Towards Trustworthy End-to-End Communication in Industry 4.0

Ani Bicaku[1,6], Silia Maksuti[1,6], Silke Palkovits-Rauter[1], Markus Tauber[1], Rainer Matischek[2], Christoph Schmittner[3], Georgios Mantas[4], Mario Thron[5] and Jerker Delsing[6]

[1]*University of Applied Sciences Burgenland* - Eisenstadt, Austria
[2]*Infineon Technologies Austria AG* - Graz, Austria
[3]*Austrian Institute of Technology* - Vienna, Austria
[4]*Instituto de Telecomunicações* - Aveiro, Portugal
[5]*Insitut für Automation und Kommunikation* - Magdeburg, Germany
[6]*Luleå University of Technology* - Luleå, Sweden

***Abstract*—Industry 4.0 considers integration of IT and control systems with physical objects, software, sensors and connectivity in order to optimize manufacturing processes. It provides advanced functionalities in control and communication for an infrastructure that handles multiple tasks in various locations automatically. Automatic actions require information from trustworthy sources. Thus, this work is focused on how to ensure trustworthy communication from the edge devices to the back-end infrastructure. We derive a meta-model based on RAMI 4.0, which is used to describe an end-to-end communication use case for an Industry 4.0 application scenario and to identify dependabilities in case of security challenges. Furthermore, we evaluate secure messaging protocols and the integration of Trusted Platform Module (TPM) as a root of trust for data-exchange. We define a set of representative measurable metrics based on existing standards and use them for automated dependability detection within the whole system.**

I. Introduction

Nowadays, the world is facing a new technological revolution known as Industry 4.0, which will also affect economies and societies worldwide [1]. The novel concept Industry 4.0 addresses the challenges of the 4^{th} industrial revolution based on the logic of Cyber Physical Production Systems (CPPS) by decentralizing intelligence for independent processes and generating networking, which self-optimize, communicate with each other and optimize the production as a whole [2], [3]. The advanced features of Industry 4.0 bring new challenges in terms of design and security. RAMI4.0 [4] provides a reference architecture where the elements of assets are described based on a three axes layer model. Based on this reference model, we derive a CPPS meta-model to have a clear view on the complexity of these systems and to show the inter-domain security related dependabilities and affected components.

In the manufacturing environments, automation systems continue to become part of globally connected systems, meaning that intrusion attempts will increase and non-authorized access to information may also create a risk for the production process. Since CPPS are a fast-evolving field, where new vulnerabilities are constantly emerging due to security breaches in the cyber domain, the successful infiltration in these systems can directly impact industrial and manufacturing environments. Consequences can be in different areas or dimensions, such as interruption of an operation, modification of an operational process or sabotage with intention to cause harm. Manipulating or interrupting such systems could also affect safety in the CPPS, which can have consequences such as environmental damage, injury or loss of life.

Therefore, to maximize uptime and agility, secure end-to-end communication is required. It is important that data validation and security trust boundaries are applied to critical sections of the system, which require monitoring to provide higher level of transparency. Due to these trust boundaries between for example, different stakeholders, service level agreements (SLA) should be in place.

Thus, only an improved overall security concept considering the dependability between these aspects can address this challenge and provide trustworthy communication in CPPS. To address this, we evaluate the communication of the system from the edge devices (i.e., industrial device) to the backend infrastructure (i.e., cloud platform). We evaluate secure messaging protocols and investigate the possibility of integrating TPM as a root of trust for the CPPS components [5]. Further, we define a set of metrics for the CPPS components and map them to the corresponding objects of the meta-model. To make sure that the system is secured and the information can be trusted, measurable and automated dependabilities are needed to monitor security. By monitoring the measurable metrics we will extend our previous work [6] to address security in CPPS with a special focus on trustworthy end-to-end communication in Industry 4.0. Our main contributions and preliminary results in this position paper are:

- deriving a CPPS meta-model based on RAMI 4.0
- evaluating secure messaging protocols and proposing TPM as a root of trust for secure data exchange
- defining a representative set of measurable metrics
- using the CPPS meta-model for describing the proposed end-to-end communication use case and for showing the dependabilities between CPPS components

The remainder of the paper follows the same structure as the contributions above.

II. Related Work

This section gives an overview of existing state-of-the art work for CPPS relevant activities. First, we give an overview of existing architectural models. Second, we evaluate different secure messaging protocols and we consider the scientific work and relevant activities addressing transparency from the edge devices to the backend infrastructures related to operational security, legal and safety aspects.

A. Industry 4.0 Architectural Models

RAMI 4.0 – Reference Architectural Model Industry 4.0 describes the key elements of an object/asset based upon the use of a layer model consisting of three axes: (i) Architecture axis, (ii) Process axis, and (iii) Hierarchy axis. It consists of an Administration Shell which is a virtual representation of the real assets and gives information about the status of the assets and data during their lifetime [4].

IIRA – The Industrial Internet Reference Architecture is a standards-based open architecture under the Industrial Internet Consortium (IIC) for designing Industrial Internet Systems (IIS). Based on ISO/IEC 42010 standard specifications for complex systems with multiple components and multiple interconnected systems, the IIRA defines what are the most important industrial internet architecture components, their connections and categorize the IIS concerns on four viewpoints: implementation, functional, usage and business viewpoint [7].

