Securing IT/OT Links for Low Power IIoT Devices

Design considerations for industry 4.0

Mantravadi, Soujanya; Schnyder, Reto; Møller, Charles; Brunø, Thomas Ditlev

Published in:
IEEE Access

DOI (link to publication from Publisher):
10.1109/ACCESS.2020.3035963
10.1109/ACCESS.2020.3035963

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0

SOUJANYA MANTRAVADI[1], RETO SCHNYDER[2], CHARLES MØLLER[1], AND THOMAS DITLEV BRUNOE[1]

[1] Department of Materials and Production, Aalborg University, 9220 Aalborg, Denmark
[2] Department of Mathematical Sciences, Aalborg University, 9220 Aalborg, Denmark

Corresponding author: Soujanya Mantravadi (e-mail: sm@mp.aau.dk).

This work was supported by the Manufacturing Academy of Denmark (MADE Digital project), financed by the Innovation Fund Denmark; and the SECURE project of Aalborg University.

ABSTRACT Manufacturing is facing a host of new security challenges due to the convergence of information technology (IT) and operational technology (OT) in the industry. This paper addresses the challenges that arise due to the use of low power Industrial Internet of Things (IIoT) devices in modular manufacturing systems of Industry 4.0. First, we analyze security challenges concerning the manufacturing execution system (MES) and programmable logic controllers (PLC) in IIoT through a selective literature review. Second, we present an exploratory case study to determine a protocol for cryptographic key management and key exchange suitable for the Smart Production Lab of Aalborg University (a learning cyber-physical factory). Finally, we combine the findings of the case study with a quality function deployment (QFD) method to determine design requirements for Industry 4.0. We identify specific requirements from both the high-level domain of factory capabilities and the low-level domain of cryptography and translate requirements between these domains using a QFD analysis. The recommendations for designing a secure smart factory focus on how security can be implemented for low power and low-cost IIoT devices. Even though there have been a few studies on securing IT to OT data exchange, we conclude that the field is not yet in a state where it can be applied in practice with confidence.

INDEX TERMS Internet of Things, Information security, Manufacturing systems, Information systems, Manufacturing operations management, Manufacturing flexibility, Cyber-physical systems, Industrial cybersecurity, Smart factory

I. INTRODUCTION

The Industrial Internet of Things (IIoT) has the potential to disrupt the traditional manufacturing industry. However, this industry seems unprepared to handle the challenges surrounding its cybersecurity infrastructure, especially in wireless networks. This paper provides guidelines for managing security in a *smart factory*, which is a central concept of Industry 4.0.

Boyes et al. 2018 [1] propose the following definition of IIoT:

> "A system comprising networked smart objects, cyber-physical assets, associated generic information technologies and optional cloud or edge computing platforms, which enable real-time, intelligent, and autonomous access, collection, analysis, communications, and exchange of process, product and/or service information, within the industrial environment, so as to optimise overall production value. This value may include; improving product or service delivery, boosting productivity, reducing labour costs, reducing energy consumption, and reducing the build to-order cycle."

The Industry 4.0 vision of the smart factory concerns digitizing manufacturing operations using futuristic technologies, with a design principle of *interconnection*, which pertains to devices being connected over a network. Interconnection deals with the IIoT [2], Internet of People [3], and the Internet of Everything [4], while creating challenges and opportunities concerning the IIoT devices. The *ISA 95* hierarchy of systems [5] is becoming distributed due to the adoption of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

the IIoT. This introduces new security challenges, which are to be addressed by creating solutions for secure networks in smart factories.

Many manufacturing facilities around the world have already been subject to attacks due to failures of industrial cyber-security. A well-known case of a cyber-attack based on industrial control systems is that of Stuxnet in Iran in 2010, where over 15 Uranium enrichment facilities were infiltrated [6]. This attack was aimed at impairing the nuclear program of Iran; more than 900 uranium enrichment centrifuges were estimated to be damaged, as the attack could inflict physical damage to the equipment. There is an increasing trend of such attacks in industries around the world. Some of the recent ones are WannaCry (2017), the TRITON attack on Saudi Arabia Petrochemical (2017), and the LockerGaga attack on the Norwegian Aluminum Company (2019), as well as a recent attempt on a Tesla factory in Nevada (2020).

