Horizon 2020 Program

Dynamic countering of cyber-attacks

SU-ICT-2018

Cyber security 4.0: Protecting the Industrial Internet of Things

D7.3: <First Year Project Report>[†]

Abstract: In this report we present the progress conducted in the C4IIoT project over the period of Year 1. 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	31/5/2020
Actual Date of Delivery	30/5/2020
Deliverable Security Class	Public
Editor	*Giorgos Tsirantonakis (FORTH)*
Contributors	All *C4IIoT* partners
Quality Assurance	*Marie-Noëlle Lepareux (Thales)* *Konstantinos Fysarakis (STS)*

[†] *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. *Marie-Noëlle Lepareux (Beneficiary short name)*
2. *Konstantinos Fysarakis (Beneficiary short name)*

Revisions

Version	Date	By	Overview
7.3.3	30/5/2020	Giorgos Tsirantonakis	2nd Revised Version
7.3.2	15/5/2020	Giorgos Tsirantonakis	1st Revised Version
7.3.1	1/4/2020	Giorgos Tsirantonakis	First Draft

Table of Contents

List of Tables

List of Figures

List of Abbreviations

EC European Commission

MVP Minimum Viable Product

WP Work Package

Executive Summary

This deliverable describes C4IIoT's progress, covering active work package during the first 12 months of the project. In this context, this deliverable 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 2 Milestones within the reporting period, published all planned deliverables on time. There are no significant deviations to report.

1 Overview of project scientific and technical objectives for Year 1

The Industry 4.0 revolution has enforced industrial systems and elements to interface over Internet communication technologies, in order to form the manufacturing organizations of the future also known as Smart Factories. However, a major barrier towards the full adoption of IoT, and, in particular IIoT, lies in a diverge set of cybersecurity issues, which makes it extremely challenging to harness the full potential of these technologies.

The C4IIoT framework adopts, customizes and advances the best practices for IoT cybersecurity across the full stack of typical Industrial IoT environments. Along these lines, C4IIoT has set out some clear scientific and technical objectives as defined in the Description of Work. Specifically, (1) Develop, validate, demonstrate, & support a holistic and disruptive and end-to-end Cybersecurity 4.0 framework for prevention & protection against Industrial IoT cyber-attacks, (2) Explore C4IIoT framework in the automotive Industry and validate its potential in rea-world settings, (3) Offer real-time malicious and anomalous behavior anticipation, detection, tracking, mitigation and end-user informing, within evolving IIoT applications and processes, (4) Consolidate international and European links, collaborate with standardizations bodies and ensure transferability of project's results, and (5) Boost the effectiveness of the European Security Union against cyberattacks in IIoT infrastructures, by offering almost ready to market solutions (TRL 6).

During the first year, the project focused on defining the requirements, initial architecture and preliminary business model of the project and producing the MVP (Minimum Viable Product). Implementation and integration of the techniques in the pilots will commence in year two.

Details on the scientific and technical achievements of the project can be found in the submitted technical deliverables (namely D1.2, D1.3, D2.1, D2.2, D3.1, D3.2, D4.1 and D4.2). Achievements on the way to disseminate on the project and exploit it can be found in the deliverable of WP6 D6.1, D6.2, D6.3 and D6.4.

2 Detailed scientific and technical achievements during Year 1

2.1 WP1 – Setting the scene: project set up

2.1.1 Work-package objectives for the period

WP1 is led by UP1PS and started on M1 (June 2019). Four tasks are active during the reporting period:

Task1.1. (M1 to M4) led by UP1PS. *The critical role of C4IIOT in protecting Industrial IoT systems and technologies*, described in deliverable D1.1.

Task1.2. (M1 to M6) led by UOG. *Adapting C4IIOT security components to real-life industrial manufacturing environments*, described in deliverable D1.2

Task1.3. (M3 to M6) led by UNSPMF. *Technology convergence: specifications and C4IIOT architecture*, described in deliverable D1.3

Task1.4. (M3 to M6) led by CEA. *Demonstration protocol – real life industrial pilots*, described in deliverable D1.2

Details on the activities carried out during the reporting period in the context of these Tasks are presented below.

Task1.1:

A review of the literature and solutions on all relevant technologies has been performed and the defined C4IIoT innovations have been presented against existing solutions. This has been summarized in the deliverable D1.1.

Task1.2:

(a)The fundamental assets that must be protected, (b) The common and important security threats to these assets that C4IIoT will mitigate, both have been identified in FCA's environment: This identification is part of the deliverable D1.2.

Task1.3:

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

Task1.4:

One has specified how the demonstrators will work in real-life industrial conditions, including arrangements for how they will be run and what processes need to be put in place to check that the output is both correct and valid. It is a part of the deliverable D1.2.

2.1.2 Deliverables

D1.1 C4IIoT innovations for Industrial IoT systems:

Literature review of all relevant technologies and defined C4IIoT innovations against existing solutions.

D1.2. Positioning of C4IIoT:

Specification of FCA's environments assets to be protected, threats to these assets, together with the protocol to demonstrate the mitigation to these threats in FCA's environment.

D1.3. Architecture definition:

High-level specification of software, hardware and networking distributed architecture of the C4IIoT framework and their relationships with FCA's environment.

2.1.3 Deviations and corrective actions

There were no deviations to report during this period.

