



## Horizon 2020 Program

### Dynamic countering of cyber-attacks

SU-ICT-2018



## Cyber security 4.0: Protecting the Industrial Internet of Things

### D6.3: Interim Version of Dissemination strategy and activities <sup>1†</sup>

**Abstract:** This deliverable presents the work performed in WP6 – Task 6.2 “Communication strategy triggering awareness and new business opportunities” with respect to the framework of the dissemination strategy of C4IIoT project. The report consists of two parts, namely (i) the definition of C4IIoT dissemination strategy, and (ii) the reporting/monitoring of the respective dissemination and communication activities during the first year of the project (M1-M12).

Contractual Date of Delivery	31/05/2020
Actual Date of Delivery	29/05/2020
Deliverable Security Class	Public
Editor	<i>Spyridon Vantolas (AEGIS), Efstathios Dimakos (AEGIS), Stavroula Vanikioti (AEGIS)</i>
Contributors	All C4IIoT partners
Quality Assurance	<i>Sébastien Bardin (CEA)</i> <i>Eleftheria Marini (ITML)</i>

---

<sup>1</sup> <sup>†</sup> The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833828.

### The *C4IIoT* Consortium

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

## Document Revisions & Quality Assurance

### Internal Reviewers

1. *Sébastien Bardin (CEA)*
2. *Eleftheria Marini, (ITML)*

### Revisions

Version	Date	By	Overview
0.11	29/05/2020	AEGIS	Final document
0.10	25/05/2020	CEA	Review
0.9	21/05/2020	ITML	Review
0.8	19/05/2020	AEGIS	Draft prepared for internal review
0.7	15/05/2020	All	Individual dissemination plans
0.6	11/05/2020	AEGIS	Draft updated
0.5	04/05/2020	All	Dissemination activities
0.4	20/04/2020	AEGIS	Draft updated
0.3	06/04/2020	AEGIS	First draft
0.2	25/03/2020	All	Comments on the ToC.
0.1	26/02/2020	AEGIS	ToC.

## Table of Contents

<b>LIST OF TABLES .....</b>	<b>5</b>
<b>LIST OF FIGURES .....</b>	<b>6</b>
<b>LIST OF ABBREVIATIONS.....</b>	<b>7</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>8</b>
<b>1 INTRODUCTION .....</b>	<b>9</b>
1.1 PURPOSE OF THE DOCUMENT .....	9
1.2 RELATIONSHIP WITH OTHER DELIVERABLES .....	9
1.3 STRUCTURE OF THE DOCUMENT.....	10
<b>2 DISSEMINATION &amp; COMMUNICATION STRATEGY.....</b>	<b>11</b>
2.1 DISSEMINATION PHASES AND DEPENDENCIES .....	11
2.1.1 Dissemination phases.....	11
2.1.2 Dependencies .....	11
2.2 DISSEMINATION PRINCIPLES.....	12
2.3 TARGETED GROUPS .....	12
2.4 ROLES & RESPONSIBILITIES .....	13
2.4.1 Dissemination roadmap .....	16
2.4.2 Assets to disseminate .....	17
<b>3 DISSEMINATION &amp; COMMUNICATION TOOLS.....</b>	<b>18</b>
3.1 DISSEMINATION CHANNELS.....	18
3.2 PROJECT WEBSITE .....	18
3.3 SOCIAL NETWORK ACCOUNTS .....	19
3.3.1 Twitter.....	19
3.3.2 LinkedIn.....	20
3.3.3 Facebook.....	20
3.4 DISSEMINATION MATERIAL .....	20
3.4.1 C4IIoT Logo .....	21
3.4.2 Flyer.....	21
<b>4 MONITORING - KPI'S.....</b>	<b>22</b>
4.1 DISSEMINATION KPI'S .....	22
4.2 MEANS TO MEASURE INDICATORS .....	24
4.3 RISKS AND ISSUES .....	24
<b>5 DISSEMINATION &amp; COMMUNICATION ACTIVITIES (M1 TO M12) .....</b>	<b>25</b>
5.1 PUBLICATIONS .....	25
5.1.1 Scientific Papers .....	25
5.1.2 General & business publications.....	25
5.2 EVENTS.....	25
5.2.1 Past Events.....	26
5.2.2 Future Events .....	27
<b>6 STANDARDIZATION ACTIVITIES .....</b>	<b>28</b>
<b>7 SHORT-TERM FUTURE DEVELOPMENT AND PLANNING (M12 TO M18) .....</b>	<b>30</b>

## List of Tables

Table 1: Dissemination phases .....	11
Table 2: Identified Targeted Groups .....	13
Table 3: Dissemination plan per partner .....	16
Table 4: Dissemination roadmap.....	17
Table 5: Assets to disseminate .....	17
Table 6: C4IIoT Website Analytics.....	18
Table 7: C4IIoT Website Technical details.....	19
Table 8: C4IIoT Twitter Analytics .....	20
Table 9: C4IIoT LinkedIn Analytics .....	20
Table 10: C4IIoT Facebook Analytics .....	20
Table 11: Online Dissemination KPIs .....	22
Table 12: Scientific publications KPIs .....	23
Table 13: Organization of International Scientific Events KPIs .....	23
Table 14: System-level demonstrations KPIs.....	23
Table 15: Education and training activities for cybersecurity in IIoT KPIs.....	23
Table 16: Risk Log.....	24
Table 17: Scientific Papers.....	25
Table 18: Genera & Business publications .....	25
Table 19: Past Dissemination Events .....	27
Table 20: Future Dissemination Events .....	27

## List of Figures

Figure 1: Dissemination Strategy Steps .....	9
Figure 2. Dissemination Dependencies .....	12
Figure 3: Dissemination Channels .....	18
Figure 4: C4IIoT website .....	19
Figure 5: C4IIoT Logo .....	21
Figure 6: C4IIoT Introductory Flyer .....	21

## **List of Abbreviations**

<b>EC</b>	European Commission
<b>IoT</b>	Internet of Things
<b>IIoT</b>	Industrial Internet of Things
<b>KPIs</b>	Key Performance Indicators
<b>WP</b>	Work Package

## Executive Summary

This deliverable presents the work performed in WP6 – Task 6.2 “Communication strategy triggering awareness and new business opportunities” and consists of two parts. The first part refers to the definition of C4IIoT dissemination strategy and plan, and the second one to the reporting and monitoring of the respective dissemination and communication activities during the first year of the project (M1-M12). As the objective of WP6 is to supervise the integrity and consistency of all dissemination efforts for creating awareness on the C4IIoT achievements, the main purpose of the current deliverable is to develop the framework of an effective dissemination strategy for the project, via specific means and activities. Such activities will be continuously monitored and measured against a set of KPIs, to ensure project’s maximum awareness and at the same time its presence in relevant IIoT and IoT communities

C4IIoT consortium has drawn up a dissemination strategy whereby dissemination activities at all levels were defined in detail. This strategy sets out the plan to raise awareness, share knowledge, attract potential end-users and stakeholders, and explore future commercial use in the context of the C4IIoT project, through various means. These means include the project’s website, social networks accounts, distribution of dissemination material, publications in journals, and participation in conferences and other relevant events. As the objective of WP6 is to supervise the integrity and consistency of all dissemination efforts for creating awareness on the C4IIoT achievements, the purpose of the strategy is twofold: (i) ensuring project’s maximum awareness (measured against a set of KPIs) and at the same time its presence in relevant IIoT communities and (ii) paving the way to exploitation activities and long-term sustainability of the solution.

