we feel that this is a satisfactory outcome. Furthermore, we noticed that most of the views and new users are centred on March 2021. The reason is that E-CORRIDOR hosted its 3rd plenary meeting that month, and we generated lots of interesting content (such as news and tweets) from that. Thus, we can infer that the original content around E-CORRIDOR could attract more audience, and more efforts should be placed on generating E-CORRIDOR related content. As the project progresses with more concrete results available for public observation, we could expect a natural increase in audiences' interest and website visits.

Another two sets of data show the origin countries of our website users (Figure 9) and the top 10 pages viewed by users. Figure 9 indicates that E-CORRIDOR's audience has a great geographical coverage that is not limited to EU countries. E-CORRIDOR could attract the attention of international research powers and foster international communication.

Moreover, Figure 10 shows that most of the views of our website occur on our homepage, indicating that our target audience is still at the stage of learning about E-CORRIDOR, instead of focusing on a specific technical topic.

With a bunch of deliverables to be submitted in Month 12 and the concrete results derived from them, we can expect a better dissemination result in the following project year. We will keep monitoring the website's statistics and adjust our dissemination strategies accordingly to maintain a continuous and profound impact.

	Country	Users	% Users
1.	United States	59	10.30%
2.	Italy	46	8.03%
3.	(not set)	43	7.50%
4.	Ireland	41	7.16%
5.	France	35	6.11%
6.	China	29	5.06%
7.	Spain	22	3.84%
8.	Germany	20	3.49%
9.	Japan	20	3.49%
10.	India	18	3.14%

Figure 9. E-CORRIDOR website users by country.

	Page	Page Views ↓	Unique Page Views
1.	/	1,144 (64.67%)	683 (59.55%)
2.	/e-corridor-project/	100 (5.65%)	69 (6.02%)
3.	/our-partners/	98 (5.54%)	79 (6.89%)
4.	/about-ecorridor/	77 (4.35%)	59 (5.14%)
5.	/news/	61 (3.45%)	39 (3.40%)
6.	/resources/	57 (3.22%)	41 (3.57%)
7.	/contact-ecorridor/	44 (2.49%)	31 (2.70%)
8.	/cyrano/	24 (1.36%)	17 (1.48%)
9.	/event/	24 (1.36%)	17 (1.48%)
10.	/cve-for-kia-vulnerability/	22 (1.24%)	17 (1.48%)

Figure 10. E-CORRIDOR website page views.

iii. Social Media

The primary goal of using social media for E-CORRIDOR is to spread the messages of E-CORRIDOR in a timely and lively way and promote the level of awareness regarding the project among key stakeholders. The table below lists all the social media channels of E-CORRIDOR, but the focus of this section is on Twitter.

Table 1. E-CORRIDOR social media channels.

Social Media Channel	Link
Twitter	https://twitter.com/ECORRIDOR_EU
LinkedIn	https://www.linkedin.com/in/ecorridor/
Facebook	https://www.facebook.com/ECORRIDOR.EU
YouTube	https://www.youtube.com/channel/UCKaYxHm9DTnhAtLMfM2AaGA

The E-CORRIDOR Twitter account (@ECORRIDOR_EU) has been the primary social media channel for the project to date. E-CORRIDOR started to manage its social media account since October 2020 and has published 28 tweets and received 9679 Tweet impressions (the number

of times a tweet shows up in somebody's timeline), 796 profile visits and 45 new followers (at the time of writing which is the end of March 2021). To date, the Twitter account has a total of 1,174 followers, among which are other H2020 projects and stakeholders in the cybersecurity and transport domains.

The dissemination effect through Twitter has also been analysed by using the data from Twitter Analytics [2]. The results have been shown in Figure 11, and we can see increasing efforts being put into this channel (more Tweets published) and wider impacts (more Tweet impressions and profile visits).

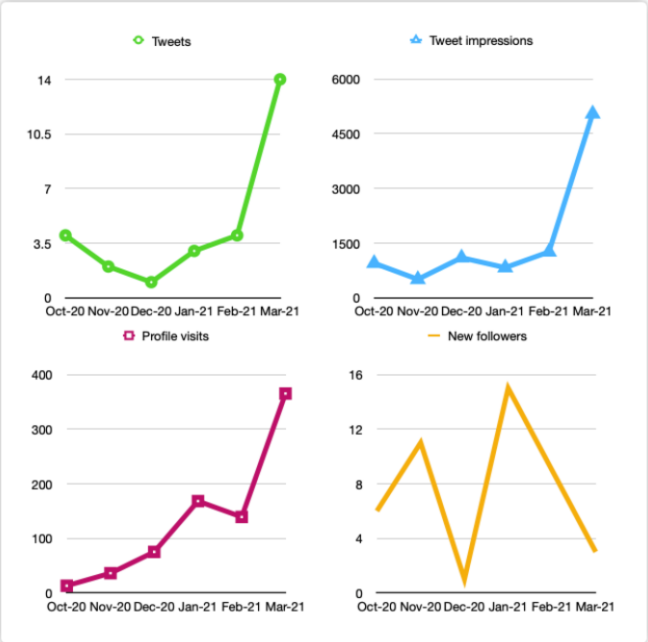

Figure 11. E-CORRIDOR Twitter Analytics statistical results.

iv. Publications

1. Press Release

The project has published several news on the website to disseminate the project messages to the public and media.