2.2 WP2 – Edge computing cybersecurity technologies

2.2.1 Work-package objectives for the period

WP2 is led by IFAG and started on M4 (September 2019). Four tasks are active during the period:

Task2.1 (M4 to M18) led by VIP. *Provision, configuration and management of edge-node assets*, described in deliverable D2.1, D2.3 and D2.4.

Task2.2. (M6 to M30) led by UNSPMF. *Deep learning trained models deployed at the edge,* described in deliverable D2.2, D2.3 and D2.4.

Task2.3. (M6 to M30) led by UOG. *Security-aware dynamic offloading decision mechanism,* described in deliverable D2.2, D2.3 and D2.4.

Task2.4. (M6 to M30) led by IFAG. *Security and trustworthiness at the edge,* described in deliverable D2.3 and D2.4.

The work carried out in these tasks is being described in the following deliverables, some of them are already submitted:

D2.1: Analysis of edge-node assets which was submitted on M6 by VIP.

D2.2: Deep learning breakthroughs and security-aware dynamic offloading mechanisms which was submitted on M12 by UOG.

D2.3: Level-1 security mechanism of C4IIOT: Hardware-enabled security, which will be submitted by FORTH on M18.

D2.4: Security and trustworthiness at the edge which will be submitted by IFAG on M30.

Details on the activities carried out during the reporting period in the context of these Tasks are presented below.

Task 2.1:

This task is led by VIP with contributions from CRF, IFAG and UNSPMF. This task started on M4 (September). This task is devoted to ensure proper provision, configuration, and management of edge-node assets, including IIoT(sensors) devices and network elements (field gateways). In order to reach that during the Plenary meeting in Turin, CRF did a gap analysis of his existing devices and communications. With this analysis, the specifications to carry out

the agreed improvements were defined and are reflected in the corresponding deliverables. Especially two scenarios were distinguished: smart factory and logistics. On M9 in the Plenary meeting in Athens, VIP and UNSPMF showed different versions of the edge node in logistics use case with the power consumption. IFAG made a secure personal identification in the edge node smart factory use case and VIP explained the field gateway architecture.

Task 2.2:

This task is led by UNSPMF with contributions from FORTH, IFAG, ITML and UOG. This task started on M6 (November) and will enable that the machine learning methods that perform detection of complex anomalous and malicious behaviour can be implemented in a distributed way. In the Plenary meeting in Turin, UNSPMF provided an explanation of different learning methods and how to carry them out in edge nodes such a using federated learning. Also made clear the collaboration with UOG to provide information to the offloading mechanism. In Athens was explained the simulated environment that it will be use to the generation of the datasets and different potentially detectable threats. It was introduced the BACS (Behavioural Analysis and Cognitive Security) framework which has different tools for different environments and models.

Task 2.3:

This task is led by UOG with contributions from IFAG, ITML, UNSPMF and VIP. This task started on M6 (November) and it will design and implement the mechanisms needed to dynamically offload security-aware tasks at the edge. UOG introduced the MEDICI service as a tool of the security-aware dynamic offloading decisions. In Athens, MEDICI architecture was explained more in depth, differentiating between layers (edge-node, field gateway and cloud) and interactions between different modules.

Task 2.4:

This task is led by UOG with contributions from FORTH, CEA, UNSPMF and UOG. This task started on M6 (November) and it will build the tools and technologies for providing a secure execution environment for the edge IoT devices. IFAG provided a set of components to use in the two scenarios discussed in Turin: smart factory and logistics. IFAG introduced the IFAG Blockchain secure element shield to use in the logistics use case and the Blockchain 2go card form-factor in order to secure authentication in both use cases. In the smart factory use case IFAG introduced the IFAG TPM2.0. In Athens, IFAG explained the progress in the integration of the secure element in the edge-node and the communication with the Blockchain (Hyperledger Fabric). FORTH showed different architectures in the smart factory edge node: Raspberry Pi, NVIDIA Jetson, Mini PC Intel NUC.

2.2.2 Deliverables

D2.1. Analysis of edge-node assets:

This deliverable is the first output of the WP2 and the T2.1. This deliverable was submitted on M6 and contains requirements analysis on the C4IIoT edge node devices and the gap analysis on the CRF's existing edge nodes, including devices mounted on supply vehicles and devices installed in factory premises. It also provides a detailed design proposal of beyond the state-of-the-art of edge devices, which will be developed and fabricated to support the C4IIoT security requirements. Finally, an overview of test and evaluation scenarios, which will be simulated and tested.

D2.2. Deep learning breakthroughs and security-aware dynamic offloading mechanisms:

In this deliverable UOG lead the discussion about the offloading mechanisms and deep learning strategies, this deliverable is a demonstration of the components related to Tasks T2.2 and T2.3. This is a brief report describes the operation and so far deployment of the components and the initial results planned for this stage of the tasks. It have been discussed the deep learning mechanism deployed at the edge, especially BACS framework and related with the offloading mechanisms, the MEDICI service, as well as the hardware where it will be implemented. This deliverable is related with the MVP on M12.

D2.3**.** Level-1 security mechanism of C4IIOT: Hardware-enabled security:

This deliverable will be submitted on M18. It is a public demonstrator that deals with the security hardware enabled in the different edge nodes and use cases. This refers to both the hardware modules used and the software used for integration with the microcontroller. For example, OPTIGA Trust from IFAG or Secure Execution Environment from FORTH. It is linked to tasks T2.1, T2.2, T2.3 and T2.4.