The main elements of C4IIoT dissemination strategy are: (i) Dissemination phases according to project’s progress (Sections 2.1, 2.2); (ii) targeted group identification (Section 2.3); (iii) roles and responsibilities and individual plans from all partners (Section 2.4); (iv) detailed roadmap for dissemination activities till the end of the project and definition of disseminatable assets of C4IIoT (Section 2.4); (v) Definition of dissemination and communication tools (Section 3); (vi) Undertaken and planned communication and dissemination activities (Section 5); (vii) Standardisation activities (Section 6); (viii) and monitoring of dissemination activities by using key performance indicators (KPIs) (Section 4).

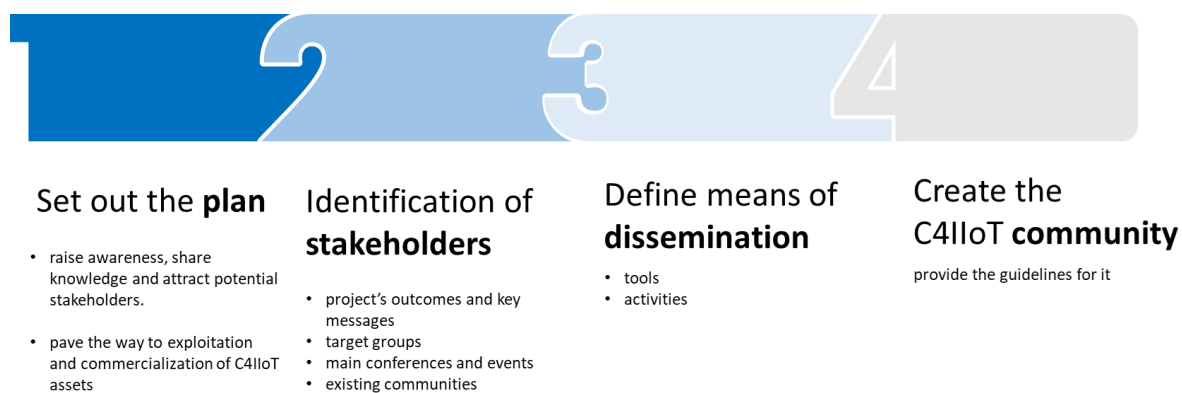
Finally, it is to note that as any dissemination itself is strongly connected to project’s partial developments and outcomes. Dissemination activities will be continuously monitored and updated (frequent adjustments are expected) with respect to project’s objectives and KPIs. Dissemination is a “living” task and this deliverable provides an overview of what is known and planned at the time of the document preparation.



# 1 Introduction

In the era of Industry 4.0, where countless elements comprising industrial systems are being interfaced with internet communication technologies to form the smart factories and manufacturing organizations of the future, cybersecurity issues make it extremely difficult to harness the full potential of the revolutionary technologies. C4IIoT will design, build, and demonstrate a novel and unified Cybersecurity 4.0 framework that implements an innovative IoT architecture paradigm to provide an end-to-end holistic and disruptive security-enabling solution for minimizing the attack surfaces in Industrial IoT systems.

To ensure the successful implementation of the C4IIoT project and sustainability and wider exploitation of its outcomes, a solid dissemination strategy has been developed in order to raise awareness and create the foundations for an active community for the project. Figure 1 below depicts the steps towards this direction.



**Figure 1: Dissemination Strategy Steps**

## 1.1 Purpose of the document

The purpose of this document is to establish clear plans and guidelines for dissemination activities and available channels in order to maximize the impact of C4IIoT to its target audiences. The present document describes the set of actions to be carried out within the C4IIoT project, organizes the dissemination activities to inform target audiences and shares knowledge to the public to inform existing networks/stakeholders on project progress and outcomes. The deliverable also provides metrics, key performance indicators (KPI), which allow the evaluation of the success of the actions during and after the project.

## 1.2 Relationship with other deliverables

The dissemination plan is a key document which gets all partners aligned in a common framework. It also relates to all exploitation tasks as well as the implementation progress. This deliverable is closely linked to other public documents, namely:

- D6.1 Project website
- D6.2 Market analysis and preliminary business modelling
- D6.4 Exploitation and standardization activities and best practices – initial version

It also paves the way to a more mature dissemination strategy and activities report that will be submitted on M24.

### **1.3 Structure of the Document**

The deliverable is organized into seven sections whose purpose is briefly described next.

Section 1 introduces the deliverable and highlights the relationship to other C4IIoT deliverables and tasks.

Section 2 presents the dissemination and communication strategy in each phase of the projects' progress, defines the targeted groups, and determines the role and responsibilities of partners in a specific roadmap.

Section 3 presents an overview of dissemination tools and channels.

Section 4 provides key performance indicators (KPI), which allow the evaluation of the success of the actions during and after the project.

Section 5 lists dissemination and communication activities for the first year of the project as well as future events consortium members planning to attend.

Section 6 shows the standardization activities during M1-M12

Section 7 highlights the overall conclusions and future plans.

## 2 Dissemination & Communication Strategy

### 2.1 Dissemination phases and dependencies

#### 2.1.1 Dissemination phases

C4IIoT dissemination and communication activities will be executed in four distinctive phases in dependence with the progress of C4IIoT framework implementation

Table 1 describes the actions and the allocated period for each phase.