Table 2. E-CORRIDOR news on the project website.

Title	Date	Link
EU H2020 ICT Security project E-CORRIDOR successfully kicked off	2020-07-06	https://e-corridor.eu/ecorridor-kicked-off/
Open Research Europe, the EC scientific publishing service for H2020 and Horizon Europe	2020-11-24	https://e-corridor.eu/open-research-h2020/
CNR researchers successfully identified KIA Head Unit vulnerability and made it a CVE entry.	2020-12-02	https://e-corridor.eu/cve-for-kia-vulnerability/
Cyrano event to be held on Dec. 16th, 2020 to share the cybersecurity observatory	2020-12-08	https://e-corridor.eu/cyrano/

E-CORRIDOR 3rd virtual plenary meeting successfully held	2021-03-19	https://e-corridor.eu/plenary3/

2. Papers

Below are all publications submitted, accepted and presented at peer-reviewed international conferences with the contribution from E-CORRIDOR partners.

Table 3. Conference papers submitted/published by the E-CORRIDOR consortium

Conference	Date	Areas	Paper Title	Authors and Affiliation
ACM ASIACCS 2021 -16th ACM ASIA Conference on Computer and Communications Security	2021-06-07	Security	Secure Role and Rights Management for Automotive Access and Feature Activation	Christian Plappert, Lukas Jäger, Andreas Fuchs (FhG)
PDP 2021 - 29th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing	2021-03-10	Security	Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain	Christian Plappert, Daniel Zelle, Henry Gadacz, Roland Rieke, Dirk Scheuermann, Christoph Krauß (FhG)
ARES'20 - 15th International Conference on Availability, Reliability and Security	2020-08-25	Security	VisualDroid: automatic triage and detection of Android repackaged applications	Rosangela Casolare, Carlo De Dominicis, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone
WAINA-2020 - Workshops of the 34th International Conference on Advanced Information Networking and Applications	2020-04-15	Security	Colluding Android Apps Detection via Model Checking	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Vittoria Nardone, Antonella Santone

IJCNN 2020 - 2020 **International Joint Conference on Neural Networks**	2020-07-19	Security	Malicious Collusion Detection in Mobile Environment by means of Model Checking	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone
IJCNN 2020 - 2020 **International Joint Conference on Neural Networks**	2020-07-19	Security	Enhanced Privacy and Data Protection using Natural Language Processing and Artificial Intelligence	Rosangela Casolare, Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone
IoTBDS 2020 – The 5th International Conference on Internet of Things, Big Data and Security	2020-05-07	Security; ML	Image-based Malware Family Detection: An Assessment between Feature Extraction and Classification Techniques.	Giacomo Iadarola (CNR), Fabio Martinelli (CNR), Francesco Mercaldo, Antonella Santone
KES 2020 - International Conference on Knowledge-Based and Intelligent Information & Engineering Systems	2020-09-16	Vehicular; ML	A Deep-Learning-Based Framework for Supporting Analysis and Detection of Attacks on CAN Buses	Alfredo Cuzzocrea, Francesco Mercaldo, Fabio Martinelli (CNR)
VTC2020-Spring - 2020 IEEE 91st Vehicular Technology Conference	2020-05-25	Vehicular; ML	Machine Learning for Driver Detection through CAN bus	Fabio Martinelli (CNR), Francesco Mercaldo, Antonella Santone

Below are all publications published at peer-reviewed journals which involve the contribution from E-CORRIDOR partners or acknowledge the project.

Table 4. Journal papers submitted/published by the E-CORRIDOR consortium

Paper Title	Journal Name	Authors	Link

Towards an Interpretable Deep Learning Model for Mobile Malware Detection and Family Identification	Computer & Security	Giacomo Iadarola (CNR), Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone	https://www.sciencedirect.com/science/article/pii/S0167404821000225
Call Graph and Model Checking for Fine-Grained Android Malicious Behaviour Detection	Applied Sciences	Giacomo Iadarola (CNR), Fabio Martinelli (CNR), Francesco Mercaldo (CNR), Antonella Santone	https://www.mdpi.com/2076-3417/10/22/7975

v. Events

Table 5. Events attended by the E-CORRIDOR consortium.

Event Name	Date	Location	Domain	Type	Attendees and Roles	Feedbacks
CSET (Cyber Security for Energy & Transport infrastructure) International Conference 2020	2020-09-17	Italy	Sec.	Wor.	Fabio Martinelli (Speaker)	E-CORRIDOR was presented and contacts were made with people especially in the cyber threat management aspects and in the data usage control frameworks developed. The interest in the data sovereignty aspects for the ISI/IAI infrastructure were noted.
CYRANO	2020-12-16	Vir.	Sec.	Wor.	Fabio Martinelli (Speaker); Stefano Sebastio (Attendee)	During the event the speakers discussed on cybersecurity and cyber-awareness in the airports, focusing on the importance of training and the sharing of threats within the sector. Fabio Martinelli introduced ISAC Pilot and its tools. They concept was well received.
EUROCONTROL: Introduction to Cyber Threat Intelligence	2021-01-28	Vir.	Sec.	Web.	Riccardo Orizio (Attendee)	The seminar provided a high level overview on the cyber-threats in avionics. The considered threats were common to any IT system (such as

