Horizon 2020 Program
Dynamic countering of cyber-attacks
SU-ICT-2018

Cyber security 4.0: Protecting the Industrial Internet of Things

D7.6: Final Project Report[†]

Abstract: In this report we present the progress conducted in the C4IIoT project over the whole duration of the project. We describe the technical work done in all the work packages of the project, and explain how the technical objectives have been met.

Contractual Date of Delivery	31/05/2022
Actual Date of Delivery	31/05/2022
Deliverable Security Class	Public
Editor	*FORTH*
Contributors	All *C4IIoT* partners
Quality Assurance	*IBM* *UNSPMF*

[†] *The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833828.*

The *C4IIoT* Consortium

FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS	Coordinator	EL
CENTRO RICERCHE FIAT SCPA	Principal Contractor	IT
INFINEON TECHNOLOGIES AG	Principal Contractor	DE
THALES SIX GTS FRANCE SAS	Principal Contractor	FR
HEWLETT PACKARD ITALIANA SRL	Principal Contractor	IT
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	Principal Contractor	FR
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	Principal Contractor	IL
AEGIS IT RESEARCH UG	Principal Contractor	DE
UNIVERSITE PARIS I PANTHEON-SORBONNE	Principal Contractor	FR
INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP	Principal Contractor	EL
SPHYNX TECHNOLOGY SOLUTIONS AG	Principal Contractor	CH
UNIVERSITY OF NOVI SAD FACULTY OF SCIENCES	Principal Contractor	SRB
UNIVERSITY OF GREENWICH	Principal Contractor	UK
VIP MOBILE D.O.O.	Principal Contractor	SRB

Document Revisions & Quality Assurance

Internal Reviewers

1. *Gilad Ezov (IBM)*
2. *Dusan Jakovetic (UNSPMF)*

Revisions Version	Date	By	Overview
1.0.0	May 31, 2022	FORTH	Final version
0.0.9	May 26, 2022	IBM/UNSPMF	Review and quality assurance
0.0.3	May 15, 2022	FORTH	First revision
0.0.2	May 10, 2022	FORTH	Integrated input from the consortium members
0.0.1	March 20, 2022	FORTH	First draft released

Table of Contents

List of Tables

Executive Summary

This deliverable describes C4IIoT's progress, covering all work packages during the full duration of the project, more specifically from M1 to M36. In this context, this deliverable provides a report on the completed tasks and deliverables for all the work packages.

1 Detailed scientific and technical achievements during the full duration of the project

1.1 WP1 – Setting the scene: project set up

Work-package objectives:

The objectives of this work package are:

1. *To identify and demonstrate the role of C4IIoT in protecting industrial IoT systems;*
2. *To gain insight into the parameters that drive the needs for security, assurance and privacy in an IIoT system;*
3. *To identify and critical updates in terms of available tools and technologies, taken place in the period between proposal submission and project's initiation;*
4. *To design the architecture of the C4IIoT integrated platform*
5. *To describe the C4IIoT demonstration protocol*

Progress:

WP1 reached its end with the completion and submission of Deliverable D1.1, Deliverable D1.2, and Deliverable D1.3. This marked the end of the preliminary phase of the project, as all preliminary requirement elucidation and design work were completed in conjunction with the successful submission of Deliverable D6.2 at M4. This in turn shone light on the task at hand and also served as a guide for the subsequent work carried out in the other WPs. In sum, all of the above objectives were completed, and the project was able to successfully start and commence work on all other tasks of all other WPs.

Partner Contributions:

- **FORTH** sent input for Deliverable D1.2 and Deliverable D1.3. For Deliverable D1.2, FORTH contributed to Section 3.7 which describes threats and vulnerabilities that may occur in the "Smart Factory" and "Inbound Logistics" use cases and more specifically the sections about "Violation of rules and regulations / Breach of legislation / Abuse of personal data" and "Failure to meet contractual requirements". For Deliverable D1.3, FORTH contributed in Section 2.1 by presenting the overview of the architecture and how the modules connect with each other. In Section 2.5.1 and 2.5.2, FORTH described the modules for the behavioural analysis & cognitive security and traffic analysis, their requirements and how they communicate with the rest of the consortium tools. In Section 7, FORTH described the security aspects of the project, level-by-level: Level 1 – Hardware-Enabled Security, Level 2 – Security by horizontal device-to-device communication, Level 3 – Security by ML-based behavioral analysis & cognitive security capabilities.
- **IBM** contributed to Deliverable D1.1 and provided a section called "Decentralized selective access management" with a SotA review for the decentralized selective access management domain. IBM has participated in Task 1.3, contributing to the definition of the C4IIoT architecture and the architecture of the decentralized access control solution, as part of Deliverable D1.3. IBM has also been a reviewer for Deliverable D1.2.
- **UOG** lead Task 1.2 (titled "Adapting C4IIoT security components to real-life industrial manufacturing environments") and Deliverable D1.2 (titled "Positioning of C4IIoT"), as detailed below. UOG also contributed to Task 1.3 (titled "Technology convergence:

specifications and C4IIoT architecture") and Deliverable D1.3 (titled "Architecture definition"), and especially to the section relevant to the dynamic security-aware offloading decision support component of the architecture and its technical requirements. Finally, UOG contributed to Task 1.1. (titled "The critical role of C4IIoT in protecting Industrial IoT systems and technologies") and Deliverable D1.1 (titled "C4IIoT innovations for Industrial IoT systems"), and especially in Section 9 of the report, by summarizing the significant new research results and new commercial products that have been published or released on the market, since the submission of the project proposal in August 2018, in the technological areas of security-aware offloading decision support.

- **A1** provided contributions regarding Deliverable D1.1 by writing the introductory section and provided analysis about the edge nodes and the field gateway deployment in scope of Deliverable D1.2. A1 also helped in refining the field gateway layer architecture and technical prerequisites for its implementation as part of the architecture definition in Deliverable D1.3, as well as providing insights into deployment of secure communication infrastructure.

- **STS** participated in Task 1.1 (titled "The critical role of C4IIoT in protecting Industrial IoT systems and technologies") and, more specifically, the update of the literature review that was carried out in the context of this task, updating on the cybersecurity and privacy technologies adopted in the Industrial IoT context that were identified at the proposal phase. Of specific focus for STS were the state-of-the-art developments on Vulnerability analysis and mitigation, which were documented in Deliverable D1.1 (titled "C4IIoT Innovations for Industrial IoT Systems"). Moreover, in the context of Task 1.3 (titled "Technology convergence: specifications and C4IIoT architecture"), STS provided its description of the assurance platform components that is integrated into the C4IIoT solution, providing input to Deliverable D1.3 (titled "Architecture definition"). Said aspects where also discussed extensively with partners whose components interact with said assurance platform to refine the static and dynamic architecture of the framework.

- **ITML**'s technical achievements for this reporting period include contributions to the definition of the demonstration protocol (execution parameters, plan and processes) within Deliverable D1.2 (titled "Positioning of C4IIoT") and the description of Privacy aware, Trustworthy Data & Analytics modules within Deliverable D1.3 (titled "Architecture definition"). ITML also provided its contribution regarding Deliverable D1.1 (titled "C4IIoT innovations for Industrial IoT systems"). ITML also reviewed Deliverable D1.1 (titled "C4IIoT innovations for Industrial IoT systems").

- **IFAG** contributed in this WP in the definition of the C4IIoT architecture, focusing on Level-1 ("Hardware enabled security"); this contribution is reflected in Deliverable D1.3. Regarding Deliverable D1.2, IFAG contributed in the specification of edge nodes, while for Deliverable D1.1, IFAG contributed in the review of state-of-the-art approaches.

- **CRF** has provided a description of the industrial security challenges, as well as a detailed description of the pilots with scenarios and narratives. CRF has also described all the assets involved, potential threats and their mappings in the FCA environment. Finally, CRF has provided an initial demonstration protocol with all experimentation variables (e.g. validation methodology, KPIs and benchmarks, actors, time plan) and a detailed description of the two use cases (namely "Smart Factory" and "Inbound Logistics") that will be used to evaluate the C4IIoT framework.

- **TSG** contributed to the Deliverable D1.1 by writing the section on “Encrypted traffic analysis”.
- **CEA** contributed to Task 1.1 and Deliverable D1.1 and to the architecture definition in Task 1.3 and Deliverable D1.3, regarding the use and interface of the BINSEC analyser. Finally, it coordinated the work of Task 1.4 on the demonstration protocol, which resulted to Section 4 of Deliverable D1.2.
- **UP1PS** led this WP, as well as Task 1.1 and Deliverable D1.1. It also made contributions to sections of Deliverable D1.1 and Deliverable D1.3.
- **UNSPMF** led Task 1.3 and Deliverable D1.3 and contributed to sections of Deliverable D1.2 and Deliverable D1.3.
- **HPE** actively participated to the virtual meetings and made contributions to Deliverable D1.1, Deliverable D1.2, and Deliverable D1.3.
- **AEGIS** contributed to Deliverable D1.1 (titled “C4IIoT Innovations for Industrial IoT Systems”), by presenting the state-of-the-art on research advances and innovations about forensics visualizations since the C4IIoT proposal submission. AEGIS also participated in telcos and sent input for Deliverable D1.2 (titled “Positioning of C4IIoT”) and more specifically for the “Threats and vulnerabilities” section. AEGIS also participated in telcos and sent input for Deliverable D1.3 (titled “Architecture definition”), about the User Interface section and the integration of Advanced Visualisation Toolkit.

Progress per Task:

Task1.1. The critical role of C4IIoT in protecting Industrial IoT systems and technologies:

This task was concerned with performing a detailed literature review on cybersecurity and privacy technologies, as adopted in the IIoT context, not only for the automotive industry but also for the EU digital economy such that we could ascertain the adequacy and innovation of the aims and objectives of the C4IIoT and that of those of the individual tools that compose the project. This was done through the identification and subsequent communication to the relevant partners of anything (in technological or methodological terms) that may have been subject to change between the submission of the project and the commencement of the work for the C4IIoT project. This task came to completion with the submission of Deliverable D1.1, at M4.

Task1.2. Adapting C4IIoT security components to real-life industrial manufacturing environments:

The outcome of Task 1.2 was part of the Deliverable D1.2 which identified and described the critical assets that need to be protected in Industry 4.0, mapping them to the real-life industrial manufacturing environment, provided by the use-case partner CRF. It also provided the most common and important security threats in such an environment, mapping them to each of the assets and assessing the impact that each attack could have. Initial high-level user requirements were provided and mapped to the C4IIoT components, that were used to define the two pilot scenarios of C4IIoT and also the C4IIoT architecture in Deliverable D1.3.

Task1.3. Technology convergence: specifications and C4IIoT architecture:

The high-level software, hardware and networking distributed architecture of the C4IIoT framework and their relationships with FCA’s environment has been specified and submitted in Deliverable D1.3.

Task1.4. Demonstration protocol – real life industrial pilots:
This task was used to specify the demonstration protocol and their use in the automotive pilots use cases, in many dimensions. In particular, the task helped to clarify the pilots use cases, identified the cybersecurity requirements that can address the industrial challenges faced by the pilots, identified the relevant benchmarks, standards, and key performance indicators that could be used to measure the success of the C4IIoT solution, specified the edge node and field gateway and proposed a deployment plan, and proposed a validation plan used to verify the effectiveness of the demonstrators. The results of this work are integrated into Deliverable D1.2. This task also produced a document on the validation the requirements by external stakeholders from various industrial/manufacturing domains. It was created as an extension of D1.2, as a result of the mid-term review.

Deliverables:

D1.1. C4IIoT innovations for Industrial IoT systems:
Deliverable D1.1 is an up-to-date state-of-the-art summary on cybersecurity technologies applied to IIoT systems. Its approach hinged on the analysis of the current state of technology (and its industrial and commercial offerings) in each of the different technological areas that the project targets. This was done with the aim of ensuring the alignment of the technology both being used and being built with the current state of affairs in technology.

D1.2. Positioning of C4IIoT:
Deliverable D1.2 is a confidential deliverable on how C4IIoT positions in the Industry 4.0 environment. We identified and classified fundamental CRF assets that need to be protected and corresponding threats and vulnerabilities. We also mapped the assets to threats, denoted their criticality and suggested the nature of impact that is most likely in each case, considering both cyber and physical impact. The deliverable also provided the initial description of C4IIoT's two pilot scenarios: namely "Smart Factory" and "Inbound Logistics". The findings in Deliverable D1.2 were used as a starting point and feed to Task 5.1 (titled "Demonstration protocol alignment"). Deliverable D1.2 also serves as a reference, to identify the attacks that will be used to evaluate the C4IIoT framework, setting the base for defining the threat model (which needs to provide protection from at least 10 real-world threats [KPI-1.6]).

D1.3. Architecture definition:
Architecture definition delivered on M6 included a specification of deployment layers, functional components and the data and control flow between; it also specified the choice of component integration and deployment technologies: Docker containers communicating through REST API and orchestrated on the cloud through Kubernetes, supporting seamless continuous integration and scalability.

