Horizon 2020 Program

Dynamic countering of cyber-attacks

SU-ICT-2018

Cyber security 4.0: Protecting the Industrial Internet of Things

D6.4: C4IIOT Exploitation and standardization activities and best practices †

Abstract: This deliverable first describes the best practices and standards used by each partner at this step of the project. It then describes the possible routes towards the exploitation of the results, including the possible presentations of the results in the SDOs, depending on the participation of the different partners in these SDOs. Then it identifies the possible recommendations and influence in standardization.

Contractual Date of Delivery	31/05/2020
Actual Date of Delivery	27/05/2020 (revised version: 01/03/2021)
Deliverable Security Class	Public
Editor	*Antonio Escobar (IFAG)*
Contributors	All *C4IIoT* partners
Quality Assurance	*Giorgos Tsirantonakis (FORTH)* *Marine Eleftheria (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	Coordinator	EL
CENTRO RICERCHE FIAT SCPA	Principal Contractor	IT
INFINEON TECHNOLOGIES AG	Principal Contractor	DE
THALES SIX GTS FRANCE SAS	Principal Contractor	FR
HEWLETT PACKARD ITALIANA SRL	Principal Contractor	IT
COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	Principal Contractor	FR
IBM ISRAEL - SCIENCE AND TECHNOLOGY LTD	Principal Contractor	IL
AEGIS IT RESEARCH UG	Principal Contractor	DE
UNIVERSITE PARIS I PANTHEON-SORBONNE	Principal Contractor	FR
INFORMATION TECHNOLOGY FOR MARKET LEADERSHIP	Principal Contractor	EL
SPHYNX TECHNOLOGY SOLUTIONS AG	Principal Contractor	CH
UNIVERSITY OF NOVI SAD FACULTY OF SCIENCES	Principal Contractor	SRB
UNIVERSITY OF GREENWICH	Principal Contractor	UK
VIP MOBILE D.O.O.	Principal Contractor	SRB

Document Revisions & Quality Assurance

Internal Reviewers

1. *ITML, (Marine Eleftheria)*
2. *FORTH, (Giorgos Tsirantonakis)*

Revisions

Version	Date	By	Overview
1.1.2	26/02/2021	ITML	After midterm review version, first revision
1.1.1	26/02/2021	FORTH	After midterm review version, first revision
1.1.0	25/02/2021	IFAG	After midterm review version
1.0.2	27/05/2020	FORTH#2	Second revision.
1.0.1	25/05/2020	ITML#1	First revision
1.0	20/05/2020	IFAG	First version
0.5	05/05/2020	Thales	First draft

Table of Contents

List of Tables

List of Figures

N/A

List of Abbreviations

3GPP	3rd Generation Partnership Project
AIOTI	The Alliance for the Internet of Things Innovation
C4IIOT	Cyber security 4.0: Protecting the Industrial Internet of Things
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEH	Certified Ethical Hacker
COBIT	Control Objectives for Information and Related Technologies
CoAP	Constrained Application Protocol
COOLP	Constraint Object-Oriented Logic Programming
CSA	Cloud Security Alliance
CWE	Common Weakness Enumeration
DCA	Decentralized Access Control
DLT	Distributed Ledger Technologies
EC	European Commission
ECSO	European Cybersecurity Organization
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
GA	General Agreement
GSMA	Global System for Mobile Communications Association
HLF	Hyperledger Fabric
IEC	International Electrotechnical Commission
IEC-MSB	Market Strategy Board of the IEC
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IoT	Internet of Things
ISO	International Organization for Standardization
ISO/IEC JTC1	Joint Technical Committee of the ISO and the IEC
IT	Information Technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MQTT	Message Queuing Telemetry Transport
MQTT-SN	MQTT For Sensor Networks
NB-IoT	Narrowband-IoT
NIST	U.S. National Institute of Standards and Technology

OASIS	Organization for the Advancement of Structured Information Standards
ONF	Open Networking Foundation
OSSTMM	Open Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PKI	Public-Key Infrastructure
SDN	Software Defined Network
SDO	Standards Developing Organization
TCG	Trusted Computing Group

Executive Summary

This deliverable is a joined reporting of the Task 6.3 (Exploitation activities), started in December 2019, and of the Task 6.4 (Standardization activities and best practices), started in June 2019.

It identifies the plan to make the project exploitable by all partners, and especially through the means of guidelines and through the leverage of standardization promoted by different European and international organizations.

It consists on an identification of the directives, open source software and standards in close relation with C4IIoT; these used by the partners in their respective technical contribution and the more relevant for the C4IIoT innovations. It underlines the organizations in which at least one of the partners is member and therefore can bring contributions.

Before a full exploitation plan, due at the end of the project, the initial version of this deliverable also provides the individual exploitation plans of each partner.

1 Introduction

1.1 Purpose of the document

The current deliverable (D6.4: Exploitation and standardization activities and best practices – initial version, due in M12), provides the initial list of relevant standardization bodies, alliances and associations, in which the C4IIoT partners either participate or follow, due to their close alignment with the project's goals.

Starting with the European standards cited in the GA, a comprehensive list of relevant international entities is provided, as a first index of bodies that we must closely follow and, when possible, comply with.

After that, the partners detail their contribution in the overall standardization effort, with a focus on enforced standards, applied recommendation and relevant entities in which they participate.

A follow-up of the compliance with the identified shall be provided in the final version of the deliverable (D6.5, due in M24).

Moreover, a detailed (per partner) description of the exploitation efforts is provided, and it should also serve as the basis for a comprehensive and ambitious exploitation plan in the final version (D6.5).

1.2 Relationship with other deliverables

The exploitation plans defined in this deliverable are closely linked to the market opportunities previously identified in *D6.2 – Market analysis and preliminary business modelling (M4)*, and have a strong influence on the dissemination strategy, preliminarily defined in *D6.3 – Interim Version of Dissemination strategy and activities (M12)*. This deliverable will be completed, in particular the joint exploitation plan, in *D6.5 – Exploitation and standardization activities and best practices – final version (M24)*.

1.3 Structure of the Document

The body of the current document has the following structure:

- In *Section 2*, standards of special relevance for the C4IIoT project are identified.
- In *Section 3*, every partner individually defines the guide lines, best practices and standards they follow, or plan to follow, during the project lifetime.
- In *Section 4*, the individual exploitation plans of every partner are presented.

2 Identification / Classification of main standards for C4IIoT

In order to distinguish the standards and directives used by C4IIoT and the possible influence of C4IIoT in SDOs, one can classify the SDOs in 2 categories: the organizations which define technology standards and the SDOs which are application specific, these SDOs are in C4IIoT mainly those related to the manufacturing or logistic security aspects. While C4IIoT uses the technology standards already defined without directly modifying them, C4IIoT will hopefully be able to influence the second category of SDOs through dissemination actions, for example thanks to the participation to whitepapers.

In the following subsections we will address the European and International standards, which we want to closely follow due to their special relevance for the C4IIoT project.

2.1 European standards cited in the GA

ENISA: Since 2004, ENISA supports the pan-European Cybersecurity Exercises, the development and evaluation of National Cybersecurity Strategies and the CSIRTs cooperation. It performs studies on IoT and smart infrastructures, addressing data protection issues, privacy enhancing technologies and privacy on emerging technologies, eIDs and trust services, identifying the cyber threat landscape, and others. It assures the development and implementation of the European Union's policy on matters relating to network and information security and assists the European institutions in establishing and implementing vulnerability disclosure policies on a voluntary basis. Since 2019, it draws up cybersecurity certification schemes.

FORTH and HPE are members of ENISA.

AIOTI: The AIOTI (Alliance for Internet of Things Innovation) is a partner for the European Commission on IoT policies and programs, helping to the deployment of IoT Innovation in Real Scale Experimentation in Europe. It is a member driven organisation with equal rights for all members. The document published by the WG3 in October 2019 “IoT LSP Standard Framework Concepts” provides a list of IoT Standards Developing Organisation (SDO), Alliance and Open Source Software (OSS) landscapes to be used as input for the recommendations for Large Scale Pilots (LSPs). In addition to the WG3 on IOT standardization, the topic of the WG11 is “Smart Manufacturing” and the topic of one horizontal WG is on Distributed Ledger Technologies. The Distributed Ledger Technologies WG is working on mapping current Blockchain implementations, rate the models toward current legal compliance (incl. GDPR), assist all existing AIOTI WG’s on Blockchain implementations and develop Blockchain ecosystems across verticals.

IBM, IFAG and CEA are members of AIOTI. In particular, IFAG is a founding member, while also being very active in the Distributed Ledger Technologies Working Group.

ETSI: The European Telecommunication Institute works in different types of committees: TC (Technical Committees) addressing standardization activities in a specific technology area, Projects (EP) similar but established for a fixed period of time, ETSI Partnership Project established when there is a need to cooperate with other organizations to achieve a standardization goal and Industry Specification Group (ISG) focusing on a specific activity.

