Horizon 2020 Program

Dynamic countering of cyber-attacks

SU-ICT-2018

Cyber security 4.0: Protecting the Industrial Internet of Things

D7.5: Second Year Project Report[†]

Abstract: In this report we present the progress conducted in the C4IIoT project over the period of the second year. 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	31/05/2021
Actual Date of Delivery	31/05/2021
Deliverable Security Class	Public
Editor	*FORTH*
Contributors	All *C4IIoT* partners
Quality Assurance	*Jlenia Puma (CRF)* *Cabrera Gutierrez Antonio Javier (IFAG)*

[†] *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. *Jlenia Puma, (CRF)*
2. *Antonio Javier Cabrera Gutierrez, (IFAG)*

Revisions Version	Date	By	Overview
1.0.0	31/05/2021	FORTH	Final version
0.0.3	28/05/2021	FORTH	First revision
0.0.2	01/05/2021	FORTH	Integrated input from the consortium members
0.0.1	01/04/2021	FORTH	First draft released

Table of Contents

List of Tables

List of Figures

Executive Summary

This deliverable describes C4IIoT's progress, covering active work package during the second year, more specifically for the months between M13 and M24. In this context, this deliverable provides a 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. There are no significant deviations to report.

1 Detailed scientific and technical achievements during Second Year

1.1 WP2 – Edge computing cybersecurity technologies

Task 2.1. Provision, configuration and management of edge-node assets:
After initial requirements and gap analysis of existing CRF's edge node solution, the aim of this task includes the design and implementation of a novel, secure-by-design, architecture of C4IIoT edge node devices. The process of designing, implementing and testing was separated for two use cases: (i) Smart Factory edge node, provided by IFAG; (ii) Logistic 4.0 Edge node provided by UNSPMF.

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, and currently is being integrated with IBM's Hyperledger Fabric (HLF) component. TPM was completely integrated with the Raspberry Pi platform. Moreover, its security functionalities (such as system and data integrity, authentication, secure communications, secure data storage) have been tested. In addition, the edge node is able to sign transactions and send them to the HLF. Further actions and tests include the installation/integration and testing of other components, such as the BACS tool. Sensors integration with the Smart factory Edge node and test environment definition is in progress, in coordination with CRF.

For the Logistics 4.0 use case, about 50 custom designed edge nodes were fabricated and are ready for deployment for the Logistic 4.0 use case. An initial field trial has been performed with 5 NB-IoT devices for the purpose of device testing, data collection and training of anomaly detection using the BACS edge and fog module. The devices have been deployed in a limited scale trial, where 5 NB-IoT devices are attached to the delivery containers and are driven in five vehicles around the city of Novi Sad. The duration of the field trial was approximately 5 days, and more than 10.000 data points of NB-IoT device sensor measurements (inertial measurement unit and GPS unit data) have been collected under normal driving conditions. Another data set containing more than 1.000 data points is collected by occasionally introducing a delivery container overturning event and labelling the data points when the overturning event happened. The data sets are then used to train autoencoder-based anomaly detection algorithms as part of BACS edge and fog modules. The preliminary results are reported in a scientific publication entitled "Deep Learning Anomaly Detection for Cellular IoT with Applications in Smart Logistics", to be published in IEEE Access journal.

The 50 fabricated edge nodes were designed having in mind the specific requirements of a Smart Logistics environment: tracking and monitoring the vibration of the shipping containers and other environmental parameters.

Features supported by the new edge node:

1) Cellular connectivity: BG96 cellular module from Quectel is used to support NB-IoT and LTE-M. In addition, EGPRS is supported to ensure the connectivity in areas where LTE carrier might not be available. The integrated GNSS module provides the geolocation information.
2) On-board sensors: Apart from the localization data provided by the GNSS module, on-board environmental sensors are used to measure parameters relevant to the logistics use case. The 6-axis Inertial Measurement Unit (IMU) provides information about the vibrations and the magnetic field. An additional set of sensors is used to measure the atmospheric conditions such as air temperature, pressure and humidity. The designed platform provides additional metadata. For example, the cellular modem is capable of

providing the standard set of radio condition metrics (SNR, RSSI, RSRP, etc.). In addition, our design includes precise measurements of power consumption by the BG96 module.

3) The MCU and memory: The main MCU inside the edge node is a low-power 32-bit ARM Cortex M0+ with 256KB of FLASH and 32KB of SRAM, operating at 16MHz.
4) Hardware Security: Hardware crypto module provided by Infineon (OPTIGA Trust M) enables offloading the computationally expensive asymmetric cryptographic algorithms (elliptic-curve cryptography and RSA) from the resource-constrained MCU. Tampering resistant memory within the crypto chip is used to store security credentials, making FW on the host MCU oblivious of the sensitive information such as the encryption keys and certificates.

Task 2.2. Deep learning trained models deployed at the edge:

The task has started on M6 (November 2019) and enables machine learning methods for the detection of complex anomalous and malicious behaviour in a distributed way. Artificial intelligence driven protection at the edge within the C4IIoT project is implemented within the Behavioural Analysis and Cognitive Security component (BACS). It is a software component offering anomaly detection in IIoT sensory data and network traffic flows based on machine learning and deep learning algorithms. BACS includes unsupervised and supervised machine learning schemes and packages stretching through all three layers of C4IIoT architecture.

BACS autoencoders for smart factory C4IIoT edge nodes are implemented in Python using the Tensorflow2 library. Standalone autoencoder implementation trains the model by minimizing the mean square error using the Adam method – a stochastic first-order gradient-based method. Federated learning autoencoders, also implemented using Tensorflow 2, brings faster training times and privacy preservation. BACS includes two schemes of collective training - federated learning: the incremental learning scheme and the concurrent scheme.

Micro controllers used at the edge in Logistics 4.0 use case are low powered narrow-band IoT (NB-IoT) devices. In this case BACS implements routines performing anomaly detection for a given data point on a pretrained model with lightweight autoencoders. They are lightweight in the sense that those autoencoders have exactly one hidden layer. The implementation is done in C without using any external libraries and it is integrated in the firmware of C4IIoT NB-IoT devices - micro controllers. The training of lightweight BACS autoencoders is performed offline.

In February 2021, about 50 new microcontroller edge node devices for the Logistics 4.0 use case, with enhanced design, have been fabricated and delivered to UNSPMF. First tests of those devices have already resulted in new datasets useful for future development and testing.

Task 2.3. Security-aware dynamic offloading decision mechanism:

This task started on M6 (November 2019) and is related with designing and implementing the mechanisms needed to dynamically offload security-aware tasks for enhancing the performance of the anomaly detection mechanisms. During the second year, the MEDICI offloading service has been successfully integrated with the BACS anomaly detection modules, located at the field gateway and cloud layers. MEDICI is able to collect historical data, such as execution times and confidence scores, from previous offloaded tasks and gather real-time network-based information from MEDICI agents that are deployed in each BACS module. MEDICI is then able to use this execution and network information to inform its decision-making process.

Additionally, the MEDICI service has been enhanced to automatically consider newly added BACS anomaly detection modules. It is able to gather initial execution information through an additional server process, which informs of newly added BACS module by sending a number of dummy tasks to the new BACS module in rapid succession to obtain initial execution and confidence information. This allows BACS modules to be added dynamically at runtime, meaning more BACS modules can added and used after an initial deployment.

Lastly, in order to avoid making decisions based on outdated information, MEDICI has an additional service, which sends dummy tasks to BACS modules which haven't been selected as an offloading destination recently and thus have not reported up-to-date information.

Task 2.4. Security and trustworthiness at the edge:

This task started on M6 (November 2019) and builds 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: smart factory and inbound logistics.

During the second year of the project, IFAG has developed two shields for integration in the edge nodes. Firstly, IFAG developed a Raspberry Pi shield which contains the Infineon OPTIGA TPM2.0, as well as different sockets to integrate sensors via I2C. Second, IFAG developed a USB security token, which has been integrated with the Infineon OPTIGA Trust M security controller. The USB token has the capability to run with the blockchain network and perform security operations, adding the functionality of authentication in the edge devices for the operators in the factory. VIP uses the Infineon Trust M in the logistic use case edge node.

1.1.1 Deliverables

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.

1.1.2 Deviations and corrective actions

No deviations or corrective actions have been reported.

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

Task 3.1. Resource management and orchestration:

During the second year of the project, this task performed the installation of EJBCA, which included the setup of rootCA and SubCAs, as well as the internal validation of certificates (Cloud Gateway K8s Ingress). Moreover, the task achieved the installation of Harbor Private Docker Registry, which included the 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).

Overall, this task concurs to project objectives ensuring the provision and configuration of infrastructure resources through efficient resource management and orchestration.

Task 3.2. Behavioural analysis and cognitive security framework:

This task develops the core of C4IIoT's Level-3 security mechanisms which consist of the development of behavioural models that enables the analysis of the behaviour of multiple IoT devices, using the Behavioural Analysis and Cognitive Security (BACS) component.

BACS is a part of the C4IIoT framework, that implements anomaly and outlier detection and AI driven protection mechanisms. BACS consists of three main packages: BACS Cloud Layer (BACSCL), BACSPY and BACSC. BACSC is a lightweight anomaly detection software implemented in C used for low processing power devices at the edge. BACSC package performs AD detection only at the edge node layer in Logistics 4.0 use case and belongs to level-1 security mechanisms. Detailed description can be found in Deliverables 2.2 and 3.2. BACSPY contains an implementation of various traditional machine learning anomaly detection methods implemented in Python: outlier detection, classification and representation learning algorithms 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 time series analysis tool.

The goal for the BACSCL is to have a pool of algorithms with different unsupervised and supervised anomaly detection models. The algorithms have been designed to work in a uniform way with a shared interface to be compatible with the rest of the platform. The conducted work has been split to several phases. Detailed description of the development phases can be found in Deliverable 3.3.

