Horizon 2020 Program

Dynamic countering of cyber-attacks

SU-ICT-2018

Cyber security 4.0: Protecting the Industrial Internet of Things

D5.3 Assessment report and impact analysis[†]

Abstract: This deliverable includes the reporting regarding the final evaluation and impact analysis, as result of activities related to T5.2 and T5.3. More specifically, the KPIs final values are presented and described, according to their definition presented previously in the project. This document also includes the description of last steps related to the final execution of the demonstrators.

Contractual Date of Delivery	31/05/2022
Actual Date of Delivery	24/06/2022
Deliverable Security Class	Public
Editor	Gianmarco Genchi, Jlenia Puma (CRF)
Contributors	All C4IIoT Partners
Quality Assurance	Camilo Correa Restrepo (UP1PS) Giorgos Stamatis, Nikolaos Evangeliou (ITML)

[†] *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	FORTH	Coordinator	EL
CENTRO RICERCHE FIAT SCPA	CRF	Principal Contractor	IT
INFINEON TECHNOLOGIES AG	IFAG	Principal Contractor	DE
THALES SIX GTS FRANCE SAS	TSG	Principal Contractor	FR
HEWLETT PACKARD ITALIANA SRL	HPE	Principal Contractor	IT
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	CEA	Principal Contractor	FR
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	IBM	Principal Contractor	IL
AEGIS IT RESEARCH UG	AEGIS	Principal Contractor	DE
UNIVERSITE PARIS I PANTHEON-SORBONNE	UP1PS	Principal Contractor	FR
INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP	ITML	Principal Contractor	EL
SPHYNX TECHNOLOGY SOLUTIONS AG	STS	Principal Contractor	CH
UNIVERSITY OF NOVI SAD FACULTY OF SCIENCES	UNSPMF	Principal Contractor	SRB
UNIVERSITY OF GREENWICH	UOG	Principal Contractor	UK
A1 SRBIJA D.O.O.	A1	Principal Contractor	SRB

Document Revisions & Quality Assurance

Internal Reviewers

1. Camilo Correa Restrepo (UP1PS)
2. Giorgos Stamatis, Nikolaos Evangeliou (ITML)

Revisions

Version	Date	By	Overview
0.0.1	13/04/2022	Jlenia Puma, Gianmarco Genchi (CRF)	ToC
0.1	31/05/2022	All C4IIoT Partners	First integrated version, including partners' contribution
0.2	16/06/2022	All C4IIoT Partners	Second integrated version with additional partners' contribution
0.3	24/06/2022	Jlenia Puma, Gianmarco Genchi (CRF)	Final version, after addressing internal reviewers' comments

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ABE	Attribute Based Encryption
AGV	Automated Guided Vehicle
AVT	Advanced Visualization Toolkit
BACS	Behavioral Analysis and Cognitive Security
C4IIoT	Cyber security 4.0: protecting the Industrial Internet of Things
CA	Certificate Authority
CPU	Central Processing Unit
D	Deliverable
DAC	Decentralized Access Control
DFB	Data Fusion Bus
DISCO	Distributed SDN COntrol plane
DL	Deep Learning
EC	European Commission
EE	End Entities
ETA	Estimated Time of Arrival
FG	Field Gateway
FGR	Field Gateway Receiver
GPRS	General Packet Radio Service
HAD	Hierarchical Anomaly Detection
HLF	Hyperledger Fabric
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IIoT	Industrial Internet of Things
IOT	Internet of Things
KPI	Key Performance Indicator
NB-IoT	Narrow Band Internet of Things
OEE	Overall Equipment Efficiency
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
RP	Raspberry Pi
RPS	Response per Second
SAM	Security Assurance Model
SDN	Software Defined Networking

SME	Small and Medium Enterprise
T	Task
TEE	Trusted Execution Environment
TCM	Trusted Computing Module
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TPM	Trusted Platform Group
UDP	User Datagram Protocol
WP	Work Package

Executive Summary

In the context of the C4IIoT project, it has been possible to develop a solution to address the need for understanding and managing, even in advance, possible failures in IoT devices installed both on the AGV of the Assembly plant and on the containers of the Inbound Logistics. In fact, the C4IIoT solution has functionalities that allow the monitoring, notification, and mitigation of potential threats to IIoT infrastructure, not only in the Automotive sector, but also in other industries. In order to do so, the solution has been developed according to the requirements provided by CRF as end-user, but also verifying and validating them through the involvement of external industrial stakeholders.

In order to finally assess the benefits deriving from the usage of the C4IIoT solution, a comprehensive set of KPIs has been identified in the first phase of the project and has been evaluated after the implementation of the demonstrator in both the Smart Factory scenario and in the Logistics4.0 scenario.

1 Introduction

This deliverable aims to present the final evaluation and impact assessment of the C4IIOT solution, as a result of the last phase of WP5 activities. In fact, within WP5, not only have the demonstrators been implemented in a real-world environment, but also the analysis of the added value due to its utilization has been performed. Both an analysis of the architecture components and overall project KPIs are described in this deliverable.

CRF has led WP5, coordinating all the related activities, including the finalization of the demonstrator and evaluation phase. In particular, concerning the factory deployment, here we present the last steps and technical evaluation of the components that were not included in D5.2 [1] because their tests were still in progress.

Moreover, as an Annex, a requirement table is also included. This table describes the requirements defined during the project and later validated also by the external stakeholders (resulting from WP1 activities). In addition, it shows the results of the validation of the C4IIoT solution requirements by CRF as the project's end-user.
Finally, the table showing the components impacting each KPI, already included in D5.1 [2] is presented as an Annex as well.

1.1 Purpose and Scope

The main objective of the deliverable is to describe the final evaluation of the C4IIoT solution, through the analysis performed in WP5. The results achieved in the project have been analysed, also through the evaluation of the pilot tests executed in the real-world environment. The analysis has been performed by mean of the utilization of KPIs, that were identified in the first phase of the project, as presented in D5.1[2], and that have been constantly monitored. Moreover, additional contents with respect to the D5.2 [1] are reported here, to describe the final scenario on which the impact assessment has been based.

1.2 Relation to other Work Packages

The current deliverable describes the results of the activities performed within WP5 but it is strictly linked to the output of other Work packages.

First of all, the demonstrator execution and the related impact analysis have made possible thanks to results of the WP4 activities, and in particular Deliverable 4.3 [3], where the integrated architecture has been presented.

Moreover, within the activities of WP1, the requirements of the industry environment were identified and then, in the context of WP5, these requirements have been finally verified and validated through the final demonstrators' execution.

Finally, this document collects the results of the project, that have already been presented during the Info Day organized by CRF on the 26th May 2022 to show the project results and attract potential customers, in the context of WP6, dedicated to the project results exploitation and dissemination.

1.3 Contribution to WP and Project objectives

This deliverable describes the C4IIoT solution's final assessment and impact analysis. Thanks to this document, it is possible to have a picture of the validation of the architecture developed within the project, how it has been evaluated, and the results obtained.

1.4 Structure of the Document

In the current introductive chapter, the contents and the objectives of the document are presented. Then, Chapter 2 describes the final architecture tests' execution in both the Smart Factory and the Logistics4.0 scenarios, including the final technical evaluation of some components, in order to integrate what already described in D5.2 [1]. Then, Chapter 3 is dedicated to the KPIs monitoring, including the KPIs overall report and the evaluation and impact analysis for the real-life industrial demonstrators.

After the conclusion chapter and references, two tables are included as annexes, describing the requirements fulfilment and the contribution of each C4IIoT components in the KPIs measurement.

2 Final execution of real life industrial pilot

In this chapter, the final experiment execution allowing to evaluate the C4IIoT solution is presented. In particular, any update following the contents already included in D5.2[1], for example the technical evaluation outputs that were still in progress during the writing of the aforementioned document, have been described here.

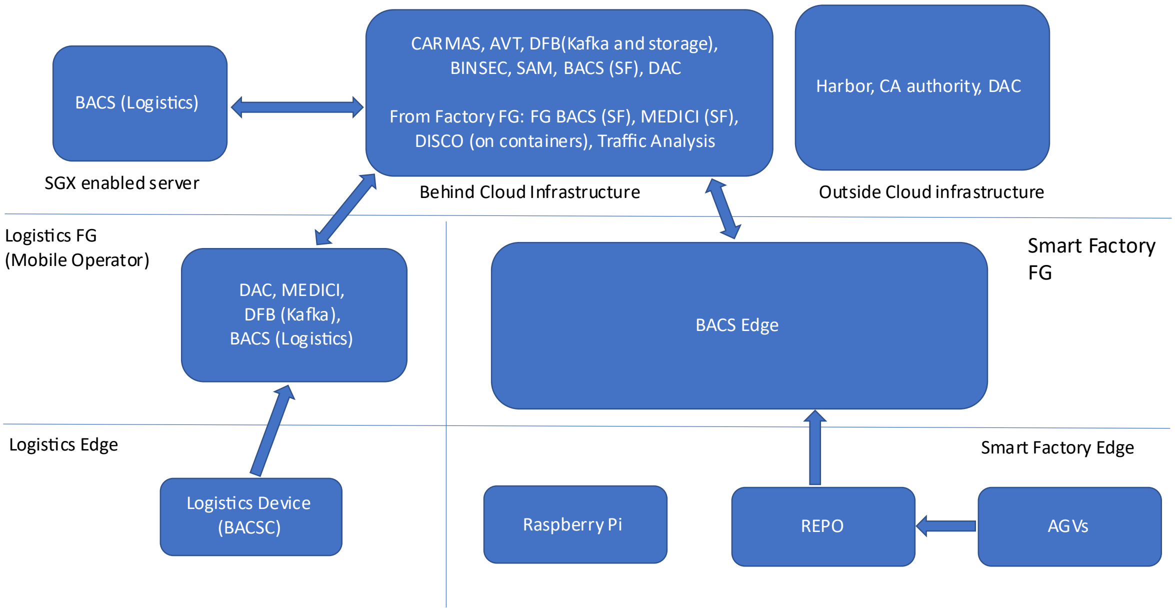
2.1 Smart Factory scenario

Some adjustments were made in the Smart Factory scenario in the last months of the project due to some limitations involving the field gateway layer and the edge of this scenario. In fact, at the time of writing of this deliverable, some connection issues still affect the communication between the mentioned layers in the plant. The motivation is due to the restricted time for deployment in the Campus Melfi, that has been subject to delays starting from 2020 due to covid-19 restrictions, causing a limitation in the access to the plant and also in the involvement of the expert people (i.e. ICT or external supplier of the sensor system).

This section presents details about these refinements that allowed to validate the C4IIoT solution despite the points mentioned above.

These limitations prevented the stable deployment of modules on two layers, the field gateway and the edge, leading to a mandatory adjustment of the architecture, moving essentially the two layers one level up. As presented in Figure 1, Edge BACS is now deployed on the field gateway layer, while MEDICI, Field Gateway BACS, the Traffic Analysis Module and DISCO are now deployed on the Cloud layer.