To support the understanding of complex systems, such as CPPS, a meta-model based on RAMI4.0 is derived. The CPPS meta-model shown in Fig 1 is an example usage of RAMI4.0, which can be easily adopted and scaled to the needs of Industry 4.0 application scenarios.

B. Secure Messaging Protocols

MQTT[1] – Message Queue Telemetry Transport is an OASIS standardized protocol designed to be lightweight, flexible and simple to implement. MQTT uses different routing mechanisms, such as one-to-one, one-to-many or many-to-many, making possible the connection for IoT and M2M devices/applications. MQTT is a publish/subscribe messaging transport protocol on the top of TCP/IP protocol consisting of 3 components (subscriber, publisher, and broker). To define security, MQTT uses user/password authentication and SSL/TLS for secure data communication. In terms of Quality of Service (QoS), it supports three levels: (i) 0 - the message will be delivered once, with no confirmation, (ii) 1 - the message will be delivered at least once, with confirmation, (iii) 2 - the message will be delivered exactly once by using a handshake.

AMQP[2] – Advanced Message Queuing Protocol is a binary application layer protocol standardized from ISO/IEC 19464. It is a message centric protocol on top of TCP/IP, which provides publish-subscribe and point-to-point communication. AMQP supports message-oriented communication via message-delivery guarantees including: (i) at-most-once, when the message is delivered once or never, (ii) at-least-one, when the message is delivered and (iii) exactly-one, when the message will certainly delivered only once. It provides different features, including routing and storing messages within the broker using message queues. In terms of security, it supports SASL authentication and TLS for secure data communication.

CoAP[3] – Constrained Application Protocol is a web transfer protocol which supports unicast and multicast requests for use in constrained devices and networks. It is based on a request-response architecture between endpoints. CoAP clients after sending the requests using an URI, can receive as a response GET, PUT, POST and DELETE resources from the server. The messages are exchanged over UDP between endpoints and also it supports the use of unicast and multicast requests. CoAP provides security via the DTLS, a secure protocol for network traffic which supports handling packet loss and reordering of messages. In terms of QoS, CoAP provides two levels: (i) *'confirmable'* when no packet is lost and the receiver respond with an ACK; and (ii) *'nonconfirmable'* when the message do not require an ACK.

XMPP[4] – Extensible Messaging and Presence Protocol is a TCP communication protocol based on Extensible Markup Language (XML) used for real-time messaging, online presence and request-response services. Clients communicate via a distributed network and do not rely on a central broker. XMPP supports publish/subscribe model and provides security such as authentication via SASL and secure communication via TLS but does not provide any level of QoS.

DDS[5] – Data Distribution Service is based on a publish-subscribe principle, which provides real-time and high performance data communication. DDS uses a bus to connect the publishers and subscribers by providing a set of QoS policies (e.g., data availability, data delivery, data timeliness, resource usage, etc). In terms of security, each device/application has to assure its own security.

The main focus of messaging systems is to guarantee the delivery, routing and storage of the information without the necessity of implementing different mechanisms. Different standard organizations (i.e., W3C, IETF, EPCglobal, IEEE and ETSI) have been created to provide secure messaging protocols for the IoT. Based on these standards and relevant scientific works [8], [9], we have compared MQTT and CoAP (shown in table I) as the most suitable communication protocols with respect to security of industrial devices, Industrial IoT (IIoT) components and cloud services in Industry 4.0. applications. Even though they are both designed for use on lightweight environments, they have different fundamentals and fields of applications. MQTT uses TCP, which requires less resources consumption than UDP. Also it has a publish/subscribe communication model, whereas CoAP uses an asynchronous communication model. This communication

[1] www.mqtt.org
[2] www.amqp.org
[3] www.coap.technology
[4] www.xmpp.org
[5] www.portals.omg.org/dds

model offers to MQTT several benefits, such as Time Decoupling where the nodes publish their information regardless of other nodes state. The QoS, another important aspect in Industry 4.0, is provided in 2 levels from CoAP and in 3 levels from MQTT.

Property	Protocol	
	MQTT	CoAP
Transport Layer	TCP	UDP
Communication Model	Publish/Subscribe	Asynchronous
Security	SSL/TLS	DTLS
Header Size	2 Byte	4 Byte
Message Types	16 types	4 types
Message Reliability (QoS)	3 levels	2 levels
RESTful	No	Yes
Time decoupling	Yes	No
LWT Message	Yes	No
Message Store	Yes	No

TABLE I
COMPARISON OF MQTT AND COAP PROTOCOLS

Furthermore, MQTT supports 16 types of messages, while CoAP supports only 4 types. Another important feature of MQTT is the Last Will and Testament (LWT) used to inform other clients about an unexpected disconnected client. In terms of security CoAP supports DTLS and MQTT supports SSL/TLS, which are protocols used for secure communication.