The latest development within this task related to BACS covers privacy preserving machine learning algorithms. Privacy preservation has been achieved using the novel concept of differential privacy. Differential privacy is a system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset. Latest version of BACS includes implementations of differentially private k-means and principal component analysis (PCA) methods.

Task 3.3. Mitigation engine:

Starting from the mitigation engine design document that was written at M12, the role of this year's task was to implement a full version of the mitigation engine and integrate with the rest of the project. The work was carried out along two main axes: mitigation of network attacks by dynamic reconfiguration, and mitigation of software vulnerabilities by incremental and targeted verification.

Network mitigation: The CARMAS tool (previously named VariaMos) has been implemented in the Logtalk programming language (an Object-Oriented extension to ISO Prolog) as a knowledge-based reasoning tool to determine corrective actions (mitigations) to attacks that occur at runtime in the system. In CARMAS, we used the SWI-Prolog engine as the underlying engine for Logtalk to reuse its web service and constraint logic programming libraries. CARMAS has been implemented such that it exposes an API endpoint that is query-able by AEGIS' Advanced Visualization Toolkit once an attack has been reported to it. CARMAS leverages a formal representation of the domain of Cybersecurity in IIoT environments (including the possible threats faced and the corresponding possible mitigation strategies), implemented as an ontology, based in part off of the internal models of STS' Security Assurance Module and the latest literature on the subject, to perform the necessary reasoning to propose appropriate mitigation actions to the problem at hand. The responses to the query's posed by the Advanced Visualization Toolkit are "mitigation plans", composed of a series of actions that are deemed to be the best possible mitigation to the attack at hand, based on the detection information, and the confidence of the detection. The search performed by CARMAS is based on the dynamic construction and subsequent solution of a Constraint Optimization Problem. The results of this work have been submitted to an international conference.

To provide security at the network level for the C4IIoT infrastructure, Thales has implemented a SDN controller DISCO. This controller manages a set of Open vSwitch switches that handles the IoTs network traffic at runtime. The controller speaks with the switches using the Openflow protocol that specifies how to manipulate the data plane. Moreover, to fit inside the Mitigation engine architecture, Thales has extended the DISCO SDN controller with a rest API. This new API allows the CARMAS engine to emit network mitigation plan inside the network. In addition, this new connection needs to interpret the high-level order contained in the mitigation plan and to translate it to a lower level while splitting it correctly for each managed switch.

Software mitigation: This part of the mitigation was performed around the BINSEC platform. By working on the requirements of the C4IIoT framework, we equipped our BINSEC tool with a new patch-oriented-testing method, that allows to focus the testing on specific targets of the code. Its role is to help incremental testing by a targeted patch differential analysis (i.e., trying to find security vulnerabilities by focusing on the recent additions to the code). This relies especially on the integration of the greybox fuzzing engine AFL.

We successfully used the tool on the BACSC component developed in the project by University of Novi Sad. In detail, we found issues in different versions of BACSC, including division by zero errors, null pointer dereferences, and memory leaks. This allowed the BACSC developers to introduce security patches before an attacker could do it. We also launched an extensive campaign on the last version of BACSC, that does not suffer from these issues, and is thus more secure than the initial version. Finally, the software mitigation component was integrated with the Advanced Visualization Toolkit developed by ITML, so that a C4IIoT user can easily use the tool to verify the security of different versions of a binary that was provided to him, e.g. to check for security updates.

Different extensions of the work are being performed, to improve automation and applicability, such as integration with the Ghidra tool developed by the NSA, and support for x86-64 executables.

Task 3.4. Trustworthiness of data flows:

This task includes the development of IBM's decentralized access control (DAC). In the reported period, IBM has finalized the design and implementation of DAC prototype for C4IIoT's first complete prototype of M18. A detailed design was prepared, including the functionality and interfaces exposed by the DAC to its various users within the project. An effort was made to implement the various Hyperledger Fabric related (HLF) and Attribute-Based Encryption related (ABE) functionalities, including utilizing existing solutions and developing components and functionalities for C4IIoT prototype such as HLF and ABE clients, and HLF smart contracts. The DAC prototype was deployed at the integration environment provided by ITML for the M18 prototype and integration efforts were made with ITML and DAC's users.

After M18, further scientific and technical work was made towards the final version of DAC. An initial work was made, and is on progress, to utilize the new Blockchain Database (BCDB) technology in the project, that is planned to enable further auditability and trust in C4IIoT. A work was done to enable expiration and revocation of ABE secret keys. The query mechanism of HLF peers and the decryption mechanism of ABE clients were improved in order to support the needs of C4IIoT DAC users, and performance tests were conducted. Further work was made to develop proxies for HLF network to allow using HLF from the edge nodes.

In addition, specific integration work was made between IBM's DAC and IFAG's secure element, and between IBM's DAC and HPE's identify management solution. DAC was developed in a way that allows an interface with IFAG's secure element, and the secure element was successfully tested by IFAG to communicate with HLF components and sign HLF transactions. Integration efforts with HPE's certificate authority are ongoing, and IBM was able to successfully operate the DAC prototype with certificates generated by HPE's certificate authority, trusting this CA, in an initial experiment.

This task also includes FORTH's traffic analysis tool. It uses a database of signatures, which is generated from publicly available datasets of attacks (with a main focus on IoT environments). Each signature is a sequence of packet payload lengths, which has been observed to remain the same in known attacks. The use of packet lengths allows us to detect malicious or abnormal behaviour even in encrypted traffic. In addition, our tool is also compliant with the popular JA3 signatures, which is a method of fingerprinting the handshake of SSL/TLS connections and identifying malicious encrypted traffic. Furthermore, we investigated techniques for auditing the encrypted connections for outdated/deprecated protocols, inadequate key lengths, etc. Such cryptographic assessment or compliance, once integrated, will alert and report such cases, which might pose a serious security risk otherwise.

This task also includes the Privacy Aware Trustworthy Data and Analytics (PATDA). During this period, Data Fusion Bus core was developed and tested in ITML's lab, while the rest of DFB components were tested in the integrated environment.

1.2.1 Deliverables

D3.3. Level-2 and Level-3 security mechanisms of C4IIOT

Deliverable D3.3, describing C4IIoT's level-2 and level-3 security mechanisms, was submitted on time on M18. This deliverable, led by IBM, was contributed by the following partners: FORTH, HPE, IBM, IFAG, UNSPMF, CEA, UP1PS, TSG and ITML. It included sections about the various technologies that form the level-2 and level-3 security mechanisms: Identity Management (HPE), Decentralized Access Control and Distributed Ledger (IBM), Distributed Ledger Integration with Infineon's Secure Element (IFAG), Behavioural Analysis and Cognitive Security module (UNSPMF, HPE), Traffic Analysis (FORTH), Mitigation Engine (CEA, UP1PS, TSG) and Privacy aware, Trustworthy Data & Analytics (Data Fusion Bus) (ITML).

The ToC was circulated by IBM in June 2020, and two main rounds of contribution from all the involved partners took place at August 2020 and September 2020. An internal review of the document was made by CEA and CRF and the deliverable was submitted on time at the end of November 2020.

1.2.2 Deviations and corrective actions

No deviations or corrective actions have been reported.

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

Task 4.1. Assurance, privacy and accountability in all Industrial IoT processes:

The task was active within all months of the second year of the project (M13-M24) and contributed towards the development and integration of the components for the release 1 (R1) of the C4IIoT framework. This work contained the development of the Distributed Access Control (DAC) and Blockchain Database (BCDB) by IBM, the Identity Manager (IM) and Risk Management (RM) by HPE, the Security Assurance by STS, the Behavioural Analysis and

Cognitive Security (BACS) by UNSPMF, the Distributed ledger technologies by IFAG and Data Fusion Bus DFB by ITML. After M18 and the release of the R1 version of the platform, the task's efforts focused on the definition and confirmation of the final release (R2) features of the above-mentioned components exploiting the experience and feedback from the R1 development and evaluation, to better accommodate the expected interactions with other components, as well as their role within the C4IIoT solution in general. After the definition of those features, activities within Task 4.1 included the involved development of the R2 version, using components by all involved partners; an activity that is currently ongoing. The partners also participated to the regular WP4 calls presenting the progress of the task, discussing and planning the next steps as well as the organization of ad-hock calls as required for discussion and clarification of implementation technical details. Moreover, the progress and the planning of this task was presented and discussed during the participation in the two C4IIoT plenary meetings that took place on end of July and end of December 2020. Finally, the outcomes of this task were presented to the review meeting of the project's first reporting period on mid-January 2021.

Task 4.2. Advanced informative mechanisms and interactive visualizations:
The task was active for all second year of the project. Based on the MVP version of the Advanced Visualisation Toolkit (AVT), this task has added more features and functionalities and at the same time improved the appearance and ease of use of the existing dashboards. More specifically, the first milestone of this period was the release of the 1st integrated prototype of C4IIoT framework on M18. Following the development and integration process of C4IIoT we have improved the real time monitoring of sensor's data and real-time monitoring of results from the anomaly detection process. Moreover, we have added the attack monitoring dashboards with real-time alerts and information for attack plans detected from the Security Assurance Module and the option to request possible mitigation plans and select and apply the most appropriate one. Additionally, we have added visual screens to perform a binary-level security analysis, BINSEC by selecting the desired options and get the results of the analysis. Historical data are also available. Finally, integrated in AVT the decentralized access control with attribute-based encryption to read encrypted data.
After the release of the 1st integrated framework, we were focused to improve the appearance and usability of the implemented visualisations and initiated the implementation of forensics services based on timeline analysis. More graphs were added, and we are improving the overall look and feel of the dashboard. Detected anomalies are represented in a time line and we are looking for correlations between detected events.