Figure 1 - Updated deployment architecture


BACS (Logistics)
SGX enabled server
CARMAS, AVT, DFB(Kafka and storage), BINSEC, SAM, BACS (SF), DAC
From Factory FG: FG BACS (SF), MEDICI (SF), DISCO (on containers), Traffic Analysis
Behind Cloud Infrastructure
Harbor, CA authority, DAC
Outside Cloud infrastructure
Logistics FG (Mobile Operator)
DAC, MEDICI, DFB (Kafka), BACS (Logistics)
BACS Edge
Smart Factory FG
Logistics Edge
Smart Factory Edge
Logistics Device (BACSC)
Raspberry Pi
REPO
AGVs

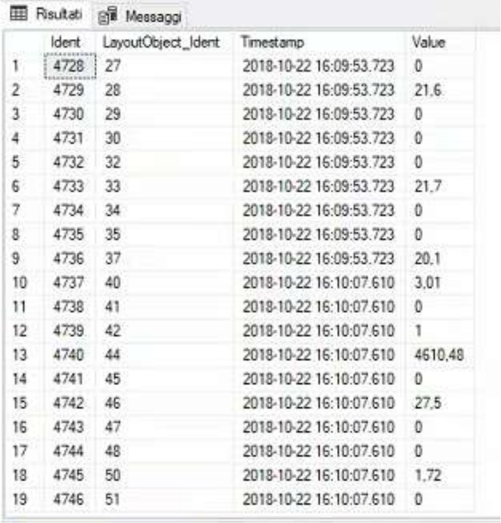
In the following paragraphs we present details about the Smart Factory scenario focusing on the edge node layer, where the differences with the logistics use case are found. The final version of the edge component needs to ingest data from the Microsoft SQL Server database which runs on the CRF premises. The robotic equipment is limited to writing its data (collected from sensors) to this database, so the data cannot be collected directly on the edge devices, which in the case of the Smart Factory use case are the Raspberry Pi devices.

With this in mind, UNSPMF has written an adapter software program with the purpose of reading the data from the mentioned database and writing it in a streaming fashion to the Data Message Bus (Kafka). The adapter program runs periodically, reads the data from the database and forwards it to the Kafka message queue. This program has, in addition to the pyodbc (Microsoft SQL driver for Python), the same dependencies as the other components such as BACS Edge and can be deployed at all levels of the architecture (Edge Raspberry Pi's, Smart Factory Field Gateway, Smart Factory Cloud). Our experiments were on the Smart Factory field gateway as that is where most of the relevant components are intended to be: the database, Kafka runtime (Docker) and Decentralized Access Control (IBM's DAC, Docker). However, for Kafka and DAC, as mentioned above and shown in Figure 1, the cloud version of these components is actually used at the moment of writing this deliverable

The adapter program performs data transformation from the raw shape of the data which is written to the database into the format used by machine learning models of BACS. BACS requires a simple data format of just the timestamp, acceleration, and velocity values. The database raw data contains all this information but needs to be processed in a certain way before the analysis (machine learning model inference).

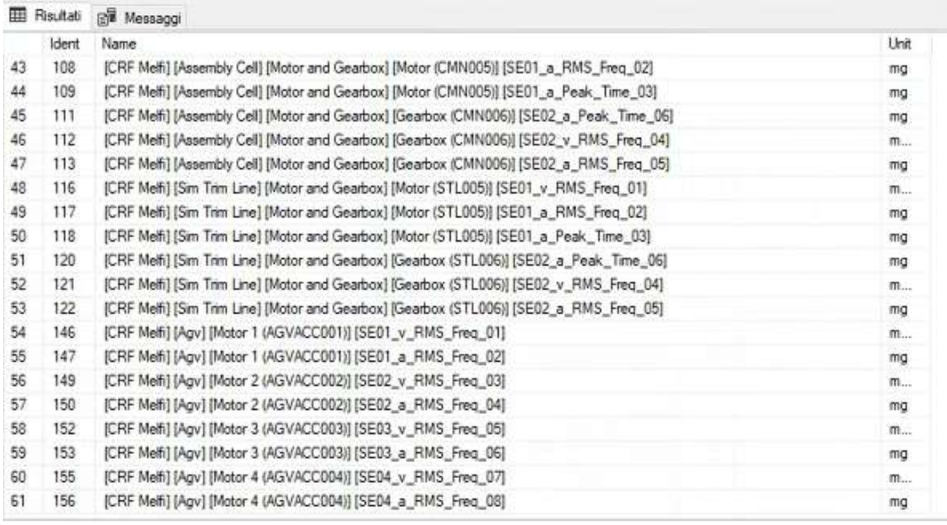
In Figure 2 and Figure 3**Error! Reference source not found.**, we present how the raw data looks like in the MSSQL database.

Figure 2 - Sensory data in the table UnitProcessData



	Ident	LayoutObject_Ident	Timestamp	Value
1	4728	27	2018-10-22 16:09:53.723	0
2	4729	28	2018-10-22 16:09:53.723	21,6
3	4730	29	2018-10-22 16:09:53.723	0
4	4731	30	2018-10-22 16:09:53.723	0
5	4732	32	2018-10-22 16:09:53.723	0
6	4733	33	2018-10-22 16:09:53.723	21,7
7	4734	34	2018-10-22 16:09:53.723	0
8	4735	35	2018-10-22 16:09:53.723	0
9	4736	37	2018-10-22 16:09:53.723	20,1
10	4737	40	2018-10-22 16:10:07.610	3,01
11	4738	41	2018-10-22 16:10:07.610	0
12	4739	42	2018-10-22 16:10:07.610	1
13	4740	44	2018-10-22 16:10:07.610	4610,48
14	4741	45	2018-10-22 16:10:07.610	0
15	4742	46	2018-10-22 16:10:07.610	27,5
16	4743	47	2018-10-22 16:10:07.610	0
17	4744	48	2018-10-22 16:10:07.610	0
18	4745	50	2018-10-22 16:10:07.610	1,72
19	4746	51	2018-10-22 16:10:07.610	0

Figure 3 - LayoutObject table metadata (devices and units)



	Ident	Name	Unit
43	108	[CRF Melfi] [Assembly Cell] [Motor and Gearbox] [Motor (CMN005)] [SE01_a_RMS_Freq_02]	mg
44	109	[CRF Melfi] [Assembly Cell] [Motor and Gearbox] [Motor (CMN005)] [SE01_a_Peak_Time_03]	mg
45	111	[CRF Melfi] [Assembly Cell] [Motor and Gearbox] [Gearbox (CMN006)] [SE02_a_Peak_Time_06]	mg
46	112	[CRF Melfi] [Assembly Cell] [Motor and Gearbox] [Gearbox (CMN006)] [SE02_v_RMS_Freq_04]	m...
47	113	[CRF Melfi] [Assembly Cell] [Motor and Gearbox] [Gearbox (CMN006)] [SE02_a_RMS_Freq_05]	mg
48	116	[CRF Melfi] [Sim Trim Line] [Motor and Gearbox] [Motor (STL005)] [SE01_v_RMS_Freq_01]	m...
49	117	[CRF Melfi] [Sim Trim Line] [Motor and Gearbox] [Motor (STL005)] [SE01_a_RMS_Freq_02]	mg
50	118	[CRF Melfi] [Sim Trim Line] [Motor and Gearbox] [Motor (STL005)] [SE01_a_Peak_Time_03]	mg
51	120	[CRF Melfi] [Sim Trim Line] [Motor and Gearbox] [Gearbox (STL006)] [SE02_a_Peak_Time_06]	mg
52	121	[CRF Melfi] [Sim Trim Line] [Motor and Gearbox] [Gearbox (STL006)] [SE02_v_RMS_Freq_04]	m...
53	122	[CRF Melfi] [Sim Trim Line] [Motor and Gearbox] [Gearbox (STL006)] [SE02_a_RMS_Freq_05]	mg
54	146	[CRF Melfi] [Agv] [Motor 1 (AGVACC001)] [SE01_v_RMS_Freq_01]	m...
55	147	[CRF Melfi] [Agv] [Motor 1 (AGVACC001)] [SE01_a_RMS_Freq_02]	mg
56	149	[CRF Melfi] [Agv] [Motor 2 (AGVACC002)] [SE02_v_RMS_Freq_03]	m...
57	150	[CRF Melfi] [Agv] [Motor 2 (AGVACC002)] [SE02_a_RMS_Freq_04]	mg
58	152	[CRF Melfi] [Agv] [Motor 3 (AGVACC003)] [SE03_v_RMS_Freq_05]	m...
59	153	[CRF Melfi] [Agv] [Motor 3 (AGVACC003)] [SE03_a_RMS_Freq_06]	mg
60	155	[CRF Melfi] [Agv] [Motor 4 (AGVACC004)] [SE04_v_RMS_Freq_07]	m...
61	156	[CRF Melfi] [Agv] [Motor 4 (AGVACC004)] [SE04_a_RMS_Freq_08]	mg

In SQL table UnitProcessData there are the following columns:

- Ident: Event id
- LayoutObject_Ident: id of the source of the event (foreign key from the LayoutObject table), exact sensor of the exact device. Sensor type is also known.
- Timestamp: timestamp of the event
- Value: value reported by the source of the event

The other table LayoutObject describes the sources of the streaming IoT events:

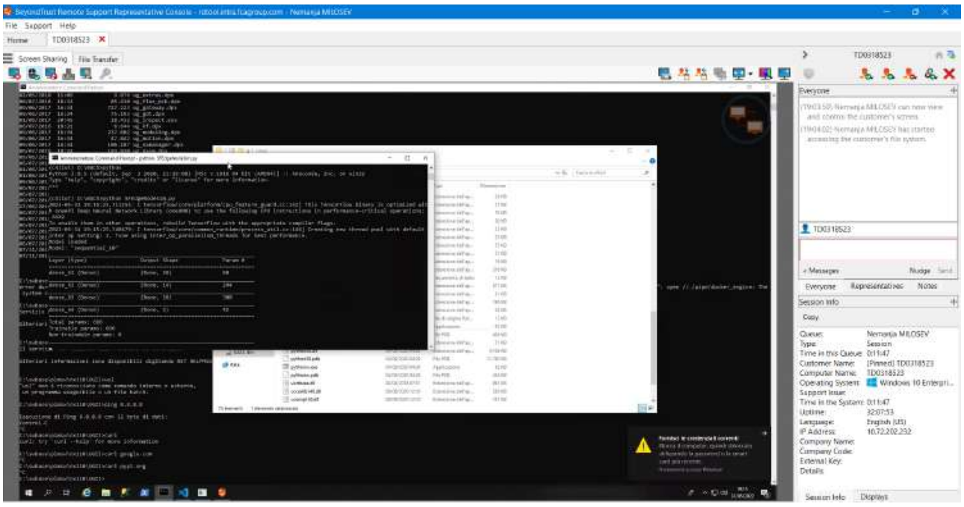
- Ident: Device id
- Name: Device name, also contains unique string id's, device position
- Unit: in which units the device reports its data (for example "mg" for acceleration (micro g's) and mm/s for velocity (millimetres per second)

From these two tables the adapter program reads the data and transforms it into format expected by BACS. The adapter program runs in an infinite loop and every 60 seconds it polls the database for changes (since the last observed timestamp) and publishes the data to the Kafka message bus.

The adapter program is setup in such a way so that it can run both inside a Docker environment (on any architecture layer) or on the Field Gateway directly. In Figure 4, we can see how the BACS Edge for the Smart Factory runs directly on the field gateway hardware.