						malware or ransomware attacks). The AT and ISAC pilots consider security and sharing of security-related information among stakeholders. Cybersecurity information organized by the ISAC could support the activity of the CERT teams
EUROCONTROL: Introduction to Cyber Threat Intelligence	2021-01-28	Vir.	Sec.	Web.	Stefano Sebastio (Attendee)	Same as above.
SESAR-JU: ATM Cyber-security - The industry view	2021-02-05	Vir.	Sec.	Web.	Stefano Sebastio (Attendee)	The seminar introduced the rising need of cybersecurity solutions in the air traffic management as more and more digitalized solutions are used for critical systems.
EUROCONTROL: Vulnerability management	2021-02-18	Vir.	Sec.	Web.	Stefano Sebastio (Attendee)	The EUROCONTROL efforts in providing CTI and feeds for the aviation sector was introduced as well as the support offered by EUROCONTROL to all the airports in the cybersecurity domain. The ISAC pilot in E-CORRIDOR aims to share security-related data. The privacy-aware solutions and controlled data sharing could provide incentives to the airports in sharing their cyber-threats potentially improving the security of the whole sector.
ATHENE Secure Mobility Dialogue	2021-03-24	Vir.	Sec.	Wor.	Roland Rieke (speaker)	E-CORRIDOR flyer has been presented in context with the analytics that Fraunhofer

						develops in E-CORRIDOR. Automotive intrusion detection and prevention solutions have been shown.
Automotive Security Research Group Waterford (ASRG-WAT)	2021-03-03	Vir.	Sec.\ Aut.	Web.	Ruisong Han (Attendee)	A meeting gathering the automotive security researchers and engineers. It has been a fruitful opportunity to discuss some E-CORRIDOR ideas with partcicipants.
CCAM Association 1st General Assembly	2021-04-14	Vir.	Aut.	Event	Ruisong Han (Attendee)	European Partnership on "Connected, Cooperative and Automated Driving". This event has been useful to make more visible the E-CORRIDOR activities in automotive, in particular the one related to data spaces in the field (data usage control). It is interesting to promote the capability to share data generated by the car.

vi. Liaison with Related Communities and Projects

- *H2020 Cyberwatching.eu – The European watch on cybersecurity & privacy (https://cyberwatching.eu/).* It is the European observatory of research and innovation in the field of cybersecurity and privacy aiming at promoting the uptake and understanding of cutting-edge cybersecurity and privacy services emerging in Research and Innovation projects. By partnering with Cyberwatching.eu, the E-CORRIDOR project will enhance the visibility of its ICT products, services and software in particular towards SME and European citizens. Potentially proposing novel cybersecurity services in the European Digital Single Market. Ruisong (WIT) and Stefano Sebastio (RTRC) promoted E-CORRIDOR on cyberwatching.eu (EU observatory of research and innovation in the field of cybersecurity and privacy). (https://cyberwatching.eu/projects/2456/e-corridor-edge-enabled-privacy-and-security-platform-multi-modal-transport).
- *H2020 SPARTA (https://www.sparta.eu/).* It is a novel Cybersecurity Competence Network, supported by the EU, with the objective of developing and implementing top-tier research and innovation collaborative actions. Thanks to its mix of partners from the academia and industrial sectors, one of its main goals is the definition of an ambitious research and innovation roadmap in the cybersecurity strengthening the EU

strategic autonomy in the field. E-CORRIDOR will be able to reach out to different stakeholders belonging to the SPARTA network (e.g., cybersecurity practitioners, service provides, and technology providers) and promote the novel results and products in the field of security and privacy.

- *CYRANO - CYbeR Awareness diploma (https://www.bologna-airport.it/en/the-company/business/european-projects/?idC=62586).* It is a co-funded EU project managed by the Bologna Airport, Italy (Aeroporto Guglielmo Marconi di Bologna S.p.A.) within the Connecting Europe Facility programme. It aims at increasing awareness of airport, critical infrastructures and essential services operators on cybersecurity aspects. The liaison of E-CORRIDOR and CYRANO will provide mutual benefits as both are oriented at improving the cybersecurity of the transportation domain with a special focus on the airways (see in particular the AT-pilot in E-CORRIDOR).
- *H2020 CitySCAPE* (https://www.cityscape-project.eu/). Fabio Martinelli (CNR) was a speaker for one cybersecurity workshop held by CitySCAPE. E-CORRIDOR also liaised with Cityscape and contributed to one interview for the Autobus and Trasporti Pubblici magazine on cybersecurity and privacy in their multimodal public transport and one event.

2.2Innovation and Exploitation

The overall mission of E-CORRIDOR is to design and provide a flexible, secure and privacy aware framework allowing confidential, distributed and edge enabled security services, as threat analysis and prevention as well as privacy-aware seamless access mechanism in multi-modal transport systems.

The E-CORRIDOR framework includes collaborative privacy-aware edge-enabled information sharing, analysis and protection as a service. The project plans to show the applicability of this framework in at least two domains: (i) collaborative and confidential cyber threat management and (ii) seamless access mechanism in multimodal transport systems.