Several ETSI committees provide opportunities to demonstrate and validate proposed standards and to contribute project results to them. The TC CYBER works to develop standards that increase privacy and security by means of practices applicable across different domains, IOT security is one of them.

ECSO: The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016. ECSO is the private counterpart to the European Commission in implementing the contractual Public-Private Partnership (cPPP) on cybersecurity. We unite a variety of European cybersecurity stakeholders across the EU Member States, the European Free Trade Association (EFTA) and H2020 Programme associated countries. ECSO's main goal is to develop a competitive European cybersecurity ecosystem, to support the protection of the European Digital Single Market with trusted cybersecurity solutions, and to contribute to the advancement of the European digital autonomy.

FORTH, Thales and CEA are members of ECSO.

2.2 International standards

IEC- MSB: In the IEC, the Market Strategy Board (MSB), has established whitepapers closely related to C4IIoT: *IoT 2020: Smart and secure IoT platform, Factory of the future* and *Edge intelligence. IoT 2020: Smart and secure IoT platform* provides an overview of where IoT currently stands, identifies IOT system designs, architecture patterns and the deficiencies of the current IoT frameworks, especially in terms of security.

ISO/IEC JTC1 is a Jointed technical committee of ISO and IEC created to promote standards in the fields of Information Technology and Information and Communication Technology. The interesting subgroups related to IOT are WG3 on IOT architecture, WG4 on IOT interoperability and WG5 on IOT applications.

ISO/IEC JTC1 WG5 deals with standardization in the IOT applications and considers societal aspects of IOT with new technologies such as Blockchain, Artificial Intelligence and Cloud/Edge technologies

ISO/IEC JTC1/SC41 jointly works with ISO/IEC JTC1/SC27 Information security, cybersecurity and privacy protection for the security and privacy related standards for IOT.

The international Standard: ISO/IEC 27030 “Guidelines for security and privacy in IOT” is being developed under ISO/IEC JTC1/SC27

ITU-T is the United Nations specialized agency for ICTs. The most interesting Study Groups for C4IIOT are:

SG20: This Study Group initially focus on IOT applications and Smart cities communities. This SG put forward the vision of IOT in Recommendation ITU-T-Y.2060 with a study of end-to-end architectures for IOT and is defining application specific reference architectures in particular in smart manufacturing.

SG17: Security: This Study Group coordinates security-related actions across all ITU-T SGs together with a broad range of standardization issues. It is working for the security of applications and services for the IOT and the smart grid.

SG 13: This Study Group has produced ITU-T Y.2060, a standard which identifies IoT functional characteristics, high-level requirements and an IoT reference model

IETF: Internet Engineering Task Force is an open international community of network designers, operators and researchers concerned with the evolution of the Internet architecture at different layers. The IRTF (Internet Research Task Force) is a parallel organization focusing on longer term research issues. The technical work is done in Working Groups (Research Groups for IRTF) organized by topic into several areas. Much of the work is done by mailing lists, while meetings take place 3 times per year. An IETF standard is published as a Request for Comments (RFC), and it starts out as and Internet Draft (ID). Several IETF working groups, spanning multiple Areas are developing protocols that are directly relevant to the IoT on the communication and security aspects. These protocols are used by a variety of companies, as well as IoT standards organizations and alliances, to build and specify interoperable systems. Due to the distributed nature of IoT protocol development and use, there is often need for coordination across different groups working on IoT. The IETF IoT Directorate is an advisory group of experts selected by the IETF Area directors and the IoT Directorate Chairs. The main purpose of the IoT Directorate is coordination within IETF on IoT-related work and increasing the visibility of IETF IoT standards visibility to other standards development organizations (SDOs), industry alliances, and other organizations. A post from the IETF Blog provides an overview of IoT-related work underway within the IETF.

IEEE P2805 Standards are being developed for defining protocols for self-management, data acquisition, and machine learning through cloud–edge collaboration on ECNs. IEEE P2805.3 - Cloud-Edge Collaboration Protocols for Machine Learning is accessible via subscription only, but would be precious for C4IIOT.

OneM2M brings together several major ICT SDOs around the world, such as ARIB (Japan), ATIS (North America), CCSA (China), ETSI (Europe), TIA (North America), TSDSI (India), TTA (S. Korea) and TTC (Japan).which share the objective of developing common standards for a common service layer that applies across different industry segments. The Partners have acted strategically to achieve a much-needed convergence in the IoT standards landscape. Instead of developing IoT standards individually and for their local markets, they agreed, in 2012, to collaborate through the oneM2M partnership project. To promote oneM2M, they facilitate the development and publication of oneM2M specifications as their own standards.

TCG: Trusted Computing Group. The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry specifications and standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. TCG's core technologies include specifications and standards for the Trusted Platform Module (TPM), Trusted Network Communications (TNC) and network security and self-encrypting drives. TCG also has work groups to extend core concepts of trust into cloud security, virtualization and other platforms and computing services from the enterprise to the Internet of Things. Trusted Computing Group announced that its TPM 2.0

(Trusted Platform Module) Library Specification was approved as a formal international standard under ISO/IEC. TCG has published the "TCG Guidance for Secure Update of Software and Firmware on Embedded Systems Version 1.0 Revision 72" on February 10, 2020 which can be used to leverage the mitigation in case of malware detection in a specific IOT or edge node.

Thales and IFAG are members of TCG, with IFAG being one of the world leader suppliers of TPM2.0 solutions.

IIC: Industrial Internet Consortium. The Industrial Internet Consortium (IIC) was founded in March 2014 to bring together the organizations and technologies necessary to accelerate the growth of the industrial internet by identifying, assembling, testing and promoting best practices. The Industrial Internet Consortium (IIC) focuses on industrial application of the IoT, such as in the manufacturing domain. The IIC Security Working Group has published the important IIC:PUB:G4:V1.0:PB:20160926 IIC Volume G4: *Security Framework*, which purpose is to identify, explain and position security-related architectures, designs and technologies, as well as identify procedures relevant to trustworthy IIoT systems. It describes their security characteristics, technologies and techniques that should be applied, methods for addressing security. The *Industrial Internet Reference Architecture* (IIRA) is a blueprint for building Industrial Internet systems. It outlines a standards-based open-architecture framework template and methodology for designing an IIoT system. It is important to consider for the Smart Factory Use-case.

OASIS was founded under the name "SGML Open" in 1993 as a consortium of vendors and users devoted to developing guidelines for interoperability among products that support the Standard Generalized Markup Language (SGML). The consortium changed its name to "OASIS" (Organization for the Advancement of Structured Information Standards) in 1998 to reflect an expanded scope of technical work.

There are several active OASIS Technical Committees linked to C4IIoT innovations:

"Extensible Access Control Markup Language (XACML)" which represents and evaluates access control policies.

"*Message Queuing Telemetry Transport (MQTT)*" which provides a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.

"PKCS 11" which enhances PKCS #11 standard for cryptographic tokens controlling authentication information (personal identity, cryptographic keys, certificates, digital signatures, biometric data)

"Message Queuing Telemetry Transport (MQTT)" which provides a lightweight publish/subscribe reliable messaging transport protocol suitable for communication in M2M/IoT contexts where a small code footprint is required and/or network bandwidth is at a premium.

Thales and IBM are represented at OASIS

NIST. The National Institute of Standards and Technology (NIST) is a physical sciences laboratory, and a non-regulatory agency of the United States Department of Commerce. Its

mission is to promote innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.

Of special relevance for the project are the publications regarding Cyber-Physical Systems and Internet of Things[1] and Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks[2]. The purpose of these publications is to help federal agencies and other organizations better understand and manage the cybersecurity and privacy risks associated with their individual IoT devices throughout the devices' lifecycles. These publications are the introductory documents providing the foundation for a planned series of publications on more specific aspects of this topic.

3GPP. The 3GPP covers cellular telecommunications technologies, including radio access, core network and service capabilities, which provides a complete system description for mobile telecommunications. The 3GPP specifications also provide hooks for non-radio access to the core network, and for interworking with non-3GPP networks[3].

IEEE 802.1 Time-Sensitive Networking (TSN) is a set of standards under development by the Time-Sensitive Networking task group of the IEEE 802.1 working group. The standards define mechanisms for the time-sensitive transmission of data over deterministic Ethernet, designed to meet production and safety requirements.

GSMA: The GSMA represents the interests of mobile operators worldwide and the GSMA's Internet of Things Program is an industry initiative to accelerate the delivery of secure IoT solutions enabling consumers and businesses to harness a host of rich new services, connected by intelligent and secure mobile networks.

The GSMA has delivered a set of IoT Security Guidelines, backed by an IoT Security Assessment scheme, to provide a proven and robust approach to end-to-end security.

Thales and Telstra, the main Australian telecom company are working with Microsoft and Arduino to offer evolutive security of connected IOT devices through one solution allowing a trusted communication between the devices and the cloud. The solution allows mutual, instantaneous, standardized authentication between secure object and one cloud platform through cellular network in conformity with security specifications "IOT SAFE" of GSMA.