C. Relevant Activities in CPPS

FITMAN (Future Internet Technologies for Manufacturing Industries) project has the goal to integrate future internet technologies into manufacturing industries. With achieving this, FITMAN wants to make easier the adoption of FI PPP (Future Internet Public Private Partnership) technologies in EU industries by giving more access to advanced IT solutions. Also, it proposes a dynamic decision model that integrates performance metrics to monitor the performance of service oriented systems in order to ensure their sustainability [10]. The focus of the project is on providing solutions for improving the efficiency of business processes and enabling interoperability, rather than addressing security and safety of internet technologies when integrated in manufacturing industries.

ARROWHEAD[6] focus is to find methods to enable collaborative automation by networked embedded devices [11]. The project targets five application domains: (i) smart production, (ii) smart buildings and infrastructure, (iii) electro mobility, (iv) smart energy, and (v) virtual market of energy. One of the main outputs of the project is the ARROWHEAD framework, which is based on a service oriented architecture (SOA) technology, and offers interoperability between IoT and CPS devices at a service level. In order to provide adequate security and safety levels for such a framework to function properly, services such as, authorization, authentication, certificate distribution, security logging and service intrusion are considered as well. Even though the focus of the project is to provide interoperability between devices using the ARROWHEAD framework and to integrate automation systems in these devices, security and safety aspects are also considered. However legal (e.g., SLAs) aspects are not in the focus of the project.

CyPhERS[7] (Cyber-Physical EU Roadmap Strategy) project combines and expands EU competences in embedded, mobile computing and in control of networked embedded systems. The main objective is to provide a systematic overview of the technology trends and innovation associated with CPS by providing conclusions concerning the priority areas for research and action with surveys and analysis of the economic, technical, scientific, and societal significance of CPS. This project identifies the research and innovation challenges for EU competences in the field of CPS by choosing the fields of action and expanding with suggestions for actions in the specific field. The project has identified a set of research and innovation challenges related to legal aspects for the CPS to ensure trustworthiness. It also considers dependability of the CPS systems as an important challenge, but the focus of the project is to provide recommendations rather than to provide security, legal or safety solutions for the CPS.

CPSoS (Cyber-Physical Systems of Systems) project has the main goal to establish the state-of-the-art and future research challenges in the area of CPSoS by providing a roadmap on research and innovation priorities in engineering and management of CPSoS. Also, it provides a platform for related projects and communities with the main goal to define a EU research and innovation agenda on the challenges of System of Systems (SoS) in which computing and communication interact with complex physical systems [12]. The project has summarized the most important challenges in engineering and management of CPS and has proposed 11 topics on which should be the focus during 2016-2025, but without addressing legal or safety issues in these systems.

Road2CPS[8] project is a coordination and support action focused on identifying and developing opportunities for novel technologies, applications and services in the field of CPS, by identifying solutions to problems associated with it and the socio-economic issues accompanying these innovative changes through roadmaps. Road2CPS has published an e-book where are summarized all the findings of the project including the roadmap and the recommendations for the deployment of CPS. The project considers security, legal and safety issues, but the focus is on providing recommendations for strategic actions required for the future development of CPS. Thus, they do not address specifically the issues by for example, providing controls or measurable metrics.

AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) [9] project aims on developing a holistic approach for assurance and certification of CPS by considering safety, security, availability, robustness and reliability with the main goal to reduce time, costs and risks for assurance certification. Thus, even though the focus of the project is safety assurance and

[6] www.arrowhead.eu

[7] www.cyphers.eu

[8] www.road2cps.eu

[9] www.amass-ecsel.eu

certification, the main goal is to reduce time, costs and risk for certification. Security of CPS is also considered, but legal (e.g., SLAs) aspects are not in the focus of the project.

SAFURE[10] (Safety and Security By Design For Interconnected Mixed-Critical Cyber-Physical Systems) aims at developing a framework for CPS by implementing a methodology to assure safety and security by construction. The SAFURE framework is a collection of architectural concepts, functional building blocks, modelling approaches, analysis methods and tools based on Common Criteria. The project analyzes safety and security but with more focus on interoperability within and between critical systems. They do not address legal aspects.

NGCert (The Next Generation Certification) project has proposed a dynamic certification approach that adopts the common certification process to the increased flexibility and dynamics of cloud computing, based on a new semi-automated certification process and the continuous monitoring of critical parameters of cloud services [13]. To support the autonomic validation of these parameters, an approach using low level metrics of IaaS components is proposed. NGCert project addresses security, legal and organizational issues under the scope of cloud computing, without considering cyber physical devices or the communication between both.

Cumulus (The Certification Infrastructure for Multi-Layer Cloud Services) project has addressed security, privacy, and compliance issues by developing an integrated framework of models, processes and tools supporting the certification of security and assurance in the cloud [14]. They also address security and engineering models for CPS [15]. The project relies on multiple types of evidence regarding security, including service testing and monitoring data and trusted computing proofs, and is based on models for hybrid, incremental and multi-layer security certification. CUMULUS addresses security certification for service users, service providers and cloud suppliers. They also consider legal aspects and safety but focused only on the cloud.