Milestones:

- ***MS1:* *C4IIoT set-up: Requirements, initial architecture and preliminary business models (M6)***
  This milestone was successfully reached at M6 with the submission of Deliverable D1.1, Deliverable D1.2, Deliverable D1.3 and Deliverable D6.2 from WP6, which denoted the successful completion of the preliminary activities for the project.

1.2 WP2 – Edge computing cybersecurity technologies

Work-package objectives:
The objectives of this work package are:

1. *To ensure proper provision, configuration, and management of edge-node assets, including IIoT (sensors) devices and network elements (field gateways);*
2. *To ensure that machine learning methods that perform detection of complex anomalous and malicious behavior are implemented in a distributed way;*
3. *To design and implement the mechanisms needed to dynamically offload security-aware tasks at the edge;*
4. *To build the tools and technologies for providing a secure execution environment for the edge IoT devices.*

Progress:

WP2 reached its end in M30 with the completion and submission of Deliverable D2.4. Apart of this deliverable, the work carried out within this WP was delivered in the following deliverables: Deliverable D2.1 in M6, Deliverable D2.2 in M12 and Deliverable D2.3 in M18. With the achievement of these deliverables, the work developed in this WP ends in the different tasks carried out. On the one hand, in relation to Task T2.1, a configuration and management environment for IoT nodes has been developed. In Task T2.2, machine learning algorithms operating at the edge node level have been designed and developed in combination with other tools in upper levels of the architecture. Dynamic offloading decision mechanism has been developed in Task T2.3, specifically the MEDICI tool. Finally, in Task T2.4, all the hardware security mechanism providing an additional hardware security layer was developed. In summary, all the objectives of this WP have been met during the completion of these tasks and the results have been captured in the corresponding deliverables.

Partner Contributions:

- **FORTH** participated in the discussions and all the relevant telcos for WP2. FORTH worked in the traffic analysis module by adding more malicious datasets that can be used to detect more attacks and different types of threats. The traffic analysis module is described in Deliverable D2.2 and included figures demonstrating on how it works. FORTH as the deliverable leader for Deliverable D2.3, orchestrated the work and efforts and also provided input regarding secure computations at the edge and analysis of encrypted traffic. Finally, FORTH has worked on the specification of a framework that provides secure enclaves for the Android OS, described in Deliverable D2.4.
- **UOG** lead Task 2.3 (Security-aware dynamic offloading decision mechanism) and Deliverable D2.2 (Deep learning breakthroughs and security-aware dynamic offloading mechanisms) and contributed to Task 2.2 (Deep learning trained models deployed at the edge) and Task 2.4 (Security and trustworthiness at the edge) and their corresponding deliverables, on sections relevant to the C4IIoT architecture and the integration of the security aware offloading module with the anomaly detection modules at the cloud and the field gateway.
- **A1** participated in all of discussions and telcos related to WP2. As deliverable leader coordinated the work and contributions for deliverable D2.1 which was Edge node assets requirements and gap analysis, the design of a novel architecture and test and evaluation scenarios specification. Provided hardware and configured the virtual machine for Field Gateway realization inside of mobile operator infrastructure. For D2.4 contributions for Logistic case testing and evaluation environment. A1 was also coordinating inputs from IFAG and UNSPMF regarding testing and evaluation (Section 6) for deliverable D2.3.

- **ITML** in the framework of WP2 contributed to Task2.2 ("Deep learning trained models deployed at the edge) by enabling that the machine learning methods that perform detection of anomalous behavior can be implemented in a distributed way. Additionally, ITML contributed to Task 2.3 ("Security-aware dynamic offloading decision mechanism"). In this task, C4IIoT partners designed and implemented mechanisms needed to dynamically offload security – aware tasks at the edge. Last but not least, ITML also contributed to the relative deliverables connected to the above-mentioned tasks.
- **IFAG** contributed in Deliverable D2.1 in section 2.1: Edge node requirements for smart factory use case, in section 4.1: C4IIoT edge node solution in smart factory use case, section and in section 5.1: Testing in real-world environment. In this deliverable IFAG design a smart factory use case edge node based in the requirements provided by CRF on the existing edge nodes. Also providing, together with CRF, a real test environment for these nodes. In Deliverable D2.2, IFAG contributes in the section 2.4: Secure hardware support tools providing different hardware mechanisms that supports cryptographically the software algorithms implemented. In Deliverable D2.3, IFAG contributes in the incorporation of secure hardware elements, both OPTIGA TPM and OPTIGA Trust M. These components are explained in detail in deliverable D2.4, where they are described in detail as well as the IoT architecture where they are used. In summary, main contribution in the WP is the analysis, design and developed of a Smart factory edge node adding hardware secure elements in this use case as well as in the Logistics4.0 use case.
- **CRF** has actively participated to the discussion and relevant telcos for WP2. Moreover, CRF has provided the specific requirements for the C4IIoT edge nodes to be located on containers and production systems. Finally, CRF has contributed to the related deliverables connected to the activities mentioned above.
- **CEA** in this work package, CEA mainly worked on integration of the software mitigation engine for automated low-level security analysis of the software developed for the edge layer; notably we performed incremental and targeted analysis of the BACSC component.
- **UNSPMF** Development of machine learning methods that within the software component BACS related to the edge node layer of the C4IIoT architecture. Development and production of novel edge node devices used for the Logistics 4.0 use case. Testing and validation of produced devices and methods implemented within the BACS component. Task 2.2 leadership. Contributions in writing of deliverables.
- **TSG** provided a review of the D2.4 deliverable.

Progress per Task:

Task2.1. Provision, configuration and management of edge-node assets:

This task was led by A1 with contributions from CRF, IFAG and UNSPMF and it was planned and realized in months 4-30. Provisioning, configuration, and management of Edge node assets and Field Gateways were focus of this task. Requirements specification and the design of Logistic case Edge node were joint effort of UNSPMF and A1 in support role.

For the Smart factory use case the fully featured IFAG's Edge node based on Raspberry Pi platform integrated with IFAG OPTIGA™ TPM 2.0 security chip was designed and fabricated. It was shipped to CRF Campus Melfi for integration, testing, and real-life demonstration.

For the Logistic 4.0 scenario, fifty custom designed edge nodes were fabricated and provisioned with test SIM cards provided by A1. Edge nodes equipped with NBIoT communication modules were initially tested in a limited scale trial, where five edge nodes were attached to delivery containers and driven in five vehicles around the city of Novi Sad. Preliminary tests with CRF logistics fleet were performed using devices and collecting data around city of Torino. The tests were successful; however, the edge device battery was exhausted after a few days.

Based on the results of these initial trials fine tuning of several edge devices was performed (e.g. data payload format changed from JSON to binary to reduce the overhead, better management of idle mode etc.) in order to prolong the edge node battery lifetime.

Finally, a more thorough field trials are ongoing using 20 edge nodes attached to the containers located in the CRF logistics fleet trucks. The round-trip route is Torino-Budapest-Torino tracking and monitoring the vibration of the shipping containers and other environmental parameters. This was done in scope of real-life demonstrator described in deliverable D5.2.

Task2.2. Deep learning trained models deployed at the edge:

This task was led by UNSPMF with contributions from FORTH, IFAG, ITML and UOG. The task started in M6 and ended in M30. Within the task, we implemented various methods of machine learning, running at the edge, capable of detecting complex anomalous and malicious behavior in order to protect industrial systems.

Edge protection is implemented with the help of artificial intelligence within the Behavioral Analysis and Cognitive Security (BACS) component. BACS is a software component that offers anomaly detection in IIoT sensory data and network traffic flows based on machine learning and deep learning algorithms. It includes unsupervised and supervised machine learning schemes and packages that extend through all three layers of the C4IIoT architecture.

BACS autoencoders for the Smart Factory use case C4IIoT edge nodes are implemented in Python using the Tensorflow2 library. The implementation of a stand-alone auto-encoder trains the model by minimizing the mean square error using the ADAM - a stochastic first order gradient descent method.

Edge-based microcontrollers with the Logistics 4.0 use case are low-power devices that use narrowband IoT (NB-IoT) for communication. In this case, BACS implements routines that perform anomaly detection for a given data point on a pre-trained model with lightweight auto-encoders. They are lightweight in the sense that these auto-encoders have exactly one hidden layer. The implementation was performed in C without the use of external libraries and was integrated into the firmware of edge node devices designed and manufactured within this task. The training was done offline, so the firmware contains pre-trained models ready for inference.

In February 2021, the design and production of 50 innovative edge node microcontroller devices for the use within the Logistics 4.0 has been completed at UNSPMF. The first tests of these devices resulted in new data sets useful for further development and testing. In the later stages of the project, final testing was performed in a real-world environment as part of WP5.

The final steps in Task 2.2 were closely related to the exploitation of 50 new microcontrollers - edge node devices manufactured within the task. Initial meetings were held with the CRF where an initial plan was devised. Bearing in mind that another partner in the project – A1, a mobile network operator, controls the coverage of NB-IoT in Serbia, the first demonstration was done there. Subsequently, a limited number of devices (20 pieces) were sent to Italy to begin preparations for the final demonstration held under WP5.

In addition, in the Smart Factory use case, the models were deployed on Raspberry Pi devices at the edge in collaboration with IFAG and ITML. As in the Logistics 4.0 use case, the final testing was done within WP5.

Task2.3. Security-aware dynamic offloading decision mechanism:
Task 2.3 produced a security-aware offloading mechanism which enhanced the BACS anomaly detection capabilities by dynamically deciding which BACS model to be triggered at the Field Gateway or the cloud, when the confidence of the detection performed at the edge is low. The C4IIoT security-aware dynamic offloading decision module extended UOG's existing MulticritEria DecIsion support meChanism for IoT offloading (MEDICI) in the form of a Java service provision with Kafka support and network agent software for capturing historical data. In terms of decision making, its modular design allows for flexibility in the choice of algorithms. The decision mechanism has the following broad logic: Using statistical techniques, it predicts the processing time and networks delays for a task to be executed at a given device based on historical data. It then uses a combinatory goal metric for each offloading destination containing both the total detection latency (processing time + network delays) and the detection accuracy and chooses the destination with the smallest goal.
To evaluate the efficiency of our MEDICI tool, we used metrics such as detection latency and detection accuracy which were compared against the hierarchical anomaly detection scheme of executing a BACS detection first at the edge layer and moving to higher layers if the detection confidence is not high enough. We also compared it to the cases of not having the offloading mechanism; one where the BACS at the FG is always triggered and one where the BACS at the cloud is always triggered. The final version of the tool is currently being deployed in the final deployment environment.

Task2.4. Security and trustworthiness at the edge:
The outcome of this task was the Deliverable D2.4, which describes all the components developed in the edge nodes. During the task, hardware secure elements and trusted execution environment were developed in the edge nodes. In relation with the hardware secure elements used, IFAG provides blockchain2go cards in order to offer personal authentication in the smart factory edge nodes. In this use case, the main contribution is the use of the Infineon OPTIGA TPM2.0 as a hardware wallet for the blockchain network implemented in other WPs. In the Logistcs4.0, IFAG provides the OPTIGA Trust M offering cryptographic algorithms for non-operating system platform. In relation with the trusted execution environment, FORTH provides a framework called Andromeda based on Intel SGX. In addition, CEA extends the BINSEC tool for automating low-level security analysis, applying in to BACS tool, developed in the Task 2.2.

Deliverables:

D2.1. Analysis of edge-node assets
In scope of this deliverable there were several areas covered: defining requirements for edge node devices, performing gap analysis with existing CRF devices, and proposal for edge node design. Both "Smart Factory" and "Inbound Logistics" use cases were considered since they required different approaches. As a result, detailed requirements suited for design of beyond the state-of-the-art edge nodes were created as well as simulation framework for testing them. Deliverable was submitted on time, at M6.

D2.2. Deep learning breakthroughs and security-aware dynamic offloading mechanisms
This deliverable was a demonstrator deliverable. It described the components involved in Task 2.2 and Task 2.3 and their implementation up to month 12 and their operation as individual components. Their integration was described in Deliverable D4.2 through the MVP description.

D2.3. Level-1 security mechanism of C4IIoT: Hardware-enabled security

This deliverable describes the hardware security mechanisms of the edge nodes layer of C4IIoT. In essence, they provide support to securely store keys and enable data security, device trust and compliance requirements. Moreover, they can be used as interconnected modules to implement functional blocks for establishing and managing device identity, maintaining end-to-end data security and integrity and interfacing with other C4IIoT layers, such as the PKI/CA that has been deployed at Level-2/3 to serve certificates for several needs (e.g., identity provider and TLS connections). C4IIoT also enables AI-driven cyber threat detection at the edge to enable anomaly detection and encrypted traffic analysis, as well as code verification techniques on the executables that run on the edge devices.