Security in the IIoT entails the protection of industrial automation and control systems against unauthorized access, information theft, and interference with the proper functioning of the factory [7]. This is achieved for example by securing the links between devices via cryptographic encryption and authentication methods, by deploying strong firewalls, and by monitoring all access and detecting anomalies [8]. The manufacturing environment provides additional challenges compared to traditional information technology (IT) systems, especially due to the convergence of IT and operational technology (OT) systems. Some of these challenges are the use of heterogeneous components, low power devices with long lifespans, real-time requirements, and the risk of physical damage to humans, equipment or the environment [9]. Low power devices are devices with low energy consumption, though our paper predominantly focuses on devices with low processing power and memory, which often are consequences of low energy consumption. Paes et al. 2020 [10] define IT/OT convergence as follows:

> "IT/OT convergence is the integration of IT systems applied to data-centric computing with OT systems used to monitor events, processes, and devices and make adjustments in enterprise and industrial operations. IT is composed of those hardware and software system technologies that allow for corresponding information processing. OT is supported by physical devices, i.e., switches, sensors, power distribution networks, valves, motors, and software that allow for control and monitoring of a plant and its associated equipment."

Our impression from the literature is that security management in IIoT is still a nascent topic, since the majority of studies only focus on the benefits of connecting machines, devices, processes, sensors, and people over the network in a factory. However, some studies do warn about the security challenges and emphasize the need for a multi-layered security strategy around the enterprise information systems [1]. There has been a series of papers attempting to design

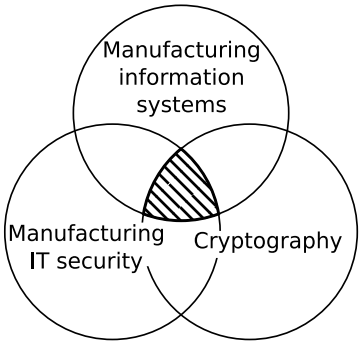

FIGURE 1. Research focus.

cryptographic protocols that are specifically suited to the low power, low latency characteristics of the IIoT, e.g. [11], [12], but there remains the question of how to apply these ideas to existing enterprise information systems. Motivated by this need, we study the inherent security challenges in the context of IIoT and analyze existing cryptographic solutions to derive design considerations for the IT/OT link. Our research objective is to identify the capabilities in a factory to connect to any IIoT device securely and easily.

The intersection of the Venn diagram in Fig. 1 shows our focus area. The IT system in the case of IT/OT convergence is usually a manufacturing operations management system of ISA 95, which in most cases is a manufacturing execution system (MES) or the like. In this paper, we use MES as representative of IT, and programmable logic controllers (PLC) as representative of OT, even though these concepts can include systems other than MES and PLCs. For example, OT could also include single-board computers such as Raspberry Pis, smart sensors, and computer numerical control systems. IT could include various edge and cloud servers or an IIoT platform separated from the MES.

A. CONTRIBUTIONS

Our work makes both theoretical and practical contributions. The following is a summary of our main contributions.

- We explore the security concerns relating to the IT/OT link for low power IIoT devices and examine the relevant smart factory design principle of interconnection in the context of ISA 95. We find that the IT/OT link and the cryptographic solutions for it are a weak point in IIoT.
- We analyze cryptographic protocols for IIoT devices with a focus on key management and authenticated key exchange. We study the feasibility of certificateless key exchange protocols in the context of the Smart Production Lab (Smart Lab) of Aalborg University, which serves as a case example of a modular manufacturing system.
- We propose design recommendations for securing the IT/OT link, using a quality function deployment (QFD) tool to translate between high and low-level require-

ments. We use the case of the Smart Lab to derive a high-level architecture for secure data exchange between the MES and the PLCs. We also outline some avenues for future research.

B. OUTLINE OF THE PAPER

Section II presents the background for the design challenge as well as related work. In Section III, we provide the methodology of our work. Section IV presents an overview of existing cryptographic security measures and Section V describes the research approach where the Smart Lab case is used. The findings from the case study and QFD are discussed in Section VI. Finally, some conclusions are drawn in Section VII.

II. BACKGROUND AND RELATED WORK

This paper is concerned with attacks that are carried out by interfering with the network connection between IT and OT. This particularly affects the IIoT, since it can involve many connections, including connections over the Internet. There are other possible attack vectors, which we do not focus on, such as in the case of Stuxnet, where a worm was installed using an infected USB drive.