The BACS Edge component works without modification from our previous report. It uses a TensorFlow based autoencoder trained on CRF unsupervised dataset to detect anomalies in real-time and report them to other components by publishing inference results to the message bus.

Figure 4 - BACS Edge for Smart Factory running on the Field Gateway at CRF



(19:03:50) Nemanja MILOSEV can now view and control the customer's screen.
(19:04:02) Nemanja MILOSEV has started accessing the customer's file system.

Queue: Nemanja MILOSEV
Type: Session
Time in this Queue: 0:11:47
Customer Name: [Pinned] TD0318523
Computer Name: TD0318523
Operating System: Windows 10 Enterpri...
Support Issue:
Time in the System: 0:11:47
Uptime: 32:07:53
Language: English (US)
IP Address: 10.72.202.232
Company Name:
Company Code:
External Key:
Details:

The two Raspberry Pis, enhanced with IFAG's modules, which were previously planned to host the BACS edge, have also been deployed in the Factory network. Despite being currently unused, BACS edge has been tested on them and is working as expected, and they are therefore ready to use, when the issues currently preventing their integration are resolved.

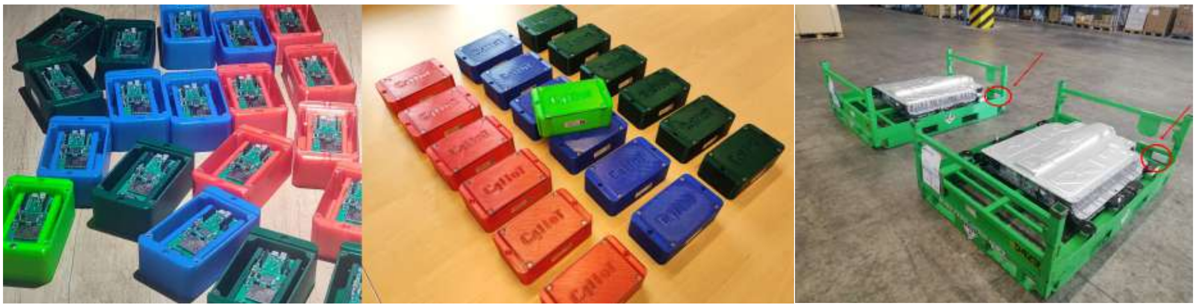
As mentioned at the beginning of this chapter, the Field Gateway modules, have also been relocated to the Cloud. MEDICI, the offloading mechanism, though it retains the same role it had before, choosing between the Field Gateway and Cloud BACS for the datapoints which have been evaluated with low confidence by BACS edge, it is now deployed on the Cloud layer. Although the two different BACS models are no longer on different layers, they are still deployed in different software infrastructure; while the Field Gateway BACS runs on a simple Docker container, the Cloud BACS is deployed behind HPE's Cloud infrastructure as it was planned. Therefore, despite running on the same virtual machine, they are completely separated.

Additionally, the Traffic Analysis module and DISCO (SDN controller) have also been relocated to the Cloud. While these modules have been deployed and tested in the Factory network, due to connectivity issues which currently remain unresolved, they cannot be used from the Cloud layer as it was planned, and for this reason they have been deployed on the Cloud, using a simulated software defined network for demonstration and further testing.

2.2 Logistics4.0 scenario

As already described in D5.2 [1] also, the focus of the tests performed for the Logistics4.0 scenario has been on the shipment of batteries from a supplier in Hungary to the manufacturing plants in Italy. For this reason, 20 edge devices (Figure 5**Error! Reference source not found.**) have been delivered to CRF to be utilized in the logistics use case demo.

Figure 5 - Edge nodes used in the Logistics4.0 scenario



The devices perform measurements by reading the on-board sensors (GPS data, acceleration and magnetic field from the IMU chip, and the temperature), as well as the anomaly detection inference results as calculated on the edge nodes. The data is transmitted to the Field Gateway using NB-IoT connectivity, or GPRS in cases when there is no NB-IoT network available. The format of the binary data which is transmitted in UDP packets is as follows:

```
typedef struct{
    //edge node info
    char IMSI[15];
    uint8_t type;
    //acceleration + magnetic field data
    float ACC_x_RMS;
    float ACC_y_RMS;
    float ACC_z_RMS;
    float ACC_x_MEAN;
    float ACC_y_MEAN;
    float ACC_z_MEAN;
    float MAG_x_RMS;
    float MAG_y_RMS;
    float MAG_z_RMS;
    float MAG_x_MEAN;
    float MAG_y_MEAN;
    float MAG_z_MEAN;
    uint32_t nb_of_samples;
    //GPS data
    float lat;
    float lon;
    float alt;
    float speed;
    uint8_t num_sats;
    //temperature
    float temperature;
    //inference outputs
    float raw_MSE;
    float score;
    uint8_t is_anomaly;
}data_payload;
```

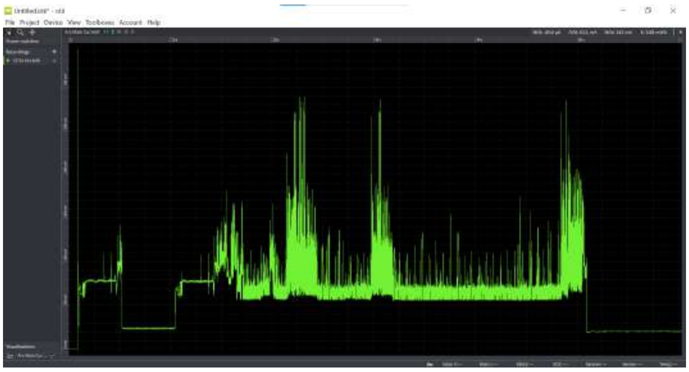
The preliminary tests were performed with a 800 mAh battery, featuring a high sampling rate, with transmission interval set to approximately 1 minute, and no sleeping intervals. This turned out to be a very intensive task, which resulted in the battery lifetime of only 24 hours. Further analysis and optimizations were conducted, resulting in the change of the setup.

In order to preserve the battery, the sampling interval has been prolonged to 1h, with ultra-low power sleep mode (I_{sleep} < 15uA) in between the measurements. The task which is performed once every hour is:

1. Wake up and connect to the network
2. Find GPS fix
3. Read the sensors
4. Send the data packet
5. Set the wakeup alarm clock and go to sleep

To estimate the battery lifetime, the current consumption was measured during a usual measure-and-transmit cycle. Figure 6Figure 6 shows the consumption profile for the "ideal" case, where the node is outdoors and outside of the housing, meaning that nothing obstructs the GPS antenna. Usually, the most time-consuming operation is getting the GPS fix. In a best-case situation such as that depicted in the graph, it takes about 1 minute to complete everything and go to sleep. However, in a less than ideal scenario, this might take a lot longer. To prevent this from going on forever and consequently draining the battery very quickly, we needed to set a timeout period, after which the node gives up trying to read the GPS position and goes back to sleep again. Based on the observations, if it fails to get the position in 5 minutes, it is unlikely that it will succeed at all. So, if we assume that the time when the device is active varies between 1min in best-case scenario and 5min in worst-case scenario, the estimated battery lifetime is between 2 and 4 months, when a large 10000 mAh battery is used. This time duration fulfils CRF's autonomy expectations for the intended use of these devices. In fact, the minimum required from CRF was to have 1 month duration, in order to fulfil the whole shipment of batteries, from the supplier to manufacturing plant and back. However, since the battery duration is higher, it will be possible to expand the utilization of the devices also to other different components' shipment, i.e. to components transported by vessels, that usually can take until 2 months to go and return back.

Figure 6 - Power consumption profile



Field Gateway Receiver modifications

Small changes were also required for the Field Gateway Receiver (FGR) program. Before the final version the FGR program has collected data from the Smart Logistics Edge devices and written it to the MySQL database on the Smart Logistics Field Gateway. For the final deployment version FGR has been modified in the following ways:

1. In addition to writing the data to the MySQL database and local log files, it now writes data also to the Kafka message bus, in the same way as FGR simulator program (from the MVP test bed implementation)
2. Before writing the data to the Kafka message bus, FGR now also contacts IBM's DAC to encrypt the payload of the messages and BCDB to write the data to the Blockchain database so it can be verified later by other components
3. The message format remains the same to preserve compatibility

While testing the new FGR implementation ITML and UNSPMF have verified the correctness of the deployed architecture and proposed security measures.

2.3 Technical evaluation output

In this section, an integration with respect to the contents presented in D5.2 45] is included. In fact, some components were not technically evaluated, or the evaluation was not completed because the tests in the real environment were still running at the moment of writing of the deliverable. So, the final output for these mentioned components is described in the following paragraphs.

2.3.1 Decentralized Access Control (DAC)

IBM's Decentralized Access Control allows to control the access to data by various entities, to enable auditability of various events and policies, and to verify the integrity of data items. The Hyperledger Fabric (HLF) technology of permissioned ledger, and Attribute-Based Encryption (ABE) are two key elements of this decentralized access control (DAC) solution. This solution is part of the architecture of C4IIoT's smart factory use-case.

The DAC was thoroughly presented and demonstrated in past deliverables, including D3.3 (chapter 3), D3.4 (chapter 5.1) and D5.2 (chapter 2.1.1.5).

As of the time of writing this document, the deployment of the DAC on the Smart Factory execution environment is on its last stages. As part of the HLF network, two HLF peer nodes have been deployed on two different machines on the C4IIoT cloud, where each transaction requires endorsement of both, for increased trust. A HLF ordering node and a HLF client have also been deployed on the cloud. This allows to perform a performance assessment of HLF deployed on the final execution environment, whose results appear in the table below.

Table 1- DAC Technical evaluation

Decentralized Access Control (IBM)			
Quality Variable	**Metric**	**Benchmark/Baseline value**	**Result**
Operational Performance	Response time	Response times for operations against the DAC to take, on average, no more than: - Transaction using HLF client: 1.5 seconds. - Query using HLF client: 0.05 seconds.	DAC components were tested and found to fulfil the

			baseline values defined.
	Throughput	Number of requests handled per second for operations against the DAC to be, on average, at least: - Transaction using HLF client: 25 requests per second (RPS). - Query using HLF client: 50 RPS.	DAC components were tested and found to fulfil the baseline values defined.

In addition, ABE keys-issuing authority and ABE client are already deployed on the cloud, serving both the smart factory and logistics use-cases. The ABE components performance assessment was done as part of deploying the logistics use-case on the final execution environment and the results were presented in D5.2 [1] (Table 6).

2.3.2 Hardware Security Modules

IFAG's hardware security modules have been explained in different deliverables as parts of the architecture and as integration with other components (Deliverables D2.3[4], D2.4[5], D3.3[6] and D3.4[7])

IFAG's secure elements are used in C4IIoT for the purpose of protecting edge nodes at the hardware level. In both scenarios, the main operations used in these devices are both key generation and key signing. In the smart factory use case, Infineon OPTIGA^{TM} TPM2.0 has been tested as it is the most important secure element used in combination with blockchain networks, in this case Hyperledger Fabric. During the development of the project, certain libraries have been used and some of them have been modified in order to achieve the integration of the TPM2.0 with Hyperledger Fabric. Once the integration has been successful, different speed tests have been carried out on the device. The following table shows an evaluation of different characteristics of the Infineon OPTIGA^{TM} TMP2.0.