D2.4 : Security and trustworthiness at the edge
This deliverable describes the hardware and software security mechanism deployed at the edge level. Summarizing, it explains the hardware and software component used in the edge nodes. In addition, we explain software mechanisms that are in strong relation with the level 2 of the architecture (Field Gateway), such as anomaly detection and behavioural analysis. Finally, we describe all the deployed components in a demonstration setup.

Milestones:

- ***MS2*: *Proof of concept through C4IIoT MVP (M12)***
  Tools developed in the WP2 as the BACS (edge and field gateway) and MEDICI were deployed in the MVP.
- ***MS3*: *Version of Integrated platform and of C4IIoT Level-1, Level-2 and Level-3 security; initial execution of demonstrators (M18)***
  Milestone was reached with an initial integration between tools developed in the WP2 on MVP Infrastructure.

1.3 WP3 – Cyber assurance and protection in an industrial cloud infrastructure

Work-package objectives:

The objectives of this work package are:

1. *To ensure the provision and configuration process of infrastructure resources through efficient resource management and orchestration for Cloud (Core) infrastructure;*
2. *To develop the C4IIoT core of Level-3 security mechanism which consists of the development of behavioural models that will enable the analysis of the behaviour of multiple IoT devices;*
3. *To develop mitigation and immune reaction mechanisms across different layers; To design and develop the building components composing the C4IIoT trust infrastructure.*

Progress:

WP3 and its four tasks finished on M30 as planned. Work for components, designed and developed in WP3, is continued in WP4 and WP5 for final integration. WP3 focused on Cloud Layer part of the framework and on the components and technologies as described in D3.4. During the course of the project, WP3 partners contributed to submission of four deliverables D3.1 and D3.2 at M12, D3.3 at M18 and D3.4 at M30. For WP3 management and integration we established to have a by-weekly WP virtual meeting for all WP3 duration.

Partner Contributions:

- **HPE** contributed to this WP with management and leading task 3.1. HPE developed the components of Task T3.1 (Cloud Gateway), integrated the software Harbor, EJBCA. HPE gave support to k8s containerization and EJBCA PKI certificates. HPE contributed to the all WP3 deliverables and managed preparation and integration of partners contribution to the deliverable D3.4.
- **FORTH** participated in the discussions and all the relevant telcos. In addition, FORTH conducted preliminary exploration on how to use the Intel SGX technology for privacy-preserving data analysis in the cloud. FORTH contributed the section "Raising security and privacy-awareness using Intel SGX" for Deliverable D3.1. FORTH offered input for Deliverable D3.3 regarding the traffic analysis and the detection of threats in network traffic, demonstrating how two different types of attacks will be discovered and reported to the corresponding modules. FORTH with UNSPMF have worked on the integration of a BACS module within a Docker container which run on a TEE supported by Intel SGX that allows the processing of sensitive data (in a privacy-preserving way) in third-party clouds that may not considered trusted. The full implementation details of this privacy- preserving data processing module, is described in Deliverable D3.4.
- **IBM** has led Task 3.4 which has started in M6 and ended in M30. IBM has worked on designing the architecture of its decentralized access control solution, in coordination with the other C4IIoT partners. IBM has put efforts to consider the interactions of the access control solution with other components in the project. IBM has made progress in implementing a prototype of its decentralized access control solution that was deployed and integrated in C4IIoT's first complete prototype (M18) and utilized Attribute-Based Encryption and the Hyperledger Fabric technology. IBM then continued to develop its solution and integrated a second Blockchain technology: the Blockchain Database, to be used in C4IIoT's logistics use-case side by side with Hyperledger Fabric for the smart factory use-case. IBM performed internal review for Deliverables D3.1 and D3.4. IBM

led Deliverable D3.3, circulated Deliverable D3.3 ToC, initiated a first and a second rounds of contributions to Deliverable D3.3 by all WP3 partners, contributed to Deliverable D3.3 providing a chapter on its decentralized access control and distributed ledger, integrated the contributions made by all the relevant partners into a final draft, addressed comments made by the reviewers and issued a final version of Deliverable D3.3. IBM contributed to deliverable D3.4, containing the most recent report about its decentralized access control solution and updates made to it since D3.3. IBM participated in the discussion and all the relevant telcos for WP3.

- **ITML** in the framework of WP3 contributed to Task3.1 ("Resource management and orchestration"), Task 3.2 ("Behavioural analysis and cognitive security framework"), Task3.4 ("Trustworthiness of data flows") as well as to the related deliverables for the above-mentioned tasks. Specifically, ITML dealt with the provision and configuration of infrastructure resources and the contribution to the development of the core of Level-3 security mechanism and mitigation and immune reaction mechanisms across different layers.

- **IFAG** contributed in the telcos carried out during the development of the WP. IFAG main contribution was the integration of the Infineon OPTIGA TPM2.0 with the blockchain network, Hyperledger Fabric, provided by IBM. The contribution was set out in the Deliverable D3.3 and in Deliverable D3.4 in section: distributed ledger integration with Infineon's secure element.

- **TSG** contributed to the WP3 work package by implementing the SDN controller used by the WP3 Mitigation Engine. A specific intent-based API was created to interface with CARMAS and provide an entry point for the mitigation at the network level. TSG also handled the configuration of the OVS switches used in the C4IIoT network. With the end-review in mind, TSG explored the possible adaptation of the SDN controller and its underlying OVS technologies to a Windows based architecture. For the demonstration, TSG prepared some targets and attacker components. TSG provided inputs in the D3.2 deliverable for the DISCO the SDN controller on its architecture, interfaces, actions and role in the Mitigation Engine. TSG provided inputs in the D3.3 deliverable on the integration of the SDN controller with other partners components to create the project Mitigation Engine. For the D3.4 deliverable, TSG provided the inputs for the delta on the SDN architecture relative to the D3.3.

- **CEA** has developed the software mitigation part of the mitigation engine, based on its BINSEC component, which was coupled with AFL to obtain a patch-oriented vulnerability detection tool, whose description was published at RAID 2020. Several enhancements were made, such that the x86-64 bit architecture support, and the import from the Ghidra tool developed by NSA to facilitate integration (WP4) and deployment (WP5). In addition, CEA has led the main task concerning the mitigation engine, which is T3.3.

- **UP1PS** contributed primarily within the context of task 3.3 and all its associated deliverables. It contributed to the overall architecture and design of the Mitigation Engine, and its interaction with other project components, in concert with project partners. Furthermore, it developed, tested, and delivered the CARMAS tool (which replaced VariaMos), a knowledge-based reasoning tool to determine corrective actions (mitigations) to attacks that occur at runtime in the system.

- **UNSPMF** Development of machine learning methods that within the software component BACS related to the field gateway and the cloud layers of the C4IIoT architecture. Integration of BACS with the MEDICI component. Testing and validation of anomaly detection methods implemented within the BACS component. Task 3.2 leadership. Contributions in writing of deliverables.

Progress per Task:

Task3.1. Resource management and orchestration:

Task 3.1 has worked on deployment, configuration and integration of the Cloud Layers components with this specific focus: (i) setting the security policies and controls to securely managing the Docker container images with the implementation of a Harbor Private Registry with these functionalities: setup of repositories with different rules (External access, Vulnerability scanning and Image signing), the load of C4IIoT generated docker images: BACS, ES_Connector, and the load of public images (for Vulnerability scanning); (ii) support for partners applications moving to k8s containers (image and manifests); (iii) development and refinement of the prototype for Cloud Gateway to provide network isolation of the modules inside the Cloud Layer and enforce network traffic encryption via HTTPS for all external communications; and (iv) installation of EJBCA CA PKI platform for access identity purposes and certificates management and its integration with the other components DAC and KAFKA. The work was initially executed in an internal laboratory and then moved on systems made available from partners (ITML and CRF).

Task3.2. Behavioural analysis and cognitive security framework:

Task 3.2 was led by UNSPMF with contributions from FORTH, HPE and ITML. The task started in M4 and ended in M30. Within the task, we implemented various methods of machine learning, capable of detecting complex anomalous and malicious behavior to protect industrial systems.

The main goal of this task was to develop the core Level-3 security mechanism, which consists of the development of behavioral models that enable the analysis of the behavior of multiple IoT devices. These functionalities were developed within the software component BACS (Behavioral Analysis & Cognitive Security Framework).

The Behavioral Analysis and Cognitive Security (BACS) component is part of the C4IIoT framework, which implements the detection of anomalies and deviations and protection mechanisms implemented using artificial intelligence methods. BACS consists of three main packages: BACS Cloud Layer (BACSCL), BACSPY and BACSC. BACSC is a lightweight anomaly detection software implemented in C that is used for low processing power devices on the edge. The BACSC package detects anomalies only at the edge node layer in the Logistics 4.0 use case and belongs to the level 1 security mechanisms. A detailed description can be found in deliverables 2.2 and 3.2. BACSPY contains the implementation of various traditional methods of detecting machine learning anomalies implemented in Python: algorithms for outlier detection, classification and representation applied to multivariate time series. BACSCL includes various anomaly detection methods developed to be used within the cloud - deep autoencoders, GRU (Gated Recurrent Unit) and LSTM (Long Short Term Memory) RNNs (recurrent neural networks) and Facebook Prophet - an advanced tool for time series analysis. The goal of BACS is to implement a set of algorithms with different unsupervised and supervised anomaly detection models. The algorithms are designed to work in a uniform way with a common interface to be compatible with the rest of the platform. A detailed description of the development stages can be found in deliverable 3.3.

The final phase of this task was related to the development of supervised learning methods for detecting anomalies based on labeled data sets. Quality labelled datasets for these purposes have proven to be a serious problem to acquire. On one hand, experiments were performed with data sets that are available for free on the Internet, while on the other hand, the use case provider, CRF, provided some labelled data sets. The indicated data sets were used for training of

implemented models, but also for validation of results of already applied unsupervised detection methods.
Integration with the MEDICI component for offloading data is also an integral part of this task. In cooperation with UOG, we implemented metrics for applied machine learning methods, which MEDICI uses to make higher quality decisions.

Task3.3. Mitigation engine:
The task was concerned with the development of the mitigation engine. Three main components were developed as part of the engine. The software mitigation is provided by BINSEC, in which a patch-oriented engine coupling BINSEC with AFL was developed. The network mitigation is provided by the DISCO SDN controller, which was extended with a new API to allow network mitigation. This mitigation is coordinated by CARMAS (formerly called Variamos), which was extended with an Ontology based on the STS security assurance module. All the components were also integrated with the Advanced Vizualisation Toolkit by AEGIS.

Task3.4. Trustworthiness of data flows:
As part of Task 3.4, a decentralized access control solution was developed, allowing to restrict access to data (at transport and at rest) using privacy-aware policies, enable auditability of events and access policies and assure the integrity of data in C4IIoT. This solution utilizes distributed ledger technologies (Blockchain) and attribute-based encryption technologies. C4IIoT's first prototype of M18 included the Hyperledger Fabric as the underlying Blockchain technology, while the final version of C4IIoT also includes a second technology: the Blockchain Database which was deployed as part of the logistics use-case. Other activities done as part of Task 3.4 include provisioning of secure elements in the edge nodes that can interact with the Hyperledger Fabric channel, and development of analytics for encrypted traffic. Integration efforts between the secure element and the decentralized access control solution were made and the interaction between the two was successfully tested. The outputs of this task were demonstrated in deliverables D3.3 (M18) and D3.4 (M30).

Deliverables:

D3.1. Behavioural analysis and cognitive security framework
This deliverable has been submitted at the end of M12. It provides a refined specification and description of current version of the Behavioural Analysis & Cognitive Security Framework (BACS) – a framework consisting of behavioural models that enable the analysis of the behaviour of multiple IoT devices. Deliverable describes solutions for building, deploying and managing heterogeneous hybrid cloud environments, with a set of technologies able to handle various platforms. Finally, the deliverable includes description of Intel SGX instructions that BACS behavioural models will use for increased security and privacy-awareness.

D3.2. Mitigation engine
This deliverable, providing the design and first results of the mitigation engine development and summarizing the work of Task3.3 for the first year of the project.

D3.3. Level-2 and Level-3 security mechanisms of C4IIoT
Deliverable D3.3 (submitted at M18) was an output of all WP3 tasks and has provided details and demonstration of the technologies that form the Level-2 and Level-3 Security Mechanisms of C4IIoT. The deliverable described the identity management solution, the decentralized access control and distributed ledger, the secure element and its integration with the blockchain, the behavioral analysis and cognitive security module (BACS), the traffic analysis technology, the mitigation engine and the privacy-aware trustworthy data and analytics (data fusion bus)

technology. The deliverable was a demonstrator one, and included demonstration of the various technologies mentioned above in their version of M18, that was also deployed as part of the C4IIoT first complete prototype.

D3.4. Cyber assurance and protection in an industrial cloud infrastructure
This deliverable, submitted at M30, presents the output of all tasks of WP3 including all the updates and enhancement related to the components, realized during WP3 work, with regards to previous deliverables (D3.1, D3.2, D3.2).
The components treated in this deliverable, for the Cloud Layer, are: Cloud Layer Orchestrator, Behavioral Analysis and Cognitive Security, Mitigation Engine, CARMAS, BINSEC, Decentralized Access Control and Blockchain Technologies, Privacy Aware Trustworthy Data & Analytics and Security Assurance.