A. DESIGN PRINCIPLE OF INTERCONNECTION FOR SMART FACTORIES

Industry 4.0 business requirements aim to address the customer responsiveness challenges by increasing product variety and decreasing the product life cycles [13], and these needs are supported by modular manufacturing systems. Easy, secure, and standards-based connections between machines, devices, sensors, and personal devices will enable the flexibility of combining equipment from different vendors, thus enabling modular manufacturing systems [14]. The technical requirements of Industry 4.0 can be derived from the following design principles for smart factories [15]: (a) Interconnection (b) Information transparency (c) Decentralized decision-making (d) Technical assistance. Here, the principle of interconnection is relevant to our study because it deals with connecting machines, devices, sensors, and people over the IIoT [2].

Industry 4.0 needs digitalization enabled by enterprise information systems such as MES [16] for real-time operations and robust information management [17]. ISA 95 presents object models which can be used as a basis for developing MES functionalities [18].

ISA 95 is an information-oriented standard, which contains models and terminology that are useful to analyze the information systems of a manufacturing company. It has a *functional hierarchy model* which separates the enterprise domain from the control domain in a manufacturing enterprise, and aims to achieve a seamless data flow between them. Scholten [18] describes the goals of the ISA 95 standards as follows:

> "The standard can be used to simplify the implementation of new software products and to ultimately have enterprise and control systems that interoperate and easily integrate."

MES takes its position in Level 3 in ISA 95 and offers a critical link between the shop floor and business (see Fig. 2). However, ISA 95 does not cover the digital interconnection to enable IIoT, therefore the traditional automation hierarchy needs to be reformed while considering security management.

For Industry 4.0, many manufacturers consider MES as a suitable candidate for IIoT data aggregation and processing. If an MES is designed with the functionalities of ISA 95, it can be deployed in the following three combinations:

1) An MES server completely hosted on the cloud;
2) An MES completely hosted on a local server (on-premise);
3) Some MES functionalities hosted on the cloud, some locally (hybrid).

In most cases, the MES is not run on the cloud, but it is connected to cloud services for analytics. Enterprise resource planning (ERP) may be hosted in the cloud as well. Even though it is attractive to have the MES as an app on the cloud for data analytics (see Fig. 2), our design recommendations primarily cater to manufacturers who are looking to host the MES on a local server.

Having (parts of) the MES hosted locally can simplify security considerations, because PLCs do not need to be directly connected to the Internet. Hence, well-established protocols like Transport Layer Security (TLS) can be employed to secure connections over the Internet, and only local connections need to take into account the limited processing power of PLCs.

B. SMART FACTORY NEEDS FOR EDGE COMPUTING

Edge computing is an attractive option for smart factories [20], [21] because it could solve the challenges of data overload and latency. Edge computing belongs to the distributed computing paradigm and involves the offloading of computation, storage of production data, and communication to physical devices on or near the shop floor. Edge computing stands in contrast to cloud computing, where production data are stored and analyzed on centralized servers, often distant from the place where it originates and where the results of the analysis are needed. By being close to the production assets of the shop floor, edge computing avoids the high latency inherent in cloud computing and is therefore better suited to fulfill real-time requirements. Furthermore, edge computing is much more reliable than cloud computing where there is a risk of Internet outages. Edge and cloud computing are often used together in factories, with less critical tasks being offloaded to the cloud.

When several edge servers are present in a factory, and PLCs send their performance data directly to them, the number of IT to OT connections that need to be secured is greatly increased. Hence, it becomes even more important to be able to automatically and efficiently establish secure connections