D2.4. Security and trustworthiness at the edge:

This deliverable is a public demonstrator about the mechanisms related to get security device-to-device such a Block-chain, it is related with tasks T2.1, T2.2, T2.3 and T2.4. In this document will be discuss about the implementation the block-chain technologies on edge devices and the integration with them. It will be submitted on M30.

2.2.3 Deviations and corrective actions

There were no deviations during the period.

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

2.3.1 Work-package objectives for the period

WP3 is led by HPE and started on M4 (September 2019). Four tasks are active during the period:

Task3.1. (M4 to M30) led by HPE. *Resource management and orchestration*, described in deliverable D3.1, D3.3 and D3.4.

Task3.2. (M4 to M30) led by UNSPMF. *Behavioural analysis and cognitive security framework,* described in deliverable D3.1, D3.3 and D3.4.

Task3.3. (M6 to M30) led by CEA. *Mitigation engine*, described in deliverable D3.2, D3.3 and D3.4.

Task3.4. (M6 to M30) led by IBM. *Trustworthiness of data flows*, described in deliverable D3.3 and D3.4.

Details on the activities carried out during the reporting period in the context of these Tasks are presented below.

Task 3.1:

The focus of Task 3.1 is the "Resource Management and Orchestration" of the cloud environment to: configure the infrastructure resources (provided by the consortium) needed by the cloud-hosted C4IIoT modules; create automates mechanism to seamless integrate and configure cloud resources; support build, deploy and manage C4IIoT modules inside a hybrid cloud environment.

During the first 12 months, the T3.1 team has set up an internal laboratory to be moved to the hosting cloud architecture as ready. The laboratory has started developing the cloud Gateway that is to host and orchestrate inside a "cloud" several modules, e.g. Mitigation Engine, Security Assurance, ML-based Behavioural Analysis, Advanced Anomaly detection, etc.

Up to now the developments contain the definition of the orchestration mechanism, the cloud gateway module and the security policies and controls to securely managing the Docker container images. Details explanation is found in deliverable D3.1 at section 3.

Task 3.2:

The main goal of this task is to develop the 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 (Behavioural Analysis & Cognitive Security Framework). These models is based on UNSPMF's work on advanced deep learning techniques to provide more powerful contextual information and form an advanced anomaly detection model for the complete IoT ecosystem considering each device not in isolation but including their interactions too.

The activities for this period includes development of the behavioural analysis experiments focusing on edge node layer scenarios, generating of the new data using our simulated environment by simulating container transportation and implementation of the outlier detection mechanisms.

The experimental analysis of anomaly detection models is based on outlier detection algorithms. It includes analysis of training time, inference time and model size. Anomaly detection in C is based on one-class Support Vector Machine and is deployed to a custom-board microcontroller device.

The BACS implementation includes three main packages: BACSCL, BACSPY and BACSC. BACSCL package implements AD models, based on deep auto-encoder/neural network forests. BACSPY is based on various outlier detection, classification and representation learning algorithms applied to multivariate time series. BACSC is lightweight anomaly detection implemented in C for constrained, low-power edge node devices. It includes lightweight auto-encoder inference C routines.

Task 3.3:

This task is led by CEA with contributions from TSG, HPE, and UP1PS. This task started on M6 (November). An important part of the work in this task consisted in obtaining a deep understanding of the inputs that can be of use in the different technologies of the C4IIOT platform, and the possible reconfiguration actions that can be done, taking example from the use cases provided by CRF. This involved, for instance, aligning the notion of thread and risks with those in other components of the framework to properly evaluate those; understanding the use case network infrastructure to understand which alternative routes are available for reconfiguration; or understanding the kind of binary executables in use by the different C4IIOT components so as to find the binary analysis technique that would be the most useful to evaluate and mitigate software-level exploits. Based on those inputs, a planned architecture for the mitigation engine was presented during the Plenary meeting in Turin, which has been continuously refined since.

Task 3.4:

This task covers the detailed design and development of the building components composing the trust infrastructure. One of the key elements in this effort is the decentralized access control (DAC) solution providing security of data at rest. In the past year, IBM has worked on designing the DAC with attention to its integration in C4IIoT, including the Hyperledger Fabric (HLF) network and clients and the attribute-based encryption (ABE) components. IBM has started to implement a prototype of the DAC. In addition, IFAG has worked on integrating their secure element at the edge node layer with the DAC, to allow securing the edge node's proprietary data when interacting with the Hyperledger Fabric network.

2.3.2 Deliverables

D3.1. Behavioural analysis and cognitive security framework:

This document 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. Next, the 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 for that BACS behavioural models will use for increased security and privacy-awareness.

D3.2. Mitigation engine:

This deliverable presents the global architecture of the mitigation engine, with all the interactions between the mitigation engine and other components in the rest of the project. In addition, the specific instantiation of the three main mitigation engine components are described, i.e. how CEA's BINSEC, UP1PS's Variamos, and TSG's DISCO will be configured and modified to fit the project, and their different inputs and outputs (both internal and external to the mitigation engine). Finally, a specific focus is made on HPE's Cloud Layer Orchestrator, which is the main gateway used by the mitigation engine to communicate with the other mitigation engine components.

2.3.3 Deviations and corrective actions

There were no deviations during the period.