Milestones:

- ***MS2*: *Proof of concept through C4IIoT MVP (M12)***
  BACS Cloud tool was included in the MVP at M12.

- ***MS3*: *Version of Integrated platform and of C4IIoT Level-1, Level-2 and Level-3 security; initial execution of demonstrators (M18)***
  Milestone was reached as a result of an initial integration between tools developed in the WP3 on MVP Infrastructure.

1.4 WP4 – An end-to-end integrated industrial IoT cybersecurity framework

Work-package objectives:
The objectives of this work package are:

1. *To design and develop services for designing, implementing and integrating an identity management solution to address the IIoT challenges of C4IIoT;*
2. *To implement the interactive visualization and monitoring toolkit for C4IIoT data and analytics;*
3. *To implement and deploy the integrated C4IIoT framework that realizes the envisioned C4IIoT technology convergence;*
4. *To support the commercialization activities of C4IoT by releasing a stable and reliable solution for primary automotive industry, and in sequence for any end-to-end Industrial IoT environment.*

Progress:
WP4 efforts included the identification of key enablers towards the assurance, privacy and accountability in all Industrial IoT processes, the advanced and interactive visualizations for C4IIoT operators, as well as the continuous integration towards the realization of C4IIoT framework. These efforts started on M8 (January 2020) and were active until the end of the project, driving the integration towards the releases of the C4IIoT solution.
Moreover, WP4 has focused on the illustration of the use case dataset selection process, data formatting and data flowing processes, bringing in the MVP architecture and demonstrating the integration between the C4IIoT components and their distinct technologies. More specifically, the continuous negotiation between ITML and AEGIS (who were leading the efforts towards the MVP release) and the C4IIoT data and component providers towards the creation of the use case scenario that was used for the design and development of the MVP (see D4.2). In this respect, ITML launched WP4 bi-weekly telcos to schedule and achieve all the relevant activities. As a result, the requirements for the MVP development (including components, basic rules and algorithms, expected output) have been defined and used for creating the infrastructure that supports the MVP. In addition, the work carried out in WP4 includes the analysis of technical and implementation requirements of all modules, as well as the deployment and management of necessary resources for implementation and integration. In addition, WP4 led the implementation of the 1st integrated version prototype (internal version) to offer security and privacy in an end-to-end industrial IoT environments in the automotive manufacturing domain. Finally, WP4 includes also the final solution and the functionality of the integrated framework verified by the C4IIoT pilots.

Partner Contributions:

- **FORTH** participated in the discussions and all the relevant telcos for WP4. FORTH provided the Component Specification Template asking from each module provider to identify the minimum hardware requirements and the minimum functionalities for the MVP. FORTH offered input on the “Security Assurance of C4IIoT Platform” for D4.1 In addition FORTH integrated its traffic analysis module to the MVP architecture and described it for deliverable D4.2. FORTH has integrated its traffic analysis module on C4IIoT’s first complete prototype (M18). FORTH also integrated its tools (i.e., traffic analysis and confidential computing module) in the final C4IIoT integrated framework, as described in Deliverable D4.3. Finally, FORTH led the activities for Deliverable

D4.4 that describes the lessons learned and the best practices for maintaining and operating the framework in the long-term.

- **IBM** contributed to deliverable D4.1 providing a chapter about its decentralized access control solution. IBM has provided information regarding the decentralized access control solution in the "Component Specification Template" that was circulated and further provided information as part of the progress monitoring that was done. IBM provided its first contribution to deliverable D4.4. IBM integrated its decentralized access control in C4IIoT's first complete prototype (M18), and is making ongoing efforts to deploy its technologies in C4IIoT's final version in the final execution environment. IBM participated in the discussions and all the relevant telcos for WP4.

- **UOG** contributed to Task 4.3 (Continuous integration towards the realization of C4IIoT framework), the corresponding deliverable D4.2 (C4IIoT Minimum Viable Product) and Task 4.4 (From the prototype to the final solution). More specifically, UOG contributed to the design and implementation of the Minimum Viable Product (MVP), in relation to the dynamic security-aware offloading decision support component of the architecture and its interactions with other C4IIoT components. The MEDICI service was deployed to ITML's field gateway and communication with the BACS modules was established through the KAFKA service and is currently deploying the final version of MEDICI to the final execution environment.

- **A1** participated in all of discussions and telcos related to WP4. Field Gateways implementation and secure communication with the edge nodes and the Cloud were major contributions for deliverable D4.2.

- **STS** actively participated in all WP4 bi-weekly telcos. Also, STS led Task 4.1 and overviewed the development work of the various related C4IIoT sub-components. As T4.1 leader, STS implemented the Security Assurance Module (SAM), composed of five components, that provides Asset Modeling, Vulnerability Analysis Assessments, Dynamic Testing Assessments and Monitoring Assessments of the involved assets and implemented the Attack Information Enhancement Middleware (AIEM). Also, STS prepared and tested the updated version of SAM, integrated at the revised (R2) version of the C4IIoT platform and provided the required C4IIoT Asset Model for the infrastructure and both use cases. STS, as D4.1 leader, compiled and delivered the "Assurance, privacy and accountability in all Industrial IoT processes" deliverable. Finally, STS contributed to the preparation of deliverables D4.2, D4.3 and D4.4 by providing the necessary inputs and reviews.
- **ITML** ensured the successful integration of the C4IIoT technologies and relevant security-enabled layers; based on an agile approach. It validated and test the integrated framework collecting feedback from both the technology providers and the end users. Specifically, in the context of this Work Package, a proof-of-concept demonstration (MVP) was delivered at M12, based on the architecture - analysis carried out in WP1 and the developments in WP2 and WP3. Finally, ITML was also responsible for a first complete prototype that derived internally at M18 and a second prototype - the final solution as well as the configuration of the framework during the two pilots.
- **IFAG** contributed in the telcos carried out during the development of the WP. IFAG contributes Deliverable D4.1 section 5.2: Hyperledger Fabric integration with Infineon's secure element. In this section the concept, background and motivation is explained as well as the approach that will be follow in other tasks. IFAG provides also contribution for the Deliverable D4.4. For the first prototype (M18), IFAG integrates

the secure elements provide in the edge nodes in the framework, and is making ongoing efforts to the final version in the final execution environment.

- **CRF** has actively participated to the discussion and relevant telcos for WP4. Moreover, CRF has provided the input for the design of the visualization toolkit from the point of view of the different typologies of users (IT security expert, non-ICT staff) and given feedback on the interfaces developed in the first half of the project. Finally, CRF has contributed to the related deliverables connected to the activities mentioned above.
- **TSG** has delivered the SDN controller, in particular for the mid-term review demonstration. During this integration, TSG verified the expected behavior of the SDN controller with the other Mitigation Engine's components. For the midterm review, TSG provided an emulated network topology using Mininet to mimic the factory infrastructure. Some efforts were also spent on the integration of the Mitigation Engine's probe onto the emulated topology. TSG provided inputs in the D4.4 deliverable on the challenges, lessons and best practices regarding the SDN controller.
- **CEA** mainly concerned with integrating BINSEC in the C4IIoT integrated framework and preparing the demo. Enhancements such that integration of Ghidra import and x86-64 bit support was done based on the feedback obtained in this integration.
- **UP1PS** participated in all WP4 conference calls and discussions. Its efforts were primarily focused on Task 4.3 and its associated deliverables. In the context of these efforts, it was deeply involved in the integration of the CARMAS tool within the larger project and the tests that guaranteed its fit and function as part of the C4IIoT framework.
- **UNSPMF** implemented several privacy preserving machine learning algorithms within BACS. Preservation of privacy has been achieved by using a relatively novel concept of differential privacy. Differential privacy is a system for publicly sharing information about a dataset by describing group patterns within the dataset while withholding information about individuals in the dataset. The latest version of BACS includes implementations of differentially private k-means methods and principal component analysis (PCA). Contributions in writing and deliverable quality assurance process.
- **HPE** has provided support to the framework with definition and integration of both its component and some common framework tools. HPE contributed to the framework with configuration of Microk8s and definition of YAML files templates for partners (to ease deploying of k8s pods and services and to integrate component API visibility into Cloud Gateway REST interface). HPE set Harbor private docker registry with sections for C4IIoT modules at different layers (and common tools) and with vulnerability scanning of uploaded images. For Cloud Gateway component, HPE configured it with HTTPS and ModSecurity Web Application Firewall. For the assurance, privacy and accountability in all Industrial IoT processes, HPE deployed the identity management and the risk assessment. Identity Management represents a strategic and essential security element, that we implement it in the way to utilize the PKI (public key management) where each identity or "end entity" is represented by a digital certificate. During the risk assessment, where we proposed the methodology and executed the assessment, we assessed the risk of undesirable events in order to define the priority or urgency of the measures necessary to keep it under control.
- **AEGIS** actively participated in all bi-weekly telcos for the WP4. AEGIS also led the process of defining the requirements and specifying the functionalities of the MVP version of C4IIoT. AEGIS, as D4.2 leader, prepared and delivered the C4IIoT MVP deliverable on time. Also, as T4.2 leader, AEGIS implemented the Advanced

Visualization Toolkit providing an interactive interface to the end-user. The AVT was implemented in three different phases described in the task report. AEGIS also collaborated with ITML and other technical partners to integrate the AVT in the C4IIoT framework with all features and capabilities requested. Finally, AEGIS also contributed to the D4.1 ("Assurance, privacy and accountability in all Industrial IoT processes")

Progress per Task:

Task4.1. Assurance, privacy and accountability in all Industrial IoT processes:

Task 4.1 provided the design, implementation, and integration of (i) an identity management solution providing smart identities to the entities present in an IIoT setting, (ii) a Risk Assessment procedure that determines whether to accept, mitigate, transfer or avoid risks and provides a security governance model for the involved assets and recommendations for maximizing the protection of confidentiality, integrity, and availability, (iii) a security assessment and certification solution for monitoring the C4IIoT platform, (iv) distributed ledger technologies that enhance the auditability, reliability and accountability of the IIoT environment and (v) privacy preservation techniques in the context of data mining. In the context of this task, the Identity Management was implemented and integrated to the revised C4IIoT platform by HPE, and the execution of the final demonstrator was performed. Also, STS developed and integrated the Security Assurance Module (SAM) and the required C4IIoT Asset Model as well as the Attack Information Enhancement Middleware (AIEM). UNSPMF provided the implementation and integration of the Behavioral Analysis and Cognitive Security (BACS) component that offers the Privacy Preservation Techniques. Furthermore, IBM implemented and integrated the Decentralized Access Control (DAC) and blockchain database (BCDB) components for revised (R2) version of the C4IIoT platform while IFAG provided the Distributed Ledger technologies offering Infineon OPTIGA TPM2.0 support. Finally, ITML provided the integration of its Data Fusion Bus (DFB) solution with HPE's CA and AEGIS AVT as well as the deployment of the final version of DFB for the final integration.

Task4.2. Advanced informative mechanisms and interactive visualizations:

AEGIS implemented the Advanced Visualization Toolkit (AVT) module which is the user interface of the C4IIoT framework. It provides the means to visualise several indicators deriving from the analysis of data coming from the Edge layer. AVT enables the final user to explore data in a high level through several interconnected, interactive visualisations that also allow drilling into more detailed information to reveal hidden relationships and insights.

The AVT provides real-time monitoring of the system, alerting mechanism, the option to request and apply mitigation actions and uses timeline analysis to look into past incidents and detect possible hidden relations between detected events. The AVT developed and integrated in C4IIoT framework in different phases guided by the releases of the corresponding C4IIoT integrated prototypes, namely the Minimum Viable Product (MVP), the 1st Integrated prototype (M18) and the final integrated prototype.

The AVT is the user interface with the C4IIoT framework and includes: (i) Real-time monitoring of devices operational data; (ii) Real-time monitoring of events detected in the anomaly detection process; (iii) Historical data overview; (iv) Interaction with Security Assurance Module to show attack plans detected and user interaction to get mitigation plans and apply mitigation actions; (v) Binsec Analysis; (vi) Verification against data manipulation; (vii) Data decryption; (viii) Timeline analysis; and (ix) Real-time monitoring in the map of devices in Logistics use case.

Task4.3. Continuous integration towards the realization of C4IIoT framework:
This task was constantly working to integrate the distinct services towards the realization of C4IIoT framework until the end of the project. ITML led the implementation of the 1st integrated version prototype (internal version) to offer security and privacy in an end-to-end industrial IoT environments in the automotive manufacturing domain at M18 and a second prototype - the final solution in parallel with the configuration of the framework during the two pilots. The final solution delivered through the second prototype – final solution and the functionality of the integrated framework verified by the C4IIoT pilots. It also customized based on the specific needs of each field. ITML drove and implemented all the deployment and management of necessary resources for the final implementation and integration.