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

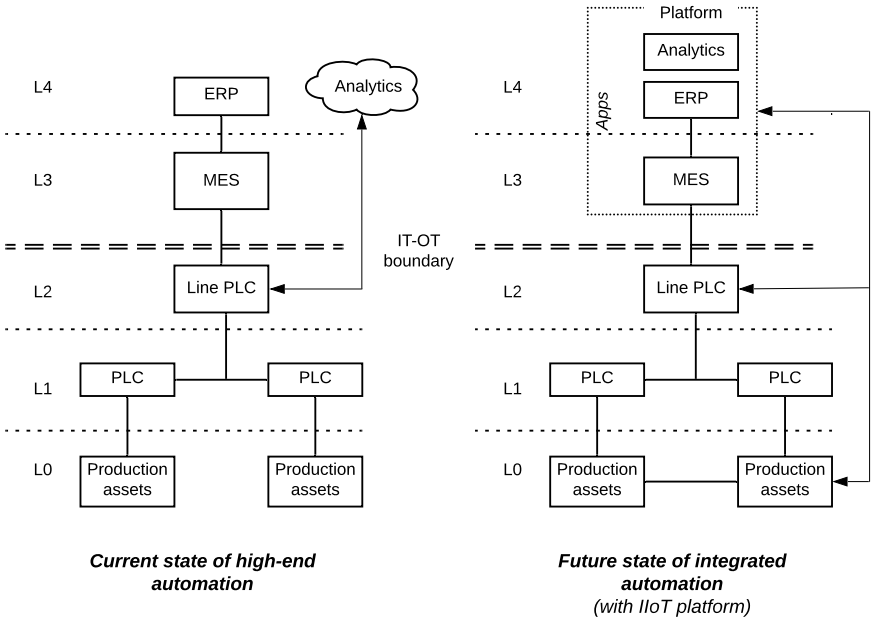

FIGURE 2. Architecture showing interconnection and digitalization of traditional ISA 95 hierarchy of systems in IIoT [19].

between newly added PLCs and MES/edge servers, which falls within the scope of our problem.

C. RELATED WORK ON SECURITY ISSUES IN IIOT

We conduct a selective literature review using Google Scholar to understand the state of the art of security issues in IT/OT interconnection in IIoT. We look specifically for recent studies concerning security issues of IIoT in the ISA 95 hierarchy. The results of our literature review are summarized in Table 1.

There is a large body of literature addressing security challenges and possible attacks in the Internet of Things (IoT) in general, e.g. [27]–[30]. However, we focus here on the literature that specifically concerns IIoT.

Several recent studies have addressed and categorized the security challenges and requirements for IIoT, from different approaches. For example, [22] categorizes security challenges based on whether they apply to IoT in general, or are specific to IIoT. In [9], the ways in which security considerations differ between IIoT and traditional IT systems are discussed. A systematic literature review of IIoT security requirements is presented in [24]. [26] describes security challenges affecting IIoT along with recent cybersecurity incidents in Industry 4.0.

Specific attacks that could be leveraged against IIoT are surveyed in e.g. [25], which gives a taxonomy of attacks at the different layers in the IIoT architecture based on the attack vector, target, impact, and consequence. In [31], attacks against IoT and IIoT, and countermeasures against them, are categorized based on whether they target the physical hardware, the network, the data, or the software. Also, [9] lists different types of attack as well as potential sources of attacks (such as nation-states, or rival organizations).

There are also a number of studies and surveys that give overviews of security solutions and standards relating to IIoT. For example, [9] presents a high-level overview of some of the most important security solutions, such as regulations and standards, cryptographic techniques, and intrusion detection. [32] discusses cryptographic algorithms and key management, and the issues regarding their implementation under the constraints of IIoT. A detailed review of cryptographic key establishment protocols is provided in [33]. A survey of existing standards for security and interoperability in Industry 4.0 is presented in [23]. In [34], the security properties of different IIoT edge and platform connectivity protocols are analyzed.

We note that there are several studies that explore security challenges, attacks, and security solutions for IIoT. However, there is still only a limited understanding of how and how well these solutions can be applied to IIoT devices in practice. This, we believe, is because most of the research we found does not consult a concrete example of a smart factory.

D. SUMMARY

The literature shows the need to develop security management methods in operational architecture. An MES has features from an enterprise-level IT system as well as an industrial control system featuring high-level process control. Since MES is the interface between the IT and OT domain, the role of secure interconnection in these layers needs a

TABLE 1. Studies on IIoT security concerning Level 3 of ISA 95 (or Purdue model).