Phase	Description – indicative actions	Duration
<b>Starting Phase: Setting the scene</b>	Dissemination activities commenced even before the preliminary results of the project were available. Starting to raise awareness about C4IIoT vision targeted group(s) have been initially identified and their characteristics, needs and relation to the project's outcomes have been defined. Dissemination activities are supported by project's web site and accounts in social media.	M1-M3
<b>Inception Phase</b>	Targeted group(s) are further researched and analysed to develop correlations between stakeholders and define the appropriate communication channels.	M3-M8
<b>Implementation Phase</b>	According to flow of relevant project information, activities to deliver the project's message to its audiences have been identified and will increasingly target professionals and events in the target sectors. Workshops, conferences, and other related events targeted, along with participation in scientific publications and with increasing use of social media. All types of activities designed and developed, aim to the rise of awareness for C4IIoT.	M8-M12
<b>Monitoring and Improvement</b>	Effectiveness and costs for all types of communication products and activities is validating and the dissemination plan is optimized.	M12-M36

**Table 1: Dissemination phases**

#### 2.1.2 Dependencies

At this point it becomes clear that the C4IIoT dissemination strategy and the respective activities cannot be regarded in an isolated way. All components of the project's dissemination strategy are either the outcome of other project's WP's or the data needed to other project's tasks. In other words, there are dependencies with respect to the C4IIoT dissemination strategy and the rest of the project's phases and tasks as demonstrated in Figure 2 below.

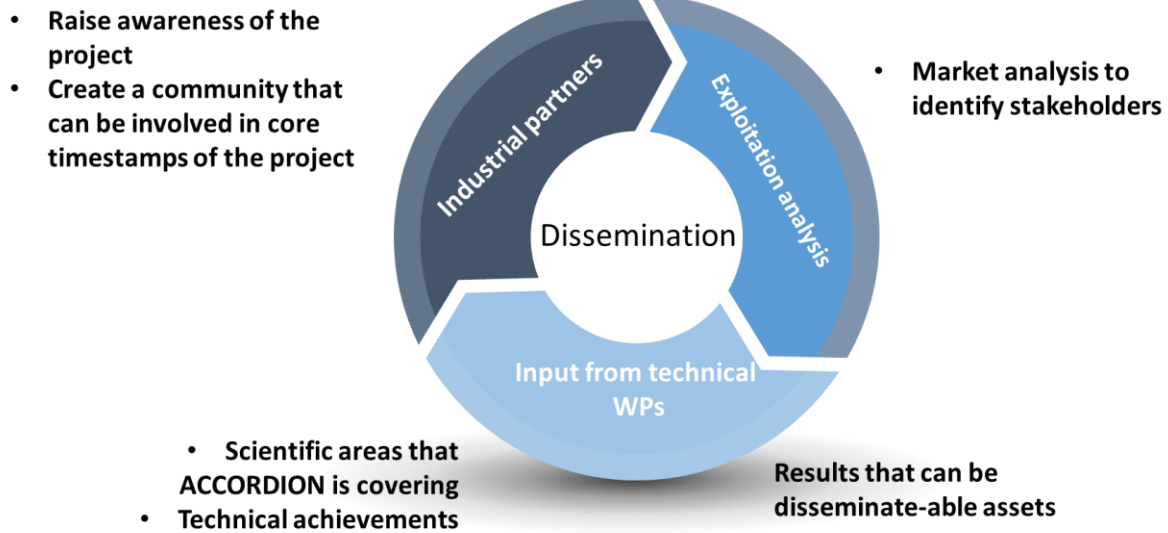


Figure 2. Dissemination Dependencies

The development of the dissemination tools and activities must be in line with the project's progress and status. Input from technical WPs (WP2, WP3, WP4 and W5) throughout the project's development must be disseminated, correlated, and communicated to corresponding target groups (WP1 and WP6). This is an ongoing process and will pave the way to exploitation and long-term sustainability (T6.3, T6.5).

## 2.2 Dissemination Principles

The development of the dissemination activities must be in line with the project's progress and status. Thus, an effective dissemination has also to consider the following principles:

- Information has to be available, accessible, adaptable, and diversified. Depending on the different purposes, target groups and cultural backgrounds, dissemination activities and tools need to be continuously updated.
- Information has to be relevant and compatible to the different user groups so as to reach its maximum understanding and impact.
- Interaction with end-users must be stressed. Analysing the end-user needs and responses creates links between the project goals and actual achievements. This interaction requires a constant adoption of dissemination activities.

## 2.3 Targeted groups

The dissemination plan should be based on an understanding of potential users, their information needs and preferences. A potential user is anyone who has a vested interest in the project, or someone who can eventually benefited from its outcomes. The different individuals, experts, groups, communities, and organizations that will be interested in the project and its results need to be identified and informed. Based on the C4IIoT identity and

objectives, the main strategic stakeholder groupings have been identified for the dissemination and communication of the project and are listed below:

- **Scientific Community:** Research & Academic organizations, Research Committees and Societies, Research driven hubs, networks, platforms, EU and national funded sister- projects.
- **Industry:** Project related industries (smart factories, manufacturing, transport & logistics), IIoT providers, research-market oriented institutions, SMEs, private investors.
- **Others:** EAB members, EC, policy makers, individuals, and experts

Even if the borders between every group are not strictly defined and sometimes overlapping, this classification can be considered as a starting point to work on.

Group	Goals – Activities
<i>Scientific</i>	<b><u>Goals:</u></b> Will be mainly interested in the research results of C4IIoT, the scientific publications generated by the project and advance beyond the state of the art. The scientific community will be able to reuse and leverage research project results in future projects.
	<b><u>Activities:</u></b> Scientific dissemination will include an emphasis on conferences, scientific workshops, academic papers and scientific magazines (online and print). The main messages include the approach taken, the results gained, the innovation and processes. The intention is to spread widespread knowledge of the project and to foster feedback on complementary approaches.
<i>Industrial</i>	<b><u>Goals:</u></b> Industrial community includes any kind of enterprise or individual that can be interested in the adoption of C4IIoT result because it brings a benefit to their business, competitiveness or return on investment.
	<b><u>Activities:</u></b> Industrial dissemination builds interest in the project to complement the exploitation plan, garner feedback from the market and identify potential partners and end-users. It will focus on typically shorter and more generic communication items (web coverage, flyers, press releases, whitepaper, magazines and, etc.). The key messages revolve around the C4IIoT superior capabilities, the benefits it will confer, the conditions under which it can be used and how and when users can become involved. The intention is to prepare the market, identify potential collaborators and users and to gather feedback.
<i>Other</i>	<b><u>Goals:</u></b> It would be an omission not to mention several other groups like EU and EAB which their role is to support and guide the project. For each one of these groups the dissemination goals differ.
	<b><u>Activities:</u></b> Already mentioned in the previous communities

**Table 2: Identified Targeted Groups**

## 2.4 Roles & Responsibilities

As part of the C4IIoT dissemination strategy, certain action items have been identified for the different partners:

- **Academic partners** will disseminate in the scientific community the research achievements obtained within the project. They will target very high-profile publication venues for the security, critical infrastructures, and system engineering domains. Academic partners will also incorporate the project results within their advanced educational activities. Integration of results in advanced studies is known to have the capability of filling the gap between classical technical disciplines and

interdisciplinary socio-technical domains like energy, health, and smart transport applications.