Task4.4. From the prototype to the final solution – TRL 6
The activities of this task include the collection of the details about how the challenges related to deploying and setting up C4IIoT framework within a real-life operating environment have been addressed. In addition, this task worked on reporting the good practices and lessons learned, so as to serve as a reference point to promote security on Industry 4.0 and Industrial IoT. Part of this task was also the end-user guide for installing, deploying and using the C4IIoT framework and its components.

Deliverables:

D4.1. Assurance, privacy and accountability in all Industrial IoT processes
The first output of Task 4.1 and, as such, documented the design and specification of the C4IIoT building blocks focusing on providing assurance, privacy, and accountability in all Industrial IoT processes. Moreover, specification and implementation details were included for each of the associated components. The deliverable was submitted with no delays, at M12.

D4.2. C4IIoT Minimum Viable Product
AEGIS was responsible for the D4.2 C4IIoT Minimum Viable Product. The result was the delivery of the C4IIoT MVP, a first working prototype of C4IIoT framework. The deliverable submitted on time.

D4.3. C4IIoT integrated framework
ITML was the leader of this deliverable. This deliverable describes the final integrated solution towards the realization of C4IIoT framework. It includes the analysis of technical and implementation requirements of all modules until M30 as well as the deployment and management of necessary resources for the implementation requirements. The described work gives emphasis to the development of the second (final) C4IIoT prototype, ensuring a smooth and effective integration of the components.

D4.4. Best practices for maintaining and operating the framework in the long-term – TRL 6
This deliverable presents the experience of the consortium and the lessons learned during the development of the C4IIoT platform. It also presents a set of security guidelines and best practices that others can use. The purpose of this deliverable is to show our experience on building the C4IIoT platform and present a set of security guidelines and best practices that others can use. These guidelines focus on security measures for industrial environments and IoT ecosystems, however many of them would apply to any connected device in general. Finally, the deliverable presents a user-guide for each and every C4IIoT component with an aim to support a long-term sustainability.

Milestones:

- ***MS2*: *Proof of concept through C4IIoT MVP (M12)***
  MVP was successfully reached at the M12 and the work is reflected in D4.2.

- ***MS3*: *Version of Integrated platform and of C4IIoT Level-1, Level-2 and Level-3 security; initial execution of demonstrators (M18)***
  A first integrated version of a functional platform was realized at M18. Security mechanisms were detailed in D3.2, D3.3 and first platform evaluation is described in D5.1.

- **MS5: Final version of integrated platform and execution of demonstrators (M30)**
  The integrated platform has been finalized in M30 and it has been tested in the context of the two demonstrators, one related to the Smart Factory and the other to the Logistics4.0, in conjunction with WP5 activities. The description of the integrated architecture has been provided in D4.3, while the demonstrator execution is better detailed in WP5 deliverables D5.2 and D5.3.

1.5 WP5 – Real-life industrial demonstrations in smart manufacturing

Work-package objectives:

The objectives of this work package are:

1. *To ensure the finalization of the demonstration protocol based on end-users' requirements;*
2. *To realize real-life industrial demonstrators.*
3. *To provide detailed validation and evaluation of the C4IIoT platform, from a usability and end-user point of view, based on KPIs defined in GA (Section 2.1) and updated in Task 1.1.*

Progress:

WP5 aimed to assess the overall performance of the C4IIOT solution in two real life examples and evaluate the value from the deployment of the proposed solution in the Automotive manufacturing sector. In this context, the objective of this WP has been to conclude on the effectiveness of the C4IIoT platform and modules through specific KPIs for business validation, impact assessment and verification of cost reduction. By doing so, this WP has provided a proof-of-concept for the industrial relevance of C4IIoT and the degree to which manufacturers in the target sector are prepared to adopt C4IIoT concepts and services.

The activities performed have been related to the refinement and finalization of the pilot scenarios (also taking into account WP1 results) in parallel with the integration of system modules, refined execution parameters and KPIs, evaluation parameters and guidelines for the demonstration execution, final evaluation both of the use cases and of the architecture components, demonstration execution and final impact assessment and evaluation, also through the measurement of the defined KPIs. In fact, in the first phase of the project, an initial definition of the demonstration protocol based on end-users' requirements was achieved, as well as the real-life demonstrators design and initial development. In addition, it provided a plan for the detailed validation and evaluation of the C4IIoT platform, from a usability and end-user point of view, based on the defined KPIs. In the final phase of the project, the demonstrators have been finalized and tested, allowing the final validation and an overall evaluation of the C4IIoT solution.

Partner Contributions:

- **FORTH** participated in the discussions and all the relevant telcos for WP5 tasks which started on M10. FORTH provided its input for D5.1 on the benchmarks of the C4IIoT project and arranged the distributions of the KPIs between the partners and their corresponding modules. FORTH provided input for Deliverable D5.2, describing how its tools operated within the C4IIoT integrated solution. Finally, FORTH reviewed both Deliverable D5.1 and D5.2.
- **IBM** participated in the discussions and all the relevant telcos for WP5. IBM contributed to deliverables D5.1 and D5.2.
- **UOG** contributed to Task 5.2 (Framework deployment and execution of real-life industrial demonstrations) and Task 5.3 (Evaluation and Impact analysis) and the corresponding Deliverables D5.1 (C4IIoT Demonstration - initial execution and evaluation) and D5.2 (C4IIOT Demonstration - final execution) on matters relevant to the deployment and description of the MEDICI tool and the assessment of the related KPIs, its technical evaluation in respect to the evaluation indicators and the monitoring of the KPIs assigned to UOG.

- **A1** participated in all of discussions and telcos related to WP5. Input was provided to deliverable D5.2 regarding Logistic 4.0 scenario demonstration execution. Mobile operator services were used to secure the communication between edge nodes and the field gateway. NBIoT service was presented with the basic structure of the network (with 3GPP GPRS as backup) and main characteristics of radio protocols, with emphasis on power saving mode description. A1 was also the internal reviewer for this deliverable.

- **STS** actively participated in the discussions and telcos related to WP5. Also, STS provided the necessary input towards the compilation of deliverables D5.1, D5.2 and D5.3. Work was also performed on the technical evaluation, impact analysis and KPIs related to the Security Assurance Module and demonstrated the MVP and the final version of the platform focusing to the Assurance Certification.
- **ITML** in the framework of WP5 contributed to Task5.1 ("Demonstration protocol alignment") Task 5.2 ("Framework deployment and execution of real-life industrial demonstrations") and Task 5.3 ("Evaluation and Impact analysis"). ITML was also the leader of D5.1 including the refinement of pilots, integration of system modules, refined execution parameters, KPIs, evaluation parameters and guidelines for the demonstration execution are reported.
- **IFAG** participates in the relevant telcos in the WP. IFAG contributes to Deliverable D5.1 and Deliverable D5.2. Both contributions deal with the final implementation and demonstration environment.

- **CRF** has led the discussion and organized relevant telcos for WP5. CRF has provided the refined industrial challenges and cybersecurity requirements, the Business KPIs for the evaluation of the impact of the C4IIoT platform, a detailed description of the pilots in terms of architecture and scenario. Furthermore, CRF provided the use cases, actors involved in the use cases evaluation and method for the evaluation of the use cases. CRF provided a framework for the evaluation and impact analysis for real-life industrial demonstrators. Then, CRF has led the activities related to demonstrator deployment and execution both in the Smart Factory and in the Logistics4.0 scenarios, including also the installation of the logistics devices in a supplier premises. Finally, CRF has contributed to D5.1 and has led D5.2 and D5.3, where all the activities mentioned above have been reported.

- **TSG** participated on the factory demonstration elaboration and implementation for the final review. This encompassed the delivery and configuration of the SDN controller on CRF premise. For this occasion, TSG configured and shipped a cluster of Raspberry Pi to support the demonstration as OVS switches. TSG provided input in the D5.1 deliverable on the for the initial analysis of outputs for the SDN controller. TSG provided inputs inside the D5.2 deliverable on the deployment of the SDN controller and its technical evaluation output.

- **CEA** 's work in this task mainly concerned in coordinating its work towards the goal of the real-world demonstrations, and contribution to the deliverables.

- **UP1PS** participated in the WP5 discussions and conference calls. It contributed to both Deliverable 5.1 and 5.2. It also prepared a containerized distribution of the CARMAS tool for use within the final technology demonstration and aided in its deployment and testing. It has also contributed to the monitoring of all its assigned KPIs through regular contact with project partners for status updates.

- **UNSPMF** Integration of BACS component to the C4IIoT framework at all three layers of the architecture. Testing and validation of machine learning methods implemented within the BACS component. Testing and validation of novel Logistics 4.0 use case edge node devices.
- **HPE** has contributed to the demonstrator with installations and ongoing support of both its component and some common framework tools. HPE contributed to the framework with installation of Microk8s and building of templates of YAML files. HPE installed and configured Harbor private docker registry and periodically extracted reports for each image of C4IIoT components on Harbor. For Cloud Gateway component, HPE configured it with HTTPS and ModSecurity Web Application Firewall. For EJBCA private PKI/CA, made configuration of Root CA and SubCAs and certificate profiles. On this component, HPE setup credentials for C4IIoT partners needed to request certificates and gave ongoing support for any issue on EJBCA (eg. Certificate profiles updates for new requirements, etc.).
- **AEGIS** participated in all meeting organized for this WP. AEGIS contributed in the guidelines and documentation for the execution and evaluation process, the definition of use cases and the collection and initial analysis of the output. Furthermore, AEGIS contributed in the definition of evaluation parameters and performed a technical evaluation of Advanced Visualisation Toolkit. Finally, contributed in the development of a guideline to execute and evaluate C4IIoT framework.

Progress per Task:

Task5.1. Demonstration protocol alignment:

The task started at M10 and was active until M18. Its achievements include the refinement of the demonstration protocol alignment, a provision of a detailed description of the framework deployment and execution of real-life industrial demonstrations and additionally an initial technical evaluation of the C4IIoT platform, based on defined KPIs. The execution of two demonstrators in automotive and manufacturing industry (Logistics 4.0 and Smart manufacturing) will validate the solution in real-world settings. The Demonstration phase will comprise real-life demonstrators in Fiat Chrysler Automobile's (FCAs) smart manufacturing environment as part of WP5 activities. CRF will define in detail C4IIoT's demonstration protocol (e.g., testing use cases, actors to perform the tests) and will ensure the smooth deployment and execution of C4IIoT real-world demonstrators. The execution of trials will be performed by the end users while the C4IIoT's community will validate C4IIoT against its objectives.

Task5.2. Framework deployment and execution of real-life industrial demonstrations:

The task started in M10 and has been active until the end of the project. Its main achievements include the finalization of the demonstration protocol and the demonstrator execution in real-life environment. Two different scenarios have been considered: the Smart Factory scenario, including the deployment and test of the integrated architecture in Campus Melfi; the Logistics4.0, dealing with the utilization of logistics devices in the Inbound Logistics of components from the supplier plant to the vehicle production plant. The actors involved in the demonstration have been identified: ICT Team Leader, ICT Team member, Manufacturing and Logistics Engineers, Supplier, Transporter. The requirements and use-cases have been defined, related to the Monitoring, Analysis, Mitigation and Access.

In conjunction with the other tasks of WP5, in this task the definition and evaluation of KPIs have been performed, in order to validate the C4IIOT solution and analyze its impact in the Automotive Industry.

Task5.3. Evaluation and Impact analysis:

The task started in M12 and has been active until the end of the project. In the first phase, activities regarded mainly the definition of KPIs, in conjunction with the other WP5 tasks. In fact, the initial focus was the definition of the framework for the technical evaluation, in particular on the C4IIoT platform and its modules through testing by using appropriate benchmarks/baseline values. For this evaluation, a set of indicators has been adapted to the needs of each C4IIoT component. Indicators are extracted, either directly or indirectly, after carefully examining the user requirements and challenges. KPIs have been defined, together with Task 5.1, for measuring the added value of the platform when applied within the FCA processes: a 1 to 5 scale has been selected for the evaluation of the use cases by the actors (i.e., ICT Team Leader, Manufacturing engineer, Supplier, etc.), through individual tests of the platform. Then a unique evaluation has been done in several assessment and consensus meetings. Finally, in the last months of the project, the main objective has been the final evaluation of the solution. The use-cases, as defined in D5.1, were evaluated, from the point of view of the involved end-users.

Deliverables:

D5.1. C4IIoT Demonstration - initial execution and evaluation

Deliverable D5.1 was delivered successfully on M18. It included a report on the specification of the demonstration protocol, the framework deployment and execution of real-life industrial demonstrators as well as initiated the evaluation and impact analysis through KPIs and their impact. All the information on this deliverable will be the key to the continuation of the project covering the efficient execution and the evaluation outcome. More specifically and taking into consideration the guidelines from Task T1.3 and the experimental protocol from Task T1.4 and all relevant achievements, the deliverable also produced time plans and guidelines for execution and evaluation processes. This deliverable is the outcome of the work carried out within WP5 of the C4IIoT project. It is closely related to activities carried out in other Work Packages, with each having its own role.