Author(s)	Goal of paper	Key takeaway	Method	Challenges identified
Boyes, 2018 [1]	Analysis framework and taxonomy for IIoT	Purdue model is used to give background, definitions, and taxonomy to classify IIoT devices; and to explain IIoT including security	Review	Security considerations for installing IIoT devices in an operational architecture
Yu, 2019 [22]	To survey security challenges around IIoT	IIoT has specific security concerns mainly for critical industrial control systems	Literature survey	Industry-specific challenge due to IT and OT convergence, cyberattacks on OT
Watson, 2017 [23]	To give an overview of existing Interoperability and security standards, such as IEC 62443, the ISO 27000 series, IEC 62541, OPC Unified Architecture and TSN (IEEE 1722-2016)	Industry 4.0 architecture features interconnection where security challenges need to be sufficiently addressed	No method identified	Additional testing and extensions are required for security and interoperability standards due to IIoT
Tange, 2020 [24]	To survey the security requirements of IIoT	Fog computing as a security solution for the IIoT	Systematic literature review	Safety requirements compete with security in terms of resources
Panchal, 2018 [25]	To discuss the potential security threats to the Industries adapting to IIoT	Listed various possible attacks on the components in the layered IIoT architecture, along with a taxonomy	No method identified	No challenges identified
Bajramovic, 2019 [26]	To describe some of the security challenges and best practices in IIoT	Merging IT and OT exposes technologies with identified vulnerabilities Also studied the Reference Architecture Model of Industry 4.0	No method identified	Establish a need for security standards
Morariu, 2018 [7]	To study security challenges in distributed MES architectures and provide a policy-based security mechanism for transport and document security	Usage of public key infrastructure on the shop floor	Experiment	Mentioned the security need for preventing unauthorized access to information, theft of proprietary information and impersonation

better understanding, both theoretical and practical. Hence, we pose the following questions for this paper:

Q1) Is it possible for the MES to connect securely and wirelessly to PLCs in IIoT, given the need to readily add new OT devices to the network?

Q2) What special considerations are necessary for security between the MES and PLCs in the IIoT?

To address these questions, there is a need to look into cryptographic developments in IIoT. We elaborate on this in Section IV.

III. METHODOLOGY

Based on a selective literature review on security in IIoT (see II-C), we have identified the gap in securing the link between IT and OT devices concerning the ISA 95 levels. To address the gap, we have made a critical analysis of existing cryptographic protocols that are suitable for the low power restrictions common in OT devices (see IV-B). We then conducted an exploratory case study to test the feasibility of one such type of protocol in the Smart Lab (see V-A). Based on this case study, we have drawn the design requirements for interconnection and linked them with the relevant characteristics for cryptographic protocols using QFD (see VI-B). Finally, we will provide design recommendations on secure interconnection around the MES and the PLCs (see VI-D). We synergize relevance and rigor with a pragmatic research approach inspired by the three cycle view of design science research by Hevner 2007 [35].

IV. CRYPTOGRAPHY FOR IT/OT LINKS IN IIOT

A. SECURITY CHALLENGES FOR IIOT INTERCONNECTION

The inclusion of end devices in the network introduces various security issues, which need to be addressed through different means. Especially if wireless technology is employed, it can become feasible for attackers to infiltrate a network and attempt to read or modify transmissions, or imitate legitimate nodes, for example to execute a man-in-the-middle attack. An attacker who can modify transmissions can disrupt production or even damage the equipment, among other things.

We focus on the challenges of confidentiality, integrity, and authenticity in IT/OT data exchange, as well as key management in IIoT. Our motivations for choosing these foci are: First, when surveying the cryptographic developments in IIoT, we found that a majority of studies and protocols focus on these four issues. Second, to limit the scope of this paper, we restrict our attention to challenges that directly concern the data transmission between the MES and the IIoT devices, and that are commonly addressed by cryptographic means. There are many other challenges to security in IIoT that we do not focus on, such as:

- Authorization, which is the verification that an entity is permitted to carry out certain operations or access certain data [36];
- Non-repudiation, which means that the sender of a transmission should not be able to credibly deny having

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

sent it;
- The protection of data in storage from unauthorized access or modification;
- Availability, which is the guarantee that the services and resources of a system are always accessible, including protection against denial-of-service attacks;
- Intrusion detection, which is the ability to detect ongoing attacks [9];
- Post-incident management, which is the ability to recover from an attack and to mitigate the damage done [9];
- Accountability, which is the ability to pinpoint the source of unauthorized behaviour.

Due to its limited presence in the literature, we do not focus on non-repudiation, even though it may fall within our scope.

1) Confidentiality, integrity, and authenticity of IT/OT data exchange

To prevent transmissions between IIoT devices and MES servers from being read or modified, and to prevent forged transmissions from being inserted, confidentiality, integrity, and authenticity need to be guaranteed [32].

Confidentiality means that the data being transmitted cannot be read by unauthorized parties. Confidentiality prevents an attacker who has gained access to the network of a factory from extracting trade secrets, such as production recipes, or information about the current performance of the factory. It is achieved using encryption. For example, a fast symmetric cipher, such as the Advanced Encryption Standard (AES), can be employed.