SECCRIT[11] (Secure Cloud computing for Critical infrastructure IT) project has analyzed and evaluated cloud computing technologies addressing security risks in sensitive environments. The project has developed methodologies and best practices including risk assessment, policy specification and assurance evaluation for critical infrastructure. In order to achieve these goals, SECCRIT has identified and established legal challenges to provide evidence and data protection for cloud services; methodologies and tools for risk assessment; best practices for secure cloud implementations including a cloud assurance evaluation methodology to aggregate and simplify monitoring information related to high level security properties. SECCRIT project addresses operational security and legal issues for critical infrastructure providers who want to migrate their services in the cloud, thus the focus is only on the backend infrastructure.

[10]www.safure.eu

[11]www.seccrit.eu

The approaches and frameworks developed as part of the above projects address trustworthiness based on the edge devices or the backend infrastructure without considering the whole system. Projects such as NGCert, Cumulus, CTP and SECCRIT provide best practices and solution for transparency but with focus entirely on the cloud. Other projects, such as MORE, AMASS and SAFURE consider safety and security on the edge devices without considering the whole system. Furthermore, BEinCPPS, CyPhERS, CPSoS, and Road2CPS provide evaluations of the current state of the art related to CPS with the main goal in priority areas for research and action. The goal of this work is to achieve CPPS transparency and trustworthiness in security by considering the cloud and the edge devices as highly networked systems, incorporating large numbers of IT systems and automation components. We consider security as not independent from other issues such as legal and safety and we will enhance our previous work [6] to address security in the CPPS with a special focus on secure end-to-end communication in Industry 4.0.

III. The CPPS Meta-model

Taking the RAMI 4.0 reference model into account, we derive a CPPS meta-model to model all relevant entities of these systems and their dependabilities on different levels. Using the ADOxx tool and UML notation is implemented a combination of both diagram types, Class and Object Diagram, illustrated in Fig 1. This meta-model aims to describe Industry 4.0 scenarios and to identify the dependability of components in case of security issues. The CPPS meta-model consists of five levels and the corresponding components:

The **Business / Governance** level aims to aggregate the business and governance view on the CPPS. Core element within this aggregation is the *Process* that provides a direct or indirect contribution to the value chain of an organization and has a defined starting and end point. Other objects within this level include:

- *Product*: products are sales units with a certain price
- *IT Service*: the provision of one or more technical systems to enable or support a business process
- *Requirements*: represents a technical requirement with respect to one or more architecture elements
- *Contract/Agreement*: service level agreements (SLAs)

The **Architecture&Service** level is composed of:

- *Application Group*: a logical grouping of applications
- *Application*: describes operational software from a functional point of view
- *Application Component*: a modular, interchangeable, and installable component of an application
- *Service*: a well-defined and business-oriented functionality that supports business processes
- *Interface*: allows communication between applications and/or application components
- *Data*: different types of structured or unstructured data or information within an organisation

The **Technology** level has the following objects:

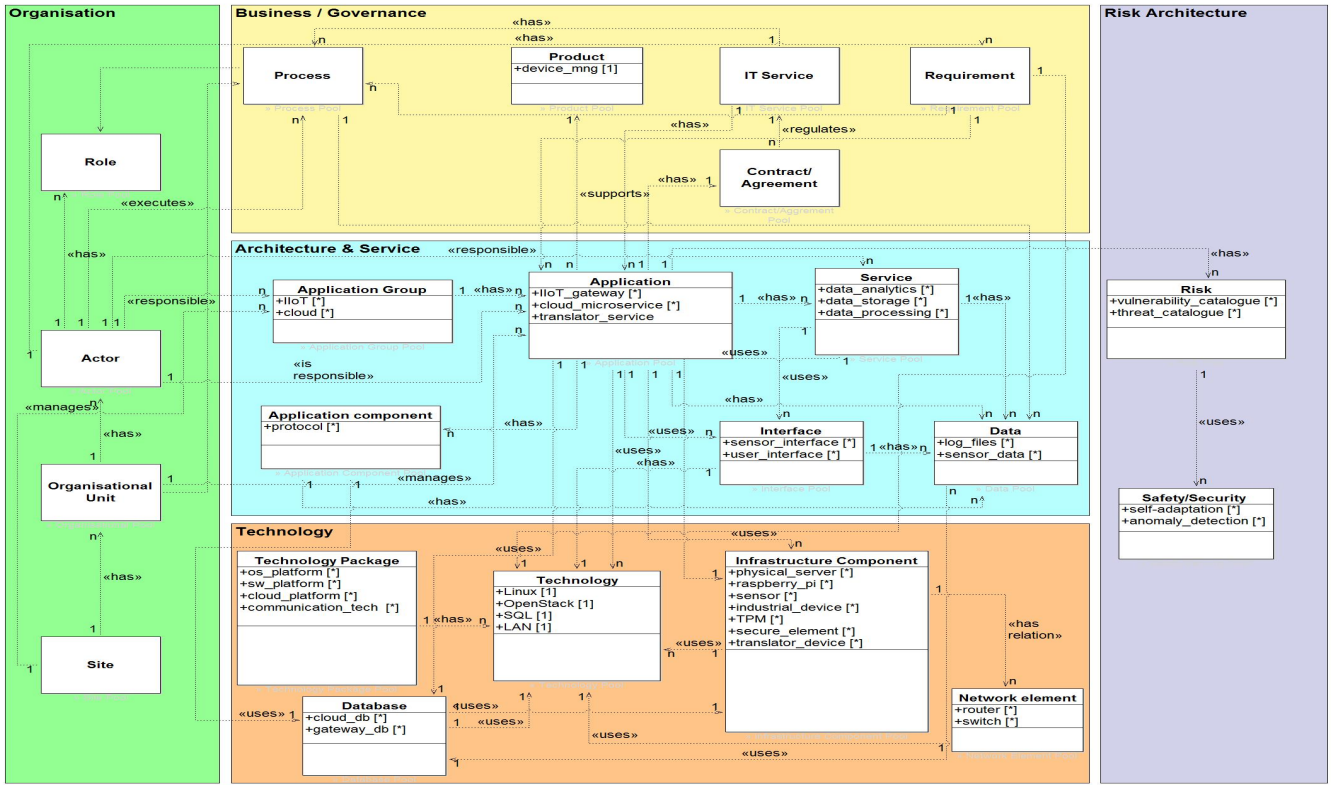

Fig. 1. The CPPS meta model composed of five main levels and the corresponding objects, addressing the RAMI4.0 axes, used to describe an end-to-end communication use case for an Industry 4.0 application scenario

- *Technology Package*: different technology products
- *Technology*: product consisting of hardware or software
- *Infrastructure Component*: a resource, usually a server or cluster, on which applications, application components, or databases are installed and then run
- *Database*: data storage in which business objects can be managed in a structured manner
- *Network Element*: the interface between infrastructure modules or between spatially separated networks

The **Organisation** level contains:

- *Role*: functions carried out by one or several persons
- *Actor*: a concrete person who can assume responsibility
- *Organisational Unit*: independent unit of an organisation characterized by its own resources
- *Site*: geographic location of components

The **Risk Architecture** level groups the objects:

- *Risk*: a critical situation of the specific environment
- *Safety/Security*: strategies to prevent risk

Each of the above-mentioned components has a set of attributes that describes the characteristic features of the underlying CPPS. In context of this work, the meta-model is used as a tool: (i) to map an end-to-end communication use case for an Industry 4.0 application scenario presented in section IV-A, and (ii) to see the dependability between the CPPS components presented in section IV-C. The derived meta-model can be easily adopted and scaled to the needs of Industry 4.0 application scenarios. As different use cases and viewpoints should be considered and researched, the chosen meta-model allows incremental enhancements that can be proven by research activities in the CPPS.

IV. Security in CPPS

The CPPS are a fast-evolving field where new vulnerabilities are constantly emerging due to security breaches in the cyber domain. These vulnerabilities can be exploited by attackers with a wide spectrum of motivations ranging from criminal intents aimed at financial gain to industrial espionage, and cyber-sabotage. For instance, the Dragonfly attack [16], is a type of cyber-espionage attack against energy suppliers, which could have caused damage or disruption to the energy supply in the affected countries. This assumption is consistent with the concern that the physical processes/systems of CPPS become increasingly more susceptible to the security vulnerabilities of the cyber domain, as the interaction between the physical world and the cyber world increases in Industry 4.0. Therefore, ensuring security is of utmost importance, since any disruption or outage of CPPS can severely affect not only the physical processes being controlled but also the people who depend on them [17]. Towards this direction, a security baseline for CPPS is essential to be identified. To this end, different existing standards and best practices guidelines, such as NIST SP 800-series or ISO/IEC 270xx series, have to be evaluated. These existing standards and guidelines are expected to be

used in several aspects of CPPS environments so as to ensure secure interconnection of production systems and production plants in the supply chain, while at the same time ensure data confidentiality, data integrity and availability (CIA). However, to increase efficiency and enable agile production, all information handled by the CPPS has to be trusted. Hence, the CIA triad needs to be extended towards all the CPPS processes, including computing, networking and control, so that not only the stored data within CPPS can be secured and trusted, but also all the in-transit data. Particularly, to ensure secured and trusted in-transit data, secure messaging protocols that take advantage of a root of trust have to be employed for data exchange. The communication between industrial devices, IIoT components and cloud services can be achieved in several ways. The use of messaging systems based on message queues with the same interface makes possible the communication through the same interface of devices and applications. The most popular messaging protocols are reviewed in section II and a comparison of the architecture, message reliability, security and performance characteristics of MQTT and CoAP as leading messaging protocols is presented in table I. To provide a higher level of security we propose the integration of TPM as a root of trust for these systems. Implementing hardware security in existing CPPS is more complicated, because in facilities different architectures and devices are applied. These devices might not be able to store certificates or perform cryptographic calculations; therefore other solutions have to be applied. TPM is a hardware root of trust, providing a set of interoperable features used to protect the integrity and authenticity of embedded devices and systems. The most relevant features in the context of an end-to-end communication are: the secured key generation and storage and the secured execution of the cryptographic processes associated with the keys. In general, the TPM standard, which is specified by the Trusted Computing Group organization, defines various levels of security, ranging from hardware-based down to software-based realizations. However, for industrial applications, where cyber-attacks could lead to severe financial losses, the usage of a hardware-based *Discrete TPM* is recommended, since it also protects keys and manufacturer certificates during shipping or transit of CPPS equipment and during regular maintenance by third-party companies.