D5.2. C4IIOT Demonstration - final execution

The deliverable is a report of the final execution of the demonstrators in the Smart Factory and Logistics4.0 scenarios. This document was delivered in M34, while the initial delivery was planned by the end of M30. The reason behind that is related to the limited access to both Campus Melfi and supplier premises, due to the Covid-19 pandemic, causing delay in the deployment of the C4IIOT solution in the real environment. In addition to the demonstration scenarios description, also two different C4IIOT architectures for the two scenarios are described in this report, together with the use-cases evaluation by the actors involved as end-users and also the evaluation of the architecture components.

D5.3. Assessment report and impact analysis

The deliverable is a report of the final assessment of the C4IIOT solution, following the demonstrator execution, and the analysis of the impact. Here, the KPIs defined in D5.1 are evaluated at the end of the project, in order to quantify the added-value due to the utilization of the C4IIOT platform.

Milestones:

- **MS5: Final version of integrated platform and execution of demonstrators (M30)**
  The milestone was reached thanks to the deployment of the integrated platform in the

real-life industrial scenarios and the related tests, allowing to achieve the validation of the C4IIOT solution.

- ***MS6*****:** ***Final assessment, impact analysis and business plan (M36)***
  MS6 will be achieved through the final assessment report in Deliverable D5.3 and the definition of business models in Deliverable D6.6. The Deliverable D5.3 has not been finished as to the time of submitting this document, but rather in a later point in time.

1.6 WP6 – Exploitation, sustainability and business continuity

Work-package objectives:

The objectives of this work package are:

1. *Raise awareness about the project concept, developments and findings to all key actors (large industry, SMEs, academics, policy makers);*
2. *Develop the dissemination and communication strategy of the project, including social presence, participation in EU events, collaboration with other related projects; and implement it;*
3. *Implement an interactive C4IIoT user-friendly portal to inform the general public and relevant stakeholders about C4IIoT;*
4. *Develop the business model for C4IIoT and strategies for incetivising/promoting project adoption by various stakeholders within the financial ecosystem during and after project;*
5. *Investigate the delivered solution by considering the platform's minimum viable product (MVP) and prepare market entrance by evaluating strength, weaknesses, opportunities, and threats of the market offering, as well as marker viability by considering standardization aspects and approval through authorities;*
6. *Create a marketing strategy that focuses on commercialization including the produces costs (TCO), benefits (TBO), and return on invest.*

Progress:

WP6 covers six main threads that are: the market definition and analysis, the definition of communication strategies, the exploitation activities, the standardization activities and best practices, as well as the long-term sustainability and commercialization. All these objectives are reflected in WP6 tasks. We provided a final version for the dissemination strategy and activities in D6.6 (M24). We have also provided a clear standardization plan and best practices for the security modules and products developed in C4IIoT (D6.5, M24) as well as a clear alignment with six standardization groups and associations targeted by the project. In the remaining period, efforts were concentrated on the final business model and long-term sustainability report (D6.7, M36).

Partner Contributions:

- **FORTH** participated in the discussion and all the relevant telcos for WP6. Also, FORTH provided its dissemination activities for Deliverable D6.3 and its individual exploitation plan for Deliverable D6.4. Additionally, presented its dissemination activities in D6.6 and its exploitation activity in D6.5 and D6.7. FORTH was involved actively in planning dissemination activities, and presenting C4IIoT project through conferences, webinars, and publications such as *"A Survey on Encrypted Network Traffic Analysis Applications, Techniques and Countermeasures"* Journal published on ACM 2021 and *"Andromeda: Enabling Secure Enclaves For The Android Ecosystem"* presented on ISC 21'. FORTH presented an overview of the C4IIoT project in the 3rd CYSARM workshop and presented a poster of C4IIoT in the CyberHOT summer school 2021.
- **IBM** contributed to deliverable D6.2 (titled "Market Analysis") and provided details on its dissemination activities for deliverable D6.3 and its individual exploitation plans for deliverable D6.4. IBM also contributed to deliverable D6.5 regarding exploitation

efforts, to D6.6 regarding dissemination strategy and to D6.7 regarding its exploitable assets. IBM has cooperated with UP1PS contributing to a joint paper “A Blockchain auditability model for Intent-based SDN Applications”. IBM was a presenter in a conference by Cyberwatching where it presented its technology in C4IIoT.

- **UOG** contributed to Task 6.2 (Communication strategy triggering awareness and new business opportunities) and Task 6.3 (Exploitation activities) and the corresponding deliverables D6.3 (Interim Version of Dissemination strategy and activities), D6.4 and D6.5 (Exploitation and standardization activities and best practices – initial and final version) and D6.6 (Dissemination strategy and activities) on the exploitation assets and dissemination plans and disseminating our work through publication, social media, by participating to C4IIoT’s INFODAY and Winter School and co-organising the international workshop on Secure and resilient smart manufacturing environments (SecRS).
- **A1** participated in all discussions and telcos for WP6 and contributed to market overview, analysis, and business modeling. Exploitation plan, with best practices and standards used was provided in scope of activities within this WP. Actively involved in planning dissemination activities, promoting and presenting C4IIoT project through digital channels, conferences, webinars, and publications.
- **STS** participated in all WP6 call following the respective tasks coordination while leading task 6.7. while contributed in all WP task activities such as dissemination and communication activities, exploitation planning, standardization potential investigation, market analysis, business planning and more. Following up, STS provided the necessary contribution for WP6 respective deliverables, such as STS profile for D6.1, STS business vision, goal and objectives in project, C4IIoT assurance-related competitors, relevant IoT security regulations/initiatives for D6.2. STS dissemination and communication activities for RP1, for D6.3, the Assurance-related best practices and standards in D6.4, STS exploitation plan, Recommendations for development of a common assurance model, enabling model-based security assessment, certification and mitigation schemes and the potentials of model elements release in association with innovation 5 in D6.5, STS dissemination and communication activities for RP2, and contribution to final business model, exploitable assets, SWOT analysis etc. for D6.7.
- **ITML** in the framework of WP6 contributed to Task6.1 (“Market definition and analysis”) Task 6.2 (“Communication strategy triggering awareness and new business opportunities”), Task 6.3 (“Exploitation activities”), Task 6.4 (“Standardization activities and best practices”), Task 6.5 (“Long-term sustainability and commercialization”) as well as the corresponding deliverables of these tasks. Specifically, ITML in the context of this WP contributed to the exploitation, strategies and the business model for C4IIoT for promoting project adoption by various stakeholders within the financial ecosystem during and after project.
- **IFAG** contributes in Deliverable D6.2 named Market Analysis and preliminary business modelling. The Deliverable D6.4 was leaded by IFAG. This deliverable introduces different SDOs related to the C4IIoT project as well as individual exploitation and standardization activities. Finally, it introduces a joint plan of exploitation and dissemination, which will be developed in detail in Deliverable D6.5. In this deliverable IFAG contributes developing in detail the joint exploitation plans and providing value chain analysis of the components developed by IFAG in the project. IFAG products as SECORA family or USB Dongle Trust M are promoted in the exploitation activities related to the task which IFAG leads.

- **CRF** has actively participated to the discussion and relevant telcos for WP6. CRF identified the industry megatrends addressed by C4IIoT with the characteristics of the exploitable results: the product and the market, starting with the Campus Melfi and Melfi plant and other potential early adapters. CRF disseminated the project results internally to Stellantis, involving staff from departments in Manufacturing Engineering, Logistics Engineering, Advanced Manufacturing, Advanced Planning, and Marketing. CRF has also contributed to the project dissemination providing contents for social channels and also presenting C4IIOT during another public event organized by CRF in the context of the project CYRENE. Finally, CRF has contributed to the related deliverables connected to the activities mentioned above.
- **CEA** has participated to the WP6 telcos and participated to all the deliverables in which it was involved. It contributed to disseminate the results of C4IIoT, in particular by its publications to the RAID and BlackHat conference.
- **UP1PS'** performed key contributions to WP6 lies through its validation of the achievement of Milestone 1 through the success of Task 6.1. It also performed dissemination activities for the project through social network channels with regular blog posts. UP1PS has also published a paper describing the design and implementation of its attack mitigation search tool CARMAS in the proceedings of the 2021 CRISIS conference. It has also contributed to the C4IIoT architecture paper in collaboration with project partners to be submitted to IEEE access. UP1PS is finalizing the organization of the 2022 spring school virtual event on cybersecurity for the IIoT. UP1PS has also presented CARMAS in detail to TSG.
- **UNSPMF** Representing C4IIoT in Seminar at Telecommunications Technology Center of Catalonia, Train the Trainer Program - HLRS Parallel Programming Workshop – MPI and OpenMP for beginners and advanced topics in parallel programming, Math for Industry 4.0 - Models, Methods and Big Data, European Consortium for Mathematics in Industry (ECMI), 21st ECMI Conference on Industrial and Applied Mathematics (ECMI 2021), The 16th International Conference on Availability, Reliability and Security (ARES 2022), International Workshop on SecRS: Secure and resilient smart manufacturing environments (SecRS), 2nd Joint Workshop - Dynamic Countering of Cyber-attacks Achievements and Standardisation. Participation in publication of four scientific papers. Organization of one C4IIoT winter school. Development of scientific paper related to the description of the C4IIoT system architecture with all partners participating. Scientific and technical leadership.
- **HPE** has organized and participated to an INFODAY for dissemination. HPE is internally pushing to exploit the solution. The event is a Italian national wide event (held virtual due to covid) organized by many entities (CNR, Regione Toscana, chamber of Commerce, RAI and others) to convey a cybersecurity status message. Attendees were around 500 industrial and academic, more than 300 attending the C4IIOT slot.
- **AEGIS** was the Leader of T6.1 and T6.2 and organized several meetings to guide the actions on these tasks. In this context AEGIS led the market analysis, defined the communication and dissemination strategy and guided the related activities during the whole project's lifetime. Also, AEGIS followed the guide by the other tasks leaders and contributed in the exploitation and standardization activities.

Progress per Task:

Task6.1. Market definition and analysis:

In the context of this task we studied the IoT and IoT Cyber Security Market and examined the competitors and C4IIoT positioning in this market segment. Finally, a preliminary business model was formulated to describe, design, challenge, and pivot potential C4IIoT business model.

AEGIS was leading D6.2. “Market definition, analysis and preliminary business modelling”. A comprehensive market study using different analytical tools (e.g. PEST and SWOT analysis). We have successfully coordinated and gathered the content needed for submitting D6.2. The deliverable was submitted on time. After the mid-term evaluation and comments received by the reviewers we have enriched and resubmitted the deliverable.

Task6.2. Communication strategy triggering awareness and new business opportunities:

From the early stage of the project, this task developed and designed the project’s website. The task regularly updated the website with informational content, scientific achievements, news and activities of the consortium. Moreover, we have created C4IIoT accounts in major social media like LinkedIn, Twitter, Facebook and update them regularly. Other communication actions include newsletters, dissemination material like brochures and videos and the listing events and publications made by consortium members in scientific journals, magazines and conferences.

The task was regularly monitoring the communication and dissemination activities to ensure that the C4IIoT findings are promoted to the scientific and industry community as well as to the general public. All the aforementioned actions are part of Dissemination strategy defined and reflected to D6.3. At the end of the project’s duration a detailed report on communication and dissemination actions is planned to be submitted.

Task6.3. Exploitation activities:

This task includes the different exploitable features of the project. In this sense, different ways of carrying out exploitation activities have been studied: on the one hand, the attendance/organization of info days, conferences, events related to the technologies developed in the project. On the other hand, the exploitation of different technologies after the project with potential commercialization. In this way, the task developed a USB Dongle with a secure element placed in order to personal authentication. Combining this with blockchain networks related to users becomes in a perfect use case that can be exploit in the future. Furthermore, IFAG SECORA family is promoted by the use of the secure elements with blockchain networks through the lessons learnt from the development of this project.

Task6.4. Standardization activities and best practices:

TSG as a leader for the standardization activities has identified a set of standardization bodies to target for each security product or service. In particular, TSG has provided a list of best practices and standards ranked by practices. Moreover, it provides a standardization plan that calls also for new open-source contributions, and participations to associations such as OpenCTI, ENISA or TCG. Furthermore, we disseminate the standardization activities of the project in a joint workshop with other projects from the same call: 2nd Joint Workshop in February 2022.

Task6.5. Long-term sustainability and commercialization

The activities of this task focused on the sustainability of the C4IIoT proposed solution after the project's end. The exploitable assets of the C4IIoT framework were identified and documented (in the respective deliverable D6.7) as well as joint exploitation potentials were identified. Moreover, efforts were devoted to the identification of the C4IIoT foreseen stakeholders and respective domains. A potential business plan has been drafted including updated business canvas, market needs and trends, swot analysis, revenue stream possibilities etc.