Table 2 - OPTIGA Technical evaluation

OPTIGA^{TM} TPM2.0 (IFAG)			
Quality Variable	**Metric**	**Benchmark/Baseline value**	**Result**
Operational performance	Response time.	Time required to create a key: <1s Time required to sign: <1s	<1s response time observed for create a key: 0.57 s <1s response time observed for sign: 0.6 s

Availability	Resistance to crashes and manipulation	Demonstrate ability to resist crashes when a malicious act occurs in order to break it and gain access to the data contained therein or attempt to tamper with it maliciously	TPM2.0 was designed in order to offer tamper resistance. Keys created and stored inside are not be able to get extracted by an attacker.
Data Security	Privacy and integrity in the data stored	Data stored cannot be modified or readable	TPM2.0 was designed in order to protect all the sensitive data stored inside.

2.3.3 Traffic Analysis (FORTH)

The traffic analysis module runs both in the cloud (see Figure 1) and the edge inside a Raspberry Pi. Its function is to monitor the network flows for threats in encrypted traffic and trigger alerts to the AVT.

Table 3 - Network Traffic Analysis Technical evaluation

Network Traffic Analysis (FORTH)			
Quality Variable	**Metric**	**Benchmark/Baseline value**	**Result**
Operational performance	Response time.	Time required to detect an attack and create an alert	• Maximum time for threat matching: 1 sec • Maximum time for threat detection: 20 sec • Maximum response time: 21 sec
	Data Throughput.	Maximum number of packets processed per second.	Line-rate processing in 100Mbit/s industrial networks
Availability	Uptime.	Calculate uptime percentage in real world environment.	N/A
Data Security	Data flows integrity, confidentiality, and availability.	Detect and report attacks in a real environment.	1. Detection of real attacks using

			pcaps from the IoT23 dataset [1]. 2. Detection of Weak SSL/TLS ciphers and versions. 3. Whitelisting access control using JA3 signatures.
Privacy	Compliance with current security and privacy regulations.	Verify that the module follows all privacy regulations.	The module only uses packet metadata to craft signatures for malicious activities and does not store any other data. Any alert is forwarded to the AVT through an end-to-end encrypted connection.
Accuracy	Measure accuracy rating of attacks detected in network traffic.	Attack detection accuracy in real network traffic.	To test our tool with real attacks in network traffic as described in D3.4 we used the IoT23 dataset[2] which contains malware activity in an IoT setting. For certain malware actions we were able to reach 100% True positive rate with 0% False positive from benign traffic from the same dataset. More details can be found in our paper [3]. We tested the signatures in CRF's premises and

[1] https://www.stratosphereips.org/datasets-iot23

[2] https://www.stratosphereips.org/datasets-iot23

[3] Eva Papadogiannaki, Giorgos Tsirantonakis, Sotiris Ioannidis. Network Intrusion Detection in Encrypted Traffic. In Proceedings of the 4th International Workshop on Secure Smart Societies in Next Generation Networks, 2022

			did not encounter any false positives.

2.3.4 Advanced Visualization Toolkit (AVT)

The AVT has been upgraded during the reported period to include new features provided by C4IIoT components and has been adapted to improve user experience in the already implemented features. The final version of AVT as it was deployed in the production environment has been tested from technical perspective by employing users (threads) accessing various pages on the C4IIoT interface. Table 4 - AVT Technical evaluation presents a compact view of the technical evaluation of the AVT against quality variables.

Table 4 - AVT Technical evaluation

Advanced Visualisation Toolkit (AEGIS)			
Quality Variable	**Metric**	**Benchmark/Baseline value**	**Result**
Operational performance	Response time.	7-10 sec	Initial Page Loading: 8,63 s (average). Internal Pages Loading: <1s
Availability	Uptime.	>95% of the time.	No downtime was experienced during the operation of the platform. Platform was only not available during planned maintenance and version updating
Reliability	Fault Tolerance.	Interface responsive in case of data errors. Informative messages to users.	Messages and alerts inform the user for errors.

Several performance tests have been executed for both single (one page) or combined actions (sequence of navigation). Table 5 presents the results of ten different users accessing the real-time monitoring page.

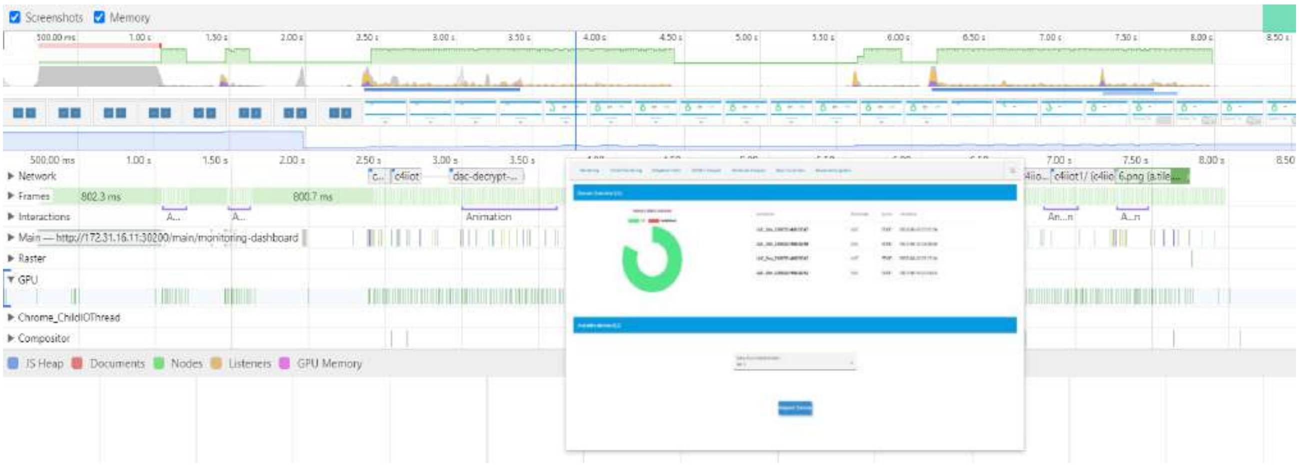
Table 5 - Monitoring Dashboard Test

#	Thread Name	Label	Sample Time (ms)	Status	Bytes	Latency
1	TG 1-1	HTTP Request	307	Success	7875	307
2	TG 1-2	HTTP Request	119	Success	7875	117
3	TG 1-3	HTTP Request	95	Success	7875	91

4	TG 1-4	HTTP Request	97	Success	7875	97
5	TG 1-5	HTTP Request	96	Success	7875	94
6	TG 1-2	HTTP Request	94	Success	7875	92
7	TG 1-3	HTTP Request	95	Success	7875	93
8	TG 1-4	HTTP Request	96	Success	7875	91
9	TG 1-5	HTTP Request	97	Success	7875	96
10	TG 1-2	HTTP Request	96	Success	7875	94

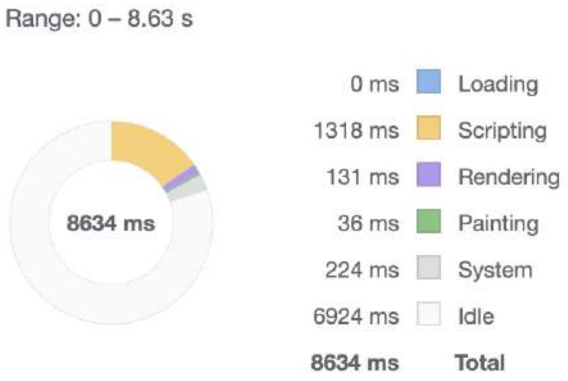
Figure 7 presents the timeline viewer on Chrome developer tools for a user that performs a common action on the dashboard for the Logistics use case. The user selects the Logistics Monitoring tab, has an overview of the system and selects a specific device to view more details on it.

Figure 7 - Timeline viewer



Finally, Figure 8 shows the CPU activity breakdown for the same action.

Figure 8 - CPU activity breakdown



Range: 0 – 8.63 s

0 ms	🟦	Loading
1318 ms	🟨	Scripting
131 ms	🟪	Rendering
36 ms	🟩	Painting
224 ms	⬜	System
6924 ms	□	Idle
8634 ms		**Total**

2.3.5 CARMAS (UP1PS)

CARMAS's purpose within the C4IIoT architecture is the analysis of a set of attack actions suspected to be occurring in the factory network as an HTTP request coming from the AVT. It constructs an HTTP response containing a set of network reconfiguration mitigation actions that best mitigate these attack actions given some optimization criteria and as a function of the characteristics of the attack action set. Interoperation with other C4IIoT tool is ensured through a OpenAPI specification that clearly delimits the form and content of both its inputs and outputs.

Internally, its services are declaratively implemented by composing objects that encapsulate automated reasoning rules. It is deployed as Docker image that stacks the CARMAS objects on top of the Logtalk object-oriented logic programming interpreter, the SWI-HTTP service-oriented logic programming library and the CLP(FD) constraint logic programming library. All three are in turn stacked on top of the SWI-Prolog logic programming inference engine itself stacked on top of Linux.

CARMAS has gone through several rounds of testing, all at different levels of abstraction and integration with the rest of the framework. As work has continued and updates have been made to the tool, an initial low-level testing strategy has first been employed. This strategy consists of performing unit tests on the individual components of the application following a completely white-box approach. The next set of tests performed concerned the behavior of the application, as one complete unit, retaining the white-box view, to ensure non-regression of application behavior as new elements are added. This was achieved using semi-automated test case generation based on the underlying ontology of the application. Once done, a black-box level testing strategy leveraging the Open API specification together with the REST web service testing automation tool Insomnia was performed to ensure that the outward-facing interface of the tool was conformant to the specifications.

Once all these tests were passed and the application was determined to be stable, it was packaged as a Docker image, as mentioned above, and sent over to project partners responsible for integration testing. The tool was subsequently evaluated in conjunction with the rest of the framework. Having successfully been integrated as part of C4IIoT's technology stack, the tool has then been used for evaluating the final prototype as part of the consolidated and integrated framework. In addition, the following table states the results of the technical evaluation with respect to the previous deliverables.

Table 6 - CARMAS Technical evaluation

CARMAS (UP1PS)			
Quality Variable	**Metric**	**Benchmark/Baseline value**	**Result**
Operational performance	Response time.	Time required to detect an attack and create an alert (<3 seconds at previous evaluation)	<1s response time observed for test requests from AVT.
Availability	Resistance to crashes	Demonstrate ability to resist crashes when faced with unexpected inputs or internal errors (new benchmark)	CARMAS has been designed such that each request is handled in its own isolated thread where any failure leads simply to a graceful stop, reporting an error code as HTTP response but avoiding stopping the server
Privacy	Compliance with current security and privacy regulations.	Verify that the module follows all privacy regulations. (new benchmark)	CARMAS treats only information related to network attacks and does not persist this data in any way that would allow a malicious agent to gain access to this information. Hence data privacy is respected.
Reliability	Proportion of sub-space of attack plan diversity conforming to input Open API schema for which non caught errors occur.	Cover the entirety of the OpenAPI specified inputs with no errors.	Final OpenAPI schema fully covered in the implementation.
Accuracy	Proportion of sub-space of attack plan diversity conforming to input Open API schema for which CARMAS can propose valid mitigation plans.	Be capable of proposing mitigations for the entirety of the OpenAPI specified inputs.	Final OpenAPI schema fully covered in the implementation.