VIP is member of GSMA.

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf

[2] https://csrc.nist.gov/publications/detail/nistir/8228/final

[3] https://www.3gpp.org/news-events/3gpp-news/1805-iot_r14

3 Best practices and standards used in the C4IIOT architecture

3.1 FORTH

N/A

3.2 CRF

N/A

3.3 IFAG

IFAG's main contribution to the project, the hardware security elements, are standardized by the Trusted Computing Group (TCG), and follow the Trusted Platform Module (TPM) 2.0 specification.

In addition, all the cryptography algorithms used by IFAG's security elements are also standardized. In particular, the proposed PKI infrastructure follows the X.509 from ITU-T, and the NIST P-256 ECC curve to sign the data.

Moreover, IFAG supports the usage of IBM's standard blockchain: Hyperledger Fabric, by integrating and fostering the usage of IFAG's TPM as a hardware wallet to securely store the user's credentials, following the PKCS#11 standard, from OASIS.

Within the project, and together with IBM, IFAG plans to advance in the efforts to standardize the mechanisms that define the interaction between hardware security elements and blockchain technologies.

3.4 Thales

Thales contribution to C4IIoT includes the SDN controller, which communicates through appropriate switches and appropriate routers using the OpenFlow protocol elaborated by the ONF (Open Networking Foundation).

OpenFlow is a communication protocol which gives remote access to the forwarding plane of a switch or a router, standardized by the ONF. The main idea is to administer the forwarding plane of the network equipment by a separate machine: the controller. It was developed in the spirit of Software Defined Networking and has been transferred to the Open Networking Foundation.

SDN indeed lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.

In C4IIOT the SDN controller is used as a mitigation action in order to move away the information flows from a suspicious area in the network.

3.5 HPE

The scope of the C4IIoT project is very broad and touches various aspects of security both in the IoT and IT fields, and in different parts of the industrial area, including Safety.

More generally, it deals with numerous transversal consortia and work groups that work to create reference standards and make technologies more open in the IoT world.

With this premise, we would like to address the aspects of standardization following what the consortia and organizations indicate.

In this chapter, we will introduce a set of standards that cover the security aspects of C4IIOT, used as a point of reference for evaluating security or level of quality of the components.

The benchmarks will be derived from the company/entity that composes the C4IIOT consortium based on the respective experience and on the market standards.

The main objective is to try to provide the indications to reduce the attack surface of the C4IIOT technologies, leveraging on the standards currently available and to trying to follow the suggestions, rules, and best practices that they define.

As we know the cyber threats are becoming more active for the industrial and automation systems: security-by-design is key.

The first standard that we would like to introduce is the IEC 62443 standards that allow covering part of the ICS domain and IACS.

This standard suggests best-practices for:

- adequate level of security against external threats;
- increase the level of data protection
- increase the reliability of the systems.

It works at different levels and components:

- Industrial Control Systems (ICS) and Distributed Control Systems (DCS).
- Programmable Logic Controllers (PLCs).
- Remote Terminal Units (RTUs).
- Intelligent Electronic Devices (IEDs).
- Supervisory Control and Data Acquisition (SCADA).
- Networked Electronic Sensing & Control and Monitoring & Diagnostic Systems (SIS).

Moving on to the IT field, we, of course, mention the ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems as main asset where we can leverage.

The Information security standards, like ISO/IEC 27001:2013 Information security management systems – Requirements, Code of practice for information security controls, will help to identify if all the security gaps are covered, we think that in this kind of project where no payment is involved, the PCI/DSS could not be involved.

For security benchmark and standards at the cloud level we refer to CSA (Cloud Security Alliance) and, if appropriate, the ISA 99 / IEC 62443 (Standards Address Industrial Security).

Generally, also debatable, if personal information is involved in C4IIOT, we suggest to follow the GDPR directive and relate to privacy regulation. To consider that in in the EU the GDPR does not replace the local regulation, as instance the “Italian Privacy Law D.lgs 196/2003” update to D.lgs 101/2018 or the German Bundesdatenschutzgesetz (BDSG).

Related to privacy area, valid inputs come from the ISO/IEC 29100:2011 Privacy framework, ISO/IEC 29101:2013 Privacy architecture framework and CEN CWA 16113:2010 Personal Data Protection Good Practices.

It is also worth mentioning, regarding security assurance mechanisms and quality control, the following standard: Vulnerability Assessment (VA). We also have the methodological foundation in the ITSEC and Common Criteria (ISO 15408) standards used internationally, which provide a common reference framework. The framework applies both if the assessment is configured as a "Zero Knowledge" or black-box type activity, i.e. without knowledge of the services present or access credentials, whether it is a white-box type, i.e. with detailed documentation of the modules and available services. We will adopt the OWASP methodologies (Open Web Application Security Project), CWE (Common Weakness Enumeration), OSSTMM (Open Source Security Testing Methodology Manual) and the practices of Ethical Hacking CEH (Certified Ethical Hacker).

Related to authentication we follow the RFC standard related to the X509.v3 and the PKI. In cryptography, X.509 is a standard defining the format of public-key certificates. There are several RFC starting from the RFC5280 that help the C4IIOT in this area and we closely follow.

3.6 CEA

N/A

3.7 IBM

IBM's contribution to C4IIoT includes designing and developing a decentralized access control (DAC) solution. One of the DAC's key elements is the Hyperledger Fabric (HLF), which is an open source project of a permissioned blockchain infrastructure with modular architecture, allowing to manage consensus and trust among different entities.

HLF is part of the Hyperledger open source community started by the Linux Foundation. IBM teams have contributed and are continuing to contribute to the HLF project.

In C4IIoT, IBM plans to use the HLF to enable auditability of various events, such as when generating data items (e.g. sensor readings by IoT devices), when storing data at a persistent cloud storage service, and when issuing alerts or insights by the analytics. Access policies to data items, determined by the data generators themselves, will also be logged in the ledger. In addition, HLF will be used to assure the integrity of data stored on the cloud storage, by having the data generators document the hash of the data in the tamper-proof ledger upon data creation.

To support the above, IBM will deploy HLF network and set up HLF channel, to allow maintaining a distributed ledger in C4IIoT. This channel will consist of HLF peer nodes (each storing a copy of the ledger) and ordering nodes (used to create and distribute new blocks).

The open source HLF SDK, that allows applications to interact with HLF network, will be used by IBM to develop HLF client for the various C4IIoT entities to use in order to write and read records from the distributed ledger.

3.8 AEGIS

N/A

3.9 UP1PS

UP1PS is responsible for the VariaMos component in charge of modelling and searching the space of possible network reconfigurations that can mitigate threats alerts triggered by the anomaly detection components. It is a sub-component of the top-level cloud-deployed mitigation engine component. The result of its search is a set of possible reconfigurations ranked in order of their business impact in terms of trading-off security with other non-functional requirements such as safety, availability and confidentiality.

The possible reconfiguration actions include traffic rerouting among network switches and hosts and modification of the application software stack running on the hosts. The formers are to be carried out by leveraging an intent-based northbound API provided by TGS' Software Defined Network (SDN) controller component of the mitigation engine. The latter are to be carried out by leveraging HPE's container orchestrator component.

The rank mitigation plans resulting from the search carried out by VariaMos will be passed to AEGIS' security dashboard user interface component as proposals for the factory security manager to choose from. In addition to traffic rerouting and software reinstallation actions, it may also include actions to be carried by factory security employees such as firmware reinstallation on edge devices or physical actions.

The threats and mitigations modelled by VariaMos will be largely inspired from those specified in recommendations published by ENISA and the Cybersecurity Framework from the US National Institute of Standards and Technology (NIST).

VariaMos models and searches the configuration space uniformly within the *Constraint Object-Oriented Logic Programming (COOLP)* paradigm. It allows making the model simultaneously modular, formally verifiable, executable and testable. This approach allows circumventing the introduction of errors in the traditional translation step of a formally verified but non-executable model into executable code. It also allows leveraging the highly optimized state-of-the-art search algorithms built in COOLP platforms.

3.10 ITML

N/A

3.11 STS

3.11.1 Assurance Profiles

The Common Criteria for Information Technology Security Evaluation (Common Criteria or CC[4]) is the technical basis for an international agreement (namely the Common Criteria Recognition Arrangement (CCRA)) which ensures that:

- Items can be assessed by skillful and autonomous authorized research centers in order to decide the satisfaction of specific security properties, to a certain extent or assurance.
- Supporting documents, are utilized inside the Common Criteria accreditation procedure to characterize how the criteria and assessment strategies are applied while guaranteeing explicit innovations.
- The certification of the security properties of an assessed item can be given by various Certificate Authorizing Schemes, with this certification being founded on the consequence of their assessment.
- These certificates are recognized by all the signatories of the CCRA.

As part of the monitoring assessment, Security Targets and/or Protection Profiles[5] (i.e. the generic form of the former) are taken into consideration in order to construct the certification process and the monitoring rules.