In the first period of the E-CORRIDOR project, some foundational work has been ongoing to support specific business modelling, development and exploitation activities in subsequent phases. A 4-step exploitation approach has been identified to coordinate the exploitation activities within the project:

2. **Discovery:** much of the effort to date has concentrated on activities in this phase. In tandem with user requirements elicitation which is happening through the course of pilot actions in WP2, WP3 and WP4, efforts in WP9 have focussed on market research, in particular, a comprehensive business environment analysis the outputs of which are documented in D9.1. In addition to a macro environmental analysis, several sectors of relevance in the cybersecurity and mobility technologies domains were identified and analysed. This research enabled the creation of an updated SWOT analysis, and insights will be used to inform business planning and exploitation activities. Furthermore, strategic tools, including Kotler's product levels [3] and Porter's competitive framework [4], have been used to describe E-CORRIDOR products and the marketplace. These tools will serve as a useful basis to further develop business and exploitation ideas and plans.

3. **Define**: this phase will be a collaborative exercise to define and refine the E-CORRIDOR value proposition and to advance business modelling activities. To date, a very high-level description of the business model for E-CORRIDOR exists and has been updated. Specific detail and hypotheses underpinning this business model need to be teased out, including identifying channel partners, pricing strategies etc. This work will be supported by Industry & SME partners as well as the Exploitation Board and business networks. Additionally, business models will need to be developed for alternative commercial propositions, e.g., subsets of E-CORRIDOR components.
4. **Validation**: this phase will involve testing the hypotheses, models and plans that have been developed. Activities will include pilot feedback, demonstrations and pitch presentations. Feedback from the Exploitation Board and business networks will also support this phase.
5. **Go-To-Market Plans** will be finalised closer to the end of the project. The plans will guide exploiting and commercialising E-CORRIDOR's outputs.

a. Overall Exploitation Progress

Exploitation activity will intensify in the final stages of the project and relies heavily on learnings and outcomes from the pilots. However, as previously mentioned, some foundational work is ongoing. In this regard, an exploitation survey has been distributed to all partners to help them identify the key exploitable results and make exploitation plans. The survey also contributes to establishing the Exploitation Board and the future internal exploitation workshops since it will provide valuable insights into partners' exploitation interests and plans. Thus, the project-level exploitation plan can be fine-tuned to reflect the will of all partners and coordinate the partners' exploitation strategies and activities.

This survey asks each project partner to identify and categorise the exploitation assets it expects to develop as part of its work on the project. Categories of assets can include knowledge, software, documents (e.g., training), data (e.g., statistical data from the pilots), protected items (e.g., patent applications, licenses, copyrighted/copylefted material, registered designs), standards etc. Additionally, partners are asked to identify IPR that may be developed, and their exploitation plans for individual assets, as well as E-CORRIDOR as a whole. The exploitation survey template has been attached in the annex of this report. Some responses are still pending, and more comprehensive insights will be obtained with more results collected. A collation of exploitable assets identified to date is found in the following table. It should be noted that this may change as design, development and testing efforts advance through the project.

Table 6. Exploitable results definition/ description

Exploitation Asset	Category	Exploitation Type	Explanation
Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Technologies [CNR]	Knowledge Software	Research	The acquisition of new technologies within the E-CORRIDOR project will allow to compete in the national and international arena.

Usage control methodologies and tools [CNR]	Knowledge Documents	Research	The methodologies considered in the E-CORRIDOR project will further enhance the research and development competence of the groups involved making even more competitive in the area.
Privacy preserving analytics [CNR]	Software Documents	Research	The analytics developed within the E-CORRIDOR project will sprint up the competence of the group that has the possibility to enlarge its visibility in national and international venues
Automotive security approaches (Trusted Platform Module - TPM / IDS) [FhG]	Knowledge	Industrial Training Fraunhofer Academy Courses	The Fraunhofer Academy offers specialists and managers outstanding courses of study, certificate courses and seminars based on the research activities of the Fraunhofer institutes. As the leading organisation of institutes of applied research and development in Germany, the primary objective of Fraunhofer-Gesellschaft is to improve information and technology transfer from research institutes to industry.
Machine Learning (ML) IDS techniques [FhG]	Knowledge	Lecture	Darmstadt University of Applied Sciences course
ML test toolset [FhG]	Software	Commercial	Machine learning modules for intrusion detection security analytics in the multi modal transport domain, e.g., in-vehicle IDS.
Advancing the Open Source TPM Software [FhG]	Software	Training Lectures	Advancing the development of the Open Source TPM software that can be integrated into trainings and lectures.