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

2.4.1 Work-package objectives for the period

WP4 is leaded by ITML and started on M8 (January 2020). The below-listed three tasks are active during the 1st year of the project implementation:

Task 4.1. (M8 to M30) led by STS. *Assurance, privacy and accountability in all Industrial IoT processes,* described in deliverable D4.1, D4.2 and D4.3.

Task 4.2. (M8 to M30) led by AEGIS. *Advanced informative mechanisms and interactive visualizations,* and described in deliverable D4.2 and D4.3.

Task 4.3. (M8 to M36) led by ITML. *Continuous integration towards the realization of C4IIOT framework,* described in deliverable D4.2 and D4.3.

Specifically, the work carried out within the tasks above is being described in:

- D4.1. Assurance, privacy and accountability in all Industrial IoT processes which was submitted on M12 by STS
- D4.2. C4IIOT Minimum Viable Product which was submitted on M12 by AEGIS and
- D4.3. C4IIOT integrated framework which will be submitted due M30 by ITML.

Details on the activities carried out during the reporting period in the context of these Tasks are presented below.

Task 4.1:

STS is leading Task 4.1 "Assurance, privacy and accountability in all Industrial IoT processes" with contributions from FORTH, IFAG, HPE, IBM, AEGIS, ITML, and UNSPMF. Activities in the context of T4.1 started on M8 of the project, i.e. on January 2020. As technical lead of T4.1, STS defined the ToC of the first output of the task, i.e., deliverable D4.1 ("Assurance, privacy and accountability in all Industrial IoT processes"), as well as defined a detailed time plan for the progress and contributions within the task and the associated deliverables. These, along with a presentation on the goals and scope of the deliverable, were communicated to the involved partners during the monthly calls and re-iterated during the Plenary meeting in Athens, whereby all involved partners agreed and committed on the suggested time plan and assignments. Consequently, by M8 (Jan. 2020) all partners agreed upon the finalised ToC and defined specific components that each will develop in the context of the Task. These included: (i) Identity Management; (ii) Risk Assessment; (iii) Security Assurance of C4IIoT Platform; (iv) Distributed Ledger Technologies for Auditability, Reliability And Accountability technologies, and; (v) Privacy Preservation Techniques. Building on this, by M9 (Feb. 2020) all involved partners presented the key research aspects pertaining to their components (rationale, background work and motivation). By M10 (March 2020) high level design specifications of the involved components where identified and documented within the deliverable (D4.1), while during the last phase, ending in M12 (May 2020), all partners provided implementation details and validation of the first versions of components, with particular focus on the features to be integrated into the MVP release (see D4.2).

Task 4.2:

AEGIS is leading "Task 4.2: Advanced informative mechanisms and interactive visualizations" which started on M8 (January 2020). Following (i) the definition of use cases; (ii) the description of the datasets that will be used in each use case scenario; and (iii) the description of visualisation needs in the GA we initially described the information we had to visualise. The interactive visualization and monitoring toolkit provided interfaces to visualize information coming from the runtime operation and at this stage the synthetic and sample data agreed for the MVP. Provided initial mock-ups served as a basis for discussion and commend from other partners and and-users. Given this feedback we modified and optimized the front-end design to end-up with user-friendly and efficient interfaces. The interfaces serve the scope of Situational Awareness and Data Monitoring for the information coming from the Cloud Layer. Also defined the format of exchanging data, which would be json and started implementing the communication methods.

Task 4.3:

ITML is leading "Task 4.3. Continuous integration towards the realization of C4IIOT framework" which started on M8 (January 2020) and will be active until the end of the project, driving the integration towards the envisioned releases of C4IIoT solution, namely a proof of concept demonstration (Minimum Viable Product (MVP) at M12, a 1st complete prototype that will be delivered internally at M18 and a 2nd prototype – the final solution that will be delivered on M30.

The work carried out by this task includes the following activities:

- Prevision of the preliminary analysis of the testing and integration plan for the C4IIoT platform (see D4.2).
- Analysis of the main tools and components (e.g. cyber assurance and protection, IoT, machine (deep) learning, edge/cloud computing, block-chain and Big Data technologies and tools) needed for the integration of our solution and especially for the MVP (see D4.2).
- Definition of the basis for the integration of developed components and provision of the hardware infrastructure used in the frame of the C4IIoT project (see D4.2).
- Illustration of the use case dataset selection process, data formatting and data flowing processes (see D4.2).
- Bringing in the MVP architecture and demonstrating the integration between the C4IIoT components and their distinct technologies (see D4.2).
- Driving the integration towards the 1st C4IIoT Prototype to offer security and privacy in an end-to-end industrial IoT environment in the automotive manufacturing domain (see T5.2, T5.3).

More specifically, this reporting period included 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 has 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 (see Del 4.2).

The main result of this reporting period is the delivery of the C4IIoT MVP, based on the architecture and the analysis carried out in WP1 and on the developments of the C4IIoT components in WP2 and WP3. The MVP was designed in order to demonstrate two real-life use case scenarios (Logistic 4.0 and Smart Factory) based on 2 complementary architectures.