- **Industrial partners** will present the project results in industrial fairs, exhibitions and gatherings of decision makers, creating the opportunity for one-on-one, bilateral communication with key decision makers. Events will include major international forums for cybersecurity solution providers and consumers.

The Table 3 includes a short description for the action items from each partner point of view:

Business Partner	Dissemination & communication plan
FORTH	As project coordinator, FORTH will be deeply involved in the dissemination strategy. It will also be the main contact point for Collaboration activities and liaison with other initiatives. FORTH will take advantage of its large network of stakeholders, collaborators, and community members to aware them of C4IIoT through all available means. FORTH will also publish articles, papers and book chapters in topics related to C4IIoT. As a member of the association, FORTH will disseminate the project in BDVA.
CRF	Dissemination activities in CRF regard mainly the organization and/or participation to events, as workshops or fairs, for presenting the results and Lesson Learned deriving from the implementation of C4IIoT framework both in Smart Factory and Logistics.  Events can be organized both internally, involving different areas in FCA, and also with external companies. The implementation in Campus Melfi is crucial for educational and training purposes, since it is an Innovation Centre with the aim of testing new technologies and methodologies and also to train companies, especially SMEs, in the application and usage of innovative solutions. Events as workshops or demonstrations would be an opportunity for companies to learn more details on the project and understand how they can improve their own internal processes.
IFAG	IFAG is raising the awareness about the results of the C4IIoT project, e.g. the Hyperledger Fabric Hardware wallet, through its periodical participation in several tradeshows, conferences, and standardization bodies, such as the NFC forum and the Silicon Alps Security Week. Furthermore, synergies with concurrent EU funding projects, e.g. COLLABS, are exploited, by promoting the work among the different consortia. First prototype of Blockchain-enabled secure edge nodes have already showcased to customers, obtaining favorable early impressions. Furthermore, high-impact journal publications to further disseminate the results are expected during the second half of the project.
TSG	Thales will promote C4IIoT in the cybersecurity events where it is regularly active and in the other collaborative projects related to the cybersecurity of industrial domains.  Concerning the standardisation organisations, Thales will disseminate on C4IIoT in the Trusted Computing Group (TCG) as an active member.  Closer to its specific activity in the project and in the scope of enhancing the 5G security, Thales will disseminate on the usage of Software Defined Networking to limit attack surfaces by taking advantage of having the lead of the WG Security in the 5G PPP.  Thales will organise the first INFODAY on C4IIOT which unfortunately postponed due to COVID 19 issues.
HPE	As a leading industrial organization in IT relevant domains, HPE will utilize its large network of contacts and customers to raise awareness of the project. Examples of such activities is internal conferences like Network Security bootcamp, Bi-Weekly WW Security COE, NWI Workplace & IOT Sec. Furthermore, HPE discussing on how to disseminate C4IIoT in a public event according to company's policy.
CEA	CEA is promoting C4IIoT among its partners in other (EU-, national, or industrially) funded projects, raises awareness through its participation in events such as A/A*

	cybersecurity conference, invitation to seminars, or workshops. Finally, some of the results of C4IIoT will be integrated in the open-source BINSEC platform, ensuring a wide distribution among users of the platform.
IBM	IBM plans to contribute to C4IIoT dissemination efforts by sharing content regarding its work in the blog page of C4IIoT website. The content will include information of IBM's decentralized access control solution in C4IIoT and its integration and usage within the project.
AEGIS	AEGIS guides all dissemination activities and fosters dissemination while being responsible of coordinating and monitoring all C4IIoT dissemination activities. AEGIS constantly raising awareness for C4IIoT among its customers and partners in other EU-funded projects that is engaged to. Finally, AEGIS is promoting C4IIoT achievements through its website and social networks and by participating in events and workshops.
UP1PS	<p>UP1PS will disseminate the project activities by publishing its results in peer-reviewed international conferences and journals. It will also organize a summer school in Paris in the spring of 2022 on the topic of Cybersecurity for the Industrial Internet-of-Things where it will invite several C4IIoT partners to present the cutting-edge technologies that they are developing and integrating in an industrial setting for the project.</p> <p>As the VariaMos tool that UP1PS contributes to C4IIoT is based on Artificial Intelligence (AI) technologies, in particular constraint optimization and automated planning, UP1PS will also demonstrate the tool as an industrial innovative application example of these AI technologies to the vast ecosystem of the 80 partner strong H2020 AI4EU Project <a href="https://www.ai4eu.eu/">https://www.ai4eu.eu/</a> A European On-Demand Artificial Intelligence Platform and Ecosystem sole laureate of the ICT-26-2018 call and in which UP1PS leads the Verifiable AI task of the Filling AI Technology Gaps work package.</p> <p>The AI4EU ecosystem is currently been integrated with those of the four European Network of AI Excellence Centres laureates of the H2020 ICT-48-2020 call and will also be integrated with the laureates of the open H2020 ICT-49-2020. These integrations will bring together an exceptionally large and diverse set of industrial, societal and academic partners making the integrated ecosystem a high-impact dissemination medium</p>
ITML	ITML has a global business division whose mission is to seize the opportunities within the digital world and deliver new growth through venture capital, global partnerships and digital services. The dissemination strategy is based on the use of the know-how generated in this project to maintain and expand the visibility of ITML in machine learning and anomaly detection. Additionally, ITML is connecting with local and EU big solution providers and potential stakeholders in order to disseminate C4IIoT assets and services (big data management tools, integration methodology, services and processes). Furthermore, ITML is establishing dissemination activities particularly with regard to social media, existing collaborations and partnerships while also aims to deliver and transfer knowledge regarding technological advancements to the academic partners enhancing and strengthening its positioning within the EU market and research domain and built new collaborations and partnerships in the research domain of Europe.
STS	STS is responsible for the long-term sustainability and commercialisation of the C4IIoT framework, and its dissemination and communication efforts focus on promoting C4IIoT -related updates and events through the company's communication and social media channels. A number of industrial and academic events are planned where C4IIoT will be promoted, while the project is also indirectly disseminated in the context of promoting STS' activities and expertise to customers and partners
UNSPMF	UNSPMF constantly disseminates information about the C4IIoT project through seminars and workshops (for instance: "NB-IoT Testbed and Use Cases: Device Design and Experience with Real-World Operator Network" workshop held in Barcelona in 2020) and similar activities. Publications related to the project outcomes and results in scientific journals and conferences have been planned for the 2020-2022 period. Moreover, we plan to organize the C4IIoT Summer School on Cyber Security for IIoT in November 2020, M18 of the project



UOG	UOG plans to publish papers related to our security aware offloading mechanism. We will target high-profile journal papers in the area, such as IEEE Internet of Things Journal and Elsevier Decision Support Systems. We also plan to incorporate the project results within our teaching, by introducing to post-graduate students the concepts of Industrial Internet of Things and computation offloading
VIP	VIP contributes to dissemination activities through internal activities, within company and group of companies (Vip mobile is part of Telekom Austria Group) – workshops and Hackathons. Contribution through external activities is done through workshops with IoT Partners and ICT/IoT conferences. In cooperation with UNSPMF publications will be prepared.