Contribution to Trusted Computing Group (TCG) [FhG]	Standards	Standard	Introduction of the solution to TCG, possibly resulting in a new standard.
Multi-modal transport security knowledge Transfer to SMEs [FhG]	Knowledge	Commercial	The E-CORRIDOR project will put Fraunhofer SIT in a leading position with respect to competence in multi modal transport security and will consequently open further possibilities in that domain.
Privacy-preserving analytics and security techniques [UTRC]	Knowledge Software Evaluation on the field (with ADP, and SNCF in the AT pilot) Patent applications	Research Commercial	Privacy-preserving techniques supporting enhanced passenger experience in multi-modal transportation
Advanced authentication techniques [UTRC]	Knowledge, Patent application	Research	Model-based approach for safety and security in airport authentication systems
Multi-modal Trip Planning Tool [WIT]	Software Knowledge Patent application	Research Commercial	A multi-modal trip planning tool can predict the best multi-modal travel itineraries for end-users with users' interests and preferences, carbon footprint, price, time and number of connections considered. The software will be the trip planning tool; knowledge will be the routing algorithms and data analytics methods developed. Patent application concerns the commercial application of the asset such as trip planning tool and service for commercial vehicles (e.g., taxi and truck)

Carbon Footprint Analytics [WIT]	Knowledge	Research	Carbon Footprint Analytics estimates the CO2 footprint in the multi-modal transport system, and is of great importance under the background of the European Green Deal. The research outputs here can be used to support other ITS applications and research.
Micro-subsidies platform [FACTUAL]	Software	Commercial	FACTUAL is developing a micro subsidies calculation engine which can be plugged on to any Mobility as a Service (MaaS) and Transport Service Provider platform to nudge certain type of travel behaviour, user segment or vehicle used.

2.3 E-Corridor Technology Readiness Level and Exploitation

E-CORRIDOR aims at providing a flexible, secure and privacy aware framework allowing confidential, distributed and edge enabled security services, as threat analysis and prevention as well as privacy aware seamless access mechanism in multi-modal transport systems.

The framework includes collaborative privacy-aware edge-enabled information sharing, analysis and protection as a service. The project plans to show the applicability of this framework in at least two domains: (i) collaborative and confidential cyber threat management and (ii) seamless access mechanism in multimodal transport systems.

The TRL of the finished systems will be **TRL-7**. The experience being brought by partners will be invaluable in achieving this.

The final TRL level of 7 will not be achieved until the end of the E-Corridor project. In the first year there is just a minimal integration between the work packages. Development in this phase will be focused on requirements gathering and data modelling with POC development of individual components by the various WPs

The outline of a plan to continue the exploitation process have been put in place and will be implemented in the coming years as from DoA.

In order to develop and stimulate the growth and attitude to exploitation, we will propose a series of exercises done in small groups with the aim to develop a value proposition and key testable hypotheses.

The output of this workshop will be some specific statements related to the product and market which can then be tested. As mentioned in D9.1 a testing plan will need to be developed and supported by all partners.

Specific exploitation plans will need to be further developed by each of the partners at a later stage in the project and depending on the commercial intent these should be supported by business plans (including financial projections) where appropriate.

2.4 Standardisation Overview

The E-CORRIDOR consortium aims at impacting international standardisation activities, as well as influencing domain specific initiatives on the topics relevant to E-CORRIDOR. Standardisation will facilitate technological cooperation, knowledge transfer and market take-ups of E-CORRIDOR results and innovation, therefore increasing the project impacts outside the consortium, in particular to the Industry and Society.

The initial plan for advancing standardisation activities has been defined in Deliverable 9.1. Standardisation activities are tightly coupled with the research, development, and innovation efforts within the project.

The project has been in close cooperation with existing standardisation bodies related with the project topics. The relevant standardisation possibilities of E-CORRIDOR results have been continuously monitored and reported to make the project in sync with latest standardisation progress. To provide meaningful contributions to the international standardisation landscape, E-CORRIDOR keeps evaluating the potential of turning its research and development (R&D) outputs (such as deliverables and R&D experience) into a set of localised best practices.

2.5 Standardisation Activities

This section presents information on the main standardisation organizations and activities that project partners have participated in during the last reporting period. A list of the working group(s)/committee(s) in which a partner of the consortium is a member is provided, together with a brief explanation of the specific standard or area in which a partner of the consortium is involved and the current status in that activity.

Table 7. E-CORRIDOR standardisation activities.

Standardization Organization	Description of Contribution	Status	Members
ETSI - European Telecommunications Standards Institute	Design and Development of security and privacy preserving solution for V2X	Specification and Design	FhG; CNR
TCG - Trusted Computing Group	Implementation of Feature API (FAPI) in TSS and Tools WG Attestation (co-chair) https://trustedcomputinggroup.org/work-groups/attestation/ WG Dice https://trustedcomputinggroup.org/work-groups/dice-architectures/ WG Infrastructure https://trustedcomputinggroup.org/work-groups/infrastructure/ WG Network Equipment https://trustedcomputinggroup.org/work-groups/network-equipment/	Bugfixing FAPI Co-chair in WG Attestation; Actively working in several other WGs	FhG