Task 4.3. Continuous integration towards the realization of C4IIOT framework
The task includes the continuous integration towards the realization of C4IIoT framework which started on M8 and will be active until the end of the project, driving the integration towards the releases of C4IIoT solution. During the second-year project (M13-M24), this task was constantly working to deliver a first integrated version (prototype-internal), based on agile approach. The interim version was given to the PO and reviewers for our first review at M18. The task deployed and managed the necessary resources for the implementation and integration of this prototype along with all C4IIoT partners and their corresponding modules to offer security and privacy in an end-to-end industrial IoT environment in the automotive manufacturing domain. Specific details on the integration and participation of the modules can be found within the technical report submitted to the PO and reviewers.

1.3.1 Deliverables

D4.3. C4IIOT integrated framework (Interim Version M18):

An interim version has been delivered to the PO and reviewers at the first project review (M18). The final D4.3 will be delivered on M30 along with C4IIoT framework.

1.3.2 Deviations and corrective actions

No deviations or corrective actions have been reported.

1.4 WP5 – Real-life industrial demonstrations in smart manufacturing

Task 5.1. 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.

Task 5.2. Framework deployment and execution of real-life industrial demonstrations:
Within this period, the real-life industrial demonstration has proceeded with the preparation of the platform execution tests. Architecture and scenarios for the pilots have been identified, by mean of the choice of components and description of objectives, and how they will be reached thanks to the implementation of C4IIOT. Use-cases and actors involved in the demonstration have been identified and described and the industrial challenges and cybersecurity requirements have been redefined. This information has been described in D5.1. First tests have been executed in partner’s premises and also utilizing already existing data that have been shared by CRF with the technical partners. Finally, periodical calls have been organized to progress with the task activities and plan the subsequent steps.

Task 5.3. Evaluation and Impact analysis:
The task has proceeded by analyzing the data sources and defining the KPIs calculation method. The specific metrics for the evaluation of each use case and an initial output from real-life demonstrators have been analysed. An overall KPIs report has been assigned for monitoring as well as a strategy on how it will be reached by the end of the project. Specific KPIs that correspond to each C4IIoT tool have been identified. An initial impact analysis report has been provided with respect to the expected project innovation and achievements through technical evaluation outputs. The first results of this task have been reported in D5.1.

1.4.1 Deliverables

D5.1. C4IIOT Demonstration - initial execution and evaluation:
The deliverable submitted on time (M18). It includes a report on the specification of the demonstration protocol, the framework deployment and execution of real-life industrial demonstrators. It also initiated a technical evaluation through KPIs and their impact. This deliverable will be the key to the continuation of the project covering the efficient execution and the evaluation outcome.

1.4.2 Deviations and corrective actions

No deviations or corrective actions have been reported.

1.5 WP6 – Exploitation, sustainability and business continuity

Task 6.2. Communication strategy triggering awareness and new business opportunities:
The task is active throughout the second year of the project. The communication and dissemination strategy sets out the plan to raise awareness, share knowledge, attract potential end-users and stakeholders, and explore future commercial use in the context of the C4IIoT project, through various means. In this period, we increased our activity in the website contents and posts in social media accounts and consequently increased engagement. The C4IIoT consortium has organized an Info Day hosted by Thales and an International winter school on cybersecurity. Furthermore, we are organizing an International Workshop on Secure and resilient smart manufacturing environments in collaboration with other EU projects, on August 2021. In regular basis we update the website and social media accounts with information related to C4IIoT development progress and achievements as well as with information on scientific publications and participation in conferences and events by the consortium members. An updated dissemination plan is reported in deliverable D6.6

Task 6.3. Exploitation activities:
The task started at M6 aiming to collect the exploitation plan of partners and published them in D6.4. The individual exploitation plans of each partner is consolidated and a true exploitation plan for the whole projects results is elaborated. This is the purpose of the deliverable D6.5 at M24. During the second year of the project, the exploitation activities were focused in the exploitation of the capabilities in different potential products developed by the companies. In this sense, the security controller integration with blockchain networks was pushed. Following this way, a USB token with the capability of connection with blockchain networks is proposed that allows user authentication.

Task 6.4. Standardization activities and best practices:
The task is active throughout the project. During the second year, the task has completed the identification and classification of the organizations producing standards, directives and open-source software relevant to the project and in parallel it has completed the identification of the technologies used in C4IIOT, which are based on standards or open-source software. The initial cross-table of the first deliverable has been finalized.
A standardization plan has been written in order to identify the possible ways to participate to a standardization activity, rather on the form of a recommendation in a SDO, and it has identified the open-source contributions from the C4IIOT developments.
The on-going standardization activities with the projects of H2020-SU-ICT-2018 have been identified, with the intent to write common whitepapers related to the Common Threat Intelligence, applied to Industry 4.0 domain.

1.5.1 Deliverables

D6.5. Exploitation and standardization activities and best practices – final version:
D6.5 is the second and final deliverable to describe both the Exploitation and the Standardization activities. The “collaborative” exploitation is a new part for which TSG has proposed a template available in any collaborative research project to formalize a value chain analysis. This formalization helps to explain the causal business links between the partners own interest and the shared objective of the project (or rather a shared contribution by at least 2 partners in C4IIOT).
Regarding the standardization activities, the deliverable D6.5 identifies additional standardization organizations which offer recommendations and describe standards that the

developments of C4IIOT follow. The deliverable explains also the on-going contributions in regard to the standardization plan added in the second version of the previous deliverable D6.4. It also includes all open-source contributions.

D6.6. Dissemination strategy and activities:
This deliverable presents the work performed in WP6 – Task 6.2 “Communication strategy triggering awareness and new business opportunities” with respect to the framework of the dissemination strategy of C4IIoT project. The report consists of the reporting/monitoring of the respective dissemination and communication activities during the 2nd year of the project (M12-M24) and planning for the following period. As the objective of WP6 is to supervise the integrity and consistency of all dissemination efforts for creating awareness on the C4IIoT project, the main purpose of the deliverable is to present the achievements made during the second year of the project based on the framework of the dissemination strategy presented on D6.3.

1.5.2 Deviations and corrective actions

No deviations or corrective actions have been reported.

1.6 WP7 – Project Management

Task 7.1. Project quality planning:
As part of this task, different tools for good project quality planning were deployed, including a retro-planning with internal deadlines. The planning ensures that the different maturity steps of the deliverable are ready in due date, as well as an internal review process where each of the project deliverable is reviewed by at least two consortium members, using a strict review evaluation notice that guarantees the quality of the deliverable. Thanks to this process, the project deliverables maintain a high quality and have been delivered on time.

Task 7.2. Day-to-day management, project & financial control and resource monitoring:
The purpose of this task is to ensure the quality of results for the project activities, and that the tasks and target dates for deliverable deadlines are achieved. FORTH as the coordinator of the project established the project management procedures, which was initially documented in Deliverable D7.1 (titled “Initial version of project handbook”), and have been further updated in Deliverable D7.4 (titled “Final Version of Project handbook”).

Task 7.3. Innovation Management:
During the second year of the project, the plan for IPR management has been established and documented in Deliverable D7.4 (titled “Final Version of Project handbook”).

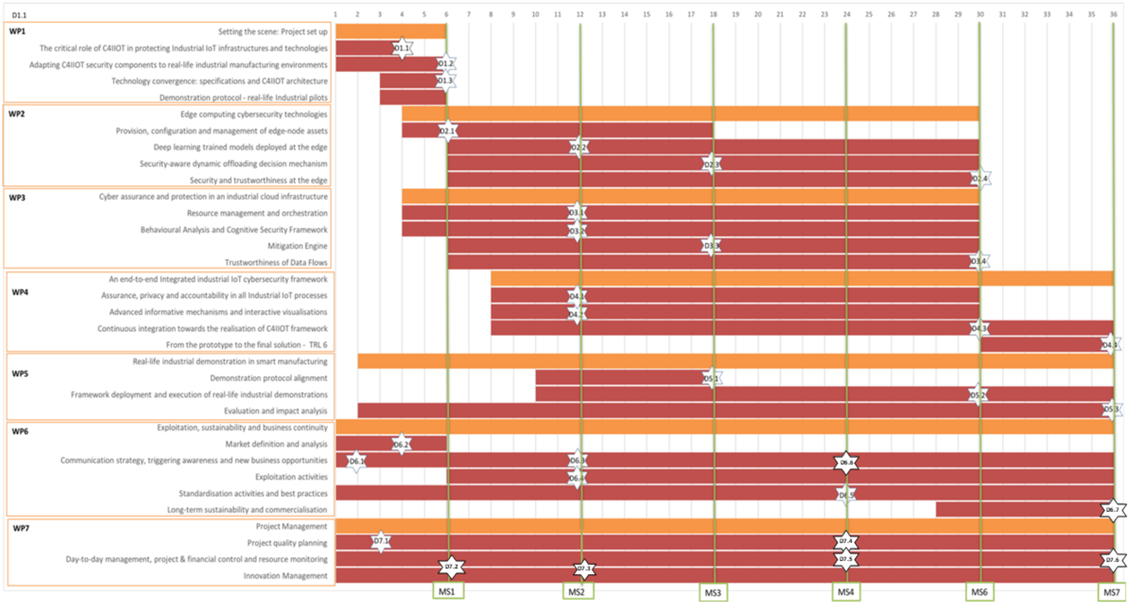

Figure 1: Milestones and Deliverables

1.6.1 Deliverables

Deliverable 7.4 – 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.

Deliverable 7.5 – 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.