<u>Deliverables:</u>

D6.1. Project website

AEGIS was responsible for Deliverable D6.1 (titled "Project Website"). The deliverable describes the design and development of the project's website and submitted on time.

D6.2. Market analysis and preliminary business modelling

AEGIS led this deliverable which determines the market context of C4IIoT and the relevant business requirements and challenges. Moreover, it performs a market analysis using different tools to quantify the size of the market and identify key competitors, market needs and trends, stakeholders and potential customers and users. AEGIS collected input from all partners and combined them into a preliminary business modelling which is the actually the first step to a successful business model for C4IIoT. The deliverable submitted on time.

D6.3. Interim Version of Dissemination strategy and activities

AEGIS was responsible for Deliverable D6.3 (titled "Interim Version of Dissemination strategy and activities"). The deliverable presents a detailed roadmap for a successful dissemination strategy with specific responsibilities for each partner. AEGIS requested contributions from all partners regarding their dissemination activities and individual dissemination plans. The deliverable submitted on time.

D6.4. Exploitation and standardization activities and best practices – initial version

Deliverable D6.4 initially describes the best practices and standards used by each partner at M12 of the project. It then describes the possible routes towards the exploitation of the results, including the possible presentations of the results in the SDOs, depending on the participation of the different partners in these SDOs. In this deliverable, each partner introduces different SDOs related to the C4IIoT project, individual exploitation and standardization activities and finally it is called in the future to carry out a joint plan of exploitation and dissemination (Deliverable D6.5). Organizations like TCG or AIOTI are included in this deliverable.

D6.5. Exploitation and standardization activities and best practices – final version

This deliverable provides the list of relevant standardization bodies, alliances and associations, in which the C4IIoT partners either participate or follow, due to their close alignment with the project's goals. Starting with the European standards cited in the GA, a comprehensive list of relevant international entities is provided, as a first index of bodies that we must closely follow and, when possible, comply with. After that, the partners detail their contribution in the overall standardization effort, with a focus on enforced standards, applied recommendation and relevant entities in which they participate. The standardization plan is updated in this deliverable and a follow-up of the compliance with the identified standardization plan is provided. Regarding the exploitation, a detailed description per partner of their exploitable assets is provided, and it is followed by a collective exploitation plan based on the description of how the different technologies complement each other's to deliver exploitable functional capabilities in relevant market sectors.

D6.6. Dissemination strategy and activities

AEGIS was responsible for Deliverable D6.6 (titled "Dissemination strategy and activities"). The report consists of the reporting/monitoring of the respective dissemination and communication activities during the second year of the project (M12-M24) and planning for the following period along with evaluation of the progress made with respect to the communication and dissemination KPIs. The deliverable was submitted on time.

D6.7. Final business model and long-term sustainability report

This deliverable is the outcome of the long-term sustainability and commercialization task of C4IIoT in order to provide the vision for sustainability of the outcomes after the end of the project. A report on the C4IIoT exploitable assets has been compiled with details on tis exploitation potentials. Moreover, potential for joint exploitation activities have been drafted. An overview of the C4IIoT potential stakeholders is presented. Moreover, a final business model with business canvas and swot analysis concludes this deliverable.

Milestones:

- ***MS1:* C4IIoT set-up: Requirements, initial architecture and preliminary business models (M6)**

  MS1 has been achieved through the completion of Task 6.1 and Deliverable D6.2 (in addition to Deliverable D1.1, Deliverable D1.2, and Deliverable D1.3), as this completes the delivery of all C4IIoT requirements analysis, set-up, architecture and dissemination/exploitation plans.

- ***MS4:* Dissemination, Exploitation and standardization landmark (M18)**

  Dissemination, Exploitation and standardization landmark (M18): Initial version of the Dissemination Strategy + INFODAY, YouTube channel and Winter School; Individual exploitation plans; List of standard and recommendations applied.

- ***MS6*: Final assessment, impact analysis and business plan (M36)**

  MS6 will be achieved through the final assessment report in D5.3 and the definition of business models in D6.6. The Deliverable D5.3 has not been finished as to the time of submitting this document, but rather in a later point in time.

1.7 WP7 – Project Management

Work-package objectives:

1. *To establish a strong project management scheme;*
2. *To establish the appropriate communication and reporting channels to the European Commission;*
3. *To achieve a common scientific and technical direction within the project;*
4. *To ensure successful achievement of the project objectives on time and within budget;*
5. *To establish an efficient electronic service for communications, and document exchanging;*
6. *To realize synergies amongst the project members and effective exploitation of the project's' results;*
7. *To conduct continuous quality assurance activities for the operation of the project and the production of its scientific and technical results within its lifespan;*
8. *To ensure continuous monitoring of the project's progress and timely initiation of corrective actions (if needed);*
9. *To coordinate the organization and execution of the various project meetings, and/or participation of the project in various external or self-organized events;*

Progress:

FORTH continuously monitored the progress of each work package and scheduled monthly meetings to discuss updates regarding the progress of the project and its objectives and KPIs. This has been described in all of the 3 yearly reports (D7.3, D7.5 and D7.6) which FORTH led. In D7.1 and D7.4 the initial and final version of the project handbook was presented with an overview of the management and administrative procedures of the C4IIoT project in order to ensure efficient project execution as well as high quality project results and an updated risk management plan and a plan for IPR management. Finally, in D7.2 a Data Management Plan (DMP) was created for the data used for the C4IIoT project.

Partner Contributions:

- **FORTH** organized monthly teleconferences in cooperation with UNSPMF. To support the C4IIoT technical and management meetings, Microsoft Teams was setup. Moreover, FORTH created the corresponding mailing lists for the project, the svn repository for the project-related entries (deliverables, minutes, reports, etc.), as well as the required templates for reports, deliverables and presentations. It also took all the necessary actions for the preparation of the plenary and technical meetings. Moreover, FORTH took all the necessary actions to ensure the quality of the submitted deliverables, and was the lead beneficiary for Deliverable D7.1, D7.2 and D7.3, D7.4 D7.5 and D7.6. Finally, FORTH made plans on monitoring the KPIs of the project.
- **IBM** contributed to deliverables D7.3 (titled "First Year Project Report"), D7.5 (titled "Second Year Project Report") and D7.6 (titled "Final Project Report"), provided periodical reports of its progress in the project, and provided thorough inputs for the midterm review.
- **UOG** contributed to Task 7.2 (Day-to-day management, project & financial control and resource monitoring) and the deliverables D7.3 (First year project report), D7.5 (Second year project report) and D7.6 (Final year project report). This involved general project management activities, including participating in meetings, recruitment, reporting, communication between partners, technical progress monitoring and financial reporting.

- **A1** worked on periodical progress reports and contributed to deliverables D7.3 and D7.5. Participated on monthly technical meetings and prepared detailed financial reports.
- **STS** participated in all WP7 calls contributing to the day to day management of the project both from its own perspective (management if its own resources) as well as from the project perspective, participating in decision making for the project progress and risk management and providing contribution to the WP7 deliverables and projects periodic reports.
- **ITML** in the framework of WP7 contributed to Deliverable D7.3 (titled "First Year Project Report"), D7.5 (titled "Second Year Project Report") and D7.6 (titled "Final Project Report") by describing the technical work done in all the work packages of the project and by submitting the internal financial report over these periods.
- **IFAG** contributes to deliverable D7.3 and D7.5 named First- and Second-Year Project Report respectively. IFAG provided periodical reports of the tasks and contributions in the project as well as inputs for the midterm review.
- **CRF** has participated to monthly project meetings. Other activities in this WP are related to the general project administration for financial control and resource monitoring and the preparation of the required project management documentation, i.e. project reports, financial reports, etc.
- **CEA** was the lead of Task 7.1, and worked with Forth in preparing the deliverable schedule, quality planning and monitoring the deliverable progress. In addition, we participated in all WP7 activities, such that monthly meetings and periodic reports.
- **UP1PS** has participated in all regular meetings of WP1 (which it also organized), WP3, WP4, WP5 and WP7. It also attended WP6 meetings as needed. It also contributed to deliverables D7.3 and D7.5 (First- and Second-Year Project Reports). In addition, it participated in all plenary meetings and the midterm evaluation.
- **UNSPMF** Scientific and technical leadership. Organization and moderation of monthly scientific and technical meetings. Contribution in writing and in quality assurance process for deliverable development.
- **HPE** has worked on Task 7.3 providing a paragraph on Intellectual propriety, describing the different meanings and providing guidelines for C4IIOT source code developed.
- **AEGIS** followed the guidelines of the WP leader, participated in related telcos and contributed in the corresponding deliverables. Also took over the day-to-day management effort by submitting periodic progress reports and financial reports.
- **TSG** participates to the different telcos, and contributed to the three deliverables D7.3, D7.5 and D7.6 to better present our work progress in all the work packages.

Progress per Task:

Task 7.1. Project quality planning:

The work in this task first consisted in setting up a precise deliverable quality plan featuring a retro planning, quality assurance checklist etc. which was applied to every deliverable, and designing internal reviewers for each deliverable. Following this retro planning, we were able to monitor the progress of the deliverable, and guaranteeing its quality.

Task 7.2. Day-to-day management, project & financial control and resource monitoring: FORTH set up a mailing list for the project, an SVN to store code and deliverables for the project and requested quarterly reports from the partners regarding their progress. A Zenodo community account was created for C4IIoT to include publications and data from the project and lastly FORTH organized a plan to distribute KPIs among the partners and have updates on their progress as the project progresses. FORTH organized regular and on-demand meetings for the need of the projects which were attended by all of the partners and additional WP - specific meeting.

Task 7.3. Innovation Management:
HPE has elaborated paragraph 2.4 of deliverable D7.4 on Intellectual Property Rights and Publications Management.

Deliverables:

D7.1. Initial version of project handbook
This document provides an overview of the management and administrative procedures of the C4IIoT project in order to ensure efficient project execution as well as high quality project results. It also provides the project participants (referred to as "Beneficiaries") with a concise reference to the project management structure, tasks and responsibilities on all levels of project execution and cover Administrative and Technical Project Management as well as external communication and dissemination procedures.

D7.2. Data management Plan
This document provides an evaluation on how research data will be handled during and after the end of the project, what data will be collected, processed and/or generated, which methodology and standards will be applied, whether data will be shared/made open and how data will be curated and preserved.

D7.3. First year project report
This deliverable describes C4IIoT's progress, covering active work package during the first 12 months of the project. It provides a first report on completed and ongoing tasks, along with planned steps for future project activities. As reported within, the project successfully achieved both of its two milestones within the reporting period and submitted all planned deliverables on time.

D7.4. Final Version of project handbook
This deliverable describes the final version of the project handbook which includes an enhancement of the risk management strategy and a plan for IPR management.

D7.5. Second year project report
This deliverable describes the progress conducted in the C4IIoT project over the period of the second year; in particular, the technical work done in all the work packages of the project and explain how the technical objectives have been met.

D7.6. Final project report

This deliverable describes the progress conducted in the C4IIoT project over the whole period of the project; in particular, the technical work done in all the work packages of the project and explain how the technical objectives have been met.

Project Meetings

Both physical meetings and teleconferences have proven very efficient to support the required discussions when elaborating deliverables. For the whole duration of the project, M1 to M36 we had several plenary meetings, monthly teleconferences, along with several other for WP related like the WP4 & WP3 monthly call, KPI update meetings and other specific reasons. After March 2020, all meetings have been performed online due to health safety reasons.

Physical Meetings

The following physical meetings have been held during the whole period of the project:

- The kick-off meeting has been held in FORTH premises, in Heraklion, Greece on June 26th and 27th, 2019. It was attended by researchers from all partners except CRF who joined remote.
- The 2nd plenary meeting was held in the CRF headquarters in Turin, Italy on October 23rd and 24rth, 2019. It was attended by researchers from all partners.
- The 3rd plenary meeting took place in Athens, Greece on February 25th and 26th, 2020. It was hosted by ITML and attended by researchers from all partners except our Italian partners who could not join physically due to health safety reasons (HPE, CRF).