2.3.6 MEDICI (UOG)

The purpose of UOG's Multi-critEria DecIsion support meChanism for IoT offloading (MEDICI) is to provide security-aware dynamic offloading of anomaly detection tasks for UNSPMF's BACS component within the C4IIoT environment. More specifically, MEDICI is to be deployed at the Field Gateway (FG) layer and received anomaly detection tasks from BACS edge modules with low confidence. Upon receiving these requests, MEDICI will dynamically decide whether an intermediate complexity BACS model located at the FG layer, or an advanced complexity BACS model located at the Cloud layer (see Section 5 in D3.3[6] for further details) should be triggered. Moreover, MEDICIs experimental procedure for the smart factory and logistics use case are detailed in Section 2 in D5.2[1].

In the below table we provide results compared to the Hierarchical Anomaly Detection (HAD).

Table 7 - MEDICI Technical evaluation

MEDICI (UOG)			
Quality Variable	**Metric**	**Benchmark/Baseline Value**	**Result**
Operational Performance	Detection Time Average amount of time for anomaly detection task to be offloaded and investigated by anomaly detection models.	Average detection time with all anomaly detection tasks offloaded and investigated by cloud anomaly detection model: 1.37 seconds	With MEDICI making active offloading decisions: 1.13 seconds
	Accuracy Average F1 score (accuracy measurement) for anomaly detection tasks being successfully identified	Average F1 score with all anomaly detection tasks offloaded and investigated by FG anomaly detection model: 0.863	With MEDICI making active offloading decisions: 0.924

3 Evaluation and Impact analysis

3.1 KPIs monitoring

3.1.1 Overall KPIs report

This section includes the overall KPIs report, describing the information about the achievements related to the set of KPIs that were defined within D5.1 [2].

[KPI-1.1] Successful integration and orchestration of C4IIoT security-enabled layers.

ITML ensured the successful integration of the C4IIoT technologies and relevant security enabled layers, based on an agile approach. It continuously validates and tests the integrated framework collecting feedback from both the technology providers and the end users. The functionality of the integrated framework is verified by the C4IIoT pilots.

[KPI-1.2] 20% improved resilience for an end-to-end Industrial IoT system.

IFAG provides hardware secure elements to the IoT edge nodes in order to improve the resilience of the system. The secure elements are integrated in upper security layers in the C4IIoT framework. The integration with blockchain network also improves the resilience. Building on the IoT nodes that CRF provided, resilience has been increased by more than 20 percent with the incorporation of the technologies mentioned above.

[KPI-1.3] 80% reported cybersecurity incident investigations resolved within an organizationally defined timeframe.

According to the type of incidents and related risks, different timeframes have been considered as acceptable. However, C4IIoT has been able to report all the cybersecurity incidents occurred in the accepted timeframe.

[KPI-1.4] Reduction of detection time by at least 10%.

The C4IIoT framework provides several components that are capable of reducing the time required to detect a malicious event or attack. First, the Traffic Analysis module provides a lightweight, yet efficient way to match malicious signatures on network traffic, which can run on the Field Gateway or even on the edge devices. Second, the MEDICI tool is also deployed at the Field Gateway layer and receives anomaly detection tasks from BACS edge modules with low confidence. Upon receiving these requests, MEDICI can dynamically decide whether an intermediate complexity BACS model located at the FG layer, or an advanced complexity BACS model located at the Cloud layer should be triggered.

These mechanisms are pushing detection functionalities closer to the edge, hence eliminating extra movements or communications.

While all BACS models have similar inference time, we emphasize high Edge model performance and local execution paradigm which ensures zero network latency. BACS supports both embedded Edge models and Python based models with performance results (e.g. F1 scores) reported in the paper on the C4IIoT architecture submitted to IEEE Access and in the EUSIPCO 2022 conference paper "BACS: A comprehensive tool for deep learning-based anomaly detection in edge-fog-cloud systems"

[KPI-1.5] Increased accuracy of security monitoring by 35%.

C4IIoT accuracy of the security monitoring is achieved through a few components namely the anomaly detection system, the scanning of container images and the security logs as listed here after.

BACS is mostly dealing with unsupervised anomaly detection as labeled data is difficult to obtain for C4IIoT specific use cases. Since the beginning of the project we added multiple levels of model verification and validation to check if our models perform well on unlabeled data sources found in this project. We added validation with synthetic data (synthetically injected anomalies in real data) and also configurable model thresholds (based on Machine Learning model loss distributions). Another improvement is the addition of various complex Deep Neural Network architectures (such as recurrent gated models, variational autoencoders and so on) which should ensure good real-world performance.

In our tests these new, tuned models see anywhere from 10 to 50% increase in performance (measured through F1-scores with synthetic test data) compared to our baseline autoencoder models, which were developed for the initial stages of the project.

Trivy vulnerability scanning of container images stored on Harbor has been used to assess the vulnerability status of C4IIoT component images, spotting out the security related actions to be performed to cleanup C4IIoT components. After the cleanup actions, new container images have been created and stored to Harbor (and used by the trial): next Trivy scans showed 84% decrease of total number of found vulnerabilities, and specifically 91% for Critical ones.

The EJBCA and in general the PKI systems have these following types of logs:

- Security Audit Log: Used for PKI auditors to audit important security PKI events that the system performs.
- System Log: Used to monitor daily operations in the system, debug and track down errors etc.
- Transaction Log: Used for accounting of specific functions, mainly validation (OCSP).

The Security Audit log, logs important events such as "Certificate issued", "Certificate Profile edited", "Administrator accessed resource". One of the most important aspects to consider is that the Security Audit log does not log things that do not happen. The Security Audit Log is stored in the database and the System Log is stored in log files. The nfo/debug output sent to external logsystem, there is no protection from alteration and events sent to this device cannot be fetched back to EJBCA for display in the Admin GUI.

[KPI-1.6] Protect an IIoT real-life environment from at least (10) types of related threats and attacks.

As described in deliverable D5.2[1], the following threats are provided with a protective and/or reactive mitigation by the C4IIoT components:

- Denial of Service (SAM, BINSEC DISCO).
- Malware (SAM, TEE, SEEN, BINSEC, DISCO, TAM).
- Manipulation of hardware & software (SAM, TEE, SEEN, BINSEC).
- Manipulation of Information (SAM, DAC, DFB, TEE, SEEN, BACS).
- Targeted attacks (SAM, BINSEC, DISCO, BACS).
- Abuse of personal data (SAM, DAC, TEE).
- Brute force (SAM, SEEN, DISCO, TAM).
- Man-in-the-Middle attack / Session hijacking (SAM, DAC, SEEN, DISCO, TAM, BACS).
- IoT communication protocol hijacking (SAM, DAC, SEEN, DISCO).
- Network reconnaissance (SAM, DISCO, TAM).
- Vandalism and theft (SEEN, DISCO).

- Sabotage (SEEN).
- Unintentional change of data or configuration in the OT system (DISCO).
- Erroneous use or administration of devices and systems (DISCO).
- Damage caused by a third party (DISCO).
- Failure or malfunction of a sensor / actuator (DISCO, BACS).
- Failure or malfunction of a control system (PLC, RTU, DCS) (DISCO, BACS).
- Software vulnerabilities exploitation (SAM, BINSEC).
- Failure or disruption of service providers (DISCO).
- Communication network outage (DISCO).
- Violation of rules and regulations / Breach of legislation / Abuse of personal data (SAM, DAC).
- Failure to meet contractual requirements (SAM).

[KPI-2.1] More than (20) novel services and tools utilized and integrated from diverse multi-domain technological areas.

Several novel services have been added and listed here:

1. Harbor Docker Private registry – it hosts container images for C4IIoT components
2. Trivy vulnerability scanning (integrated with Harbor) – automatic vulnerability scan enabled on Harbor for all stored images
3. Microk8s single node Kubernetes cluster – cloud layer engine hosting and protecting all C4IIoT cloaud layer components – it includes Cloud Gateway
4. OWASP Modsecurity - Web Application Firewall integrated into Cloud Gateway
5. EJBCA PKI/CA – which enrolls and manages all certificates for the identities of components and actors inside C4IIoT project
6. NB-IoT a novel protocol for communication between IoT devices and mobile network operator
7. Facebook Prophet - a procedure for forecasting time series data based on an additive model – used for anomaly detection within BACS.
8. The OpenABE library
9. Hyperledger Fabric
10. Blockchain Database
11. Traffic Analysis tool
12. Data fusion bus (DFB) - it is based on Apache Kafka and Elasticsearch, enhanced with custom Spring Boot applications (DFB admin and Storage Connector). Kafka is an open-source tool, often used with Elasticsearch which is also open source.

[KPI-2.2] Innovative ML/DL models deployed at the edge and a security-aware offloading mechanism for almost real-time critical security decisions.

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. Security aware offloading mechanism has been integrated with ML/DL components.

[KPI-2.3] Test edge computing framework in terms of speed and quality.

The components placed in the edge node have been tested in terms of speed and quality. The main reasons for these tests have been done to avoid bottlenecks. The operations performed by the secure elements located on the edge nodes have also been tested to prevent physical attacks and timing attacks.

BACS Edge models achieve low inference times (~100 ms on average, depends on the model) and small memory footprint (<500MB) making them suitable for various Edge applications. We also support custom architectures such as embedded and ARM64. The quality of the models is also high which is reflected by high accuracy and F1-scores as reported in the C4IIoT architecture submitted to IEEE Access and in the EUSIPCO 2022 conference paper "BACS: A comprehensive tool for deep learning-based anomaly detection in edge-fog-cloud systems".

[KPI-2.4] Accuracy of encrypted flows classification over the Internet more than 90%.

The Traffic Analysis, according to FORTH's measurement, is able to detect malicious actions inside encrypted traffic with more than 90% accuracy.

[KPI-2.5] At least (6) services for secure communications, access control management and authentication.

The C4IIoT framework includes the following services for secure communications, access control management and authentication:

- Attribute-based encryption mechanism.
- Decentralized access control logging with Blockchain.
- Identity management with EJBCA Public key infrastructure (PKI). The technology for identity management in IoT, including certificates for the identities of components and actors in C4IIoT, allows data integrity, authentication and encryption.
- The Cloud Gateway HTTPS encryption. Cloud Gateway, configured as HTTPS ingress for Microk8s single node Kubernetes cluster – protecting all C4IIoT cloud layer components by providing secure HTTPS access to cloud layer services. The HTTPS encryption is enforced by X509 certificate enrolled by EJBCA (PKI system for C4IIoT).
- The cloud layer firewall: OWASP ModSecurity - Web Application Firewall integrated into Cloud Gateway.
- Encryption and read/write permissions with Data Fusion Bus. Data fusion bus (DFB) offers a secure and resilient way for transferring data with the use of the underlying Kafka. The communication with the topics is handled using certificates issued by the private Certificate Authority of C4IIoT being encrypted. Additionally, access (read and write) is restricted per topic, and therefore each certificate has access to the topics each module requires.

[KPI-2.6] Upgrade ML/DL models to be realized in an automotive IIoT environment.