1.6.2 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. For year 2, M13 to M24 we had 3 plenary meetings, 1 midterm review and 10 monthly teleconferences along with several other for WP related and other specific reasons.

Plenary Meetings

The project has held three plenary meetings and a midterm review during the period.

- The 4th plenary was done online due to health safety reasons, it was done through Microsoft teams on 20th & 21st of July 2020. It was attended by all partners.
- The 5th plenary was again done online due to health safety reasons, it was done through Microsoft teams on 24th of November 2020. It was attended by all partners.
- The midterm review happened on 13th of January 2021, it happened online through Microsoft teams due to health safety reasons. It was attended by all partners.

- The 6th plenary was again done online due to health safety reasons, it was done through Microsoft teams on 18th of May 2021. It was attended by all partners.

Teleconferences

For work-package related activities, the project is holding on-line meetings using Microsoft Teams. 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 second period of the project.

Work package	Date	Duration	Attendees	Summary
All	25-06-2020	1h	All	Info day organization, Kafka components further integration, Requirements for Kubernetes cluster.
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	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	31-03-20221	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	26-05-2021	1h	All	Status update on all WPs, M24 deliverables, Addressing comments from review, Questionnaire status update.

Table 1: List of C4IIoT Teleconferences

1.6.3 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.

1.6.4 Deviations and corrective actions

No deviations or corrective actions have been reported.

1.6.5 Consortium Changes

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

1.6.6 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
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	At the time of writing this deliverable, we foresee a two-week delay in order to increase the quality of the document
D7.4	Final Version of Project handbook	PU	M24	M24	
D7.5	Second year project report	PU	M24	M24	

Table 2: Deliverables submitted

	Milestone Title	WP	Lead	Due	Verification	Comments
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	

					demonstrators report (D5.1)	
MS4	Dissemination, Exploitation and standardization landmark	WP6	TSG	M18	Exploitation, dissemination and standardization reports (D6.3, D6.5)	This milestone will be reached by the submission of D6.5

Table 3: Milestones reached

1.6.7 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.

1.6.8 Financial statements and summary financial report

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

2 Project planned activities for next period

2.1 WP2 – Edge computing cybersecurity technologies

Task 2.2 – Next Steps:
A major line of next steps in Task 2.2 is closely related to exploitation of the 50 new microcontrollers – edge node devices that have been fabricated in February 2021. Initial meetings with CRF have been held and initial plan has been devised. Having in mind that another partner in project – VIP, a mobile network operator, controls the nation-wide coverage of NB-IoT in Serbia, the first demonstration will be done in Serbia. At the same time, a limited number of devices will be sent to Italy to start preparations for final demonstration that will be held there.
In addition, we plan to cover fully smart factory use case with Raspberry Pi devices at the edge in cooperation with IFAG. First results in this direction have been reported in other tasks. Another line of work planned within this task is the usage of existing ensemble learning schemes using field gateway.

Task 2.3 – Next Steps:
The next steps for Task 2.3 are to further enhance the offloading decision-making process of MEDICI by investigating other metrics apart from execution time and accuracy, based on the parameters used in new models currently under investigation for BACS. We will also incorporate in the decision the concept of age of information, to investigate whether we can remove the need of probing BACS models that have not been recently selected and thus keeping the information used by the MEDICI decision process up-to-date. We will also, perform extensive experimentation to fine-tune the MEDICI decision making process and evaluate its effectiveness.

Task 2.4 – Next Steps:
Once the edge nodes are ready, the next steps are to integrate with the rest of the components of the architecture. The integration with sensors in the edge device would be the first steps, then, the installation of different components, for example BACS, would be carry out in the edge nodes. Finally, the testing of the use cases with the whole architecture will be performed.

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

Task 3.1 – Next Steps:
HPE foresee the following steps for the coming period:

- Private Docker Registry
    - Onboard new images
- Cloud Gateway
    - Onboard modules
- Cloud orchestration
- CA
    - The EE with the X.509 certificate is the baseline of the concept behind the identity management and will start the configuration of CA
    - Start managing Identity with Registration Authority
    - Integration between CA certificates and ABE [beyond M18]

- Deploy all components on CRF Platform.

Task 3.2 – Next Steps:
The most important task left to do within Task 3.2 is related to the development of supervised learning anomaly detection methods based on labelled datasets. Quality labelled datasets for these purposes have proven to be a serious problem to come by. On one hand, we plan to experiment with datasets that are freely available on the internet, while on the other hand we work with CRF on obtaining labelled datasets and validating results of already implemented unsupervised detection methods.

Further integration with MEDICI offloading mechanism is planned and the work is in progress. In cooperation with UoG, we agreed to implement metrics for the implemented unsupervised learning methods that will be used by the offloading mechanism to reach more quality decisions.

Moreover, we plan to finalize the work on various light versions of BACS that run within secure environments that support Intel SGX by compiling and successfully running an instance that supports TensorFlow execution in this environment.

Task 3.3 – Next Steps:
While the mitigation engine begins to be working satisfactorily, we would like to enhance it using different points. We would like to improve CARMAS search heuristic, in the case where the number of mitigation actions for each new attack class becomes too numerous, and in case the currently implemented search heuristic would be too inefficient. We would like to mature the mitigation engine frontend, CARMAS, especially by writing documentation UML model, user manual, video tutorials. We would also like to continue adding new rules based on the attack detection stack of FORTH's traffic analyzer, UNS BACS and STS SAM.

We would also like to expand our SDN controller in 3 possible different ways, by deploying Open vSwitch switches inside the edge layer to manage the traffic has close as possible to the source of the traffic; extending the high-level controlling API with additional actions; and exploring the possibility to create Moving Target Defence mechanisms using the SDN controller.

Finally, we would like to improve the automation and widespread applicability of the software mitigation, notably by importing CFG information using the Ghidra tool developed by the NSA; and by performing analysis on x86 64-bit executables, in addition to the 32-bit executables that we currently analyze.

Task 3.4 – Next Steps:
This task includes the development of IBM’s decentralized access control (DAC). In the next and final period of the project, IBM plans to continue developing the DAC towards its final version. Utilizing the Blockchain Database (BCDB) technology and integrating it in the project is one of the main planned activities. BCDB will enable increased trust and auditability of events in C4IIoT such as outputs of the analytics, mitigation actions decided on etc. In addition, further integration efforts are planned against HPE’s identity management solution and IFAG’s secure element, two components the DAC works closely with and relies on. Finally, some work is expected in dealing with integrating and deploying the DAC into C4IIoT’s final version in CRF’s environment.

Further steps in the scope of this task include the testing and deployment of the DFB core as part of the C4IIoT solution along with the activation of authentication and authorization features of the Kafka infrastructure.

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

Task 4.1 – Next Steps:
Next steps within this task include the continuation of the work from all involved partners towards the implementation of the defined R2 features of the offered components and their delivery, integration, testing and finetuning for the final release of the platform. Moreover, the contribution of all partners to the successful delivery of Deliverable D4.3 is foreseen, as well as the participation on all remaining regular work package 4 and ad hoc calls as well as consortium plenary meetings. Of course, the outcomes of the remaining activities (within the 3rd year of the project lifecycle) in this task will be reported in deliverable D7.6 (Final project report) as well as they will presented in the final review of the project.

Task 4.2 – Next Steps:
AEGIS continually work in collaboration with other partners to support visualizations for new features developed in technical work packages (attack plans detection, mitigation plans, mitigation actions etc). Also, during the coming period, we plan to update interfaces in order to increase usability and user-friendliness of the dashboard according to feedback from the evaluation process. Finally, the main goal is to enrich the timeline analysis section to support forensics, by providing dashboards allowing the end-user to identify hidden relation between detected anomalies. The aforementioned developments will be included in the final release of C4IIoT framework and will be reported on deliverables D4.3 and D7.6.

Task 4.3 – Next Steps:
ITML is constantly working to integrate the distinct services towards the realization of C4IIoT framework until the end of the project. The final solution will be delivered on M30 through the second prototype – final solution and the functionality of the integrated framework will be verified by the C4IIoT pilots. It will also be customized based on the specific needs of each field. ITML will drive and implement all the deployment and management of necessary resources for the final implementation and integration. Additionally, ITML is going to deliver D4.3 on M30 including the integrated framework.

2.4 WP5 – Real-life industrial demonstrations in smart manufacturing

Task 5.2 – Next Steps:
Within the next period (M24-M36) the task will proceed with the real-life industrial demonstration, executing the last trials that will allow to prove the C4IIOT security and privacy offerings by the end of the project. The final version of the solution will be tested and outputs from all real-life industrial demonstrators will be collected and analysed.

Task 5.3 – Next Steps:
This task will consist mainly in the final evaluation of the benefits derived from the project results, both from technical and operational views. To this aim, an impact analysis will be carried out with respect to the demonstration protocol, taking into account the KPIs that have been defined in D5.1.

2.5 WP6 – Exploitation, sustainability and business continuity

Task 6.2 – Next Steps:
What is expected for the following period is to increase C4IIoT dissemination and communication activities towards the release of the final version of C4IIoT framework.
Emphasis will be given to the organization of events for specific target groups and general audience, our presence in industrial and scientific events and collaboration with other EU projects and SME clusters. Intensifying efforts towards the further increase in numbers with respect to the C4IIoT online dissemination and communication channels remains a priority as well. Finally, dissemination and communication activities will be reported at the end of the project.

Task 6.3 – Next Steps:
The next steps in the exploitation plan will be to carry out the exploitation plan described in the deliverable D6.5. Exploitation activities carried out during this period will be based on the plan described above and will be focused at the system level.

Task 6.4 – Next Steps:
The next steps in the standardization activities is to carry out the standardization plan described in D6.4. It can be completed by new involvements depending on the emerging standardization groups.