2.4.2 Deliverables

D4.1. Assurance, privacy and accountability in all Industrial IoT processes:

This deliverable is the first output of T4.1 ("Assurance, privacy and accountability in all Industrial IoT processes"), and as such it documented the progress within the task, as reported in the task update above. The ToC, partner assignments and time plan for contributions was defined and agreed upon by M8, and three rounds of contributions were followed by all participating partners (first round by M9, second by M10, and final by M12). Throughout this

time, STS as the deliverable's main editor, was responsible for aggregating inputs, handling merging and version release, as well as the final editing of the deliverable.

D4.2. C4IIOT Minimum Viable Product:

AEGIS led the discussion about the definition of the use cases and scenarios and how these could be mapped to the MVP. In collaboration with other partners decided the use of both use cases defined in GA, Smart Factory and Logistics. Datasets for both cases described and for the purposes of MVP and we decided to use synthetic datasets that aim to be as realistic as possible to the datasets of the real-life environment. In parallel with the integration process we defined the modules which consist the MVP version of C4IIoT framework and the role of each module. For the scope of this deliverable we requested contribution from partners involved to describe the functionality of their offered module. Finally, we described an end-to-end process flow with well specified role for each component and submitted the deliverable on time.

D4.3. C4IIOT integrated framework:

The final version of D4.3 will be delivered in M30 by ITML. D4.3 constitutes the 2nd prototype of the C4IIoT integrated solution that will be implemented in the defined real-life use case scenarios in order to be evaluated and validated. The 1st prototype will be delivered internally and will be circulated among the partners in M18.

2.4.3 Deviations and corrective actions

There were no deviations during the period.

2.5 WP5 – Real-life industrial demonstrations in smart manufacturing

2.5.1 Work-package objectives for the period

WP5 is led by CRF and started on M10 (March 2020). Three tasks are active during the period:

Task5.1. (M10 to M18) led by ITML. *Demonstration protocol alignment*, described in deliverable D5.1.

Task5.2. (M10 to M36) led by CRF. *Framework deployment and execution of real-life industrial demonstrations*, described in deliverable D5.1, D5.2 and D5.3.

Details on the activities carried out during the reporting period in the context of these Tasks are presented below.

Task 5.1:

The task has been active from M10. Taking up the results of T1.3, the partners in the task are drafting the preparatory actions for the field demos as well as the integration of the system modules for the trials execution: this includes the definition of systems, actors and steps.

Task 5.2:

The task has been active from M10. The partners in the task are defining the demonstration environment in which the C4IIOT platform will be demonstrated. To this respect a sandbox implemented in the Campus Melfi facility and enabling the test of different architectures,

combining simulated and real hardware and software is being sketched. Preliminary and historical data from the Campus Melfi industrial systems has been shared within the consortium.

2.5.2 Deliverables

D5.1. C4IIOT Demonstration - initial execution and evaluation:

This deliverable includes the reporting regarding the demonstration protocol alignment and relevant activities. More specifically refinement of pilots, integration of system modules, refined execution parameters, KPIs, evaluation parameters and guidelines for the demonstration execution will be reported. This deliverable will also include results of the initial execution of the demonstrators and evaluation outcome.

D5.2. C4IIOT Demonstration - final execution:

This deliverable will include the reporting regarding the two pilots developed in CRF for both Logistics and Factory use-cases and the relevant activities carried-out for the development of the demonstrator. In particular, the usage of C4IIOT architecture in CRF premises will be explained, describing all the tests carried out, the equipment that have been involved, the parameters evaluated and the results obtained.

2.5.3 Deviations and corrective actions

There were no deviations during the period.

2.6 WP6 – Exploitation, sustainability and business continuity

2.6.1 Work-package objectives for the period

WP6 is led by Thales and started on M1 (June 2019). Four tasks are active during the period:

Task 6.1. (M1 to M6) led by VIP. *Market definition and analysis*, described in deliverable D6.2.

Task 6.2. (M1 to M36) led by AEGIS. *Communication strategy triggering awareness and new business opportunities*, described in deliverable D6.1

Task 6.3. (M6 to M36) led by IFAG. *Exploitation activities*, described in deliverable D6.3

Task 6.4. (M1 to M36) led by Thales. *Standardization activities and best practices*, described in deliverable D6.4

Details on the activities carried out during the reporting period in the context of these Tasks are presented below.

Task 6.1:

This task is led by AEGIS and has been active during the 6 first months of the project and was initiated in the Section 2.2.4. of the Description of Work. It has been concretised in D6.2 by a market analysis and a formulation of the business models.

The task has consisted in a comprehensive market study, focusing the scope of IOT, IIOT and IOT cybersecurity. It has quantified the size of the market, identified the key competitors, the market needs and trends, the stakeholders, the possible clients and users. It has used different analytical tools such as PEST and SWOT to quantify the competitive advantages.

The study has formulated potential business models to exploit the project outcomes.

The methodology employed in this task is based on desk research techniques via literature review, partner knowledge and targeted analysis of domain experts and market research companies.

Task 6.2:

This task also led by AEGIS is active throughout the project. During the first year, it has consisted in a preparation of the communication tools especially the C4IIOT dedicated web site and an identification of the events relevant to the project where it will be possible to communicate. The C4IIOT website is the most powerful tool for boosting information flow between the entities involved.

Task 6.3:

This task led by IFAG started at M6. It collects the exploitation plan of each partner and published them in the deliverable D6.4.

Task 6.4:

The task led by Thales is active throughout the project.