During the project, within the BACS framework, UNSPMF developed a unified architecture for creating and using various Machine Learning and Deep Learning models. These models include neural network models, autoencoders, recurrent neural networks, support vector machines and other models. UNSPMF also includes differentially private methods. All the models can be easily swapped and used in an automotive IIoT scenarios where sensory data is available: in our case both for the smart factory use case and the smart logistics use case. BACS framework is also designed with portability in mind, it works on x86 and ARM platforms, and it also provides support for custom hardware (embedded microcontrollers).

[KPI-3.1] More than 10 system vulnerabilities exploited by the system and threat actors.

STS's Security Assurance Module (SAM) was able to identify more than 100 prominent system vulnerabilities affecting the subcomponents of the second release (R2) of the C4IIoT platform. The known and exploitable vulnerabilities can be detected by SAM's Vulnerability Analyzer and Dynamic Tester.

[KPI-3.2] 20% of system vulnerabilities for which patches (including firmware patches) have been applied or that have been otherwise mitigated.

Trivy vulnerability scanning of container images stored on Harbor has been used to assess the vulnerability status of C4IIoT component images, spotting out the security related actions to be performed to cleanup C4IIoT components. After the cleanup actions, new container images have been create and stored to Harbor (and used by the trial): next Trivy scans showed 84% decrease of total number of found vulnerabilities, and specifically 91% for Critical ones.

By analyzing the subcomponents of the second release (R2) of the C4IIoT platform using STS's SAM we were able to identify the vulnerable software components, their installed version, and their known vulnerabilities. After performing the available security patches and updates we re-analyzed all the subcomponents and confirmed that at least 30% of the identified vulnerabilities were successfully mitigated.

CEA's UAFuzz analysis, based on the platform BINSEC and part of the C4IIoT mitigation engine, has been used to detect vulnerabilities on C4IIoT components and notably BACS. The tool has been used to find several memory corruptions that could make the program crash. A second version of BACS was provided, and another error (a NULL pointer dereference) was found in this new version. After this second version has also been patched, we launched an extended test campaign and did not discover any more mistakes. Thus, 100% of system vulnerabilities found using BINSEC have been patched.

[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.

By manually testing and analyzing SAM's EVEREST monitoring accuracy using 20 Monitoring Rules STS has been able to confirm a 100% activation accuracy.

Moreover, UNSPMF applied the BACS tool to improve behavior detection, where BACS has been utilized to detect anomalies with the CRF logistic and smart factory data, reaching detection accuracy and F1 scores upwards of 90% depending on the machine learning model used.

UNSPMF provides extensive results for the BACS anomaly detection component in the paper on the C4IIoT architecture submitted to IEEE Access and in the EUSIPCO 2022 conference paper "BACS: A comprehensive tool for deep learning-based anomaly detection in edge-fog-cloud systems". Here, UNSPMF reports high measured performance (accuracy, f1-scores) for majority of the models available in BACS for both use cases.

[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 C4IIoT framework includes the following safety mechanisms for privacy, accountability and trustworthiness:

- SEEN.
- Attribute-based encryption.
- Blockchain solutions.
- Traffic analysis.
- DFB.
- Harbor. Trivy vulnerability scanning integrated with Harbor – automatic vulnerability scan enabled on Harbor for all stored docker images.
- SAM.
- Risk Assessment. The risk assessment is a process to identify potential threats by analysing what would happen if a hazard occurred. In C4IIoT we analysed the RISKs in the current industrial environment where C4IIoT live, introducing the solution in the industrial model.

- SGX execution in the cloud.
- Attribute-based encryption and the DFB has privacy-preserving features.

[KPI-3.5] Enforce automated monitoring, mitigation and visualization for more than (4) threats in IIoT.

This KPI has been achieved, since C4IIoT is able to monitor, mitigate and visualize the following threats:

- Denial of service
- Malware
- Manipulation of information
- Targeted attacks
- Brute force attacks
- Eavesdropping
- IoT communication protocol high jacking
- Network reconnaissance
- Validation and theft
- Software vulnerability exploitation

UP1PS has monitored this KPI though frequent correspondence with project partners.

[KPI-3.6] Built on top of (10) existing cybersecurity products and services and customize them to be applied in IIoT.

The C4IIoT framework is built on top of the following existing cybersecurity products and services:

- The OpenABE library.
- Hyperledger Fabric.
- Blockchain Database.
- The Open Vulnerability Database.
- The MITRE ATT&CK.
- The OpenVAS.
- Cisco's JOY.
- JA3 fingerprinting method.
- SCONE.
- python3-pcapy.
- python3-kafka.
- Dpkt.
- pyja3.
- Pyshark.

[KPI-3.7] Significant hidden information revealed (number of concrete warnings and conclusions) based on systems analysis.

The BINSEC tool, developed by CEA, is able to reveal hidden vulnerabilities and bugs in executable files and produce warnings for the BACS tool.
In addition, the TRIVY tool, integrated in Harbor and utilized in C4IIoT as part of HPE's solution, is able to detect vulnerabilities in docker images. It was successfully used in C4IIoT to detect and significantly reduce the number of vulnerabilities in some of C4IIoT's components in their early versions.

[KPI-4.1] Successful collection of data for demonstrating cybersecurity monitoring and anomaly detection from multiple diverse and heterogeneous IIoT systems.

Three types of datasets have been collected. The first type is industrial real datasets provided by CRF. The second type of datasets are those acquired from edge node devices – microcontrollers used and developed within the project. The third type is synthetic datasets created for both use cases.
CRF has also provided labels for one of the real-world datasets. This labelled dataset was particularly valuable for training and validation purposes.

[KPI-4.2] Delivery of 3 integrated versions of the C4IIoT framework.

ITML integrated 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 and the integration of few modules. A version which encompassed all software modules, using simulators for the production of data at the edge on the test environment, was delivered at M18. Finally, ITML delivered on M30 the final integrated version with the deployment and execution of real-life industrial and logistics demonstrators. This version also included the analysis of technical and implementation requirements of all modules as well as the deployment and management of necessary resources for the implementation requirements. However, due to restrictions related among others to Covid-19 in the CRF factory, adjustments have been made up to M36 in order to facilitate the validation of the C4IIoT platform.

[KPI-4.3] Execution of (2) demonstrators in automotive manufacturing industry, together validating at least 95% of tools.

Two demonstrators have been executed, one is the Smart Factory, developed in the CRF Campus Melfi, and the other is the Logistics4.0, deployed on the shipments of components from and to the Mirafiori plant (Turin). All the C4IIoT architecture tools have been validated.

[KPI-4.4] More than (10) field trials to demonstrate C4IIOT tools' applicability and performance within an automotive real-world environment.

Logistics devices were installed in Italy and the data is still being collected. Containers travel towards Hungary and then come back to Italy, so the whole route is being monitored, thanks to 20 devices installed in total.
Moreover, in the Smart Factory, tests on different datasets, coming from different AGVs, have been performed.
In total, more than 10 trials have been executed for testing the C4IIoT applicability and performance.

[KPI-4.5] Construction of an informative mechanism for both security and non-security experts.

AEGIS built an interactive informative mechanism in the context of Advanced Visualization Toolkit module that provides real-time monitoring of the system and alerting mechanisms that provide even to non-experts the ability to be aware about the situation of the system. In addition, experts may apply mitigation actions in detected security attacks while they have the option to look into past data using the time line analysis and reveal hidden relations between detected incidents.

[KPI-5.1] All C4IIoT security solutions, products and services aligned and harmonized with regulations and EU standards.

Security solutions produced during the C4IIoT lifetime have been aligned with considering the recent regulations and EU standards. We provide recent guidelines provided by the ENISA for securing the Internet of Things. Furthermore, we identified in D6.5 the standardization plan for the major security modules provided by the consortium.

[KPI-5.2] Define a concrete dissemination strategy to raise awareness [dKPIs]. Uptake more than (6) standards from several IIoT related technologies.

We have targeted the six following standards for several IIoT related technologies that are: ISA, ENISA the pillars of IIoT guidelines, CSA, TCG, GSMA and OASIS.

[KPI-5.3] More than (20) entities (e.g. academics and enterprises) to use C4IIoT offerings.

AEGIS has allowed two entities to utilize the C4IIoT offering: Power Evolution srl, in the context of Probotain project they have participated along with UNSPMF, and Qtechnik (a Greek SME which is AEGIS customer). In fact, in Probotain, a sub-project of the H2020 project Market 4.0, the UNSPMF's BACS tool has been used by Power Evolution Srl, a robotics industry SME, in the context of the Probotain solution for predictive maintenance of robotic parts.

In CRF, about 10 SMEs visiting the Campus Melfi had the possibility to have a demonstration of the C4IIoT components installed there and see how they are utilized in both the Smart Factory and the Logistics4.0 scenarios.

[KPI-6.1] Ready to market integrated solution for the overall IIoT system and independent security solutions (TRL 6).

The C4IIoT solution has been demonstrated in two real-world industrial scenarios: the Smart Factory deployment in Campus Melfi, and the Logistics4.0 deployment in the CRF Inbound Logistics. Then, the final solution has TRL 6.

[KPI-6.2] At least (4) C4IIoT tools reach market readiness level (8) at the end of the project.

The final TRLs of the C4IIoT tools are reported in D4.4[8]. there are 3 tools that reach TRL 8-9 and 3 tools that reach TRL 7.

[KPI-6.3] At least 6 third-party collaborations to be established for further applicability verification.

Six collaborations with other H2020 projects: CARAMEL, CyberSANE, GUARD, SOCCRATES, SAPPAN, COLLABS. This has been done both through direct engagement for joint standardization activities and though joint workshop participation. In addition, representatives from CyberSANE and COLLABS have been invited to present their approaches during the first C4IIoT Winter School. UP1PS monitored this KPI through regular correspondence with project partners.

[KPI-6.4] More than (10) critical aspects (e.g. maintenance and software updates) will addressed to ensure long-term sustainability of the solution.

D4.4[8] describes the challenges faced and the actions taken.
By closely monitoring and reviewing the work of Task 4.4 we confirm that more than 10 critical aspects of the long-term operation and maintenance of the final C4IIoT solution are addressed. These critical aspects are reported in Deliverable D4.4 [8] with a dedicated section and are the following: (1) SOI platform design, (2) virtualized/containerized components, (3) 3-layer platform design, (4) OSS development, (5) EAB assistance, (6) feedback via Info Days, alignment with (7) ENISA Good Practices for Security of Internet of Things in the context of Smart Manufacturing, (8) NIS Directive, and (9) ECSO's ECSO's cyber security related

challenges addressing the ICS and industry 4.0 sector. Furthermore, using STS's SAM, (10) outdated/vulnerable components can be identified so that security updates can be performed accordingly. Finally, SAM can also (11) identify new or altered components, providing information about their security status.

[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.

Followed discussions about the business plan have been held throughout the project, and the initial draft of the overall C4IIoT business plan has been written.

[Impact KPI (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.

D5.2 [1] lists all the threats that are covered by C4IIoT framework, namely Denial of Service, Malware, Manipulation of hardware and software, Manipulation of Information, Targeted attacks, Abuse of personal data, Brute force, Man in the middle attack/Session hijacking, IoT Communication Protocol hijacking, Network reconnaissance, Vandalism and theft, Sabotage, Unintentional change of data or configuration in hte IoT system, Erroneous use or administration of devices and systems, Damage caused by a third party, Failure or malfunction of a control system, Software vulnerabilities exploitation, Failure or disruption of service providers, Violation of rules and regulations, Failure to meet contractual requirements, for a total of 20 threats, fulfilling 133% of the goal.