**Table 3: Dissemination plan per partner**

Finally, all partners will support C4IIoT's circle of continuous technical communication with the community through presence in social media groups and on forums. These communications will be aimed at secondary targets and at increasing the general awareness.

### 2.4.1 Dissemination roadmap

With respect to the dissemination strategy planned for C4IIoT, for each dissemination channel, a series of tools and means with specific purpose of use have been identified as part of the dissemination and communication roadmap (Table 4) for the project.

Dissemination Channel	Mean/Tool	Purpose	Delivered
<b>Online Dissemination</b>	Project website	The site is a key instrument for supporting the dissemination of the research results. Key results will be published on the website, but also added value services will be offered such as support in using C4IIoT methodology.	M2
	Social Media Accounts	Will be a major instrument for recruiting interested parties and for continuous informal communication with stakeholders and target groups that are active on social media.	M2/ M4/ M16
	Newsletter	The newsletter will rely on well-balanced mix of dissemination and infotainment content. All partner organizations will contribute to the newsletter, which will be made available free of charge through electronic means.	M14
	Technical Video	A professional C4IIoT technical video of estimated 5 minutes of duration will be developed by M4. The video will focus on the technical advancements of the C4IIoT methodology and approach, targeting the technical and business community of IIoT.	M18
<b>Scientific publications</b>	Journals	All publication venues will be carefully selected based on their scientific excellence and impact privileging where possible open	M1 - M36
	Magazines		



	Conferences	access publishing.	
	Special Issues in Scientific Journals		
<b>Organization of International Scientific Events</b>	Conference	C4IIoT will organize one significant international conference in the core research areas of the project. Our goal will be to enhance the visibility of our contributions at an international level.	TBA
	Workshops	C4IIoT will organize two international scientific workshops throughout its duration.	TBA
	Summer Schools on Cyber Security for IIoT	To be cost-effective, three of consortium academics, namely UP1PS, CEA and UNSPMF will organize three summer schools.	M18
<b>System-level demonstrations</b>	Demonstrations in fairs and exhibitions	C4IIoT will seek to organize at least one demonstration of the project's technical results in major international fairs and exhibitions.	TBA
	Demonstrations in EU related events	C4IIoT aims to organize at least two demonstrations of the project's technical results in EU related events	TBA
	Demonstrations in major international conferences	C4IIoT aims to organize at least two demonstrations of the project's technical results in major international conferences	TBA

Table 4: Dissemination roadmap

#### 2.4.2 Assets to disseminate

Asset to Disseminate	Description	Target Group
<b>Public Deliverables</b>	All deliverables documented during the project's progress will be available via the C4IIoT Website	EC, Consortium Partners, Industrial and scientific stakeholders
<b>MVP</b>	The minimum Viable Product stands out from the rest of the deliverables as the first tangible outcome of the project	EC, Consortium, partners, Industrial end-users, investors, Academic and scientific stakeholders
<b>C4IIoT integrated framework</b>	The 1 <sup>st</sup> integrated prototype of C4IIoT that will demonstrate most of the proposed capabilities	EC, Consortium, partners, Industrial end-users, investors, Academic and scientific stakeholders
<b>Final product</b>		Industry 4.0 community
<b>Use Cases Lessons Learned</b>	All conclusions and lessons learned from the application of the framework through the use cases are knowledge that needs to be shared.	EC, Consortium, partners, Industrial end-users, investors, Academic and scientific stakeholders

Table 5: Assets to disseminate

### 3 Dissemination & Communication tools

#### 3.1 Dissemination channels

The C4IIoT's dissemination efforts aim to influence stakeholders' view, so that they will become aware of the project's new ideas, services, and results, and ultimately adopt it. To this end, four distinct channels have been identified accompanied by a specific execution plan for each of them. This combined approach ensures efficient dissemination. C4IIoT dissemination strategy has established four distinct channels as depicted in Figure 3 below:

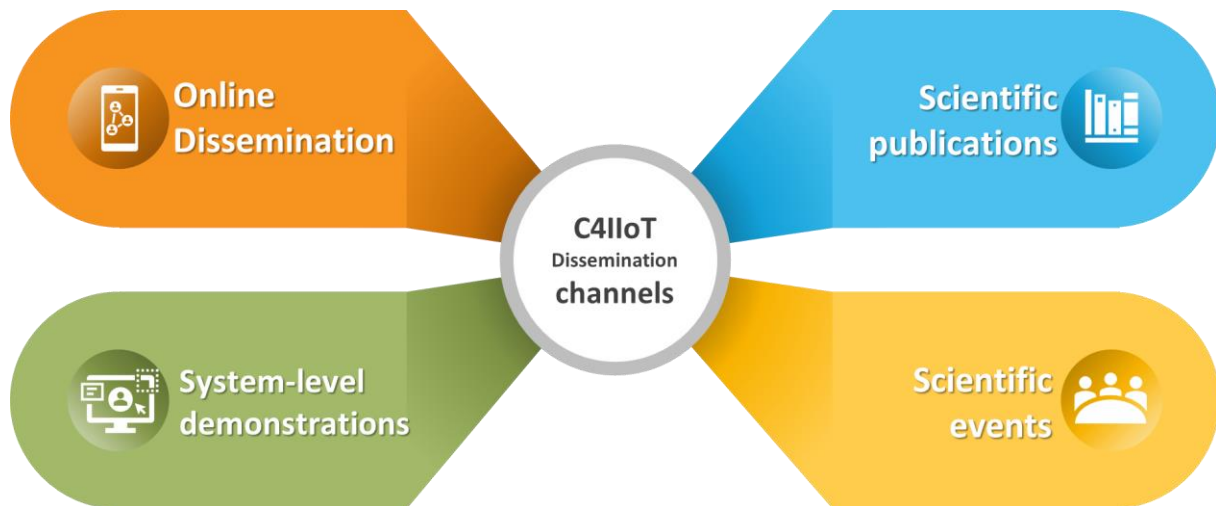


Figure 3: Dissemination Channels

#### 3.2 Project Website

C4IIoT website has been designed and developed by AEGIS. The developing activities started in M1 (June 2019) and by the beginning of M2 (July 2019) it was fully operational.