A. CPPS End-to-End Communication Use Case

An end-to-end communication use case for an Industry 4.0 application scenario, including the technologies, is illustrated in Fig 2. By providing these details we can show how the components of the use case can be mapped in the corresponding objects of the CPPS meta-model as illustrated in Fig 1.

Industry plants have a different range of devices (M1, M2, and M3), including new devices (M3) that already support secure messaging protocols, such as MQTT and "legacy" devices(M1 - usually connected via RS-232, RS-485 or USB interfaces) that need a translator for translating the device protocol to MQTT. The industrial devices are equipped with sensors, actuators and communication technology. To collect

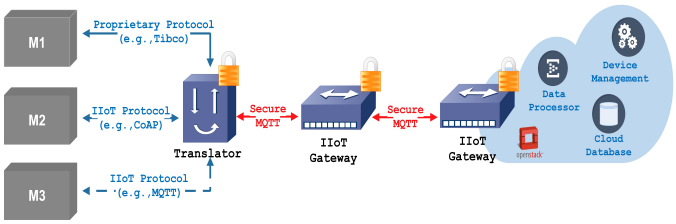

Fig. 2. CPPS end-to-end communication use case

the data from these devices the IIoT components, such as IIoT gateways, are used. In this use case, the IIoT gateway is build in a Raspberry Pi equipped with macchina.io [12]. Macchina i.o is an open-source toolkit for building embedded IoT applications and supports different communication protocols, including a MQTT plug-in for enabling the applications to communicate with various sensors, devices on one side, and cloud services on the other side. The collected data are preprocessed from the gateways and sent to the cloud services for further processing or storage. For a secured communication between the gateways we propose to use the MQTT protocol, which also supports the communication from the IIoT components to the cloud services. All these connected devices including industrial devices, IIoT components and cloud services increase the possibility for a potential attack. To achieve a trustworthy end-to-end communication it is necessary to provide security for each connected device by integrating Secure Elements or TPMs in the industrial devices, IIoT gateways and cloud platforms. One important usage of the TPM is the secured authentication, using integrated manufacturer certificates to check the authenticity of the connected devices. Furthermore, the TPM can be used for separating the crucial PKI key generation and RSA or ECDH key exchange operations into the trust anchor environment. Finally, with the help of hash and signature features, the TPM can be used to check the authenticity of firmware and software updates of connected industrial devices.

B. Measurable Security Indicators

To ensure trusted and secured data exchange we propose to use intermediary systems to gather the data, such as IIoT gateways, as described in the use case above. Additionally, technologies that offer hardware security protection such as TPM are integrated in the IIoT gateways to provide integrity protection and a root of trust for the gateways. However, considering the increasing number of interconnected components, focusing only on security that addresses CIA is no longer sufficient. It is very important to consider as well the other related aspects such as legal and safety. Thus, deriving and monitoring measurable security metrics related to operational security, legal (e.g., SLAs) and safety aspects can provide a higher level of transparency for the entire supply chain.

Following, we show a set of representative example metrics based on an evaluation of the most relevant standards related to operational security, legal, and safety with the aim to

[12]www.macchina.io

identify MSIs for the CPPS components. For each metric we give: (i) an ID, respectively **MSI** (Measurable Security Indicator), **MSSI** (Measurable Security SLA Indicator) and **MSFI** (Measurable Safety Indicator), (ii) a general description and (iii) the definition source based on standards and best practices guidelines.

- MQTT Metrics

[MSI-1] - *Secure authentication of clients by server*

`Source: NIST SP 800-82 [18], ISO 27002 [19]`

This property supports confidentiality by assuring that the client and the server identify each other and assure each other of their identities. Data exchange without authentication (clear text) gives the possibility to attackers to easily access and imply damage or illegal actions on the communication.

[MSI-2] *Detecting abnormal behaviours*

`Source: ISO 27001 [20], ISO 15408 [21]`

This property supports integrity by monitoring the client behaviour to detect potential security incidents (e.g., repeated authentication attempts).

- IIoT Gateway Metrics

[MSI-3] *Secure key/sensitive data storage*

`Source: NIST SP 800-82 [18], CCSC [22]`

This property supports confidentiality by assuring that keys are stored within a cryptographic module and encrypted form. The IIoT gateway needs to gain the trust that the public key used to verify a signature belongs to the proper client and to achieve this is required a secure storage of keys.

[MSI-4] *Secure Boot*

`Source: ISO 15408 [21]`

This property supports integrity by checking and identifying if the firmware of each device, operating system and each software is valid. Without secure boot, attackers can easily take advantage of several pre-boot points including the system firmware and running a non-secure operating system.

- Cloud Database Metrics

[MSI-5] *Unauthorized data observation*

`Source: ISO 27001 [20]`

This property supports integrity by checking if the system supports mechanisms to protect the data stored in the database from unauthorized access or malicious actions in general by assuring the security of a database.