Teleconferences

The following online meetings have been held during the whole period of the project:

Work package	Date	Duration	Attendees	Summary
All	01/07/2019	1h	All	Creation of mailing lists, deliverable templates.
All	02/08/2019	1h	All	D1.1 and D1.2 preparation.
All	25/09/2019	1h	All	WP1 Deliverables, Q1 quarterly reports, organize next plenary.
All	30/10/2019	1h	All	D1.3 architecture and other M6 Deliverables.
All	27/11/2019	1h	All	D3.1, D3.2, D4.1, D4.2
All	18/12/2019	1h	All	Q2 quarterly reports, Discuss MVP.
All	29/01/2020	1h	All	D3.1, D3.2, D4.1, D4.2 and other M12 deliverables, Organization for next plenary.
All	25/03/2020	1h	All	Preparation for MVP and M12 Deliverables, Q3 quarterly reports.
All	29/04/2020	1h	All	Final preparation for M12 Deliverables and MVP.
All	27/05/2020	1h	All	Financial and Q4 quarterly reports, Organization for next plenary.
All	25-06-2020	1h	All	Info day organization, Kafka components further integration, Requirements for Kubernetes cluster.
All	20-07-2020	2d	All	Technical Meeting
All	26-08-2020	1h	All	Progress for integrated framework for M18 per module, Updates and contributions on M18 Deliverables

All	30-09-2020	1h	All	Progress for integrated framework for M18 per module, Updates and contribution on M18 Deliverables, Set timeline for Demo preparation for the project review
All	28-10-2020	1h	All	Discuss demonstrators of stand-alone tools, organization of next plenary meeting, M18 Deliverables
All	24-11-2020	1d	All	Technical Meeting
All	16-12-2020	1h	All	Initial discussion on M24 Deliverables, preparation of demonstrators and periodic reports.
All	27-01-2021	1h	All	First discussion of the initial comments made by the reviewers, revised periodic reports.
All	24-02-2021	1h	All	Revisions for D1.2, D6.2 and D6.4, Organize workshop with other EU projects, Enhance risk management Strategy because of Covid19
All	31-03-2021	1h	All	Discussion to address reviewers' additional comment on D1.2, M24 Deliverables preparation.
All	28-04-2021	1h	All	Questionnaire for external validation of requirements. Progress update on M24 Deliverables
All	18-05-2021	1d	All	Technical Meeting
All	26-05-2021	1h	All	Status update on all WPs, M24 deliverables, Addressing comments from review, Questionnaire status update.
All	30-06-2021	1h	All	Status update on all WPs, Questionnaire status update, CRF deployment update.
All	28-07-2021	1h	All	Status update on all WPs, Questionnaire status update, CRF deployment update. Organization of next plenary meeting.
All	25-08-2021	1h	All	Final version of Questionnaire for external validation of requirements, D4.3 TOC discussion, Deployment progress, Update on all WPs and Ongoing tasks
All	13-09-2021	1d	All	Technical Meeting
All	29-09-2021	1h	All	Update on all WPs and Ongoing tasks, discuss access to the server to execute final demonstration, Resolve sending data from edge devices to the cloud
All	27-10-2021	1h	All	M30 Deliverables update, Update on all WPs and Ongoing tasks, discuss immediate access to the server to execute final demonstration, delay by cloud provider because of ongoing security upgrades, Schedule another call for unresolved issues and integration deadlines

All	24-11-2021	1h	All	M30 Deliverables update, Update on all WPs and Ongoing tasks, discuss unresolved issues regarding integration
All	22-12-2021	1h	All	Update on all WPs and Ongoing tasks, discuss possible delays for D5.2 and integration status of all partners
All	26-01-2022	1h	All	Discuss integration issues, access to the infrastructure and transfer of devices between partners.
All	23-02-2022	1h	All	Update on all WPs and Ongoing tasks, Integration status, M36 deliverables discussion, D5.2 delayed version
All	30-03-2022	1h	All	Update on all WPs and Ongoing tasks, D5.2 submitted, KPIs, M36 deliverables, Integration status.
All	27-04-2022	1h	All	KPIs, M36 Deliverables, Integration status, issues and updates
All	25-05-2022	1h	All	KPIs, M36 Deliverables, Integration status, issues and updates

Table 1: List of C4IIoT Teleconferences

Management Structure

The main Management structure of C4IIoT was defined during the proposal phase of the project. The following positions were filled and have been updated during the course of the project:

Role	Leader	Organisation
Project Coordinator	Sotiris Ioannidis	FORTH
Scientific and Technical Project Manager	Dusan Jakovetic	UNSPMF
Quality Manager	Matthieu Lemmerre	CEA
Innovation Manager	Alberto Terzi	HPE
Data Protection & Security Officer	Sotiris Ioannidis	FORTH

General Assembly (members):

No.	Partner	Member	Alternate
1	FORTH	Sotiris Ioannidis	Giorgos Vasiliadis
2	VIP/A1	Bojan Kovačević	Dragan Danilović
3	UNSPMF	Dusan Jakovetic	Srdjan Skrbic
4	ITML	George Bravos	Nikolaos Evangeliou
5	CEA	Sébastien Bardin	Richard Bonichon
6	HPE	Marco Di Girolamo	Alberto Terzi
7	IBM	Omri Soceanu	Gilad Ezov
8	IFAG	Antonio Escobar	Zheng Ji
9	UOG	Georgia Sakellari	George Loukas

10	UP1PS	Jacques Robin	Carine Souveyet
11	AEGIS	Ilias Spais	Leonidas Kallipolitis
12	CRF	Giuseppe D'Angelo	Julien Mascolo
13	TSG	Pascal Bisson	Marie-Noelle Lepareux
14	STS	Georgios Spanoudakis	Kostas Fysarakis

Work Package Leaders:

No.	Name	Leader	Organisation
WP1	Setting the scene: project set up	Jacques Robin	UP1PS
WP2	Edge computing cybersecurity technologies	Antonio Escobar	IFAG
WP3	Cyber assurance and protection in an industrial cloud infrastructure	Patrizia Ciampoli	HPE
WP4	An end-to-end integrated industrial IoT cybersecurity framework	George Bravos	ITML
WP5	Real-life industrial demonstrations in smart manufacturing	Giuseppe D'Angelo	CRF
WP6	Exploitation, sustainability and business continuity	Marie-Noelle Lepareux	TSG
WP7	Project Management	Sotiris Ioannidis	FORTH

Reporting

We have set up a written, quarterly report mechanism, where partners report on a series of accomplishments or issues that have arisen during that period. Specifically, they report on: major achievements, progress per work package, status of deliverables, deviations from the work-plan, project meetings/teleconferences attended, conferences/standardization meetings attended, status of publications, status of talks given, and any other important achievements related to the project.

Deviations and corrective actions

The deviations and corrective actions were the following:

- **Deliverable D1.2:** The consortium created a report (named 'Validation of Requirements'), as an extension of Deliverable D1.2, to further validate the D1.2 requirements with external stakeholders was identified.
- **Deliverable D5.2:** The submission of this deliverable was delayed 4 months, mainly due to limited access to the factory environment of the CRF Campus Melfi plant, as a consequence of the Covid-19 restrictions.
- **Deliverable D6.2:** The deliverable was revised and resubmitted at M22, after reviewers' comments on midterm review.
- **Deliverable D6.4:** Deliverable was resubmitted after reviewer feedback at M22.
- **Deliverable D6.5:** The submission of this Deliverable was delayed 10 days due to extra efforts in terms of exploitation plans (both individual and joint), taking into consideration all aspects of final project deliverable.

Consortium Changes

The project does not report any changes during the period with respect to the description of work.

Deliverables and Milestones tables

During the period, the following deliverables have been submitted to the European Commission, and the following milestones have been met:

Del.ID	Deliverable title	Diss.	Planned Date	Submission date	Comments
D6.1	Project website	PU	M2	M2	
D7.1	Initial version of Project handbook	PU	M3	M3	
D1.1	C4IIOT innovations for Industrial IoT systems	PU	M4	M4	
D6.2	Market analysis and preliminary business modelling	PU	M4	M22	The deliverable was revised and resubmitted at M22, after reviewers' comments on midterm review.
D1.2	Positioning of C4IIOT	CO	M6	M6	The consortium created a report (named 'Validation of Requirements'), as an extension of Deliverable D1.2, to further validate the D1.2 requirements with external stakeholders was identified.
D1.3	Architecture definition	PU	M6	M6	
D2.1	Analysis of edge-node assets	CO	M6	M6	
D7.2	Data Management Plan	CO	M6	M6	
D2.2	Deep learning breakthroughs and security-aware dynamic offloading mechanisms	PU	M12	M12	
D3.1	Behavioural analysis and cognitive security framework	PU	M12	M12	
D3.2	Mitigation engine	PU	M12	M12	
D4.1	Assurance, privacy and accountability in all Industrial IoT processes	CO	M12	M12	
D4.2	C4IIOT Minimum Viable Product	PU	M12	M12	
D6.3	Interim Version of Dissemination strategy and activities	PU	M12	M12	
D6.4	Exploitation and standardization activities and best practices – initial version	PU	M12	M22	Deliverable was resubmitted after reviewer feedback at M22.
D7.3	First year project report	PU	M12	M12	
D2.3	Level-1 security mechanism of C4IIOT: Hardware-enabled security	PU	M18	M18	

D3.3	Level-2 and Level-3 security mechanisms of C4IIOT	PU	M18	M18	
D5.1	C4IIOT Demonstration - initial execution and evaluation	CO	M18	M18	
D4.3 (interim Version)	C4IIOT integrated framework (*Interim version – Final at M30)	PU	M18	M18	The interim version was given to the PO and reviewers for our first review at M18
D6.6	Dissemination strategy and activities	PU	M24	M24	
D6.5	Exploitation and standardization activities and best practices – final version	PU	M24	M25	The submission of this Deliverable was delayed 10 days due to extra efforts in terms of exploitation plans (both individual and joint), taking into consideration all aspects of final project deliverable
D7.4	Final Version of Project handbook	PU	M24	M24	
D7.5	Second year project report	PU	M24	M24	
D4.3	C4IIOT integrated framework	PU	M30	M30	
D2.4	Security and trustworthiness at the edge	PU	M30	M30	
D3.4	Cyber assurance and protection in an industrial cloud infrastructure	PU	M30	M30	
D5.2	C4IIOT Demonstration - final execution	PU	M30	M34	The submission of this deliverable was delayed 4 months, mainly due to limited access to the factory environment of the CRF Campus Melfi plant, as a consequence of the Covid-19 restrictions.
D4.4	Best practices for maintaining and operating the framework in the long-term – TRL 6	PU	M36	M36	
D5.3	Assessment report and impact analysis	PU	M36	M36	
D6.7	Final business model and long-term sustainability report	PU	M36	M36	
D7.6	Final project report	PU	M36	M36	

Table 2: Deliverables submitted

	Milestone Title	WP	Lead	Due	Verification	Comments
MS1	C4IIOT set-up: Requirements, initial	WP1, WP6	UP1PS	M6	Delivery of C4IIOT requirements analysis,	

	architecture and preliminary business models				set-up, architecture and dissemination/exploitation plans (D1.1- D1.3, D6.2)	
MS2	Proof of concept through C4IIOT MVP	WP2, WP3, WP4	IFAG	M12	Delivery of the C4IIOT MVP to be available for proof of concept (D4.2)	
MS3	1st version of Integrated platform and of C4IIOT Level-1, Level-2 and Level-3 security mechanisms; initial execution of demonstrators	WP2, WP3, WP4	HPE	M18	1st version of C4IIOT platform functional (1st version of D4.3); C4IIOT Level-1, Level-2 and Level-3 security mechanisms delivered (D2.3, D3.3); 1st demonstrator report D5.1	
MS4	Dissemination, Exploitation and standardization landmark	WP6	TSG	M18	Exploitation, dissemination and standardization reports (D6.3, D6.5)	This milestone was reached by the submission of D6.5 at M25 which was originally planned for M24.
MS5	Final version of Integrated platform and execution of demonstrators	WP4, WP5	CRF	M30	Final version of C4IIOT platform functional (final version of D4.3); final demonstrators report (D5.2)	The milestone was delayed along with the Deliverable D5.2 and was reached at M34
MS6	Final assessment, impact analysis and business plan	WP5, WP6	TSG	M36	Final assessment report (D5.3); Business models ready (D6.6)	MS6 will be achieved through the final assessment report in D5.3 and the definition of business models in D6.6. The Deliverable D5.3 has not been finished as to the time of submitting this document, but rather in a later point in time.

Table 3: Milestones reached

Explanation on use of resources

Project resource usage in terms of personnel effort will be reported again at the second reporting period, which is at M36.

Financial statements and summary financial report

Project costs will be reported again at the second reporting period, which is at M36.

2 Risk management Analysis

The main risk risen during the development of C4IIoT was related to the COVID-19 pandemic. In particular, the pandemic enforced a temporary closure and suspension of the FCA operations (March 2020), resulting to obstacles in the development of C4IIoT building blocks/components. We note that FCA/CRF is the solo pilot of our project. To overcome this situation, the consortium decided to proceed with the integration of the components in a separate environment, hosted in a public cloud. By doing so, the integration of the components continued smoothly, without being jeopardized by the closed CRF's Campus Melfi plant. In addition, the C4IIoT consortium has adopted a remote integration process which reduced the needs of physical access to the minimum. As the suspension was moving away, the integrated platform moved to the CRF's environment.

Moreover, to counteract the cancelation of dissemination, communication and exploitation events that require physical participation, we decided to organize our events (such as summer schools, info days, etc.) online using virtual conferencing systems, allowing remote attendance. The same happened for the periodic and non-periodic meetings as well as the GA project meetings. They were hosted over teleconferencing systems (such as Microsoft Teams). In principle, the management of the project, and the corresponding coordination and collaboration activities, were shifted to a fully remote model.