3.11.2 Security Standards, processes and common terminology

The common objective of each information security assurance schemes is to provide some form of assurance that sensitive data is effectively protected. As part of the security assurance provided by STS' platform, the following security standards, processes and terminologies are taken into consideration.

Holistic standards take a general, risk-based approach to information security by endorsing controls that legitimately neutralize an association's characterized security risks. More specifically:

- ISO/IEC 27001:2013[6] is the international quality standard for Information Security Management. It assists with guaranteeing that satisfactory controls addressing the CIA triangle (i.e. confidentiality, integrity and availability) of information are set up to defend the information of interested parties.
- NIST Special Publication 800-53 rev. 5[7] is a holistic information security standard developed by NIST. It is a set of standards and guidelines to help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA).
- COBIT (Control Objectives for Information and Related Technologies) [8] is a holistic organizational security and integrity framework created by Isaca, which utilizes

[4] https://www.commoncriteriaportal.org/

[5] https://www.commoncriteriaportal.org/pps/

[6] https://www.iso.org/isoiec-27001-information-security.html

[7] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft

[8] https://www.isaca.org/resources/cobit

processes, controls objectives, management guidelines, and maturity modelling to ensure alignment of IT with business.

- ISO/IEC 27002:2013[9] provides best practice recommendations on information security management.
- ENISA Threat Landscape[10] provides an overview of threats together with existing trends. The document is based on publicly available data.
- Common Vulnerabilities and Exposures (CVE)[11] is a list of publicly disclosed computer security flaws. The list is overseen by the MITRE Corporation and is used by the assurance platform to initiate the baseline vulnerability analysis of the existing assets.

General Data Protection Law (GDPR)[12] is the core of Europe's digital privacy legislation. As part of STS' asset identification, GDPR is taken into consideration both in state of the identified data and the role of a person (i.e. controller, processor, DPO).

3.12 UNSPMF

UNSPMF is responsible for designing and fabricating IoT edge devices for the logistics use case. In the logistics use case, C4IIoT edge devices require IoT connectivity across wide areas to cover the needs of, e.g., tracking and monitoring large containers transported by trucks. C4IIoT uses latest low-power wide area networks (LP-WAN) communication standard delivered by mobile cellular 3rd Generation Partnership Program (3GPP) standardization called Narrowband-IoT (NB-IoT), which offers wide area connectivity reaching all devices which are covered by the mobile operator network (and even more, as NB-IoT extends coverage of standard 4G LTE signal for remarkable additional 20dB thus reaching underground locations and wide rural coverage). Compared to previous wide area solutions such as frequently used GPRS modems, NB-IoT offers, besides larger coverage, dramatically smaller energy consumption of IoT edge device, huge number of edge devices being able to connect to a single macro-cellular base station (up to 50.000, while this number for GPRS modems is less than 100), smaller footprint of edge devices, and many others.

From the application point of view, NB-IoT module providers provide standardized application programming interface (API) defined by the 3GPP as "AT command set for the user equipment" [13]. For the data delivery between edge device and application, there are Non-IP or IP-based data delivery options. Chipset providers recommend designers to use IP-based data delivery in order to be network-agnostic. For the IP-based data delivery there are several standardized options which could be divided into REST-based and Publish/Subscribe-based protocols. REST-based has options for HTTP (standardized by IETF [14]) over TCP (standardized by IETF[15]) protocols

[9] https://www.iso.org/standard/54533.html

[10] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

[11] https://cve.mitre.org/

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

[13] 3GPP, "AT command set for User Equipment (UE)," Technical Specification (TS) 27.007, 3rd Generation Partnership Project (3GPP), 6 2018. Version 15.2.0.

[14] HTTP protocol, https://tools.ietf.org/html/rfc2616

[15] Transmission control protocol, https://tools.ietf.org/html/rfc793

or CoAP (standardized by IETF[16]) over UDP (standardized by IETF[17]), while Publish/Subscribe-based protocols has MQTT (standardized by OASIS[18] and ISO/IEC[19]) over TCP and MQTT-SN (specified by IBM[20]) over UDP. Main advantage of the UDP based transfers is that it has the lowest overhead compared to TCP based transfers. Accordingly, UNSPMF team opted for the UDP data delivery being the most energy efficient.

3.13 UOG

N/A

3.14 VIP

Vip mobile is member of GSMA. The mobile telecommunications industry, which the GSMA represents, has a long history of providing secure products and services to customers. The GSM Association security guideline[21] describes currently available solutions, standards and best practices, regarding IoT Services.

Vip mobile also follows COBIT Security guidelines[22], related to IT security, which allows us to provide secure services to our customers. COBIT covers cybersecurity in addition to other risks that can occur with the use of IT. Vip mobile follows ISO 27001 related to Security of any digital information and ISO 27002 related to best practices for securing digital information.

[16] The Constrained Application Protocol (CoAP), https://tools.ietf.org/html/rfc7252

[17] User datagram protocol, https://tools.ietf.org/html/rfc768

[18] Message Queuing Telemetry Transport (MQTT) v5, https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html

[19] Message Queuing Telemetry Transport (MQTT) v3.1.1, ISO/IEC 20922, https://www.iso.org/standard/69466.html

[20] MQTT-SN specification, https://www.mqtt.org/new/wp-content/uploads/2009/06/MQTT-SN_spec_v1.2.pdf

[21] Official Document CLP.14 - IoT Security Guidelines for Network Operators

[22] www.isaca.org/cobit

Partner	Enforced Standard	Applied Recommendations	Participation
FORTH			ECSO, ENISA
HPE	X.509	CC ISO15408, OWASP, OSSTMM, CEH, IEC62443, ISO/IEC27001:2013, ISA 99 / IEC62443, GDPR, ISO/IEC 29100:2011	CSA, ENISA
IFAG	X.509, PKCS#11, NIST P-256, TPM	-	TCG, AIOTI
Thales	ONF		TCG, ECSO, OASIS
CEA			AIOTI, ECSO
IBM	HLF		HLF, AIOTI, OASIS
UP1PS		ENISA, NIST	
STS	ISO/IEC 27001, ISO/IEC 27002	CC ISO15408, CVE	
UNSPMF	3GPP NB-IoT	MQTT-SN, CoAP	
VIP	ISO27001, ISO27002, NB-IoT	COBIT	GSMA

Table 1: Summary of Standards/Recommendations used in C4IIOT per Organization

4 Standardization Plan

The duration of a H2020 project is hardly compatible with the full achievement of a standardization activity, given that valuable innovation is far from being achieved at the beginning of this project.

For this reason, the standardization activities within the sole C4IIOT project will often consist in the writing of recommendations to the most active appropriate committees and this standardization plan will also include the open-source contributions.

Joint standardization activities have also been considered in collaboration with other projects of the same H2020-SU-ICT-2018 call. Part of these projects focus on cybersecurity in other vertical domains, CyberSANE for Critical Infrastructures (starting from a threat taxonomy based on ENISA), Caramel: for connected vehicles, GUARD for digital services chains. Three other projects focus more on the methods and tools: SAPPAN: a platform for sharing and automation to enable privacy preserving and efficient response and recovery, utilizing advanced data analysis and machine learning; SIMARGL with advanced methods for recognition on malware; SOCCRATES with attack/defense graphs.

During a joint meeting with these projects, valuable advices have been provided by Dr. Vasileios Mavroeidis with regard to the SDOs and the way to raise a Technical Committee, even if it remains a long-term activity. His advice is to focus on OASIS for its facility of participation and even of raising a specific technical committee. We could also consider raising a WG inCSA, while the lifecycle of CSA WG is well explained on the CSA website. However, today a joint standardization plan has not yet been firmly fixed, and today we will only provide a perspective.

4.1 Standardization and open source contributions specific to C4IIOT.

To elaborate a standardization plan specific to C4IIOT, we start with the main innovations in which we extract the items that may be the purpose of standardization and the items that have given rise to an open source contribution. We do the same with other topics of the framework.

C4IIOT main innovation lies in:

1. Edge-field gateway-cloud anomaly detection orchestration
2. Encrypted network traffic analysis
3. Patch-oriented-testing methods for binary code
4. Edge node design enabling a high degree of hardware-enabled security
5. Search for the best mitigation from a close knowledge base of threats and remediation plans
6. Usage of the Decentralized blockchain-based solution

Other topics essential to the framework reside in the toolkits for:

- Security assurance
- Visualization
- Software defined control of the infrastructure
- Mobile operator security

Innovation 1 Edge-field gateway-cloud anomaly detection orchestration

We will try to exploit the full methodology to build a recommendation in a SDO related to Cyber Detection in IIOT and/or an application of federated learning in a SDO targeting IA and Cybersecurity. We are targeting the Joint activities of ESO and BDVA that are planned to start

in 2021 and possibly the participation in the writing within the IOT WG of the Cloud Security Alliance the V3 of the "Guide for the Security Controls Framework[23]".

Moreover, UNSPMF through its relations with ETSI and more especially the Industry Specification Group "Multi-Access Cloud Computing" (MEC) will try to influence the standard with the solution offered at C4IIOT.