[iKPI#1.2] At least 5 new types of advanced cybersecurity threats identified and mitigated by the C4IIoT framework in the C4IIoT pilots.

Attack Vectors:

- Malware
- Account Hijacking
- Unknown Host
- Targeted Attack
- Vulnerabilities
- Defacement
- Malicious Script Injection
- SQL Injection
- DDoS
- Misconfiguration
- Romance Scams
- Spam
- SS7 Attack

Motivation Behind Attacks:

- Cyber Crime
- Cyber Warfare
- Hacktivism
- Cyber Espionage

[iKPI#2.1] 3 tools and services for complex distributed systems handling IIoT cyber-attack incidents.

C4IIoT has produced 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 able to operate in complex distributed environments.

[iKPI#2.2] 3 cyber threats with multiple levels of risk avoided due to E2C architecture.

This KPI has been achieved and the three levels considered are the following:

- Edge node
- Field Gateway
- Cloud

[iKPI#2.3] 4 cyber threats with multiple levels of risk avoided due to secure execution environment.

Cyber threats with multiple levels of risk have been carried out in the CRF premises; different task have been carried out in which the system has been put to the test by performing different attacks on the different components of the system.

[iKPI#3.1] 3 ENISA representatives to be contacted during the project.

Several C4IIoT partners participated in ENISA's Cybersecurity Standardization Conference 2021.

[iKPI#4.1] 2 complementary fields of demonstration.

ITML ensured that the integrated C4IIoT solution has been demonstrated in two complementary fields (namely, Logistics 4.0 and Smart factory); the integrated solution has been customized based on the specific needs of each field, and has been validated by the end user (CRF) of the project.

[iKPI#4.2] At least 6 stakeholders engaged by the end of the project to further adopt C4IIoT cybersecurity framework.

We have targeted mainly the following ones that are: ISA, ENISA the pillars of IIoT guidelines, CSA, TCG, GSMA and OASIS.

[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[4] and Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity[5] innovative and disruptive technologies for cyber-security include Artificial Intelligence, Machine and Deep Learning, Big Data security analytics, Hardware cybersecure engineering and assurance cryptography, blockchain and distributed ledger, IIoT security 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[6], 2020[7] and 2021[8]) innovative technologies included: embedded AI, Adaptive ML, Self-supervised learning, Deep Learning, Low-Cost Single-Board Computers at the Edge, Edge Analytics and Edge AI.

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

[5] https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf

[6] https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019

[7] https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020

[8] https://www.gartner.com/en/articles/the-4-trends-that-prevail-on-the-gartner-hype-cycle-for-ai-2021

C4IIoT architecture is aligned with at least 5 of the technologies identified by Gartner and ECSO above through (i) UNSPMF's BACS anomaly detection (Deep Learning), (ii) IBM's decentralized access control with attribute-based encryption (Blockchain), (iii) CEA's BINSEC verification (security by design at the hardware level), (iv) IFAG's secure execution (security by design using encryption) and (v) UP1PS's CARMAS mitigation (Response and Recovery tools combining automation with human expertise). Several tools have been advanced, 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.

In the CRF Logistics4.0 pilot, before C4IIoT, no other systems allowing a secure data flow from the edge to the company's system were utilized. So, considering the overall industrial infrastructure, whose logistics edge devices are a relevant part and whose resilience is now granted by the usage of C4IIoT, we can state that we have about 30% enhancement.
Moreover, thanks to the reduction of the costs for the management of unexpected events, it has been possible to quantify a 15% reduction of costs due to components stock-out.

[iKPI#5.3] At least 3 industries engaged within C4IIoT duration to exploit innovative technologies

In the context of the project Probotain - a subproject of the H2020 project Market 4.0 - an innovative solution for predictive maintenance of robotic parts has been developed, where the Probotain partner, Power Evolution Srl (a SME in robotics industry), has in this sense exploited the BACS anomaly detection component for a predictive maintenance robotics solution.

While this may not correspond to commercial exploitation, it corresponds to exploitation of the UNSPMF's BACS tool by an external industry company outside of the C4IIoT consortium, carried out in the context of another project.

UP1PS has monitored this KPI through regular correspondence with project partners.

[iKPI#6.1] At least 3 innovative products and services of the C4IIoT pilot partner directly enhanced by the cybersecurity framework.

Edge devices both in the factory and in the Inbound Logistics have been enhanced by the C4IIoT solution. Moreover, also the field gateway machine and the cloud involved in the overall data flow have been impacted. So, the C4IIoT solution affects the entire Manufacturing and Supply Chain processes in the company and all the related products and services.

[iKPI#7.1] At least 3 industrial companies boosted exploiting C4IIoT cybersecurity capabilities.

IFAG has been disseminating the technologies used in C4IIoT to several companies. The use of hardware security modules have been promoted in different companies such as Mixed Mode, Xilinx and Utimaco. During the project, the lections learned have been applied in the products and demos developed in combination with other companies as IBM and Eesy-Innovation GmbH.

Moreover, CRF has involved both the Stellantis company but also one service provider and one components' provider in the utilization of the C4IIoT solution. This companies have enhanced their logistics and manufacturing processes thanks to the utilization of the project tools.

[iKPI#8.1] At least 3 SMEs providing security-related services within project's duration.

STS is offering the Security Assurance Module (SAM), further expanded in capabilities during the course of the project, which is responsible for the security and privacy assessment of the C4IIoT platform. Also, STS was designed and implemented the Attack Information Enhancement Middleware (AIEM) which interconnects the Traffic Analysis Tool, developed by FORTH, and the Advanced Visualization Toolkit (AVT), provided by AEGIS, and enhances the identified attack information with mitigation actions.

ITML in the context of C4IIoT is offering Data Fusion Bus (DFB) as its innovative part for the privacy aware, trustworthy data and analytics. As part of its service portfolio, ITML has already developed B2B partnerships related to security offerings with Greek enterprises. It has also participated further in other research projects to build upon the output of C4IIoT.

AEGIS has designed and implemented the AEGIS Advanced Visualization Toolkit that is an extensible software with a wide application scope, ranging from Digital Forensic Analysis to Big Data analytics. The AVT has enriched in the context of C4IIoT and is a market ready product.

[iKPI#8.2] At least 10% increase of market share for SMEs exploiting C4IIoT technologies.

During the project, STS was able to expand the capabilities of its Security Assurance Module (SAM) in order to cover the needs of the IIoT field. This development is expected to increase its market share, allowing STS to offer services tailored to the IIoT domain.

ITML's tool is expected to be launched to the market in the next 3-5 years after the end of the project with its analytics features by enriching the tool with further developments applicable to the industry 4.0 customers by confirming a relative market share. It has also participated further in other research projects to build upon the output of C4IIoT.

AEGIS has designed and implemented the AEGIS Advanced Visualization Toolkit that is an extensible software that provides Digital Forensic Analysis and has been enriched in the context of C4IIoT. The product is offered in the market but is early to quantify the impact in our market share.

[iKPI#9.1] At least 20% Increase in productivity verified on at least one (1) pilot

In the Logistics4.0 scenario it has already been possible to estimate the achievement of the 20% productivity increase, thanks to the monitoring of events happening in the Inbound Logistics of components. Moreover, the solution implemented is a starting point for further applications to other logistics processes related to other components' shipment. At industry level, it will be possible to strength the knowledge about the processes and better manage cybersecurity issues in logistics.

[iKPI#9.2] At least 15% Increase in market share for the pilot partner exploiting C4IIoT framework.

The logics behind the choice of this indicator was that, thanks to the evaluation of the iKPI#9.1, it would have been possible to quantify high level KPIs also. By the way, many other parameters should be taken into account and, because of how the demonstration scenarios were defined during the project, they are related to different plants/processes involved in the experimentation.

In fact, several plants were considered during the project, Melfi Campus for the Smart Factory and two Italian plants for the Logistics4.0.
Moreover, in 2021 and also 2020, due to the COVID-19 health crisis, many plants were closed or were working at reduced capacity.
However, from the iKPI#9.1 achievement, we are able to ensure that also the current KPI has been positively impacted by the implementation of the C4IIoT solution. Nonetheless, due to the reasons listed above, it was not possible to quantify this KPI exactly, at the end of the project.

[iKPI#9.3] At least 10% Increase in sales for the pilot partner exploiting C4IIoT framework.

Same as the iKPI#9.2 above.

[Dissemination KPI (dKPI)#1] At least 1000 Web access to deliverables, technical results and presentation material of C4IIoT and at least 100 downloads.

C4IIoT website has 13103 unique visitors and 1305 downloads.

[dKPI#2] At least 50 push announcements through social media (Twitter, LinkedIn, ResearchGate)

548 push announcements (76 LinkedIn, 367 Twitter, 95 Facebook).

[dKPI#3] At least 9 newsletters with C4IIoT technical activities

11 Newsletters have been sent informing about C4IIoT findings and achievements.

[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

1480 Downloads of C4IIoT while no hard copies have been distributed due to absence of physical events because of the COVID-19 restrictions.

[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

3055 video views

[dKPI#6] At least 10 Publications in International referred technical journals in cybersecurity related subjects

10 Publications in international referred technical journals and magazines.

[dKPI#7] At least 10 Publications in International magazines in cybersecurity related subjects

10 Publications in international referred technical journals and magazines.

[dKPI#8] At least 12 Publications in International referred technical conferences in cybersecurity related subjects

10 Publications in international referred technical conferences.

[dKPI#9] Publications of special issues in International referred technical journals and magazines (≥ 2, ≥ 10 selected papers/issue)

3 publications.

[dKPI#10] Organization of at least 1 international conference in cybersecurity related domains with 100 attendees (each)

C4IIoT sponsored an international workshop, the 3rd Workshop on Cyber-Security Arms Race (CYSARM) co-located with the prestigious ACM Conference on Computer and Communications Security (CCS), in November 2021[9].

[dKPI#11] Organization of at least 2 workshops with 30 attendees (each)

Three workshops were organised:
(i) the International Workshop on Secure and resilient smart manufacturing environments (SecRS) to be held in conjunction with the 16th International Conference on Availability, Reliability and Security (Ares2021) in August 2021[10].
(ii) contributed to the organization of the Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects in January 2021 together with other projects such as CARAMEL, GUARD, SAPPAN, SIMARGL, and SOCCRATES, and hosted by the CyberSANE project.
(iii) contributed to the organisation of the 2nd Joint Workshop - Dynamic Countering of Cyber-attacks | Achievements and Standardisation, in January 2022, together with other projects such as CARAMEL, GUARD, SAPPAN, SIMARGL, and SOCCRATES, and hosted by the CyberSANE project.

[dKPI#12] At least 1 demo at Major fairs and exhibitions such as Cyber Security Europe at IP EXPO Europe, INFOSEC

No demo was organized at a Major EU event.

[dKPI#13] At least 2 demos at Major EU events such as meetings and workshops organized by ENISA and SANS information security courses' events

No demo was organized at a Major EU event.