During the first year, from one part, it has identified and classified the organisations producing standards, directives and open-source software which are relevant to the project and from the other part, it has identified the technologies and architectures used in C4IIOT, which are based on standards or open source software. A research of the membership of each partner in the different organisations has also been performed.

A cross-table has been established to highlight the possible participation in the standardisation organisations depending on each partner and based on the innovative technics employed in C4IIOT, such as the specific usage of the block-chain or the edge computing for anomaly detection.

2.6.2 Deliverables

D6.1. Project website:

The structure of the project web site and the measure of its activity through the Google Analytics platform are described in the deliverable D6.1.

The project website has been publicly accessible since the early stage of the project and several updates will be implemented as a result of adaptation to constantly effective online dissemination activity and emerging project results.

D6.2. Market analysis and preliminary business modelling:

This deliverable includes an overview of the IOT market analysis, an IOT cybersecurity market analysis including the market segmentation from the IOT security industry, the trends in Europe, their dynamicity and a stakeholder analysis. It includes also a preliminary business model.

It is formulated with the help of Business Model Canvas which visualizes the elements to describe the nine fundamental elements that show the logic of developing profit for a company: Customer Segments, Value Proposition, Channels, Customer Relationships, Revenue Streams, Key Resources, Key Activities, Key Partners, Cost Structure

The business model of C4IIOT is a multi-sided one, as there is more than one type of customers that have interest on the service provided. From the analysis of the business model canvas, each building block considers the different types of customers that the developed platform needs to serve.

This market analysis will be revised, feeding with updated market dynamics the final business model to be adopted.

D6.3. Interim Version of Dissemination strategy and activities:

This deliverable presents the work performed in WP6 – Task 6.2 "Communication strategy triggering awareness and new business opportunities" and consists of two parts. The first one refers to the definition of C4IIot dissemination strategy, and the second one to the reporting and monitoring of the respective dissemination and communication activities during the first year of the project (M1-M12). AEGIS led the dissemination activities for the reported period and for the purposes of this deliverable collected dissemination activities and individual dissemination plans from all partners. AEGIS submitted the deliverable on time.

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

The deliverable is a joint result of the tasks 6.3 and 6.4, the standardisation activities being considered as a starting point of the exploitation of the project. Therefore, the deliverable starts by a classification of the more important organisations writing directives relevant to cybersecurity in IIOT. It identifies the directives, standards or open-source software used in the different technics brought by the partners and identifies the participation of each partner in the different SDOs. It identifies where and how the C4IIOT innovations can influence the standards, either by a participation in the writing of whitepapers as part of the dissemination strategy, either in a true active participation in a SDO.

The main suggested proposals to really influence such an SDO or an OSS foundation could concern the technics of Access control through the Hyperledger Fabric with the support of IBM, and the way to share intelligence against cyber-attacks at the edge e.g. through IEC Edge Computing WGs whitepapers writing.

2.6.3 Deviations and corrective actions

The COVID19 crisis has an impact on certain dissemination activities as both the trips and the physical meetings are forbidden. In particular the information day supposed to take place at M12 will be postponed.

2.7 WP7 – Project Management

2.7.1 Work-package objectives for the period

The active tasks during this period is T7.1: "Project quality planning", T7.2: "Day-to-day management, project & financial control and resource monitoring" and T7.3: "Innovation

Management". The deliverables for the first year were the creation of the C4IIoT handbook (D7.1), the data management plan (D7.2) and the C4IIoT first year progress report (D7.3).

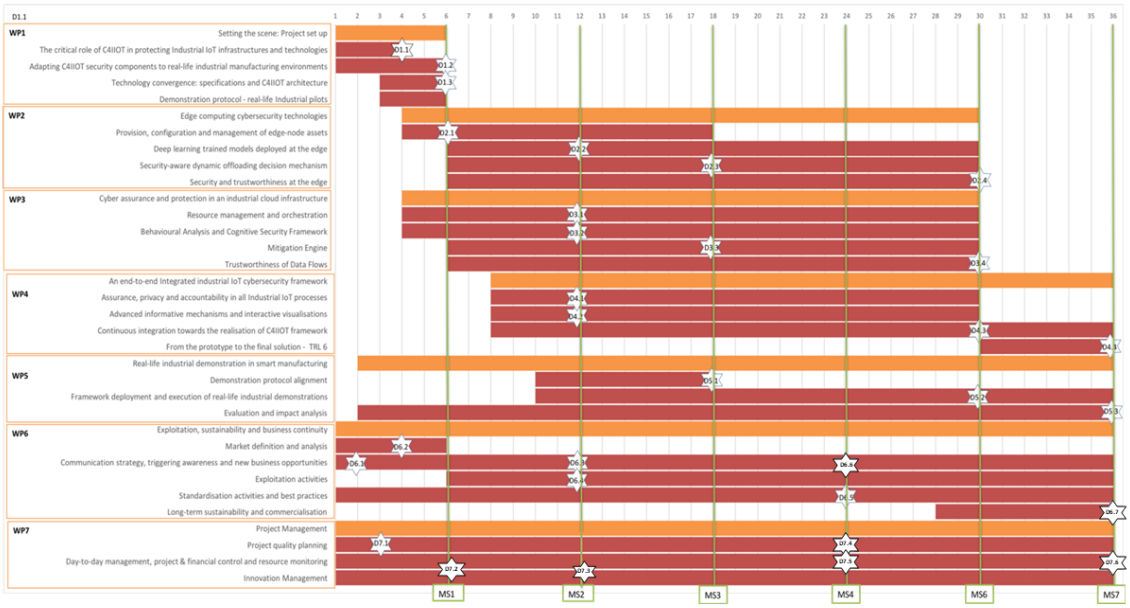

Figure 1: Milestones and Deliverables

2.7.2 Deliverables

Deliverable 7.1 – C4IIoT 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.