Innovation 2 Encrypted network traffic analysis

The code for the encrypted network traffic analysis tool will be made public using an open source license through the Zenodo C4IIoT community. along with the signatures to match malicious traffic. The code is written in python3 which facilitates the integration in OT environments and the dpkt and pcapy libraries for packet capture and parsing. Regarding alert generation, it utilizes JSON with Apache Kafka.

Innovation 3 Patch-oriented-testing methods for binary code

Many bugs can be transformed into cybersecurity exploits with serious consequences. This is in particular the case for memory corruption errors, which are both pervasive and with the highest consequences. For instance, at Microsoft ``70% of the vulnerabilities addressed through a security update each year continue to be memory safety issues". In addition to being pervasive, those vulnerabilities are also of the highest severity, as they can allow an attacker to create exploits going as far as remote control over the computer.

Fuzzing has recently rose into prominence in both academia and industry. Coverage-based Greybox Fuzzing are practical tools that leverage code coverage information in order to guide input generation toward new parts of the program under test, exploring as many program states as possible in the hope of triggering crashes.

This use can be complemented by Directed Greybox Fuzzing (DGF) which aims to perform stress testing on pre-selected potentially vulnerable target locations, with applications to different security contexts: (1) bug reproduction, (2) patch testing or (3) static analysis report verification.

Fuzzers are much easier to use at the binary level, as source codes for security-critical programs are not always available or may rely partly on third party libraries.

CEA's BINSEC work addresses the usage of Directed Greybox Fuzzing at the binary level, and should thus be recommended as a cybersecurity solution.

Innovation 4 Edge node design enabling a high degree of hardware-enabled security

C4IIoT enables hardware security devices, which add a security layer to the architecture. The use of secure elements on the edge nodes provide a robust solution and makes the technologies implemented above fall back on these devices offering a root of trust. Software alone is not enough to protect embedded systems as it can be read, copied and distributed with relative ease. Secured hardware is needed to reliably store data and software code, detect manipulation and encrypt data for safe storage and processing. A hardware-based root of trust must be established to render embedded software trustworthy.

There is no contribution to open source in the smart factory use case since the software used is open source and IFAG does not add or modify anything related to the software, while in the logistic use-case, the code related to the OPTIGA Trust M is released as open source with MIT License.

[23] Cloud Security Alliance: https://cloudsecurityalliance.org/

Innovation 5 Search for the best mitigation

CARMAS will be possibly released as an open-source tool outside the C4IIoT consortium, depending on a possible joint commercial exploitation through its integration with DISCO and potentially also FORTH's Encrypted Traffic Analyzer, STS Security Assessment Module and AEGIS Advanced Visualization Tool.

Innovation 6 Usage of the Decentralized blockchain-based solution

Recommendations of the context of usage of the Digital Ledger Technology with secure element will be provided in the most appropriate SDOs. In particular IFAG, will try to influence in different standards in the frame of the C4IIoT project where its main contribution focus to the use of secure elements joint with DLT. IFAG will try to have an influence on blockchain standards and also on the use of secure elements in these standards.

There are still no standards catering to the mass implementation of blockchain and it is very important to start to create some standardization activities to ensure a sustained survival of the DLTs. Standardization activities are very important to accelerate the implementation of the technologies such as blockchain, especially in the early stages when the technologies are trying to break into the market.

Although there are a large number of blockchain-related standards documents developed by standardization authorities, these documents provide an introduction or starting point for implementing blockchain technologies. There is a lack of more in-depth material on technical issues, this is expected to be achieved in the future with the integration of decentralized technologies. Within the C4IIoT project, we will try to influence these standards and publish new documents, an outcome is expected from the M24 in deliverable D6.5: “Exploitation and standardization activities and best practices – final version”.

In particular, in the last part of the project, we will try to influence standardization authorities to link blockchain technologies with hardware security, which at the present time does not seem very close, since a certain maturity in blockchain-related standards must be reached.

Topic a Security Assurance

While the Security Assurance Module integrated within C4IIoT is based on proprietary technologies developed in-house by STS, the model-based approach to security assurance and certification at the heart of said module, possibly in tandem with the model-based mitigation approach introduced by C4IIoT Innovation 5 (see above), can be promoted for standardization.

More specifically, the above two C4IIoT building blocks highlight the benefits of adopting a model-based approach to security (and privacy, by extension) assessment, certification and mitigation. In both cases, an underlying model is specified that defines all key elements (e.g., assets, threats, vulnerabilities, controls), the properties of said elements, and their relationships. The definition of such a model, although a complex process, can provide a structure that allows for modelling different types of environments (a model that is, by definition, extensible, will allow for future extensions and refinements to ensure that all use cases can be modelled) and enables the integration of results from different types of assessments, providing an accurate report on the security and privacy posture of any environment (from a high-level risk-oriented view, to a lower-level technical view), allowing for the generation of needed evidence (e.g., for certification), while also facilitating the response to detected incidents, by encompassing in the model the effects of attacks, controls and defense strategies.

Topic b Visualization

For the development of the Advanced Visualization Toolkit, Angular web framework is used combined with a web server written in Node.js. Both platforms are open source and for both platforms the ways to contribute are the same as any open-source application: raising questions on the official repositories, reporting issues, code contributions, or even by becoming a collaborator.

Both projects have large and active communities and well-constructed contribution frameworks [24] [25]. AEGIS is mainly acting as a user and not as a code contributor or collaborator but actively participate in technical discussions on the official repositories and is being aware of reporting issues that may came up during the development of AVT.

Topic c Software Defined Control in Industry4.0

A recommendation of usage of the Software Defined Control in the optic of Cybersecurity assurance will be made for the plants addressing Industry 4.0. It will be done via a large documentation referenced by ENISA in ENISA Good practices for IoT and Smart Infrastructures Tool — ENISA (europa.eu)[26] The recommendation will be complemented by a specific recommendation to use Openvswitch (OVS), as open-source switches and controllers instead of material of proprietary solutions for the software defined control. The objective is the capacity to maintain an external security management of the industrial plants.

Topic d Mobile operator security

The best practices applied in C4IIoT that could be a recommendation in GSMA are hereafter:

In C4IIoT project Vip mobile uses the newest NB-IoT technology dedicated to IoT device communication, providing optimal IoT device usage and secure communication through dedicated APNs.

In order to exchange data between mobile terminals and the server for further processing, a private APN (Access Point Name) is created for users of mobile terminals. The terminals send data to the field gateway, which is within the Vip mobile data network. The assurance of the traffic is performed within Vip network and the Vip's data network is connected via IPSEC VPN. Additional encryption is applied while data is sent to the server in Cloud.

An APN (Access Point Name) is the exit point from the Vip data network to external data networks. Private APN guarantee security and privacy of the customer network. Only terminals with the SIM card which is assigned to an appropriate private APN will have the right to access to LAN interconnection and server. SIM card within a private network, form a private APN and have the opportunity to obtain fixed IP addresses from the private range, which through the new NBIoT network enables two-way IP communication between terminals and servers.

4.2 Summary of the plan

Topic	Standardization activity and recommended SDO	Open-source contribution

[24] https://angular.io/

[25] https://nodejs.org/

[26] ENISA Good practices for IoT and Smart Infrastructures Tool: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Industry%204.0

Edge-field gateway-cloud anomaly detection orchestration	Participation in the BDVA-ECSO new WG Collaboration in writing recommendations within CSA WG IOT [27] Collaboration in ETSI ISG MEC [28]	No
Encrypted network traffic analysis		Contribution in Zenodo C4IIOT community
Patch-oriented-testing methods for binary code	Writing the description of the testing method in a document referenced by ENISA [29]	
Edge node design enabling a high degree of hardware-enabled security		OPTIGA Trust M is released as open source with MIT License
Search for the best mitigation from a close knowledge base of threats and remediation plans	Writing the description of the method in a document referenced by ENISA [29]	Possible in association with innovation 2 and topics a, b, c.
Usage of the Decentralized blockchain-based solution	Collaboration in writing recommendations *for example* within CSA WG Blockchain [30]	
Security assurance	Recommendation for development of a common assurance model, enabling model-based security assessment, certification and mitigation schemes.	Possible to release partial model elements, in association with innovation 5
Visualization		AEGIS Participation in technical discussions: Angular web framework combined with a web server written in Node.js
Software defined control of the infrastructure	Recommendation of Software Defined Control in Industry 4.0 via an open-source solution: Openvswitch	

[27] CSA WG IOT: https://cloudsecurityalliance.org/research/working-groups/internet-of-things/

[28] ETSI ISG MEC: https://www.etsi.org/technologies/multi-access-edge-computing

[29] ENISA Good practices for IoT and Smart Infrastructures Tool: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Industry%204.0

[30] CSA WG Blockchain: https://cloudsecurityalliance.org/research/working-groups/blockchain/

	Writing of a document referenced by ENISA [29]	
Mobile operator security	Writing GSMA Guidelines	

4.3 Choice of the SDOs to address guidelines and recommendations

4.3.1 About ENISA

The following site provides a tool to reference good practices documentation: ENISA Good practices for IoT and Smart Infrastructures Tool — ENISA (europa.eu)[31]

4.3.2 About CSA

CSA IOT WG

The IoT Working Group's mission is dedicated to understanding relevant use cases for IoT deployments and defining actionable guidance for security practitioners to secure their IoT ecosystem. This includes outlining best practices for securing IoT implementations, identifying gaps in standards coverage for IoT security, and identifying threats to IoT devices and implementations.