	WG Trusted Network Communications (TNC) https://trustedcomputinggroup.org/work-groups/trusted-network-communications/		
IETF - Internet Engineering Task Force	Operations and Management Area Working Group (opsawg) (co-chair) https://datatracker.ietf.org/wg/opsawg/about/ IOT Operations (iotops) (co-chair) https://datatracker.ietf.org/wg/iotops/about/ Remote ATtestation ProcedureS (rats) https://datatracker.ietf.org/wg/rats/about/ Software Updates for Internet of Things (suit) https://datatracker.ietf.org/wg/suit/about/ Security Automation and Continuous Monitoring (sacm) https://datatracker.ietf.org/wg/sacm/about/ Concise Binary Object Representation Maintenance and Extensions (cbor) https://datatracker.ietf.org/wg/cbor/about/ Interface to Network Security Functions (i2nsf) https://datatracker.ietf.org/wg/i2nsf/about/ Drone Remote ID Protocol (drip) https://datatracker.ietf.org/wg/drip/about/ Network Modeling (netmod) https://datatracker.ietf.org/wg/netmod/about/	Co-chair in opsawg and iotops; actively working on several documents in all mentioned WGs	FhG
C2C-CC - Car-2-Car Communication Consortium	Work Group “Security” Security Task Force “C2X PKI”	Member of WG	FhG
DKE / VDE (Electromobility)	DKE AK 353.0.8 “User authorization for charging infrastructure” https://www.dke.de/de/ueber-uns/dke-organisation-auftrag/dke-fachbereiche/dke-gremium?id=3002826&type=dke%7Cgremium	Creation of application rule	FhG
ISO/TC 22/SC 31/JWG 1 “Joint ISO/TC 22/SC 31 - IEC/TC 69 WG”	Working Group “Vehicle to grid communication interface (V2G CI)”: ISO 15118-20 https://www.iso.org/committee/5383568.html	Member of WG	FhG

3. UPDATE OF THE DATA MANAGEMENT PLAN (IF APPLICABLE)

4. Follow-up of recommendations and comments from previous review(s) (if applicable)

5. Deviations from Annex 1 (if applicable)

5.1 Deliverables

Most of the deliverables have been delivered almost on time. No major issues have been identified.

Deliverables till M12

D10.1	**Project quality handbook**	**1**	**CNR**	**Report**	**PU**	**6**
D10.2	**Risk management plan**	**1**	**CNR**	**Report**	**CO**	**6**
D2.1	**Requirements for the AT Pilot**	**2**	**ADP**	**Report**	**PU**	**6**
D3.1	**Requirements for the S2C Pilot**	**3**	**CLEM**	**Report**	**PU**	**6**
D4.1	**Requirements for the ISAC Pilot**	**4**	**MISE**	**Report**	**PU**	**6**
D5.1	**Requirements for E-CORRIDOR Architecture**	**5**	**HPE**	**Report**	**PU**	**6**
D10.3	**First periodic annual project progress report**	**1**	**CNR**	**Report**	**PU**	**12**
D2.2	**Design and Architecture for the AT Pilot**	**2**	**ADP**	**Report**	**PU**	**12**
D3.2	**Design and Architecture for the S2C Pilot**	**3**	**CLEM**	**Report**	**PU**	**12**
D4.2	**Design and Architecture for the ISAC Pilot**	**4**	**MISE**	**Report**	**PU**	**12**
D5.2	**First version of E-CORRIDOR Architecture**	**5**	**HPE**	**Report**	**PU**	**12**
D6.1	**Sharing and Analytics Infrastructures requirements**	**6**	**CNR**	**Report**	**PU**	**12**
D7.1	**Data Analytics techniques requirements**	**7**	**UTRC**	**Report**	**PU**	**12**
D8.1	**Advanced Security Services requirements**	**8**	**CEA**	**Report**	**PU**	**12**
D9.1	**First exploitation and dissemination plan**	**9**	**WIT**	**Report**	**CO**	**12**
D9.2	**First exploitation and dissemination report**	**9**	**WIT**	**Report**	**PU**	**12**

5.2 Deviations at WP level

No major technical deviations, however the pandemic hinder the contribution of several partners.

Nevertheless, pandemic influenced the effort in general, since several transport companies were forced to have less working days. Thus, in general, there is a significant underspending (~24%

in effort and ~32% in requested contribution to the EU). These figures should improve in the next period.

For WP2 for instance, ADP and SNCF could work much less than planned and partners and UTRC and UPEC complemented with additional effort being able to reach the desired technical level of results for WP2. For the future their involvement will be higher, although corrective actions should be necessary.

5.3 Deviations at Partner level

SNCF experienced an internal re-organization also due to the pandemic and thus less income at organization level and this affected the SNCF contributions.

Similarly, ADP could work much less than planned. They will likely increase their contribution now that pandemic seems over, they are extremely committed in the project and we do hope to have the final review in ADP premises.

HPE has a deviation of the actual effort against the planned effort for the time being as they have spent only 8,03 PM. That is caused by high level profile covering at higher cost tasks accomplished in less time. Over the remaining project time, effort will be realigned.