2.6 WP7 – Project Management

Task 7.1 – Next Steps:
CEA will continue monitoring the project quality planning, monitoring that the project quality planning procedures are followed.

Task 7.2 – Next Steps:
FORTH will continue the day-to-day management of the project and will monitor the effort tracking, technical progress and financial reporting.

Task 7.3 – Next Steps:
As next activity, HPE will create a table containing project components listing IPR properties with the aim to provide a consistent vision of entire solution licensing.

3 Current status of KPIs

Innovation KPIs	Status M18:	Status M24:
[KPI-1.1] Successful integration and orchestration of C4IIoT security-enabled layers.	ITML will ensure the successful integration of the C4IIoT technologies and relevant security-enabled layers; based on an agile approach, it will continuously validate and test the integrated framework collecting feedback from both the technology providers and the end users. Up to now, the infrastructure for the integrated framework has been deployed and the proof-of-concept (MVP) version of the C4IIoT solution has been integrated and presented for the two pilots of the project (namely (i) "Smart Factory" and (ii) "Inbound Logistics". In addition, a 1st integrated version (prototype) has been delivered successfully. The functionality of the integrated framework will be verified by the two C4IIoT pilots.	A 1st integrated version (prototype) was given to the PO and reviewers for our first review on M18. ITML is constantly working towards the final solution driving and implementing all the deployment and management of necessary resources for ensuring the successful integration of the C4IIoT technologies and relevant security-enabled layers.
[KPI-1.2] 20% improved resilience for an end-to-end Industrial IoT system.	The resilience of the system will be improved by more than 20%, mainly in two different ways. First, by using a secure element which prevents a plethora of threats on an IoT device (including physical attacks). Second, by using a decentralised access control which eliminates single-point of failures in the system.	The resilience of the system is improving by (i) using hardware security modules (HSM) at the edge nodes, (ii) by interconnecting them in a blockchain network. At this moment (M24), the integration of these components has been done successfully, therefore the resilience of the system is increasing.
[KPI-1.3] 80% reported cybersecurity incident investigations resolved within an organizationally defined timeframe.	CRF (as the end user of C4IIoT) will specify a suitable timeframe for the resolution of a problem, compatible with the plant ICT constraints, and verify in the pilots that the identified incidents can be resolved with this timeframe: identification, portfolio of solutions and implementation (automated/ manual) performed.	This KPI can be calculated only at the end of the project, when the whole architecture will be tested in CRF, but the results obtained until M24 are promising.
[KPI-1.4] Reduction of detection time by at least 10%	The detection time is estimated to be reduced by (at least) 10%, due to the efficiency of certain C4IIoT modules (e.g., traffic analysis module, security-aware offloading, etc.). The evaluation methodology (specified in D5.1) provides the base for testing and verifying the detection times of the C4IIoT as a whole.	The implementation is in progress and the detection times will be evaluated after the deployment on CRF premises is complete.
[KPI-1.5] Increased accuracy of security monitoring by 35%.	The proposed plan to reach this KPI is made of two phases: 1) measure the threat accuracy AS-IS; this accuracy constitutes the baseline of the measurement; 2) measure the threat accuracy with C4IIoT components active and working, to obtain and verify the improvement achieved. The first step needs to have C4IIoT logging and monitoring components only installed on CRF premises to capture the AS-IS status. The second step needs to have, in addition, all other C4IIoT security components active and working to capture the advancement obtained. Assumption to be made to threats generation, should the CRF system work off-line, threats must be generated artificially in both scenarios.	Steps are taken to execute the monitoring inside the production environment and obtain the baseline to check against the next to come monitoring using C4IIOT framework.
[KPI-1.6] Protect an IIoT real-life environment from at	The C4IIoT consists of, at least, 12 concrete technologies that cover different threat models, such as (i) the Secure Execution Environment	The technologies that cover this KPI are in ongoing development following M18's first C4IIoT prototype and towards the final version of the project. Final

least (10) types of related threats and attacks.	(FORTH), (ii) the Decentralized access control with attribute-based encryption (IBM), (iii) the Secure Element at Smart Factory Edge Node (IFAG), (iv) the Traffic analysis (FORTH), (v) The Behavioural analysis & cognitive security module – BACS (UNSPMF), (vi) the Advanced visualisation, Privacy/secure data analytics (AEGIS), (vii) the Data Fusion Bus (ITML), (viii) the Cloud Management & Orchestration (HPE), (ix) the Risk assessment (HPE), (x) the Security Assurance Module (STS), (xi) the Binary Code analyser (CEA), and (xii) the Reconfiguration Search – VariaMos (UP1PS).	assessment of this KPI and the technologies that cover it will be made once they are deployed on the final execution environment. For instance, the Secure Private Docker image registry provides protection against some of the attacks that have been identified in D1.2 at Table 2. (e.g.: Malware, Manipulation of Information, Brute Force, others). Similar for other technologies.
[KPI-2.1] More than (20) novel services and tools utilized and integrated from diverse multi-domain technological areas.	Once all the C4IIoT components are installed on the CRF premises, an assessment with inventory of the added services and tools will be made to evaluate the total number achieved.	Integration of the C4IIOT components is underway and a final inventory is due to consider all of them.
[KPI-2.2] Innovative ML/DL models deployed at the edge and a security-aware offloading mechanism for almost real-time critical security decisions.	Ongoing - UNSPMF implemented and deployed basic anomaly detection using lite autoencoder inference ML algorithm (trained offline) in edge firmware on development board for the "Inbound Logistics" use case. The development of the ML algorithm for the "Smart Factory" use case, able to be deployed on docker containers with Intel SGX support is in progress.	Ongoing, almost complete - UNSPMF implemented and deployed basic anomaly detection using lite autoencoder inference ML algorithm (trained offline) in edge firmware on development board for the "Inbound Logistics" use case. Moreover, ML/DL models have been deployed for the "Smart Factory" use case using Raspberry Pi computers in cooperation with IFAG, deployed on docker containers with Intel SGX support. Security aware offloading mechanism has been integrated with ML/DL components. Further refinement of input sent to the offloading mechanism is in progress.
[KPI-2.3] Test edge computing framework in terms of speed and quality.	IFAG provides the components, using a secure element as well as a TEE, to avoid different attacks from different levels; physical attacks will be avoided using the secure element and other attacks using a TEE. In order to reach that, the secure elements will be connected in the edge nodes. We assume the cyber threats will be generated artificially within the CRF system.	The components placed in the edge nodes have been tested in term of speed and quality in order to prevent potential bottlenecks. Operations concerning the secure element in the edge nodes is measured in time also in order to prevent physical attacks as timing attacks. Test environment will be provided by CRF and will carry out in his lab environment.
[KPI-2.4] Accuracy of encrypted flows classification over the Internet more than 90%.	Data from multiple attacks will be used in order to produce signatures with the aim to increase the classification of encrypted flows by more than 90%. The accuracy will be checked based on the sustained false and true positive rates.	Initial experimentation of the traffic analysis module show that it can detect certain malicious actions inside encrypted traffic, with more than 90% accuracy. The final evaluation results will be obtained by M30.
[KPI-2.5] At least (6) services for secure communications, access control management and authentication.	The primary components of C4IIoT that cover these features are: (i) the Decentralized access control with attribute-based encryption (IBM), (ii) the Identity management (HPE), (iii) the Data Fusion Bus (ITML), and (iv) the Cloud Gateway (HPE).	The integration of the C4IIOT components is underway and a final inventory is due to consider all of them. For example, the Identity Management module offers protection in access control and authentication by providing a PKI-based mechanism for controlling and monitoring system access, based on the following standard pattern: identify and authenticate users; determine if the access is authorized, grant or restrict access, monitor and record access attempts. Moreover, to provide network isolation of the modules inside the Cloud Layer, all incoming network requests are managed through the Cloud Gateway. Cloud Gateway enforces network traffic encryption via HTTPS for all external communications, client-side authentication. In addition, Cloud Gateway implements Web Application Firewall: OWASP ModSecurity rules are enforced on the managed traffic.