[dKPI#14] At least 2 demos at Major conferences (e.g. GLOBECOM, ICC)

No demo was organized at a Major EU event.

[dKPI#15] Organization of at least 3 events of education and training activities (e.g. hackathons, educational and training events, webinars and seminars, to promote C4IIoT cybersecurity offerings with at least 70 attendees (each)

1) C4IIoT INFO day in September 21st 2020 with more than 70 attendees.
2) International winter cybersecurity school organized 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) 2 International summer cybersecurity schools organized within the C4IIoT project with more than 50 attendees

[dKPI#16] Organization of at least 2 events of international summer schools in cybersecurity in the IIoT domain with at least 30 attendees (each)

Two international cybersecurity schools have been organized within the C4IIoT.

International winter cybersecurity school organized by UNPSMF with more than 50 attendees.

International virtual spring school organized by UP1PS with more than 50 attendees.

[9] https://www.cysarm.org

[10] https://2021.ares-conference.eu/workshops/secrs-2021/index.html

[Communication activities KPI (eKPI)#1] C4IIoT website with at least 5000 accesses annually and 500 downloads worldwide

C4IIoT website has 13103 unique visitors and 1305 downloads.

[eKPI#2] At least 10 Press echoes in Europe

14 press releases, one from each partner upon the completion of the project.

[eKPI#3] At least 10 Newspapers (business and normal) in Europe

5 posts in digital news agencies in Europe.

[eKPI#4] At least 9 Newsletters worldwide

11 newsletters have been sent.

[eKPI#5] At least 500 followers worldwide in Social Media (Twitter, LinkedIn, ResearchGate)

650 followers in social media channels.

[eKPI#6] At least 2 Public lectures and/or networking events for end users & general public with at least 50 attendees (each)

C4IIoT has organized four public events: the INFO day with more than 70 attendees, the International winter cybersecurity school with more than 50 attendees, the spring school on cybersecurity with more than 40 attendees and the second INFO Day with about 35 attendees.

[eKPI#7] At least 2 Public lecture and/or networking event for policy makers with at least 20 attendees (each)

This KPI has been achieved, thanks to the participation to the following events:

- 2nd Joint Workshop on Dynamic Countering Cyber-attacks, February 2022, with other projects in the same call.
- 1st Joint Workshop on Dynamic Countering Cyber-attacks, 2021, with other projects in the same call.

[eKPI#8] At least 4 Policy events targeting policy makers of EU, National, Regional and Local Authorities with at least 50 attendees (each)

The target is achieved with 4 Policy events hosting more than 50 participants.

3.2 Evaluation and Impact Analysis for real-life industrial demonstrators

The KPIs reported in the previous section were defined at the beginning of the project and detailed in D5.1[2]. During the evaluation and impact analysis phase, thanks to the pilot tests executed in the two scenarios Smart Factory and Logistics4.0, it has been possible to measure these KPIs in a real-world environment. The results achieved highlights the added value given by the C4IIoT solution in the prevention, monitoring, mitigation and impact analysis of cyber risks occurring not only in the Automotive processes, but that can be verified also in other industries and Supply Chains.

3.2.1 Measuring impact through KPIs

As already mentioned, the introduction of C4IIoT solution has allowed several benefits to the processes considered, that can be summarized in the following points:

- Enable the reduction of costs due to the implementation of different tools, by having a unique solution that includes many different functionalities allowing to prevent, identify, mitigate, analyse and resolve possible cyber risks.
- Possibility to decrease production costs due to unexpected stops or maintenance unexpected issues, that can cause loss of production and also additional operations required to fix the issues occurred. In this way, also the OEE (Overall Equipment efficiency) is positively impacted.
- Possibility to monitor the shipment of components, allowing to decrease production costs for additional operation due to delays or quality issues and also to decrease the costs due to stock out. In fact, as already mentioned, the shipment of batteries from the supplier plant to the Italian production plants has been monitored through the installation of NB-IoT devices, developed and tested within the project. In this way, it has been possible to reduce costs due to stock out caused by unexpected events that can affect the ETA (Estimated Time of Arrival) and the quality of the transported components, but also additional costs for express delivery and warehouse.
- Information available to more actors, each one with different user rights for information visibility/managing. In fact, the following actors have been involved:
    - ICT Team leader
    - ICT Team member
    - Manufacturing engineer
    - Supply Chain Manager
    - Logistics Team member
    - Supply service provider
- Loss of intellectual property is avoided by the C4IIoT solution, thanks to the continuous monitoring, prevention, and response to the cyber risks occurring both in manufacturing plants and in the Inbound Logistics.

3.2.2 Final SWOT analysis

A first analysis of the added value of C4IIoT was summarized in D5.1 [2] and here the updated strengths, weaknesses, opportunities and threats identified for the exploitation of C4IIoT are presented in Table 8.

Table 8 - Final SWOT analysis

Strengths • Integrated management of the manufacturing/ logistics network • KPIs measurements confirming the achievement of planned results • Near-real time support to decision making • Visual approach • Versatile solution that can be applied also in other sectors/processes	**Weaknesses** • Running costs still to be refined • Costs for replication still to be refined
Opportunities • Possibility to further exploit and improve the solution developed • Possible integration with other internal systems in the company	**Threats** • Possible changes in manufacturing industry standards

4 Conclusion

This deliverable reports the final demonstration execution, presenting updates related to the last months of the project, integration of technical evaluation outputs, and the evaluation and impact analysis results.

The major effort has been dedicated to the final deployment of the architecture and to the related tests in the real environment in CRF, both for the Smart Factory scenario but also for the Logistics4.0.

It has been possible to complete the evaluation by mean of the measurement of the KPIs that have been defined in the first phase of the project, and also all the requirements for the C4IIoT solution have been fulfilled, as shown in the following Annex 6.1. Thanks to the achievements measured through the performed analysis, it is possible to state that the results planned at the beginning of the project have been fully achieved.

5 References

[1] "C4IIoT" project, Deliverable D5.2: "C4IIoT Demonstration - final execution"

[2] "C4IIoT" project, Deliverable D5.1: "C4IIoT Demonstration - initial execution and evaluation"

[3] "C4IIoT" project, Deliverable D4.3: "C4IIoT Integrated Framework"

[4] "C4IIoT" project, Deliverable D2.3: "Level-1 Security Mechanism of C4IIoT: Hardware-enabled security"

[5] "C4IIoT" project, Deliverable D2.4: "Security and trustworthiness at the edge"

[6] "C4IIoT" project, Deliverable D3.3: "Level-2 and Level-3 security mechanisms of C4IIoT"

[7] "C4IIoT" project, Deliverable D3.4: "Cyber assurance and protection in an industrial cloud infrastructure"

[8] "C4IIoT" project, Deliverable D4.4: "Best Practices for Maintaining and Operating the Framework in the Long-term"

6 Annex

6.1 Requirements verification and validation

Final requirement	**Priority**	**Fullfilled**
1. It should be possible to have near real-time information about the security level status of all the assets involved. A graphical representation of the system could be used to visually inspect the security levels and highlight exceptions.	High	*YES*
2. Anomalies related to suspect accesses or intrusion to the Industrial IoT by authorised or unauthorised entities should be detected in real-time, displayed and communicated to the other system actors (personnel, devices).	Very high	*YES*
3. All the accesses (both from inside and outside) to the IIoT should be continuously monitored. Decentralised access control (both online and offline) and identity management should be provided.	High	*YES*
4. For certain anomalies, according to a classification based on criteria to be defined at a later stage (i.e., impact, time response), recovery actions should be implemented automatically, within predefined boundaries and enacting interaction with the user when needed. These boundaries include a clear definition of the context, in order to avoid undesirable automatic reactions.	High	*YES*
5. For certain anomalies, according to a classification based on criteria to be defined at a later stage (i.e., impact, time response), the user should be notified. Each anomaly specific notification should be sent depending on the actors.	High	*YES*
6. Impact of the anomaly on the specific part of the system should also be evaluated, taking into account the perimeter of each actor, and notified to the users (graphical interfaces could be used for this purpose).	High	*YES*
7. The solution developed should provide, whenever possible, different mitigation strategies to assist in the cybersecurity risk management decision-making process.	High	*YES*

8. Different users should be granted access to the platform, and then to the security information related to the monitored assets. In this respect, access control and identity management are key to avoid leakage of crucial information.	Very high	*YES*
9. The different categories of users should be distinguished, each one with different authorisation level, depending on their roles.	Very high	*YES*
10. Machine (Deep) Learning (ML/DL) algorithms should be implemented, to anticipate, identify, analyse and counter IIoT cyber-attacks.	Medium	*YES*
11. It should be possible to modify existing or add new encryption algorithms. This is particularly relevant for anomaly detection through Deep Learning algorithms.	Medium	*YES*

6.2 KPIs Monitoring per C4IIoT module

KPI - Code	Secure Execution Environment (FORTH)	Decentralized access control with attribute-based encryption (IBM)	Secure Element at Smart Factory Edge Node (IFAG)	Identity management (HPE)	Traffic analysis (FORTH)	Behavioural analysis & cognitive security module – BACS (UNSPMF)	MEDICI (UOG)	Edge device (VIP)	Advanced visualisation, Privacy/secure data analytics (AEGIS)	Data Fusion Bus (ITML)	Cloud Management & Orchestration (HPE)	Cloud Gateway (HPE)	Risk assessment (HPE)	Security Assurance Module (STS)	Binary Code analyser (CEA)	SDN controller (TSG)	Reconfiguration Search (VariaMos) (UP1PS)
KPI-1.1[11]	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
KPI-1.2	▨	▨	▨	▨	▨	▨	▨	▨		▨			▨	▨		▨	▨
KPI-1.3					▨	▨	▨		▨					▨			
KPI-1.4					▨	▨	▨							▨	▨	▨	
KPI-1.5					▨	▨	▨		▨					▨			
KPI-1.6	▨	▨	▨		▨	▨			▨		▨		▨	▨	▨		▨
KPI-2.1[12]	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
KPI-2.2						▨	▨										
KPI-2.3			▨					▨									
KPI-2.4					▨												
KPI-2.5		▨		▨								▨					
KPI-2.6						▨							▨				

[11,4] Entirely captured with the final integrated solution of C4IIoT framework and the integration of all C4IIoT tools.

KPI-3.1													■	■	■		
KPI-3.2														■	■		■
KPI-3.3							■		■								■
KPI-3.4	■	■			■					■	■		■	■			
KPI-3.5					■	■			■		■			■			■
KPI-3.6					■				■					■			
KPI-3.7						■			■					■			
KPI-4.1						■				■				■			
KPI-4.2[13]	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
KPI-4.3[14]	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
KPI-4.4[15]	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
KPI-4.5									■								
KPI-6.4													■				
iKPI#1.1	■	■	■	■	■	■							■		■	■	■
iKPI#1.2		■	■	■		■							■			■	■
iKPI#2.1					■	■	■									■	■

[13,7,8] Entirely captured with the final integrated solution of C4IIoT framework and the integration of all C4IIoT tools.

iKPI#2.2[16]																	
iKPI#2.3	▨		▨														
iKPI#7.1			▨														

[16] It gets addressed with the whole C4IIoT architecture (edge to cloud) and it has been captured with the final integrated solution of C4IIoT framework.