Website Analytics M1-M12	
Unique Users	588
Downloads	32
Page Views	2039

Table 6: C4IIoT Website Analytics

The design of the site was based on the ease of access and navigation to it by the end user. In addition, the presentation of the website's content (including project's objectives, consortium, etc.) follows a user-friendly approach.



Figure 4: C4IIoT website

C4IIoT Website Technical Details	
Domain	<a href="https://www.c4iiot.eu/">https://www.c4iiot.eu/</a>
Servers/hosting	Linux based Apache 2.2.15
Content Management System (CMS)	WordPress Version 5.5.2
PHP Version	5.6.25
MySQL Version	5.1.73

Table 7: C4IIoT Website Technical details

### 3.3 Social Network accounts

To amplify its web-based presence C4IIoT has created accounts in popular social media networks and platforms as the means to communicate its message online.

#### 3.3.1 Twitter

Twitter account for the C4IIoT project was created on June 2019 alongside with the website. It is remarkable that even though the account had approximately one tweet per month for the first year of the project, the audience reach was more than 17000.

Twitter analytics	
URL	<a href="https://twitter.com/c4iiot">https://twitter.com/c4iiot</a>
Tweets	13
Followers	108
Visits	363

<b>Mentions</b>	173
<b>Audience Reached</b>	17100

**Table 8: C4IIoT Twitter Analytics**

### 3.3.2 LinkedIn

LinkedIn Page for C4IIoT was published on June 2019 following the website and twitter account releases. The table below demonstrates the statistics for the C4IIoT LinkedIn Page for the first 12 months of its release.

LinkedIn Analytics	
<b>URL</b>	<a href="https://www.linkedin.com/company/c4iiot">https://www.linkedin.com/company/c4iiot</a>
<b>Followers</b>	45
<b>Posts</b>	3
<b>Total Views</b>	1041
<b>Visitors</b>	99

**Table 9: C4IIoT LinkedIn Analytics**

### 3.3.3 Facebook

A Facebook page for C4IIoT dissemination purposes has been launched since the beginning of the project. However, the page does not seem to have drawn much attention yet in comparison with the rest of the social media accounts of C4IIoT.

Facebook Analytics	
<b>URL</b>	<a href="https://www.facebook.com/c4iiot.eu/">https://www.facebook.com/c4iiot.eu/</a>
<b>Followers</b>	29
<b>Posts</b>	8
<b>Total Views</b>	189

**Table 10: C4IIoT Facebook Analytics**

## 3.4 Dissemination material

To support the dissemination activities of the project, the consortium will regularly create dissemination material in the form of documents, papers, deliverables, technical reports, presentations, fact sheets and video clips.

### 3.4.1 C4IIoT Logo

ITML designed a simple, scalable, and versatile logo for the C4IIoT project. The C4IIoT logo can be found in Figure 5: below. Each gear represents one key idea behind the project. The first one represents the “Industrial Internet of Things” and foretells that the developed framework will be tested in manufacturing environment. The second one represents the cybersecurity aspect while the last one points out that the developed framework can be implemented in various sectors (e.g. logistics, transportation etc.).

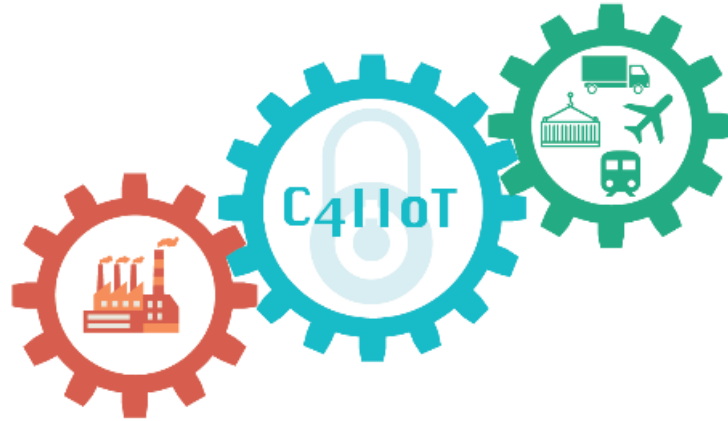


Figure 5: C4IIoT Logo

### 3.4.2 Flyer

An introductory flyer for the C4IIoT has been created from AEGIS and ITML as part of the printed dissemination material for the project.

Figure 6: C4IIoT Introductory Flyer

## 4 Monitoring - KPI's

Progress in dissemination is being monitored by using key performance indicators (KPIs) which cover all forms of dissemination and in particular emphasize the results gained rather than the quantity produced. To this end, the dissemination manager, project coordinator and exploitation manager will be facilitated in modifying the strategy and incorporate feedback into the project.

KPIs cover website statistics, event participation and quantity of publications. Beyond merely registering the number of activities, the KPIs will expressly measure the dissemination value of actions. For example, the number of “reads” of online materials, the number of queries and comments received, the number of citations and backlinks. These KPIs will be used to steer dissemination to the most valuable activities.

### 4.1 Dissemination KPI's

The following tables provides a quantification of the project's dissemination activities and sets a basis for verifying whether the project dissemination objectives have been met via key performance indicators (KPIs)

Online dissemination		
Tool	Description	Success Indicators
Project website	dKPI#1: Web access to deliverables, technical results and presentation material of C4IIoT	$\geq 1000$ accesses annually $\geq 100$ downloads
Push announcements	dKPI#2: Regular push announcements through social media (Twitter, LinkedIn, ResearchGate)	$\geq 50$ announcements
Regular Newsletter	dKPI#3: Regular quarterly newsletter with C4IIoT technical activities	$\geq 9$ newsletters
Brochure	dKPI#4: High-quality electronic brochure with the technical approach and activities of C4IIoT	$\geq 2000$ hard copies distribution in $\geq 10$ events $\geq 2000$ downloads
Technical video	dKPI#5: 5 min high-quality video presentations of the technical aspects of C4IIoT	$\geq 1000$ views $\geq 10$ event presentations

**Table 11: Online Dissemination KPIs**

Scientific publications		
Tool	Description	Success Indicators
Journal publications	dKPI#6: Publications in International referred technical journals in cybersecurity-related subjects	$\geq 10$ publications
Magazine publications	dKPI#7: Publications in International magazines in cybersecurity-related subjects	$\geq 10$ publications
Conference publications	dKPI#8: Publications in International referred technical	$\geq 12$



	conferences in cybersecurity-related subjects	
Special issues	dKPI#9: Publications of special issues in International referred technical journals and magazines	$\geq 2$ $\geq 10$ selected papers/issue