CSA is working to secure IoT in collaboration with OWASP, and the Industrial IoT Consortium

CSA WG Blockchain

The Blockchain working group investigates relevant use cases, and security implications of blockchain. Currently they are creating a framework and glossary that would help provide guidance and security for example around: wallets, exchanges, cryptography and more.

Most of the Blockchain/DLT systems suffer from new security issues. The CSA currently has a draft listing of almost 200 weaknesses and vulnerabilities in Blockchain technology, many of which are not fully understood or documented at this time. A part of the WG work is attempting to classify and publicize these weaknesses and allow other industry efforts (such as CWE [32]) to leverage them.

4.3.3 Standards around blockchain

There are different organizations/authorities that have tried to implement certain approaches to start blockchain-related standards. Some of them are mentioned below:

National Institute of Standards and Technology (NIST) published the document: *NISTIR 8202-Blockchain Technology Overview* [33]. ANSI Accredited Standards Committee X9 released the final version of the *Distributed Ledger and Blockchain Technology Study Group Report* [34]. International Organization for Standardization (ISO) released the *document ISO/TR*

[31] ENISA Good practices for IoT and Smart Infrastructures Tool: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#Industry%204.0

[32] https://cwe.mitre.org

[33] Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. NISTIR 8202 Blockchain Technology Overview; Internal Report 8202; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.

[34] Accredited Standards Committee X9 Study Group Report by the Distributed Ledger and Blockchain Technology Study Group. 2018. Available online: https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf

23455:2019 Blockchain and distributed ledger technologies—Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems[35]. German Institute for Standardization (DIN) and International Telecommunication Union (ITU) also publish a number of specifications related to blockchain technologies and distributed ledgers[36] [37] [38] [39] [40]. The European Union Agency for Cybersecurity (ENISA) published *Distributed Ledger Technology & Cybersecurity – Improving information security in the financial sector*[41]. The German Federal Office for Information Security (BSI) released the document *Towards Secure Blockchains*[42]. Finally, the European Committee for Electrotechnical Standardization (CENELEC) publish a report called *Recommendations for Successful Adoption in Europe for Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*[43].

4.3.4 Join standardization activities

In addition of the previous plan involving the sole contributions of C4IIOT, we aim to share activities with the partners of the projects of the same H2020-SU-ICT-2018 call and in particular the projects targeting technologies of cybersecurity.

Regarding a common perspective in standardization, we will have further exchanges especially with the SAPPAN project.

A common target will concern the CTI (Cyber Threat Intelligence) and the corresponding OASIS Working Groups especially CACAO.

For C4IIOT, the goal is to share the following activities and to refine them for the IIOT domain.

These shared activities will consist in:

- a standardization of the vocabulary for describing reusable knowledge about response and recovery actions for Cybersecurity, recovery actions that are often specified in «Playbooks» and that could feed the Mitigation Engine of C4IIOT.

[35] ISO/TC307. Standards by ISO/TC 307—Blockchain and Distributed Ledger Technologies. 2020. Available online: https://www.iso.org/committee/6266604/x/catalogue/

[36] DIN. 16597:2018-02 Terminology for Blockchains. 2018. Available online: https://www.beuth.de/de/technische-regel/din-spec-16597/281677808

[37] DIN. 3103:2019-06 Blockchain und Distributed Ledger Technologien in Anwendungsszenarien für Industrie 4.0. 2019. Available online: https://www.beuth.de/de/technische-regel/din-spec-3103/306199037

[38] DIN. 4996:2020-04 Blockchain-Based Approach to the Transfer of Software Licenses. 2020. Available online: https://www.beuth.de/de/technische-regel/din-spec-4996/321277534

[39] ITU. Focus Group on Application on Distributed Ledger—D1.1, Distributed Ledger Technology Terms and Definitions; Technical Report; International Telecommunication Union: Geneva, Switzerland,2019.

[40] ITU. Focus Group on Application on Distributed Ledger—D1.2, Distributed Ledger Technology Overview, Concepts,

Ecosystem; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.

[41] Network, E.U.A.F.; Security, I. Distributed Ledger Technology & Cybersecurity—Improving Information Security in the Financial Sector. 2017. Available online: https://www.enisa.europa.eu/publications/blockchain-security

[42] BSI. Towards Secure Blockchains; Technical Report; German Federal Office for Information Security: Bonn, Germany, 2019.

[43] CEN-CENELEC. Focus Group on Blockchain and Distributed Ledger Technologies, Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies; Technical Report; European Committee for Electrotechnical Standardization: Brussels, Belgium, 2018.

- a possible extension to the MISP (Malware Information Sharing Platform) data model that enable sharing of Machine Learning models as a new indicator of compromise

5 Exploitation activities

5.1 Individual Exploitation Plans

5.1.1 FORTH

FORTH's expertise lies in real-time intrusion detection, distributed network monitoring, highspeed data analysis and text processing through pattern matching in GPUs, access control, and hardware security. FORTH exploitation strategy will consider its contribution in WP7 and its coordinator role through the Distributed Computing Systems (DCS) laboratory, which is active in systems-security and network-monitoring research. FORTH's strategic exploitation and development plan is summarized as follows:

FORTH as a research and academic institution aims to perform high-quality research, to promote education and training, and to contribute to the development of the Information Society, at a regional, national, and European level. FORTH will incorporate C4IIoT results and training tools, within their advanced educational activities. Both PhD students and researchers will have the opportunity to work collaboratively with external stakeholder. Furthermore, FORTH intends to publish the research achievements and innovations obtained within the project, to the scientific community through peer-reviewed publications, in high quality journals and international conferences during the lifetime of the C4IIoT.

The Project's coordinator Dr Sotiris Ioannidis is a member of ENISA Permanent Stakeholders Group, which is strongly active in contributing to the threat intelligence landscape, ensuring a strong collaboration with ENISA and the viability of the C4IIoT solution. Finally, the knowledge, the technologies and the network gained through C4IIoT will be exploited in the future strategy of FORTH for applying to consequent EU-funded projects calls.

5.1.2 CRF

Centro Ricerche Fiat (CRF) is one of the main private research centre in Italy. It was founded in 1978, with the mission to develop and transfer innovative products, processes and methodologies to improve the competitiveness of the products of FCA (FIAT Chrysler Automobiles). With a workforce of approximately 900 full-time professionals, CRF develops research and innovation along the three principal axes of sustainability: Environmental Sustainability, Social Sustainability and Economically sustainable competitiveness. The CRF research activities imply strategic competences not only in the field of automotive engineering, but also in the fields of manufacturing, advanced materials, ICT and electronics, as well as a wide range of state-of-the-art laboratories and extensive test facilities, including advanced engine & vehicle testing facilities, EMC chambers and a dynamic driving simulator with immersive virtual reality.

The CRF department working in the project is the World Class Manufacturing Research and Innovation (WCM R&I) department, in particular the Factory Innovation Business Line. This department is part of the WCM area, where the main aim is the optimization and standardization of production processes in FCA plants worldwide.

The WCM R&I department provides its experience in modelling industrial processes in intralogistics and in adopting technology breakthrough in complex manufacturing in the areas of manufacturing and logistics.

CRF motivation started from the need to improve cybersecurity of I4.0 devices and platforms implemented both in FCA production processes and FCA supply chain. CRF is defining in detail C4IIoT's demonstration protocol (e.g. testing use cases, actors to perform the tests) and will ensure smooth deployment and execution of C4IIoT real-world demonstrators. It is also leading the assessment of C4IIoT offerings from the end-user's point of view and will provide a concrete impact analysis so as to facilitate the project's long-term sustainability.

Thanks to C4IIOT, it will be possible to test and demonstrate the usefulness given by the usage of this type of solutions within the application considered. In fact, it will be possible to estimate the added value by quantifying the benefits, in terms of KPIs, obtained thanks to the prevention and protection against cyberattacks.

Moreover, the demonstrator will be used during workshops or visits by SMEs in the plant in order to help them understanding how the use of these technologies can contribute in improving the IoT cybersecurity in their own companies. This will help to strengthen the collaboration of CRF with local companies, who will have the possibility to access C4IIoT solutions.

5.1.3 IFAG

IFAG's main Business Unit involved in the project is Digital Security Solutions (DSS). DSS is always looking for new markets and applications to extend her core business (currently secure identity and trusted computing). Within the goal of looking for novel environments, the C4IIOT project constitutes a precious test environment and provides valuable experience to deepen the knowledge of the demands and unique requirements of industrial IoT solutions.