5.4 Use of resources

					E-CORRIDOR TOTAL EFFORT in DOA					
ALL BENEFICIARIES	WP10	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	TOTAL Effort in DoA
CNR	14,00	0,00	0,00	15,00	3,00	29,00	8,00	11,00	3,00	**83,00**
MISE	0,00	0,00	0,00	23,00	4,00	0,00	0,00	0,00	3,00	**30,00**
HPE	0,00	1,00	1,00	1,00	38,00	10,00	0,00	0,00	2,00	**53,00**
CEA	0,00	1,00	1,00	1,00	0,00	10,00	14,00	22,00	3,00	**52,00**
CLEM	0,00	0,00	32,00	0,00	0,00	0,00	0,00	4,00	1,00	**37,00**
ADP	0,00	36,00	0,00	0,00	10,00	0,00	0,00	4,00	3,00	**53,00**
PIL	0,00	0,00	30,00	0,00	10,00	0,00	0,00	4,00	3,00	**47,00**
UTR	0,00	17,00	0,00	0,00	6,00	0,00	27,00	25,00	3,00	**78,00**
Fraunhofer	0,00	2,00	3,00	2,00	4,00	2,00	10,00	10,00	2,00	**35,00**
PEC	0,00	7,00	0,00	0,00	0,00	0,00	21,00	6,00	3,00	**37,00**
WIT	0,00	0,00	7,00	0,00	5,00	0,00	13,00	0,00	15,00	**40,00**
DIG	0,00	0,00	0,00	8,00	3,00	0,00	0,00	0,00	4,00	**15,00**
FC	0,00	0,00	18,00	3,00	0,00	0,00	0,00	7,00	3,00	**31,00**
AMTU	0,00	0,00	9,00	1,00	0,00	0,00	0,00	0,00	3,00	**13,00**
SNCF	0,00	12,00	0,00	0,00	0,00	0,00	0,00	0,00	3,00	**15,00**
Totale Effort	**14,00**	**76,00**	**101,00**	**54,00**	**83,00**	**51,00**	**93,00**	**93,00**	**54,00**	**619,00**

Figure 12 Total effort in DoA

		E-CORRIDOR PERIOD 1								
ALL BENEFICIARIES	WP10	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	TOTAL Effort P1
CNR	4,00			3,87	1,00	10,14	3,00	3,50	1,00	**26,51**
MISE				6,75	1,39				0,63	**8,77**
HPE		0,25	0,25	0,25	5,98	1,30				**8,03**
CEA		0,42	0,42	0,42	0,00	0,74	2,13	12,20	0,48	**16,81**
CLEM			9,45					0,33		**9,78**
ADP		1,53								**1,53**
PLD			9,90		0,30				0,80	**11,00**
UTRC		10,43			1,36		8,50	3,74	0,34	**24,37**
FhG		0,60	0,58	0,55	1,02	0,62	3,97	2,83	0,40	**10,57**
PEC		3,59					5,28	1,53		**10,40**
WIT			1,50		0,50		4,00		4,25	**10,25**
DIG				1,06	3,00				0,40	**4,46**
FC			5,22	1,42				2,37	1,09	**10,10**
AMTU			2,34	0,23					0,33	**2,90**
SNCF		1,00								**1,00**
Totale Effort	**4,00**	**17,82**	**29,66**	**14,55**	**14,55**	**12,80**	**26,88**	**26,50**	**9,72**	**156,48**

Figure 13 Effort in P1

ALL BENEFICIARIES	TOTAL effort P1 (M1-M12) (WPs)	Total Effort P1 (M1-M12)/Total Effort in DoA (%)	TOTAL PLANNED effort P1 (M1-M12) (33%*Effort in DoA)	TOTAL PLANNED effort P1 (M1-M12) (%)	Deviation (WPs)	Deviation (%)
CNR	26,51	31,94%	27,67	33,33%	-1,16	-4,18%
MISE	8,77	29,23%	10,00	33,33%	-1,23	-12,30%
HPE	8,03	15,15%	17,67	33,33%	-9,64	-54,55%
CEA	16,81	32,33%	17,33	33,33%	-0,52	-3,02%
CLEM	9,78	26,43%	12,33	33,33%	-2,55	-20,70%
ADP	1,53	2,89%	17,67	33,33%	-16,14	-91,34%
PLD	11,00	23,40%	15,67	33,33%	-4,67	-29,79%
UTRC	24,37	31,24%	26,00	33,33%	-1,63	-6,27%
FhG	10,57	30,20%	11,67	33,33%	-1,10	-9,40%
PEC	10,40	28,11%	12,33	33,33%	-1,93	-15,68%
WIT	10,25	25,63%	13,33	33,33%	-3,08	-23,13%
DIG	4,46	29,73%	5,00	33,33%	-0,54	-10,80%
FC	10,10	32,58%	10,33	33,33%	-0,23	-2,26%
AMTU	2,90	22,31%	4,33	33,33%	-1,43	-33,08%
SNCF	1,00	6,67%	5,00	33,33%	-4,00	-80,00%
Total Effort	**156,48**	**25,28%**	**206,33**	**33,33%**	**-49,85**	**-24,16%**

Figure 14 Deviations from planned (ideally 1/3 of the total).