[MSI-6] *Encryption*

`Source: NIST SP 800-82 [18], ISO 27001 [20]`

Encryption supports confidentiality by protecting the data at rest from internal and external attacks. By protecting the databases only the authorized user/device with the key can decrypt these data. This can be applied to data when being stored on secure storage or transmitted on a network.

As mentioned above, considering only security is not sufficient in a scenario where numerous stakeholders are involved. For example, to deal with legal and organizational issues between two different stakeholders contract agreements, such as SLAs, which include security related metrics should be in place. It is important to specify security requirements upfront, but it is even more important to be able to monitor and verify whether these security requirements are being met throughout the lifetime of the contract. Further, with the increase of the complexity and the interconnection of CPPS components it is of utmost importance to ensure that safety requirements are identified and addressed as well.

- Security SLA metrics

[MSSI-1] *Service availability*

`Source: ENISA [23], C-SIG [24]`

Availability is the property of being accessible and usable upon demand by an authorized entity. It is an important service level objective (SLO), which describes when the services can be operated. Relevant SLOs can be: (i) service uptime, (ii) percentage of successful requests, (iii) average response time, (iv) max response time and (v) service reliability.

[MSSI-2] *Data Isolation*

`Source: ENISA [23], C-SIG [24]`

Data isolation supports confidentiality, integrity and availability of user data and services between different parties. Relevant SLOs: (i) user authentication level, (ii) authentication, (iii) user access storage protection, (iii) cryptographic brute force resistance, and (iv) key access control policy.

- Safety Metrics

[MSFI-1] *Continuous Maintenance*

`Source: IEC 61508-2 [25]`

Inputs from Functional Safety Audits and tests of the E/E/PE safety-related system shall be used to upgrade system operation and maintenance procedures

[MSFI-2] *Ensure sufficient frequency of maintenance*

`Source: IEC 61508-2[25]`

It shall be ensured that the frequency of routine maintenance procedures is sufficient to maintain the required functional safety. A possible approach are regular proof tests.

The above set of representative metrics, based on the SemI40 project requirements and the evaluated standards is not a finite set of measurable metrics, but a working set that will be further extended for each component of the use case.

C. Dependability of the CPPS Components

In the context of this work we use the CPPS meta-model as a tool to show the dependability between the levels, and the corresponding components of the end-to-end communication use case in order to have a security view of the whole system. By mapping the derived MSIs of the use case components in the corresponding objects of the meta-model is possible to identify monitoring points, thus an enhanced level of transparency can be ensured. If the security of one component is compromised it can also affect other components of the CPPS depending directly from that component, or indirectly from other components depending on that. The dependability between the CPPS components is shown in Figure 3.

In case one of the MSIs of the IIoT gateway is compromised, for e.g., **MSI-3** *Secure key/sensitive data storage*, from the meta-model we can identify the other components that can be affected by this security issue, such as *Protocol* (e.g., MSI-1) and *Database* (e.g., MSI-6). If MSI-3 is not fulfilled, it can

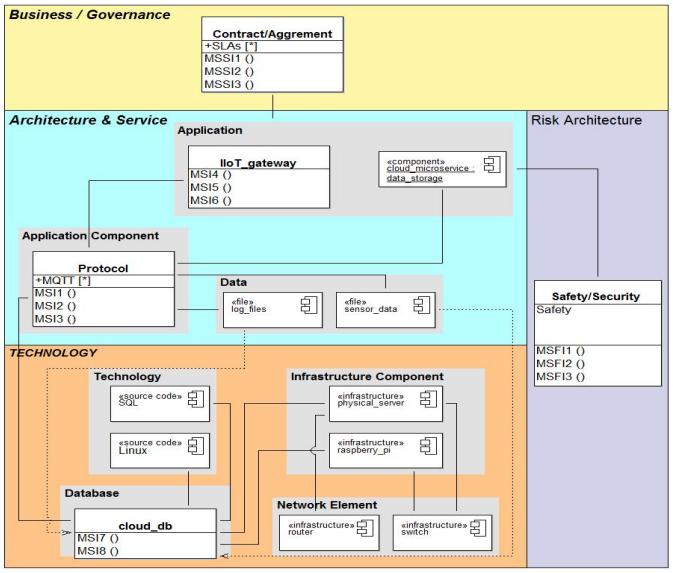

Fig. 3. CPPS meta-model used as a tool to show the dependability

result in for example, *sensor_data* loss. However, as discussed above security cannot be considered as independent from other aspects such as legal and safety. Thus, it is important to consider also MSSIs that are previously agreed in the SLA in order to prevent legal issues. The SLA metrics are mapped in the contract/agreement object in the CPPS meta-model. As future work we will derive and monitor measurable metrics related to operational security, legal and safety for all the CPPS components with the main focus to provide a higher level of transparency when implementing Industry 4.0 applications.