Deliverable 7.2 – Data Management Plan

This document provides an initial 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. This is the 1st version of this deliverable. Since DMP is a living document, it will be updated to reflect significant changes that may arise in the data sources exploited in the project and on policies and methodologies to be used as the project evolves.

2.7.3 Project Meetings

Both physical meetings and teleconferences have proven very efficient to support the required discussions when elaborating deliverables. Physical meetings take place every four months while teleconferences are scheduled every month.

Plenary Meetings

The project has held three physical meetings during the period.

- 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

For work-package related activities, the project is holding on-line meetings using Webex. Teleconferences are generally one hour on average and focused on specific action points, maximizing efficiency and attendance. The following on-line meetings have been held during the first period of the project.

Work package	Date	Duration	Attendees	Summary of
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.

Table 1: List of C4IIoT Teleconferences

2.7.4 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.

2.7.5 Deviations and corrective actions

The project did not hold an External Advisory Board (EAB) meeting during the first year. This was done on purpose as we were still working on the requirements specification as well as the development of the first round of security technologies. Overall, the project is on track in terms of scientific and technical outputs. Also all the partners are performing at a satisfactory level.

2.7.6 Consortium Changes

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

2.8 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	Del.title	Vers.	Diss.	Planned Date	Delivery date	Comments
D6.1	Project website	1.0	PU	M2	M2	
D7.1	Initial version of Project handbook	1.0	PU	M3	M3	
D1.1	C4IIOT innovations for Industrial IoT systems	1.0	PU	M4	M4	
D6.2	Market analysis and preliminary business modelling	1.0	PU	M4	M4	

D1.2	Positioning of C4IIOT	1.0	CO	M6	M6	
D1.3	Architecture definition	1.0	PU	M6	M6	
D2.1	Analysis of edge-node assets	1.0	CO	M6	M6	
D7.2	Data Management Plan	1.0	CO	M6	M6	
D2.2	Deep learning breakthroughs and security-aware dynamic offloading mechanisms	1.0	PU	M12	M12	
D3.1	Behavioural analysis and cognitive security framework	1.0	PU	M12	M12	
D3.2	Mitigation engine	1.0	PU	M12	M12	
D4.1	Assurance, privacy and accountability in all Industrial IoT processes	1.0	CO	M12	M12	
D4.2	C4IIOT Minimum Viable Product	1.0	PU	M12	M12	
D6.3	Interim Version of Dissemination strategy and activities	1.0	PU	M12	M12	
D6.4	Exploitation and standardization activities and best practices – initial version	1.0	PU	M12	M12	
D7.3	First year project report	1.0	PU	M12	M12	

Table 2: Deliverables submitted

Milestone Number	Milestone Title	WP	Lead beneficiary	Due Date	Verification	Comments
MS1	C4IIOT set-up: Requirements, initial architecture and preliminary business models	WP1, WP6	UP1PS	M6	Delivery of C4IIOT requirements analysis, 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)	

Table 3: Milestones reached

2.9 Explanation on use of resources

Project resource usage in terms of personnel effort will be reported at the first reporting period, which is at M18.

2.10 Financial statements and summary financial report

Project costs will be reported at the first reporting period, which is at M18.

3 Project planned activities for next period

3.1 WP1 – Setting the scene: project set up

WP1 has ended, so no further activities are planned.

3.2 WP2 – Edge computing cybersecurity technologies

Task 2.1 – Next Steps:

For the next period, the efforts within this task will focus on implementing machine learning algorithms on edge nodes and field gateways. The detection of anomalous behaviours or integrity failures will support an adapted and (if possible) automatic firmware updates. The establishment of a VPN connection between the field gateway and the cloud will be considered. A focus will be made on the emulation of different scenarios at the edge node, in the context of the logistics use case.

Task 2.2 – Next Steps:

The main issue and area of future work will be the generation of datasets, which is a key point to initiate the training of the machine learning algorithms. The integration with other components, such as MEDICI service and the mitigation engine, will be pursued.

Task 2.3 – Next Steps:

The improvement and the integration of the MEDICI services will be the next steps: communications of MEDICI agents with anomaly detection modules, generating initial execution history data and deployment and management of MEDICI agents on edge devices, field gateways and cloud platforms.

Task 2.4 – Next Steps:

Once the integration of the safe element in the smart factory use case the next steps are to extend the functionality to other use cases with other secure elements. For example in the logistics use case it will be integrate a programmable secure element.

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

Task 3.1 – Next Steps:

In the upcoming months T3.1 will support the deployment of the Cloud Layer C4IIoT modules as well as the provision of internal services to other layers (e.g. private docker image registry, image signing, image vulnerability scanning, s3-compliant storage, etc.). Moreover the interaction with Mitigation Engine and Attribute Based Encryption modules will be refined and integrated.

Task includes supporting activities to move the PKI in the K8S and the integration study for the C4IIOT with the creation of the supporting documents and enrolment of certificates.