			PERCENTAGE P1 EFFORTspent/ TOTAL EFFORT							
ALL BENEFICIARIES	WP10	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	Deviation Effort P1 (by standard 33,33%)
CNR	-14,29%	-	-	-22,60%	0,00%	4,90%	12,50%	-4,55%	0,00%	**-4,18%**
MISE	-	-	-	-11,96%	4,25%	-	-	-	-37,00%	**-12,30%**
HPE	-	-25,00%	-25,00%	-25,00%	-52,79%	-61,00%	-	-	-100,00%	**-54,55%**
CEA	-	26,00%	26,00%	26,00%	-	-77,80%	-54,36%	66,36%	-52,00%	**-3,02%**
CLEM	-	-	-11,41%	-	-	-	-	-75,25%	-100,00%	**-20,70%**
ADP	-	-87,25%	-	-	-100,00%	-	-	-100,00%	-100,00%	**-91,34%**
PLD	-	-	-1,00%	-	-91,00%	-	-	-100,00%	-20,00%	**-29,79%**
UTRC	-	84,06%	-	-	-32,00%	-	-5,56%	-55,12%	-66,00%	**-6,27%**
FhG	-	-10,00%	-42,00%	-17,50%	-23,50%	-7,00%	19,10%	-15,10%	-40,00%	**-9,40%**
PEC	-	53,86%	-	-	-	-	-24,57%	-23,50%	-100,00%	**-15,68%**
WIT	-	-	-35,71%	-	-70,00%	-	-7,69%	-	-15,00%	**-23,13%**
DIG	-	-	-	-60,25%	200,00%	-	-	-	-70,00%	**-10,80%**
FC	-	-	-13,00%	42,00%	-	-	-	1,57%	9,00%	**-2,26%**
AMTU	-	-	-22,00%	-31,00%	-	-	-	-	-67,00%	**-33,08%**
SNCF	-	-75,00%	-	-	-	-	-	-	-100,00%	**-80,00%**
Total Effort	**-14,29%**	**-29,66%**	**-11,90%**	**-19,17%**	**-47,41%**	**-24,71%**	**-13,29%**	**-14,52%**	**-46,00%**	**-24,16%**

Figure 15 Percentage P1 effort spent/total

		E-CORRIDOR COSTS/EC IN P1				
ALL BENEFICIARIES	E-CORRIDOR project Total cost (in DoA)	E-CORRIDOR project Maximum grant amount	E-CORRIDOR P1 Costs declared	E-CORRIDOR P1 EC requested	Deviation in Costs(standard-33%)	Deviation in EC(standard-33%)
CNR	651.250,00	651.250,00	196.549,79	196.549,79	-9,46%	-9,46%
MISE	294.325,00	294.325,00	55.951,75	55.951,75	-42,97%	-42,97%
HPE	572.000,00	400.400,00	89.632,50	62.742,75	-52,99%	-52,99%
CEA	509.000,00	509.000,00	139.406,98	139.406,98	-17,83%	-17,83%
CLEM	347.593,75	243.315,63	59.251,46	41.476,02	-48,86%	-48,86%
ADP	492.500,00	344.750,00	26.650,00	18.655,00	-83,77%	-83,77%
PLD	348.125,00	243.687,50	100.996,30	70.697,41	-12,97%	-12,97%
UTRC	727.045,00	508.931,50	153.607,18	107.525,03	-36,62%	-36,62%
FhG	384.525,00	384.525,00	98.333,24	98.333,24	-23,28%	-23,28%
PEC	352.500,00	352.500,00	110.541,83	110.541,83	-5,92%	-5,92%
WIT	403.750,00	403.750,00	97.255,75	97.255,75	-27,74%	-27,74%
DIG	199.375,00	199.375,00	46.822,05	46.822,05	-29,55%	-29,55%
FC	283.462,50	198.423,75	74.882,00	52.417,40	-20,75%	-20,75%
AMTU	93.750,00	65.625,00	17.486,51	17.486,51	-44,04%	-20,06%
SNCF	200.000,00	200.000,00	12.500,00	12.500,00	-81,25%	-81,25%
Total	5.859.201,25	4.999.858,38	1.279.867,34	1.128.361,51	-34,47%	-32,30%

Figure 16 Cost for P1

Beneficiary Short Name	Deviation (%) in effort	Deviation (%) in cost	Deviation (%) in EC requested
CNR	-4,18%	-9,46%	-9,46%
MISE	-12,30%	-42,97%	-42,97%
HPE	-54,55%	-52,99%	-52,99%
CEA	-3,02%	-17,83%	-17,83%
CLEM	-20,70%	-48,86%	-48,86%
ADP	-91,34%	-83,77%	-83,77%
PLD	-29,79%	-12,97%	-12,97%
UTRC	-6,27%	-36,62%	-36,62%
FhG	-9,40%	-23,28%	-23,28%
PEC	-15,68%	-5,92%	-5,92%
WIT	-23,13%	-27,74%	-27,74%
DIG	-10,80%	-29,55%	-29,55%
FC	-2,26%	-20,75%	-20,75%
AMTU	-33,08%	-44,04%	-20,06%
SNCF	-80,00%	-81,25%	-81,25%
	-24,16%	**-34,47%**	**-32,30%**

Figure 17 Effort/cost deviations per partner

Beneficiary Short Name	f) Other direct costs	f) Other direct costs in DoA
CNR		23.000,00
MISE		20.000,00
HPE		23.000,00
CEA	1.098,70	38.000,00
CLEM	1.730,47	20.000,00
ADP		23.000,00
PLD	878,43	20.000,00
UTRC	13,00	23.000,00
FhG		23.000,00
PEC		23.000,00
WIT	2.564,76	23.000,00
DIG		20.000,00
FC		20.000,00
AMTU		10.000,00
SNCF		10.000,00
	6.285,36	**319.000,00**

Figure 18 Direct costs