Integrity prevents modification of the data in transit, and *authenticity* prevents the impersonation of the sender by an attacker. This is needed to, e.g., prevent an attacker from sending malicious instructions to IIoT devices that would disrupt production, or from falsifying measurements sent from the devices to the MES. Both integrity and authenticity can be efficiently attained using symmetric cryptography, for example with message authentication codes.

However, to apply these symmetric protocols, both parties (the MES and the IIoT device) need to know a common secret key ahead of time. The establishment of such a shared key while verifying the identity of the other party is more challenging, and is called *authenticated key exchange*. This can be done using public key protocols, which however tend to place higher requirements on processing time and memory. Traditional choices like RSA and Diffie–Hellman are likely to be unsuitable for low power IIoT devices. Another option are password-authenticated key exchange protocols, such as [37], in which the two parties exchange a secret key based on a password (or other secret) known to both of them. This however requires having a pre-shared password for each pair of devices that need to interact, which increases the complexity of adding new devices to a modular manufacturing system.

2) Key management for IIoT devices

A requirement for authenticated key exchange is key management, that is, the generation, distribution, storage, updating, and revocation of long-term keys on IIoT devices [32]. Long-term keys installed on each device are needed to exchange shared secret keys between any two devices that need to connect. While one option for key management is to generate keys on a central key distribution center and preinstall them on each device, this method is more vulnerable to adversaries who can compromise or reverse engineer the key distribution center. Instead, each device should be able to generate its own keys.

B. KEY MANAGEMENT FOR IIOT

There is a range of cryptographic protocols that are specifically tailored to the IIoT. As explained in Section IV-A, the question of key management and authenticated key exchange between the PLCs and MES is of special interest. Below we describe the four popular cryptographic approaches to these problems that we have identified in the literature.

1) Public key infrastructure

One type of solution for key management is a traditional public key infrastructure (PKI), as is commonly used with TLS. In this case, each device has a public and a private key, and a trusted certificate authority (CA) issues certificates which guarantee that a given public key belongs to a certain device on the network. The MES and a PLC can then use these key pairs to authenticate each other and exchange shared secret keys. For example, the approach proposed by [7] is based on PKI. However, there is a large management overhead to the issuing, storage, distribution, verification, and revocation of certificates, and the necessary public key operations tend to be computationally expensive, which may make PKI unsuitable for the IIoT [38].

Fig. 3 is a Unified Modeling Language (UML) communication diagram which shows the data exchange involved in the phases of certification and key exchange for a PKI. The exchange between the CA and the other devices occurs during the initialization phase of each device, and the exchange of public keys and certificates happens when the two devices first need to interact.

2) Protocols based on symmetric cryptography

To avoid expensive public key operations on low power devices, several key exchange protocols have been proposed which only require the device to execute symmetric cryptography. These protocols depend on a pre-shared and static symmetric key known to the device and some central server. The central server then negotiates a key exchange between two devices. Kerberos [39] is a well-known protocol of this type, and the authenticated key exchange protocol by [11] is specifically targeted at IoT. The networks by, e.g., Sigfox [40] or LoRaWan [41] also use this type of protocol. One disadvantage of these protocols is the active involvement of the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

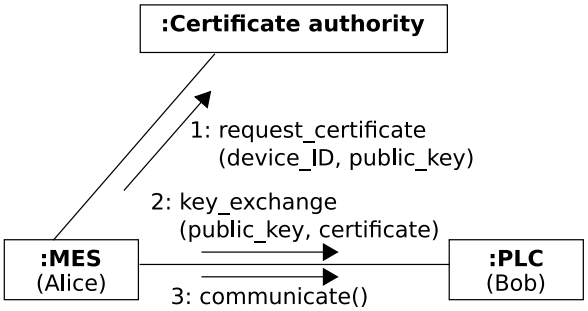

FIGURE 3. UML communication diagram showing simplified data exchange during setup and key exchange for a public key infrastructure.

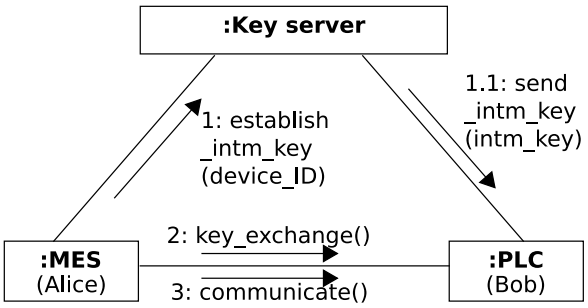

FIGURE 4. UML communication diagram showing the simplified data exchange during the three-party authenticated key exchange of [11].

central server during the key exchange, which complicates the process and increases the attack surface.