**Table 12: Scientific publications KPIs**

Organization of International Scientific Events		
Tool	Description	Success Indicators
Conference organizations	dKPI#10: Organization of international conferences in cybersecurity-related domains	$\geq 1$ event $\geq 100$ attendees (each)
Workshops	dKPI#11: Organization of workshops	2 workshops $\geq 30$ attendees (each)

**Table 13: Organization of International Scientific Events KPIs**

System-level demonstrations		
Tool	Description	Success Indicators
Exhibition demonstrations	dKPI#12: Major fairs and exhibitions such as Cyber Security Europe at IP EXPO Europe, INFOSEC	$\geq 1$ demo
EU demonstrations	dKPI#13: Major EU events such as meetings and workshops organized by ENISA and SANS information security courses' events	$\geq 2$ demos
Conference demonstrations	dKPI#14: Major conferences (e.g. GLOBECOM, ICC)	$\geq 2$ demos

**Table 14: System-level demonstrations KPIs**

Education and training activities for cybersecurity in IIoT		
Tool	Description	Success Indicators
INFO DAYS	dKPI#15: Organization of education and training activities (e.g. hackathons, educational and training events, webinars and seminars, to promote C4IIoT cybersecurity offerings	$\geq 3$ events $\geq 70$ attendees (each)
Summer schools	dKPI#16: Organization of international summer schools in cybersecurity in the IIoT domain	$\geq 2$ events $\geq 30$ attendees (each)

**Table 15: Education and training activities for cybersecurity in IIoT KPIs**

## 4.2 Means to measure indicators

Each partner will be in charge of locally monitoring its own dissemination activity and reporting the progress and pitfalls to the dissemination leader. All partners are responsible for liaising with the local and regional media for dissemination purposes. In addition, external project material will be reviewed with the dissemination leader in order to comply with quality standards.

## 4.3 Risks and issues

There are a number of risks and potential issues related to the communications side of the project. These risks will be monitored and mitigated by the Coordinator. The following table summarizes some of the possible communication risks.

Risk description	Priority	Actions to be considered
Dissemination activities fail to target the correct audiences	High	Set clear objectives based on knowledge of the target audience, set specific goals.
Poor dissemination towards relevant stakeholders. The project may fail to get the wide participation of the citizens and the relevant stakeholders	High	A clear map of stakeholders. Ensure clear message across all dissemination material
Emergencies (COVID-19 outbreak)	High	Reschedule events and actions

**Table 16: Risk Log**

The COVID-19 disease outbreak affected the operation of institutes and companies and several events cancelled or postponed. This emergency has impact on certain dissemination activities as both trips and physical meetings are prohibited. For example, information day supposed to take place at M12 postponed.



## 5 Dissemination & Communication activities (M1 to M12)

### 5.1 Publications

#### 5.1.1 Scientific Papers

Partner	Type of Publication	Title of Publication	Author(s)	Link
UNSPMF	Conference publication	Robot Task Allocation based on Greedy-Face-Greedy Algorithm, 27th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2019	J. Stanulovic, N. Mitton and I. Meze	<a href="http://www.telfor.rs/?lang=en">http://www.telfor.rs/?lang=en</a>
UoG	Journal	Dynamic decision support for resource offloading in heterogeneous internet of things environments	Jaddoa, A., Sakellari, G., Panaousis, E., Loukas, G., & Sarigiannidis, P. G.	<a href="https://www.sciencedirect.com/science/article/pii/S1569190X19301509">https://www.sciencedirect.com/science/article/pii/S1569190X19301509</a>
CEA	Conference publication	Get rid of inline assembly through inline assembly lifting.	Recoules, F., Bardin, S., Bonichon, R., Mounier, L., Potet, ML.	

Table 17: Scientific Papers

#### 5.1.2 General & business publications

Partner	Title of Publication	Main Author
UNSPMF	Robot Task Allocation based on Greedy-Face-Greedy Algorithm, 27th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2019	J. Stanulovic, N. Mitton and I. Mezei
FORTH	TrustAV: Practical and Privacy Preserving Malware Analysis in the Cloud	Dimitris Deyannis, Eva Papadogiannaki, Giorgos Kalivianakis, Giorgos Vasiliadis, Sotiris Ioannidis

Table 18: Genera & Business publications

### 5.2 Events

It is a fact that the Covid-19 outbreak from December 2019 has greatly affected the dissemination planning with respect to the participation in and/or organisation of events. Thus, the dissemination activity for C4IIoT regarding events during the 1<sup>st</sup> year of the project has been poor.

### 5.2.1 Past Events

#	Partner	Title of Event	Type of Event	Date	Venue
1	FORTH, AEGIS	NIS Summer School 2019	Summer School	16/9/2019	Heraklion, Greece
2	FORTH	FORTH Researchers Night	Social Event	28/9/2019	Heraklion, Greece
3	FORTH	Codaspy 2020	Conference	16/5/2020	New Orleans, USA
4	UNSPMF	Weekly Seminar: “NB-IoT Testbed and Use Cases: Device Design and Experience with Real-World Operator Network”	Workshop	25/2/2020	Barcelona, Spain
5	ITML	ICT Proposers' Day 2019	Networking and information event	19.9.2019-20.9.2019	Helsinki, Finland
6	VIP	ICT/IoT workshop for Sales dept. in Vip mobile	Workshop	21/11/2019	Belgrade, Serbia
7	VIP	IoT Partner workshop	Workshop	20/11/2019	Belgrade, Serbia
8	VIP	IoT Partner workshop	Workshop	7/11/2020	Belgrade, Serbia
9	VIP	IoT Partner workshop	Workshop	14/11/2019	Belgrade, Serbia
10	VIP	IoT Partner workshop	Workshop	11/12/2020	Belgrade, Serbia
11	VIP	ICT/IoT workshop for Presales and Sales dept. in Vip mobile	Workshop	4/2/2020	Belgrade, Serbia
12	VIP	IoT Partner workshop	Workshop	28/02/2020	Belgrade, Serbia
13	UP1PS	2nd Summer School on Cyber Security for the Industrial Internet of Things	Summer School	Apr-22	Paris
14	CRF	Presentation of C4IIoT project internally to FCA	Presentation	28/02/2020	Melfi, Italy
15	IFAG, TSG	Trustech	Tradeshow and conference	26/11/2019	Cannes/France
16	IFAG	Startup Safari	Tradeshow and conference	23/10/2019	Munich/Germany
17	IFAG	Intergraf	Tradeshow and conference	23/10/2019	Copenhagen/Denmark
18	IFAG	NFC forum	Workshop	25/6/2019	Stuttgart/Germany
19	IFAG	Silicon Alps Security Week	Summit	18/9/2019	Graz/Austria
20	IFAG	Infineon Hackathon	Hackathon	12/11/2019	Villach/Austria
21	IFAG	Infineon's Banking Day	Workshop	25/9/2019	Munich/Germany
22	CEA	GDR Security Days	Workshop	12/06/2019-14/06/2019	Paris, France
23	CEA	Dagstuhl seminar on constraint solving for	Dagstuhl seminar	03/02/2019-06/02/2019	Dagstuhl, Germany

		security			
24	CEA	Formal methods for security (2 <sup>nd</sup> edition)	Workshop	18/03/2019	Paris, France