In particular, the main lessons learned from the project, which we expect will allow for an important revenue in the future, are those obtained from the combination of Distributed Ledger Technologies (DLT), in particular Hyperledger Fabric, together with our hardware security devices. We expect an important market growth in the blockchain sector once it is more mature and the security threats (thanks to initiatives like C4IIoT) are better understood. A main asset of the project will be a PKCS#11 standard hardware wallet, using IFAG's secure element, and directly compatible with Hyperledger Fabric, which we expect will be in a very close-to-market stage by the end of the project, and we forecast an important demand of such a device from our customers.

Furthermore, our embedded security solutions deployed in the edge nodes, paired with novel cellular technologies, constitute important demos that we can directly show to our customers to help demonstrating the advantages and features of our secure elements in realistic scenarios and pilots, with strong partners from the automotive sector, which greatly increase their impact.

5.1.4 Thales

The 2 Global Business Units of Thales composing Thales SIX GTS, the Thales company directly involved in C4IIoT are SIX for "Secure Communications and Information Systems" and GTS for "Ground Transportation Systems". Each GBU has 4 Business Lines.

Among all of them, the Business Line CIC for "Critical Information Systems and Cybersecurity" is the one that will exploit the most the results of C4IIoT from different technical cyber-security point of view. Mastering the knowledge of the machine learning algorithms convenient to detect cyber-attacks is the ultimate goal of CIC in the next months and especially in the IOT world where the number of connections is exploding. The first target of exploitation is to master the detection of behavioral anomalies and over longer term in a more progressive approach to master edge intelligence and intelligence offered by cloud computing through safe communications, with the goal to appreciate complex situation awareness. This aspect of machine learning knowledge acquisition is expected to improve the product chain CYBELS and the core product CYBELS Analytics, one innovative platform based on Artificial Intelligence technology and Big Analytics.

The GBU GTS has 2 Business lines focusing on signaling for the railways (main lines and urban lines) and has an exploitation plan more specific regarding safety and cybersecurity close to the industrial IOT world. It concerns mainly the maintenance of a safe infrastructure and of the different sensors necessary to keep operational the railways control systems. The exploitation plan for GTS is to take advantage of the end to end integrated industrial framework to adapt it for the maintenance of the informative mechanisms in railways control.

Due to the recent acquisitions of Gemalto and Vormetric, the Thales group has another GBU called DIS Digital Identity Security closely focusing on certain main issues C4IIoT has to solve, such as the integration of identity management solutions for assurance of IIoT processes. For example, DIS has a solution of "IoT asset tracking" with secure and reliable connectivity and intends to exploit the showcases of C4IIoT to improve this solution which represents a vast market perspective[44].

5.1.5 HPE

HPE customers are frequently requesting support and competencies in their containerization effort; with the experiences gained in C4IIoT project HPE will be delivering a high degree of competence in dealing and offering security aspects.

HPE holds a large bounce of Manufacturing Companies as main customers, who are moving massively toward IoT technology in their journey toward digitalization. The experience gained in the project would be engineered by HPE to provide a valid contribution for their transformation.

An HPE dedicate worldwide Security Service division, named Security and Risk Management Practice (as a COE - Centre of Excellence), a member of which is member of the C4IIoT HPE team, is to share the outcome of C4IIoT project as part of our Security Portfolio.

5.1.6 CEA

The mission of the Software Reliability and Security Laboratory (LSL) at CEA is to perform research to develop tools and methods to improve the cybersecurity of software, and transfer these methods and tools to the industry. One of these tools is BINSEC, an open-source platform whose goal is to foster the next generation of binary-level analysis tools by proposing binary-

[44] https://www.gemalto.com/iot/industries/asset-tracking

level semantic approaches, i.e. methods based on the meaning of the program and able to cover all of its behaviors – or at least a very significant part.

These industrial transfers are at the core of the exploitation plan. They can take different forms, which are driven by the need of the industrial partner and depends on its expertise on the subject, for instance:

- It can consist in specific expertise mission, for instance to audit some software provided by the industrial partner using the tools developed by CEA;
- It can consist in training to help the industrial partner successfully use our tools to improve the quality of their software;
- It can consist in specific development of our tools to better handle the industrial partner's software;
- It can also consist in specific research to address a technological problem faced by the industrial partner.
- It can also transfer the tools and technologies to industrial partners using the following mechanisms:
    1. Joint Laboratories, consisting of specific contracts aiming at transferring some well-defined intellectual property from CEA to industry, possibly using a team of dedicated personnel.
    2. Patents and intellectual properties sale, and
    3. The creation of start-up companies. These means have already been applied in the LSL laboratory in the recent past, thus demonstrating their potential and effectiveness.

The C4IIoT project will help CEA to improve its tool and methods for the Industrial Internet of Things use case, and thus will help address more industrial partners in this market. In general, CEA has a strong involvement in the manufacturing field, and the project will help improve CEA's presence in this field.

In addition to these direct industrial contracts, the BINSEC platform is open-source, which helps disseminate the technology, both in the industry and in academia. For instance, many academic and industrial partners use the BINSEC platform, such as UGA (University of Grenoble-Alps), Loria, Université de Lorraine, Airbus Group, INRIA Rennes.

Finally, CEA will publish the research innovations obtained within the project, to the scientific community through peer-reviewed publications, in the top venue journals and international conferences in cyber security.

5.1.7 IBM

IBM established the IBM security unit which offers solutions in security intelligence, endpoint detection, security vulnerability detection, penetration testing, security analysis and more. IBM also established the IBM Blockchain unit that works on Hyperledger Fabric, on which IBM will build its decentralized solution for C4IIoT. In addition, IBM developed offerings for IoT (e.g. Watson IoT).

The IBM Research Lab in Haifa is working closely with the IBM brands and incorporate innovations into their products, for example the security products of Guardium, Trusteer and

Xforce. IBM has been named by Gartner as a leader in several security fields. The C4IIOT project will give IBM Research the opportunity to develop and exploit privacy solution for enforcing and auditing GDPR compliance in Watson IoT and Watson Health and providing extensions to IBM cloud IAM solution.

5.1.8 AEGIS

AEGIS is a Research and Development company, developing and managing innovative IT solutions for numerous business sectors. It is based on a highly effective professional team consisting of talented researchers and top-class IT experts from all over the world. This team empowers the company with a strong, diverse skillset which helps AEGIS offer innovative products and high-tech business solutions to the market.

AEGIS' main areas of expertise include Digital Forensic Investigations, adaptive Big Data visualization systems, Geographical Information Systems, secure embedded platforms, access control and network security systems, privacy preserving systems, enterprise web applications and the complete lifecycle of IT systems (design, development, deployment, optimisation and maintenance).

There are three areas where AEGIS expertise and software products have been proven, namely: (i) digital forensic investigation and analysis (both physical and cyber); (ii) advanced visualisations and consulting services related to cybersecurity and (iii) advanced, intuitive and informative mechanisms and interactive visualisations, such as visualisers and business-style dashboards, for Big Data analytics.

Specifically: 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 (FVT) to Big Data analytics (Big Data offerings as a Service for IT and not-IT users - AVT).

In the context of C4IIoT project will be expanded to support near real-time analysis and situational awareness to the end users of the operating industrial infrastructure. Temporal inspection of given metrics and combinations of relevant measurements in interactive visual representations will facilitate investigation on security alerts and can help users to better protect against future attacks and zero-day vulnerabilities.

A strategic goal of AEGIS is to extend its know-how in diverse domains and test its solutions in real-life environments in order to penetrate the market with industrial-tested, robust and user validated products.

The involvement in C4IIoT project is a great opportunity for AEGIS to improve its Visualisation Toolkit by collecting significant amount of validated learning about business requirements of the industrial, manufacturing and logistics sectors and access potential stakeholders of these domains with new commercial offerings. Building on top of its existing Visualisation Toolkit, AEGIS envisions to develop a complete digital analytics service.

Moreover, AEGIS envisions a strong collaboration with partners offering commercially established visualisation solutions or cutting-edge research results on data analytics not only during the official duration of C4IIoT but even afterwards, ensuring long-term sustainability of the service and its potential commercialisation.

5.1.9 UP1PS

VariaMos will be the first ever Docker container to integrate:

- An ontology of IIoT assets;
- An ontology of vulnerabilities, threats and the business risk associated with these assets;
- An ontology of run-time actions to mitigate these threats;
- A REST interface to receive instances of asset and business risk ontology concepts corresponding to a specific IIoT infrastructure;
- A REST interface to receive, from an anomaly detection component, alerts for instances of threat ontology concepts;
- A multi-objective optimization sub-component searching and ranking mitigation plans in order of overall business risk resulting from degraded satisficing of security, safety, availability and confidentiality requirements;
- A REST interface to drive network reconfiguration through the northbound API of an SDN controller;
- A REST interface to drive software stack reinstallation on network hosts through a container orchestration component based on industry *de facto* standards such as Docker and Kubernetes.