[KPI-2.6] Upgrade ML/DL models to be realized in an automotive IIoT environment.	Ongoing - Validation of the currently developed algorithms should be done during pilot testing.	Ongoing, almost complete. BACS component implements various kinds of algorithms being tested within the automotive IIoT environment, including: traditional machine learning algorithms related to anomaly and outlier detection, shallow and deep neural networks (such as autoencoders and GRU and LSTM recurrent neural networks) and the Facebook Prophet – a procedure for forecasting time series data based on a non-linear additive model. Validation of the currently developed algorithms should be done during pilot testing.
[KPI-3.1] More than 10 system vulnerabilities exploited by the system and threat actors.	In progress - The consortium has specified the evaluation methodology (see D5.1) and identified the pertinent C4IIoT subcomponents; will verify that at least 10 prominent system vulnerabilities are covered by the C4IIoT platform's security assessment enablers, including the: (i) Security Assurance Module; (ii) Mitigation Engine Module; (iii) Privacy aware, Trustworthy Data & Analytics Module; (iv) Risk Assessment Module	In Progress – The evaluation methodology is specified in Deliverable D5.1 and identified the pertinent C4IIoT subcomponents. By reviewing the second release (R2) of the C4IIoT platform, we will verify that at least 10 prominent system vulnerabilities are covered by the platform's security assessment components (M30).
[KPI-3.2] 20% of system vulnerabilities for which patches (including firmware patches) have been applied or that have been otherwise mitigated.	In progress - The consortium has specified the evaluation methodology (see D5.1) and identified the pertinent C4IIoT subcomponents; will verify that at least 20% of system vulnerabilities identified by security assessment components (see KPI-3.1) have been patched (validated by Security Assurance Module) or corresponding attacks have been mitigated (validated by Mitigation Engine).	In Progress - The evaluation methodology is specified in Deliverable D5.1 and identified the pertinent C4IIoT subcomponents. By reviewing the second release (R2) of the C4IIoT platform (M30), we will verify that at least 20% of system vulnerabilities, identified by security assessment components described in KPI-3.1, have been patched (validated by Security Assurance Module) or corresponding attacks have been mitigated (validated by Mitigation Engine).
[KPI-3.3] Enhance existing cybersecurity protection assets for behaviour anticipation, detection, tracking, mitigation (i.e. intrusion detection systems, intrusion prevention systems, firewalls, etc.) to 90% accuracy.	In progress - The consortium has specified the evaluation methodology (see D5.1) and identified the pertinent C4IIoT subcomponents; will monitor the accuracy of all components comprising the C4IIoT Level 3 protection layer (Security by ML-based behavioural analysis & cognitive security capabilities), through interaction with the corresponding component owners (namely, Behavioural analysis & cognitive security; Traffic analysis) and ensure accuracy of said detection capabilities at least 90%. Furthermore, it will ensure that Mitigation Engine provides at least 90% success rate in applying mitigation strategies.	In Progress - The evaluation methodology is specified in Deliverable D5.1 and identified the pertinent C4IIoT subcomponents. By reviewing the second release (R2) of the C4IIoT platform (M30), we will monitor the accuracy of all components comprising the C4IIoT Level 3 protection layer and through interaction with the corresponding component owners we will ensure that the accuracy of the detection capabilities is at least 90%. Also, during the reviewing process we will ensure that the Mitigation Engine provides at least 90% success rate in applying mitigation strategies.
[KPI-3.4] More than (5) incorporated safety mechanisms for privacy, accountability and trustworthiness in all IIoT processes – at least (2) of them privacy preserving features.	The technologies of C4IIoT that provides these features include, (i) the Secure Execution Environment (IFAG / FORTH), (ii) the Decentralized access control with attribute-based encryption (IBM), (iii) the Traffic analysis (FORTH), (iv) the Data Fusion Bus (ITML), (v) the Cloud Management & Orchestration (HPE), (vi) the Risk assessment (HPE), and (vii) the Security Assurance Module (STS)	The integration of the C4IIOT components is underway and a final inventory is due to consider all of them. For instance, the Harbor Docker Image Registry combined with server-side Enforcement of image signing at Docker push time, periodic Vulnerability check and Vulnerability number limit at Docker pull time will provide accountability and trustworthiness in all containerized IIoT processes saved in the Docker image repository. Also, Blockchain Database (BCDB) technology will be utilized in the project, which is planned to enable further auditability and trust in C4IIoT.
[KPI-3.5] Enforce automated monitoring, mitigation and visualization for more than (4) threats in IIoT.	The current C4IIoT prototype can detect, identify, and generate mitigations for 3 types of attacks (thus indicating a 75% completion of this KPI). These attacks, when detected, are aggregated by SAM tool which subsequently dispatches them to AEGIS' AVT tool, which both display's this	To manage a complex system like C4IIoT, the Prometheus monitoring system provides monitoring of system resources like: Cluster memory usage, Cluster CPU usage and File system usage; those metrics are displayed using Grafana as dashboard.

	information and can solicit mitigations from UP1PS' CARMAS tool. UP1PS will continue to monitor this KPI and update the number of attack types that can be managed augments.	
[KPI-3.6] Built on top of (10) existing cybersecurity products and services and customize them to be applied in IIoT.	The C4IIoT components that were identified as contributing to this KPI are: (i) AEGIS's advanced visualisation, privacy/secure data analytics, and (ii) STS' Security Assurance Module. Besides these, the C4IIoT consists of many other components, such as: (i) Secure Execution Environment (FORTH), (ii) Decentralized access control with attribute-based encryption (IBM), (iii) Secure Element at Smart Factory Edge Node (IFAG), (iv) Traffic analysis (FORTH), (v) Behavioural analysis & cognitive security module – BACS (UNSPMF), (vi) Advanced visualisation, Privacy/secure data analytics (AEGIS), (v) Data Fusion Bus (ITML), (vi) Cloud Management & Orchestration (HPE), (vii) Risk assessment (HPE), (viii) Security Assurance Module (STS), (ix) Binary Code analyser (CEA), and (x) Reconfiguration Search – VariaMos (UP1PS).	The technologies that cover this KPI are in ongoing development following M18's first C4IIoT prototype and towards the final version of the project. Final assessment of this KPI and the technologies that cover it will be made once they are deployed on the final execution environment.
[KPI-3.7] Significant hidden information revealed (number of concrete warnings and conclusions) based on systems analysis.	The C4IIoT components that were identified as contributing to this KPI are: (i) UNSPMF's Behavioral analysis & cognitive security module (BACS), (ii) AEGIS's advanced visualisation, privacy/secure data analytics, (iii) STS's Security Assurance Module, and (iv) CEA's BINSEC.	The technologies that cover this KPI are in ongoing development following M18's first C4IIoT prototype and towards the final version of the project. Final assessment of this KPI and the technologies that cover it will be made once they are deployed on the final execution environment.
[KPI-4.1] Successful collection of data for demonstrating cybersecurity monitoring and anomaly detection from multiple diverse and heterogeneous IIoT systems.	Ongoing - Collection of datasets within the project is on the way and with good progress. Results of the pilot testing will be used as a measure of success.	Ongoing - Collection of datasets within the project is on the way and with good progress. Two type of datasets have been collected. One type is industrial real datasets provided by CRF, and the other type is datasets acquired from edge node devices – microcontrollers used and developed within the project. There is ongoing progress related to possibilities to obtain labelled datasets, since all that have been acquired by now are unlabeled. Results of the pilot testing will be used as a measure of success.
[KPI-4.2] Delivery of 3 integrated versions of the C4IIoT framework.	ITML will integrate the distinct services towards the realization of C4IIoT framework until the end of the project. Specifically, 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 responsible for a first complete prototype that derived internally at M18 and a second prototype – the final solution that will be derived on M30 as well as the configuration of the framework during the two pilots.	In progress - In the context of C4IIoT framework, three (3) integrated versions are to be delivered. Up to now, a proof-of-concept demonstration (MVP) and a first complete prototype have been delivered. We are working towards the delivery of the final solution on M30.
[KPI-4.3] Execution of (2) demonstrators in automotive manufacturing industry, together validating at least 95% of tools.	The C4IIoT platform will be demonstrated in the automotive manufacturing industry, on two use cases: namely "Smart Factory" and "Inbound Logistics"; and it will show operation of the integrated C4IIoT Cybersecurity framework. For both the "Smart Factory" and "Inbound Logistics" use cases it will include communication across all three layers of C4IIoT architecture providing secure and reliable communication services, thus enabling software components on edge nodes and field gateway to generate and	This KPI relates to demonstration of integrated C4IIoT Cybersecurity framework, so the final assessment of the KPI will be done upon the final deployment of the C4IIoT framework in the real-life environment. Current status is development and integration of all involved tools.

	exchange data, and communicate to the cloud layer. The communicators for the "Inbound Logistics" use case will be secured by means of VIP Mobile operator, utilizing its telco infrastructure and radio network coverage.	
[KPI-4.4] More than (10) field trials to demonstrate C4IIoT tools' applicability and performance within an automotive real-world environment.	Field trials will be performed to demonstrate C4IIoT framework functionality and performance for the Inbound logistic use case by utilizing the VIP Mobile cellular communication services, such as GPRS and LPWAN NB-IoT. At the edge layer, pool of new fabricated secure-by-design devices, mounted to the logistic containers, will be used and evaluated in real life conditions against the existing CRF's infrastructure, in collaboration with the Supply Chain Management and the Manufacturing departments in FCA and the staff from the selected plant in FCA. C4IIoT framework will demonstrate successful data collection at the edge node layer in different radio conditions, communication and data exchange across all three layers and show resilience and proper response to synthesized cyberattacks.	This KPI relates to demonstration of integrated C4IIoT Cybersecurity framework, so the final assessment of the KPI will be done upon the final deployment of the C4IIoT framework in the real-life environment. Current status is development and integration of all involved tools.
[KPI-4.5] Construction of an informative mechanism for both security and non-security experts.	AEGIS has implemented the first version of Advanced Visualization Toolkit (AVT) for the MVP version of C4IIoT, displaying real-time measurements from the monitored devices and events captured from anomaly detection process. For the 1st integrated prototype, the advanced informative mechanism includes attack plans information from SAM and interaction with the mitigation engine.	AEGIS built on top of the already developed solution (M18) by adding more filters, informative annotations and made developments to increase usability. During the previous period we have introduced the timeline analysis on detected anomalies.
[KPI-5.1] All C4IIoT security solutions, products and services aligned and harmonized with regulations and EU standards.	The security solutions are aligned with GDPR and ENISA guidelines, especially the last one: "Guidelines for securing the Internet of Things (Nov 2020)", and with the several references provided by ENISA previous guidelines such as "Good Practices for Security of Internet of Things in the context of Smart Manufacturing (Nov 2018)"	D6.5 contains an updated standardization plan for all of the modules provided by members of the consortium.
[KPI-5.2] Define a concrete dissemination strategy to raise awareness [dKPIs]. Uptake more than (6) standards from several IIoT related technologies	The dissemination strategy includes online dissemination (website, social media accounts, newsletter, technical videos), scientific publications, organisation of events, system level demonstrations. Most of the technical deliverables are public, downloadable from the website. Currently we have uptake the following standards: ISA99, ENISA the pillars of IIoT guidelines, CSA, TCG, GSMA and OASIS (PKCS series from RSA)	An updated dissemination strategy can be found in D6.6. C4IIoT. The standards that are followed by the project so far can be found in D6.5
[KPI-5.3] More than (20) entities (e.g. academics and enterprises) to use C4IIoT offerings.	VIP will approach at least 30 enterprises (government and non-government segment) regarding the interest in C4IIoT offerings. Promotion of C4IIoT results is planned in scope of regular meetings, targeted events, and conferences with business partners.	Ongoing activities. VIP had approached more then 50 enterprises through regular B2B meetings, through an online conference held in April , with material available at https://a1ict.rs/
[KPI-6.1] Ready to market integrated solution for the an overall IIoT system and independent security solutions (TRL 6).	FORTH will verify that the C4IIoT framework will reach TRL 6 by the end of the project. According to the GA, it is expected to be evaluated within CRF's lab.	FORTH will verify that the C4IIoT framework will reach TRL 6 by the end of the project. According to the GA, it is expected to be evaluated within CRF's lab.