**Table 19: Past Dissemination Events****5.2.2 Future Events**

#	Partner	Title of Event	Type of Event	Date	Venue
1	STS	3rd International Conference - CyberSecurity4 Maritime - Oil & Gas - Energy	Conference (sponsored by STS)	TBD (moved to virtual format due to COVID-19)	Nicosia, Cyprus
2	VIP	ICT/IoT conference	Conference	August/September 2020	Nis/Serbia
3	VIP	ICT/IoT conference	Conference	November/December 2020	Belgrade/Serbia
4	VIP	IoT internal workshop	Workshop	July/August 2020	Belgrade/Serbia
5	VIP	IoT internal workshop	Workshop	November/December 2020	Nis/Serbia
6	VIP	IoT Partner workshop	Workshop	August/September 2020	Belgrade/Serbia
7	VIP	IoT Partner workshop	Workshop	October/November 2020	Belgrade/Serbia
8	VIP	IoT Partner workshop	Workshop	July/August 2020	Belgrade/Serbia
9	VIP	New ideas for ICT products	Hackathon	Q3/Q4 2020	Belgrade/Serbia
10	CRF	Innovative solutions in Industry 4.0	Workshop	TBA	Italy
11	AEGIS, FORTH	ICT 2020 – Leading the Digital Age	Conference	1-3 December 2020	Cologne/Germany

**Table 20: Future Dissemination Events**

## 6 Standardization activities

Standardization activities have always been one of the crucial pillars of technological progress, since standards constitute the vehicle that consolidates major research results and promotes their usability from industry and users.

A task related to standardisation is active throughout the project and more details reported in deliverable D6.4 "Exploitation and standardization activities and best practices – initial version". During the first year, the task has identified the organisations producing standards, directives and open-source software, relevant for the project. The task has also identified the technologies and architectures in use in the project which are based on standards or open source software. A research of the membership of each partner in the different organisations has also been done. Finally, a cross-table has been established to highlight the possible influence of C4IIoT in the standardisation organisations depending on the participation of the partners in them.

As a result of the investigation among the several standardisation working groups concerned, it appears that the presentation of the way of using a given standardised technology or a given open-source software is often possible in certain Working Groups. This presentation can also be performed on the form on the participation of the writing of white papers.

This way of dissemination is often possible on the condition of being a member of the organisation. In order to identify the main axes of dissemination towards these organisations, we summarise here the main parts of the C4IIoT framework.

The C4IIoT framework enables forecasting and detecting threats at the 3 different levels: hardware-enabled security; security enabled by horizontal device-to-device communication; and security enabled by machine learning-based behavioural analysis and cognitive capabilities.

- (1) **Hardware-enabled Security:** A Secure execution environment is built upon several partners' technologies, including FORTH's privacy-enhanced execution, IFAG's OPTIGA Trust X device for authentication and encryption, IFAG's OPTIGA TPM for secure booting and remote attestation and specific access control.
- (2) **Security enabled by horizontal device-to-device communication:** The Level-2 security is built upon multiple technologies brought by the partners, including IFAG's smart contracts management module and IBM's decentralized consent management.
- (3) **Security enabled by machine learning-based Behavioural Analysis and Cognitive Security capabilities:** Anomaly detection is done by implementing parallel and distributed instances of ML algorithms across all layers (edge nodes, field gateways, cloud) and coupling with decisions provided by the security offloading mechanism, to balance between reacting as quickly as possible and achieving an accurate detection.
- (4) **Global mitigation solutions:** Regarding the mitigation, the VARIAMOS tool proposes different reconfigurations of the whole targeted system, at least either by moving information flows away from the suspicious areas or by updating software of objects.

Therefore, the places to disseminate are the following:

- a) The Trusted Computing Group TCG is a place to disseminate because 2 partners are members of this SDO and especially because the technology of TPM of TCG is used in 1) regarding IFAG's TPM and in 4) the update of software in edge nodes can respect the last standard of TCG.
- b) Thales and IFAG are members of the TCG and can disseminate in TCG. Regarding the aspects of mitigation, they can even influence the versioning of "TCG Guidance

for Secure Update of Software and Firmware on Embedded Systems, the last Version 1.0, Revision 72 has been created on February 10, 2020.

- c) The Hyperledger Fabrik OSS is a place to disseminate as IBM is one of the founding members and especially because the smart contract management technology is especially used in the access control solutions of C4IIoT. It concerns the part 2) of the framework.
- d) Regarding 3) The IEEE P2805 Standards concern the Industrial Edge Computing and are being developed for defining protocols for self-management, data acquisition, and machine learning through cloud–edge collaboration on the EC Nodes s that bridge the gap between the physical world and the digital world by acting as smart gateways for assets, services, and systems. The organizations formed to promote edge computing in industrial applications include the OpenFogConsortium, OpenIOTFog and the Edge Computing Consortium.

The efficiency of the UOG MEDICI tool associated to the results of anomaly detection by machine learning from UNSPMF can be presented in these organisations.

More generally, a presentation of the way to share intelligence against cyber-attacks at the edge can be presented through the participation in the writing of whitepapers at the IEC Edge Computing WGs.

## **7 Short-Term future development and planning (M12 to M18)**

Following the goals planned and the achievements of the dissemination and communication strategy of C4IIoT during the first year of the project, the present section outlines the planned actions that will take place the following months (M12-M18):

- Development of website's Blog Page with content.
- Design and Development of YouTube Channel for the project.
- Face-to-face meetings with EAB members.
- Production of presentational/promotional videos.
- Organization of a series of events including Hackathons and Workshops.
- Presentations of the initial project result internally to each consortium member's organization.
- Collaboration with other EU projects and consortiums, etc.

During the second year of C4IIoT project, dissemination efforts will focus mainly on the more tangible assets available during that period such as the MVP. Moreover, considering the impact of the COVID-19 outbreak during the 1<sup>st</sup> year, online-based dissemination will be enhanced with organization of online events wherever possible.