It will thus constitute a breakthrough in autonomic cybersecurity. It will be exploited through partnerships beyond the C4IIoT consortium to insure its development and evolution as an open-source project. It will allow UP1PS to partnership with SME to offer consulting and training services on its use to develop practical IIoT autonomic cyber-protection solutions.

5.1.10 ITML

Information Technology for Market Leadership (ITML) is a global ICT enterprise that provides novel, tailor-made software solutions based on a variety of technologies, such as big data analytics, advanced data mining and machine learning. ITML's vision is to deliver products and services close to real customers and market needs, ultimately improving the user experience and the access to technology. The primary competence of ITML relies on the design and development of software prototypes based on technologies that include machine learning algorithms, advanced data mining techniques, data aggregation and data analytics in IoT systems, as well as visualization tools; all of which are applied in different operational domains, such as smart manufacturing, logistics, health, education, energy management, maritime, and security.

ITML has a global business division whose mission is to seize the opportunities within the digital world and deliver new growth for ITML through venture capital, global partnerships and digital services. In C4IIoT, ITML is leading the continuous integration of the developed framework and contributes in ML-based anomaly detection and analytic tools towards the envisioned C4IIoT platform. The C4IIoT project is a significant opportunity to collaborate with the manufacturing and automotive sector and adapt its platforms and tools according to this specific sector needs (specific type of data, presentation type etc.). In this context, the outcome of the C4IIoT will enable the transfer of the developed solution into new commercial offerings, improve product/service portfolio and hence ITML's competitiveness on existing market. The exploitation 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 first with local and then with the EU big solution providers and potential stakeholders, offering to provide C4IIoT assets and services (big data management tools, integration methodology, services and processes) for use in their real-world applications to secure their market position. Furthermore, ITML is establishing a direct link between the exploitation of C4IIoT solution and the contribution in dissemination activities particularly with regard to social media, existing collaborations and partnerships. ITML also aims to deliver and transfer knowledge regarding technological advancements to the academic partners and built new collaborations and partnerships in the research domain of Europe. Last but not least, ITML will exploit the project's findings in enhancing and strengthening its positioning within the EU market and research domain, establishing partnerships and agreements for further collaborations with the large corporations participating in C4IIoT.

5.1.11 STS

Sphynx Technology Solutions AG offers products and solutions, and consulting services, in the areas of cyber intelligence, analytics, incident response, assurance and certification. The technologies offered by Sphynx include sophisticated event processing and analytics, security monitoring and testing, intrusion detection, fraud management, and incident response. Sphynx deploys off-the-shelf hardware components along with its custom software to provide tools such as its analytics engine, a threat-monitoring platform and a security audit and certification platform. Via its consulting services, Sphynx has expertise in providing customized solutions depending on client needs as well as more general training on analytics, security assessment and certification and cyber intelligence

Sphynx brings into the project its solution for security assurance and certification. This platform enables clients to realize security assessments, based on industrial and international standards (e.g., cloud, network, smart metering standards), using tool supported continuous monitoring and testing. The solution makes use of industrial strength tools including vulnerability and penetration testing tools, and open source solutions. Furthermore, it enables the configuration of security assessment, reporting and certification to the needs of different stakeholders ranging from senior management to external auditors and regulators.

In the context of the project, STS will use its Security Assurance platform in ways that allow it to support the delivery of cybersecurity situational awareness. In more detail, the security assessment and certification tools provided by STS will be used for monitoring, testing and assessing the C4IIoT framework, and potentially the protected infrastructure itself. We will employ the provided tools for the assessment and certification of each individual technology component of C4IIoT, and for the unified framework as a complete situational awareness solution.

Leveraging the above, Sphynx will use the outcomes of C4IIoT for strengthening its service and product portfolio, augmenting the capabilities of its security assurance platform in ways that will enable it to support the delivery of cybersecurity situational awareness services in the IIoT domain.

From a business perspective, STS's strategy will be to explore ways of making use of its platform as a tool for end-users and system administrators of IIoT and cyber physical systems, in addition to private and public organizations in all the critical sectors which are the focus markets of the company (e.g. healthcare and telecoms). STS will also seek to develop consultancy services in setting up training programs for establishing cybersecurity dynamic certification for situational awareness, based on the outcomes of C4IIoT.

5.1.12 UNSPMF

UNSPMF will exploit the project outcomes to further enhance and enlarge its in-house testbed for massive IoT connectivity via LP-WAN technologies. Current testbed covers about 80 NB-IoT edge devices in static (indoor) environment, while for the purpose of C4IIoT, additional collection of 50 mobile NB-IoT edge devices equipped with accelerometer and GPS sensors will be designed, fabricated and integrated within the testbed. Such a testbed represents a unique cellular IoT infrastructure relying on the latest 3GPP NB-IoT standard and completely open for research use, demonstrations and testing of LP-WAN solutions.

The knowledge related to the implementation and application of the pool of anomaly detection algorithms created, tested and used within this project will further serve to increase the visibility of UNSPMF as a partner with experience in this field. This also includes the knowledge to implement and apply differential privacy in big data processing scenarios where privacy preservation is an issue. In addition to the opportunities to apply this knowledge that is opening up in the local market, UNSPMF wants to maintain and expand contacts with EU partners in this field.

5.1.13 UOG

In the first year of the C4IIoT project, UOG's MEDICI tool has been extended to be able to receive offloading requests from IoT devices that are appropriate for IIoT environments, and the decision metrics have been updated to reflect the needs of C4IIoT's anomaly detection provisions. As originally planned, the C4IIoT extension of the tool has already proven useful in supporting a PhD project carried out in UOG and its associated publications. The plan is that these improvements of the tool will also inform the teaching of a related MSc module.

At research level, UOG will increase the readiness level of its existing MEDICI tool through validation in IIoT environments. This will help generate further research opportunities and collaborations in industrial settings.

5.1.14 VIP

Vip mobile is a mobile operator in Serbia, part of A1 Telekom Austria Group. Core business for Vip mobile is to provide voice, SMS and data services to customers. Vip mobile is transforming from 'connectivity-only provider' to solution provider. ICT department in Vip mobile is responsible for delivering 'Non-Core' solutions to customers. 'Non-Core' solutions includes, but not limited to IoT connectivity (2G, 3G, 4G, NB IoT), IoT end 2 end solutions provided in cooperation with IoT solution Partners, from Fiscal Cash Registers, Fleet Management, Asset Management, Smart Home solution, IoT platform for managing IoT devices, Big Data, Machine Learning, Cloud solutions etc.

C4IIoT exploitation strategy for Vip mobile includes help to differentiate from the competition, enhance customer experience and open door to new revenue opportunities and is divided it in 3 streams:

- PR and awareness activities

  - Using local and regional media (social, newspapers, TV, etc.) as part of A1 Telekom Austria Group to raise awareness of Vip mobile as solution provider, and as a part of C4IIoT project
  - Attending conferences and ICT events to transfer use cases, technology knowledge and commercial perspective of C4IIoT outcome
  - Raising awareness in local IoT Partner network and customer 'IoT ecosystem' of how much IoT security is important in real use cases (smart factory and logistics) and benefits of using it
- Pilot projects and PoC (Proof of Concept)
  - Sharing knowledge from C4IIoT project, with focus on IoT Security and expanding portfolio cooperation with existing IoT Partners in order to provide new IoT solutions to different vertical industry segments
  - Conducting Pilot projects in logistics vertical segment
  - Exploring opportunities in manufacturing and define industries and enterprises to initiate PoC projects
- New IoT product in Vip mobile ICT/IoT portfolio
  - Vip mobile is already providing Fleet Management and Asset Management solution to business customers, with special focus on Logistics companies
  - C4IIoT product will be bundled with Vip mobile IoT connectivity (2G/NB IoT) and IoT platform and offered to end customers and Partners
  - 'Secure your shipment all the time'- Outcomes from C4IIoT project will be used to extend existing portfolio for Logistics industry vertical in order to provide enhanced and improved IoT security as key benefit for Logistic companies and their end customer
  - Customized solution – based on customer needs and in cooperation with IoT Partners Vip will adjust (HW and/or app) existing C4IIoT Products outcome in order to provide tailor made solution to end customers

5.2 Joint Exploitation Plan

The joint exploitation plan is to be developed for the final version of the deliverable (M24), based on in the individual plans and the identified cooperation activities.

6 Conclusion

Regarding standardization activities, for the initial version we have identified standardization bodies, both European and international, in which C4IIoT members directly participate or follow, due to their special relevance regarding the project requirements and goals. Then, we have identified all the standards, guidelines, and recommendations followed by the individual partners of the C4IIOT consortium.

Regarding exploitation activities, every partner has developed their individual exploitation plan, sketching also the dissemination approaches to market the technology developed within the C4IIOT project.

For the final version of the current deliverable (due in M24), a joint exploitation plan will be developed. Furthermore, a follow-up on the success regarding the alignment with the currently identified standards shall be provided.