V. Conclusions and Future Work

In this paper we propose a trustworthy end-to-end communication in Industry 4.0. In our approach the dependencies among different CPPS components are analyzed based on operational security, legal and safety. To show this we have considered a use case addressing the communication from the edge devices to the backend infrastructure (e.g., cloud) via IIoT gateways. To ensure secured and trusted in-transit data, we have proposed to use secure messaging protocols that take advantage of a root of trust such as TPM for secure data exchange. By mapping the MSIs of the CPPS components in the corresponding object of the meta-model it is possible to define the dependability between components and layers. Thus, it is possible to provide a security view of the CPPS system as a whole. As our future work, we intend to derive operational security, legal and safety measurable metrics for all the CPPS components that are part of the proposed use case and define monitoring points in the CPPS meta-model to assure a trustworthy end-to-end communication in Industry 4.0. Our research challenges are mostly not addressed and we believe that future research in the area of CPPS can provide an additional level of security for Industry 4.0.

Acknowledgement

The work has been performed in the project Power Semiconductor and Electronics Manufacturing 4.0 (SemI40), under grant agreement No 692466.

References

[1] H. Kagermann, J. Helbig, A. Hellinger, and W. Wahlster, *Recommendations for Implementing the Strategic Initiative INDUSTRIE4.0*, 2013.
[2] L. Monostori, "Cyber-physical production systems: roots, expectations and r&d challenges," *Procedia CIRP*, vol. 17, pp. 9–13, 2014.
[3] R. Drath and A. Horch, "Industrie 4.0: Hit or hype?" *IEEE industrial electronics magazine*, 2014.
[4] M. Hankel and B. Rexroth, "The reference architectural model industrie 4.0 (rami 4.0)," *ZVEI, April*, 2015.
[5] C. Lesjak, H. Bock, D. Hein, and M. Maritsch, "Hardware-secured and transparent multi-stakeholder data exchange for industrial iot," in *Industrial Informatics (INDIN), 2016 IEEE 14th International Conference on*. IEEE, 2016, pp. 706–713.
[6] A. Bicaku, S. Balaban, A. Hudic, M. Tauber, A. Mauthe, and D. Hutchison, "Harmonized monitoring for high assurance clouds," in *CLaw: IEEE 2nd Workshop on Legal and Technical Issues in Cloud Computing and Cloud-Supported IoT*, 2016.
[7] I. I. Consortium *et al.*, "Industrial internet reference architecture," *Industrial Internet Consortium, Tech. Rep., June*, 2015.
[8] A. Fuqaha, M. Guizani, M. Mohammadi, and M. Aledhari, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*.
[9] M. Singh, M. Rajan, V. Shivraj, and P. Balamuralidhar, "Secure mqtt for internet of things (iot)," in *Communication Systems and Network Technologies (CSNT), 2015 Fifth International Conference*. IEEE, 2015.
[10] T. Masood, C. B. Cherifi, and N. Moalla, "Service networks monitoring for better quality of service," *arXiv preprint arXiv:1506.01491*, 2015.
[11] J. Delsing, "Iot automation: Arrowhead framework," 2017.
[12] S. Engell, R. Paulen, M. Reniers, C. Sonntag, and H. Thompson, "Core research and innovation areas in cyber-physical systems of systems," in *International Workshop on Design, Modeling, and Evaluation of Cyber Physical Systems*. Springer, 2015, pp. 40–55.
[13] I. Windhorst and A. Sunyaev, "Dynamic certification of cloud services," in *Availability, Reliability and Security (ARES)*. IEEE, 2013.
[14] C. A. Ardagna, R. Asal, E. Damiani, and Q. H. Vu, "From security to assurance in the cloud: a survey," *ACM Computing Surveys (CSUR)*, vol. 48, no. 1, p. 2, 2015.
[15] A. Maña, E. Damiani, S. Gürgens, and G. Spanoudakis, "Extensions to pattern formats for cyber physical systems," in *31st Conference on Pattern Languages of Programs. Monticello, IL, USA*, 2014.
[16] D. Symantec, "Cyberespionage attacks against energy suppliers, version 1.21," *Mountain View*, 2014.
[17] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *System*, vol. 1, no. a2, p. a3, 2008.
[18] K. Stouffer, J. Falco, and K. Scarfone, "Guide to industrial control systems (ics) security," *NIST special publication*, no. 82, 2011.
[19] I. ISO and I. Std, "Iso 27002: 2013," *Information Technology-Security Techniques-Code of Practice for Information Security Management. ISO*.
[20] J. Brenner, "Iso 27001: Risk management and compliance," *Risk management*, vol. 54, no. 1, p. 24, 2007.
[21] I. ISO and I. Std, "Iso 15408-1: 2009," *Information technology-Security techniques-Evaluation criteria for IT security-Part*, vol. 1.
[22] T. C. for Internet Security, "The cis critical security controls for effective cyber defense," 2016.
[23] G. Hogben and M. Dekker, "Procure secure: A guide to monitoring of security service levels in cloud contracts," *European Network and Information Security Agency (ENISA) Report*, 2012.
[24] C. SLA, "Cloud service level agreement standardisation guidelines," Technical Report C-SIG SLA 2014, European Commission, Tech. Rep.
[25] R. Bell, "Introduction to iec 61508," in *Proceedings of the 10th Australian workshop on Safety critical systems and software-Volume 55*. Australian Computer Society, Inc., 2006, pp. 3–12.