[KPI-6.2] At least (4) C4IIoT tools reach market readiness level (8) at the end of the project.	FORTH will verify that at least 4 of C4IIoT tools will reach TRL 8 by the end of the project. The consortium consists of several partners from industry and SMEs, so it is expected to have at least (4) tools with TRL (8) by the end of the project.	FORTH monitors the progress of the tools inside the C4IIoT project. An update for each tool will be included in a future WP5 deliverables along with the integration in CRF premises.
[KPI-6.3] At least 6 third-party collaborations to be established for further applicability verification.	UP1PS will monitor this KPI by regularly sending emails to all C4IIoT partners asking them to report any third-party collaboration they have established so far. As of now, we have initiate joint standardization activities with other H2020-SU-ICT-2018 projects (CARAMEL, CyberSANE, GUARD, SOCCRATES, SAPPAN). Also, we have invited representatives from CyberSANE and COLLABS projects to present their approaches in our 1st C4IIoT Winter School (organized in December 2020).	C4IIoT participated actively at the "Joint Standardisation Workshop Dynamic Counter of Cyber-Attacks projects (held online on January 22)". The workshop was organized by all relevant projects under SU-ICT-01-2018.
[KPI-6.4] More than (10) critical aspects (e.g. maintenance and software updates) will addressed to ensure long-term sustainability of the solution.	The consortium has specified the evaluation methodology (see Deliverable D5.1) and will further ensure that the work of Task 4.4 and the associated Deliverable D4.4 (titled "Best practices for maintaining and operating the framework in the long-term – TRL 6") will encompass more than 10 critical aspects of the long-term operation and maintenance of the final C4IIoT solution.	In Progress – The consortium has specified the evaluation methodology in Deliverable D5.1 and this KPI will be evaluated via reviewing the work of Task T4.4, once completed. Furthermore, the associated Deliverable D4.4 (titled "Best practices for maintaining and operating the framework in the long-term – TRL 6") will encompass more than 10 critical aspects of the long-term operation and maintenance of the final C4IIoT solution.
[KPI-6.5] A concrete business plan for business continuity (including joint exploitation plans, alliances and collaborations) will be released at the end of the project.	CEA will monitor this KPI by sending quarterly emails to C4IIoT asking industrial partners if they made progress regarding this business plan, starting from June 2021.	CEA will monitor this KPI by sending quarterly emails to C4IIoT asking industrial partners if they made progress regarding this business plan, starting from June 2021.The monitoring actions for this KPI has not started yet, as it starts in June 2021.

Table 4: Status of Innovation KPIs

Impact KPIs	**Status M18:**	**Status M24:**
iKPI#1.1 At least 15 different, already reported types of advanced cybersecurity threats identified and mitigated by the C4IIoT framework in the C4IIoT pilots.	CEA will monitor this KPI by sending regular emails to WP5 participants asking for the list of threats identified and mitigated in the C4IIoT pilots	The Identity Management module provides protection to some of the listed attacks identified in D1.2 at Table 2, namely: Malware, Manipulation of information, Erroneous use or administration of devices and systems, Unintentional change of data or configuration in the OT system – all requiring access to the system that is filtered by the ID module. Brute force attacks are mitigated by using a security policy that requires authentication on the system using strong passwords.
iKPI#1.2 At least 5 new types of advanced cybersecurity threats identified and mitigated by the C4IIoT framework in the C4IIoT pilots.	The proposed plan is made of two phases: 1) collect all possible threats captured in the AS-IS that constitute the baseline of the measurement; 2) collect all possible threats with C4 components active and working, to obtain and verify the increase number and typology of threats captured. Step 1) need to have C4 logging and monitoring components only installed on CRF premises to capture the AS-IS status. Step 2) need in addition to have all other C4 security components active and working to capture the advancement obtained.	Once new threats are identified, the evaluation on the protection provided by the Identity Management module will be analysed.

	Assumptions to be made to threats generation should the CRF system work off-line threats must be generated artificially in both scenarios. New threats will be artificially generated during testing phases.	
iKPI#2.1 3 tools and services for complex distributed systems handling IIoT cyber-attack incidents.	C4IIoT has already five tools for handling IIoT cyber-attack incidents in complex distributed environments: (i) UNSPMF's BACS anomaly detection, (ii) IBM's decentralized access control with attribute-based encryption, (iii) FORTH's Traffic Analysis, (iv) IFAG's OPTIGA edge security element, (v) TSG's SDN controller, all operate in distributed environments.	Continue monitoring the C4IIoT tools that handle IIoT cyber-attack incidents in complex distributed environments.
iKPI#2.2 3 cyber threats with multiple levels of risk avoided due to E2C architecture.	The proposed plan is made of two phases: 1) collect all possible threats that have been avoided in the AS-IS that constitute the baseline of the measurement; 2) collect all possible threats that have been avoided with C4IIoT components active and working, to obtain and verify the increase number and typology of threats captured. Step 1) need to have C4IIoT logging and monitoring components only installed on CRF premises to capture the AS-IS status. Step 2) need in addition to have all other C4IIoT security components active and working to capture the advancement obtained. Assumptions to be made to threats generation should the CRF system work off-line threats must be generated artificially in both scenarios. New avoided threats will be artificially generated during testing phases.	Steps are taken to initiate the first phase to measure the as-is as a baseline. We have identified the manipulation of information as a first threat with multiple levels of risks. C4IIoT contains the security modules to protect even against powerful adversaries. For example, (i) secure elements protect against attacks that are able to compromise the hardware devices themselves, (ii) the use of strong crypto defends against MITM attacks, (iii) the use of blockchain can verify data integrity, etc.
iKPI#2.3 4 cyber threats with multiple levels of risk avoided due to secure execution environment.	IFAG provides hardware-enabled security components, using a secure element as well as a TEE, to avoid different cyber and physical attacks from different levels. In order to reach that, the secure elements will be connected in the edge nodes. We assume the cyber threats will be generated artificially in the CRF system.	In progress – At the end of the project, the edge nodes were tested in order to avoid at least 4 cyber threats. The tests will take place in CRF labs. IFAG will provide the HSMs and the hardware security layer in order to mitigate or avoid the cyber threats in the edge node.
iKPI#3.1 3 ENISA representatives to be contacted during the project.	This KPI will be monitored periodically to check whether the ENISA representatives have been contacted.	In progress – It is still a bit early to contact the ENISA representatives, as the 2nd year of the project is not over yet. Still, several C4IIoT partners participated in ENISA's Cybersecurity Standardization Conference 2021 (https://www.enisa.europa.eu/events/cybersecurity_standardisation_2021). This KPI will be monitored periodically to check whether the ENISA representatives have been contacted.
iKPI#4.1 2 complementary fields of demonstration.	ITML will ensure that the integrated C4IIoT solution will be demonstrated in two complementary fields (namely, Logistics 4.0 and Smart factory); the integrated solution will be customized based on the specific needs of each field and will be validated by the end user (CRF) of the project.	In progress – We are working towards the final integrated solution which is going to be delivered on M30 and its functionality will be verified by the C4IIoT pilots and customized based on the specific needs of each field.
iKPI#4.2 At least 6 stakeholders engaged by the end of the project to further adopt C4IIoT cybersecurity	iPKI considered at M28, as soon as the task 6.5 starts	In progress - No change