In next period will be investigation about User Entity Behavioural analytics and the feasibility of the introduction of these functionalities on C4IIOT.

Task 3.2 – Next Steps:

Plan for the next period is to finalize implementation of federated auto-encoders, to demonstrate AD on robotic arms datasets and supervised anomaly detection on FORTH netflow datasets. It is also planned to make experimental analysis of currently implemented BACS unsupervised AD models using FORTH netflow dataset and to make extended testing of the integrated AD into microcontroller firmware.

Task 3.3 – Next Steps:

The next step will consist in implementing the missing parts of the mitigation engine architecture, and working on a prototype, where all the main components of the mitigation engine (DISCO, BINSEC, Variamos) are further integrated together, with the Cloud Layer Orchestrator, and with the other components of the project.

Task 3.4 – Next Steps:

Planned activities for this task include continuing developing the decentralized access control (DAC) into a mature solution that is well-integrated within the C4IIoT framework. This includes further working on implementing the various components of the DAC and their features, and integrating the DAC with the components that use it (either as data producers, as data consumers or otherwise), with IFAG's secure element at edge nodes, and with HPE's identity management solution.

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

Task 4.1 – Next Steps:

After M12 and the release of the MVP, efforts will focus on refining the design and progress on the implementation of the various building blocks developed in the context of T4.1. In this regard, the experience and feedback from the MVP development and evaluation, along with the finalisation of the C4IIoT architecture, will be crucial to further refine the design and specification of the developed components, to better accommodate the expected interactions with other components, as well as their role within the C4IIoT solution in general. As the components' implementation progresses across the various Tasks, with more features being implemented, and moving towards the later stages of the T4.1, efforts will focus on the interplay between T4.1 and other tasks (e.g., block-chain techniques also in the scope of T3.4, or interactions with the mitigation engine of T3.3 and the visualisations of T4.2), also accommodating the various interactions anticipated in the final C4IIoT architecture.

Task 4.2 – Next Steps:

With implementation made so far as a basis for future improvements and additions the advanced. The Visualization toolkit will continue grow up to serve more advanced features needed for the C4IIoT framework. As information coming from the runtime information and more modules added to the integrated solution more features and interfaces will be added. First step will be to implement mock-ups designed for the C4IIoT MVP to a dynamic real-time environment. As information coming from the runtime information and more modules added to the integrated solution more features and interfaces will be added. The toolkit will offer informative mechanisms for predicted security threats, current incidents and the system actions to mitigate them and finally forensic information to analyse and understand the cause of a problem so us to take preventive measures for the future. The visualization toolkit offers a

flexible and expandable solution and it will be constantly adapted to support the emerging visualization needs of the real-life industrial demonstrations.

Task 4.3 – Next Steps:

After the MVP delivery, ITML's efforts will focus on (i) preparing an integration plan which will detail how and when all the individual technical elements of the C4IIOT solution will be adapted and integrated in the final common framework; (ii) defining the appropriate test cases to drive the technical evaluation of the solution and ensure that it passes key quality tests before being released. Quality tests will follow the Quality Assurance and Control procedures (ISO 9004:2018) of the project (T7.1) and will include as benchmarks those defined in T1.3, T1.4, T6.4. and (iii) releasing the 1st integrated prototype of the C4IIoT solution.

3.5 WP5 – Real-life industrial demonstrations in smart manufacturing

Within the next period (M13-M24), the work package will proceed with the elicitation of the demonstration protocol (T5.1) and the preparation of the real-life industrial demonstration (T5.2), both leading to D5.1. Concurrently the Task 5.3 will proceed by analysing the data sources and define the KPIs calculation method and proceed with a quantitative approach for a business case, built by comparing the AS-IS process ("baseline") and the TO-BE process enabled by C4IIOT, a quantification on return on investment and a qualitative approach (SWOT, other).

3.6 WP6 – Exploitation, sustainability and business continuity

Task 6.1 – Next Steps:

Revisions regarding the usability of the website with respect to the end-user will be made to update with contribution of content by all consortium members.

Task 6.3 – Next Steps:

The individual exploitation plans of each partner will be consolidated and a true exploitation plan for the whole projects results will be elaborated. This will be the purpose of the deliverable D6.5 at M4.

Task 6.4 – Next Steps:

After having identified the more relevant organisations, it will be possible to add missing ones. The ultimate goal is to be present and efficient in as many organizations as possible.

The task will also continue to investigate the technologies and their usage which are the most relevant in order to be presented in one standardisation organisation.

For the time being, the targeted technologies are focusing the edge intelligence and the block-chain. They will be more deeply considered in the next period with the goal to constitute a main purpose of the standardisation activity.

In particular, the targets of edge intelligence computing will be pursuit after having collected all results of anomaly detection by machine learning from UNSPMF and the efficiency of the UOG MEDICI tool and the presentation of the usage of Hyperledger Fabrik in access control is expected thanks to IBM involving in this OSS, or by default in another SDO focusing on block-chain.

A participation to TCG (Trusted Computing Group) is also expected due to the membership of IFAG and Thales depending on the mitigation solution of the project and of the TPMs effectively in use.

3.7 WP7 – Project Management

In terms of coordination and tools, the project is balanced between physical meetings and teleconferences. We plan to continue along the same path, in order to continue our activities.