framework.		
iKPI#5.1 At least 5 innovative tools and technologies advanced within C4IIoT (according to Gartner and ECSO).	According to ECSO's Strategic Research and Innovation Agenda[1] innovative technologies for cyber-security include Machine and Deep Learning, Big Data security analytics, Response and Recovery tools combining automation with human expertise, risk and cost-based models for Response and Recovery, Distributed trust management solutions such as Blockchain, technologies to provide security and privacy by design, etc. Also, in Gartner's prediction (2019 and 2020) innovative technologies included: embedded AI, Adaptive ML, Self-supervised learning, Low-Cost, Single-Board Computers at the Edge, Edge Analytics and Edge AI. C4IIoT architecture is aligned with at least 5 of the technologies identified by Gartner and ECSO above through UNSPMF's BACS anomaly detection (Deep Learning), IBM's decentralized access control with attribute-based encryption (Blockchain), CEA's BINSEC verification (security by design at the hardware level), IFAG's secure execution (security by design using encryption) and UP1PS's CARMAS mitigation (Response and Recovery tools combining automation with human expertise).	Continue to monitor the innovation technologies and how C4IIoT tools relate to them. Several tools have been advanced so far; for example: BINSEC is equipped with a new patch-oriented-testing method (called UAFUZZ), based on integration with AFL and IDA Pro. DAC has been improved to utilize the new Blockchain Database (BCDB) technology, that is planned to enable further auditability and trust in C4IIoT, as well the query mechanism of HLF peers and the decryption mechanism of ABE clients in order to support the needs of C4IIoT DAC users. CARMAS has been enhanced as a containerized web service that searches for the set of actions that best mitigate an input set of detected attack actions on an IIoT network.
iKPI#5.2 At least >20% Improved resilience of industrial infrastructure with 10% cost effectiveness verified on minimum one (1) pilot.	The pilots are ready for the evaluation in terms of costs and resilience, which will be performed in the second half of the project.	This KPI can be calculated only at the end of the project, when the whole architecture will be tested in CRF, but the results obtained until M24 are promising.
iKPI#5.3 At least 3 industries engaged within C4IIoT duration to exploit innovative technologies.	UP1PS will monitor this KPI by regularly sending emails to C4IIoT partners asking them to report any third-party collaboration with industrial partners outside of the automotive sector which they may have established so far.	In progress - No change
iKPI#6.1 At least 3 innovative products and services of the C4IIoT pilot partner directly enhanced by the cybersecurity framework.	This KPI will be monitored through the two use cases that will be deployed in CRF premises, and the corresponding list of products that will be utilized and enhanced within these use cases.	In progress – the C4IIoT framework begins to be fully integrated on the 2 CRF use cases. This KPI will be monitored through the two use cases that will be deployed in CRF premises, and the corresponding list of products that will be utilized and enhanced within these use cases.
iKPI#7.1 At least 3 industrial companies boosted exploiting C4IIoT cybersecurity capabilities.	IFAG will disseminate the technologies used in C4IIoT in relation to cybersecurity to several companies that use security technologies at the hardware level for example. Companies like Mixed Mode, Xilinx and Utimaco might boost the exploitation of C4IIoT cybersecurity capabilities.	This KPI will be carried out until the end of the project. The dissemination with other companies has already started, currently with companies that are staring to use the Infineon secure elements in their applications.
iKPI#8.1 At least 3 SMEs providing security-related services within project's duration.	In progress - The consortium includes three SMEs (ITML, STS, and AEGIS), which are offering security-related services in the market. The SMEs will monitor and report their service-provision activities and come back with a report at the end of the project verifying the achievement of the KPI.	In progress - No change
iKPI#8.2 At least 10% increase of market share	In progress - The consortium includes three SMEs (ITML, STS, and AEGIS), which are constantly	In progress - No change

[1] https://ecs-org.eu/documents/publications/59e615c9dd8f1.pdf

for SMEs exploiting C4IIoT technologies.	monitoring their achievements in the market and will report at the end of the project the impact of C4IIoT technologies to their market share	
iKPI#9.1 At least 20% Increase in productivity verified on at least one (1) pilot	The pilots are ready for the evaluation in terms of throughput, which will be performed in the second half of the project.	This KPI can be calculated only at the end of the project, when the whole architecture will be tested in CRF, but the results obtained until M24 are promising. It will be evaluated considering the reduction of production stops due to cyber risks or attacks in the industry thanks to the implementation of C4IIoT technologies.
iKPI#9.2 At least 15% Increase in market share for the pilot partner exploiting C4IIoT framework.	CRF will evaluate through its pilots the potential increase of market share for the end-user, enabled by the increased availability, resilience and throughput of the system. The technology providers and C4IIoT platform integrator will evaluate the same for their portfolio of products including the C4IIoT results.	This KPI can be calculated only at the end of the project. Its value is strictly linked to the iKPI#9.1, since it depends also on the productivity increase.
iKPI#9.3 At least 10% Increase in sales for the pilot partner exploiting C4IIoT framework.	CRF will evaluate in the pilot the potential increase of sales for the end-user, enabled by the increased availability, resilience and throughput of the system. The technology providers and C4IIoT platform integrator will evaluate the same for their portfolio of products including the C4IIoT results.	This KPI can be calculated only at the end of the project. Its value is strictly linked to the iKPI#9.1, since it depends also on the productivity increase.

Table 5: Status of Impact KPIs

Dissemination KPIs	Status M18:	Status M24:
dKPI#1: At least 1000 Web access to deliverables, technical results and presentation material of C4IIoT and at least 100 downloads.	C4IIot website has 1816 unique visitors and 356 downloads.	C4IIot website has 2600 unique visitors and 442 downloads.
dKPI#2: At least 50 push announcements through social media (Twitter, LinkedIn, ResearchGate)	69 push announcements (16 LinkedIn, 31 Twitter, 42 Facebook)	185 push announcements (51 LinkedIn, 71 Twitter, 63 Facebook)
dKPI#3: At least 9 newsletters with C4IIoT technical activities	4 Newsletters	6 Newsletter
dKPI#4: At least 2000 downloads of high-quality electronic brochure with the technical approach and activities of C4IIoT and at least 2000 hard copies distribution in more than 10 events	200 Downloads	442 Downloads
dKPI#5: At least 1000 views of 5 min high-quality video presentations of the technical aspects of C4IIoT and more than 10 event presentations	110 video views Event presentations: TBD	284 video views Event presentations: 1
dKPI#6: At least 10	3 publications	5 publications

Publications in International referred technical journals in cybersecurity related subjects		
dKPI#7: At least 10 Publications in International magazines in cybersecurity related subjects	No publications	No publications
dKPI#8: At least 12 Publications in International referred technical conferences in cybersecurity related subjects	8 publications	8 publications
dKPI#9: Publications of special issues in International referred technical journals and magazines (≥ 2, ≥ 10 selected papers/issue)	3 publications	3 publications
dKPI#10: Organization of at least 1 international conference in cybersecurity related domains with 100 attendees (each)	This is planned towards the end of the project and initial planning is currently underway.	In progress - No change
dKPI#11: Organization of at least 2 workshops with 30 attendees (each)	These are planned for the second half of the project with the first planned around M20.	1) International Workshop on SecRS: Secure and resilient smart manufacturing environments (SecRS) to be held in conjunction with the 16th International Conference on Availability, Reliability and Security (Scheduled for August 2021) 2) Third workshop on Cyber-Security Arms Race (CYSARM) which is co-located with the ACM CCS (scheduled for November 2021)
dKPI#12: At least 1 demo at Major fairs and exhibitions such as Cyber Security Europe at IP EXPO Europe, INFOSEC	This KPI will be monitored periodically by polling relevant C4IIoT partners regarding the set-up of demos or exhibition.	No demo was organized at a Major fair or exhibition yet. This KPI will be monitored periodically by polling relevant C4IIoT partners regarding the set-up of demos or exhibition
dKPI#13: At least 2 demos at Major EU events such as meetings and workshops organized by ENISA and SANS information security courses' events	SME's or industrial partners of the consortium typically participate in major EU events. It would be feasible for them to perform such demonstrations.	No demo was organized at a Major EU event yet. SME's or industrial partners of the consortium typically participate in major EU events. We speculate that will have the chance to perform such demonstrations.
dKPI#14: At least 2 demos at Major conferences (e.g. GLOBECOM, ICC)	Academic partners typically attend and participate in several conferences and workshops. It would be feasible for them to perform such demonstrations.	No demo was organized at a conference yet. Academic partners typically attend and participate in several conferences and workshops. We speculate that will have the chance to perform such demonstrations
dKPI#15: Organization of at least 3 events of education and training	33% fulfilment - C4IIoT INFO day in September 21st 2020 with more than 70 attendees.	1) C4IIoT INFO day in September 21st 2020 with more than 70 attendees. 2) International winter cybersecurity school organized

activities (e.g. hackathons, educational and training events, webinars and seminars, to promote C4IIoT cybersecurity offerings with at least 70 attendees (each)		within the C4IIoT project with more than 50 attendees. 3) International Workshop on SecRS: Secure and resilient smart manufacturing environments (SecRS) to be held in conjunction with the 16th International Conference on Availability, Reliability and Security (Scheduled for August 2021). 4) Another international cybersecurity school is planned to be organized in the final 6 months of the project.
dKPI#16: Organization of at least 2 events of international summer schools in cybersecurity in the IIoT domain with at least 30 attendees (each)	50% fulfilment - International winter cybersecurity school organized within the C4IIoT project with more than 50 attendees.	50% fulfilment - International winter cybersecurity school organized within the C4IIoT project with more than 50 attendees. Another international cybersecurity school is planned to be organized in the final 6 months of the project.

Table 6: Status of Dissemination KPIs

Communication Activities KPIs	Status M18:	Status M24:
eKPI#1: C4IIoT website with at least 5000 accesses annually and 500 downloads worldwide	2500 sessions 350 downloads	3200 sessions 420 downloads
eKPI#2: At least 10 Press echoes in Europe	No	0
eKPI#3: At least 10 Newspapers (business and normal) in Europe	No	3
eKPI#4: At least 9 Newsletters worldwide	4 Newsletter	6
eKPI#5: At least 500 followers worldwide in Social Media (Twitter, LinkedIn, ResearchGate)	285 Followers	336
eKPI#6: At least 2 Public lectures and/or networking events for end users & general public with at least 50 attendees (each)	C4IIoT has already organized two public events: the INFO day in September 21st 2020 with more than 70 attendees and the International winter cybersecurity school with more than 50 attendees.	C4IIoT has already organized two public events: the INFO day in September 21st 2020 with more than 70 attendees and the International winter cybersecurity school with more than 50 attendees.
eKPI#7: At least 2 Public lecture and/or networking event for policy makers with at least 20 attendees (each)	NIS Summerschool 2019 : FORTH, AEGIS Trustech conference 2019 : IFAG, TSG	No change
eKPI#8: At least 4 Policy events targeting policy makers of EU, National, Regional and Local Authorities with	Trustech Tradeshow 2019 Cannes IFAG,TSG Startup Safari Tradeshow Munich : IFAG Intergraf Tradeshow Copenhagen : IFAG Silicon Alps Security week: IFAG	No change

at least 50 attendees (each)		

Table 7: Status of Communication Activities KPIs