Fig. 4 shows the simplified data exchange involved in the key exchange phase for the protocol of [11]. The initiating device and the key server first establish an intermediate key using their pre-shared secret key. The key server sends that intermediate key to the second device, encrypted using their pre-shared secret key. Then, the two devices use this intermediate key to perform authenticated key exchange.

3) Certificateless protocols

An alternative proposal is *certificateless cryptography*. This is a variant of identity-based cryptography [42], in which the identity of a device (e.g., its address) serves as its public key, and private keys are generated by a trusted central server called the private key generator. This has the advantage that there is no need for devices to send public keys back and forth, nor to validate them. However, identity-based cryptography brings with it the key-escrow problem, which is to say that the private key generator has access to the private key of every device. Thus, the compromise of the private key generator is particularly damaging.

In a certificateless protocol, there is still a central server, called the key generation center (KGC), which generates partial private keys for devices based on their identity [43]. From such a partial private key and a self-chosen secret value, a device creates its final private key. The KGC therefore does not know the private key of the device. The device also creates its own public key. Fig. 5 and Fig. 6 show

Input: The public parameters `params` of the KGC and the identity ID_A of device A
Output: The public key P_A and private key S_A of device A

1: $r \leftarrow$ a private pseudo-random value
2: $x_A \leftarrow \textsc{Set\_Secret\_Value}(\texttt{params}, \mathrm{ID}_A, r)$
3: $P_A \leftarrow \textsc{Set\_Public\_Key}(\texttt{params}, \mathrm{ID}_A, x_A)$
4: $D_A \leftarrow$ partial private key requested from the KGC for identity ID_A
5: $S_A \leftarrow \textsc{Set\_Private\_Key}(D_A, x_A)$

FIGURE 5. Key generation for certificateless cryptography. This is run on device A to generate its key pair. Notation from [43].

Input: The public parameters `params` and master secret key `master_key` of the KGC, and the identity ID_A of device A
Output: The partial private key D_A of device A

1: $D_A \leftarrow \textsc{Partial\_Private\_Key\_Extract}($ `params`, `master_key`, $\mathrm{ID}_A)$

FIGURE 6. Generation of the partial private key on the KGC. This is run in response to device A requesting a partial private key.

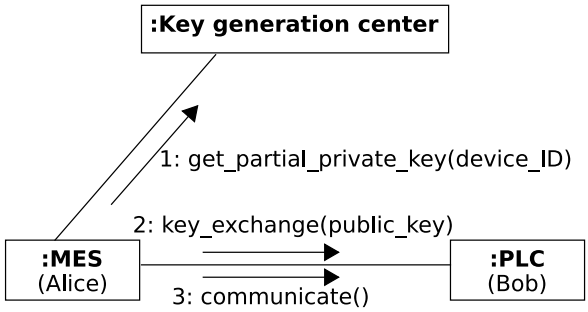

FIGURE 7. UML communication diagram showing simplified data exchange during setup and key exchange for a certificateless cryptographic scheme.

the process of key generation for a device, showing the operations performed by the device and the KGC.

Fig. 7 shows the data exchange involved in the phases of setup and key exchange for a certificateless key exchange protocol. The exchange from the KGC to the other devices occurs during the initialization phase of each device, and the exchange of public keys happens when the two devices first need to interact. Multiple proposed certificateless schemes, also for other purposes than key exchange, are targeted at the IIoT, for example [12], [44]–[46]. However, some of them have been broken, and since this type of scheme is relatively new, there is not yet much confidence in many of the protocols. Furthermore, the need to distribute public keys reintroduces some of the overhead of PKI-based protocols that identity-based cryptography avoids, and the problem of key revocation needs to be addressed as well. So it is not clear if this approach is currently preferable to PKI in practice.

4) Physical unclonable functions

Another approach for device authentication and key exchange for low power devices is the use of a physical un-

clonable function (PUF). A PUF is a hardware circuit that, given an input, generates an output which (ideally) depends deterministically on the input but is otherwise unpredictable. The output is determined by the physical characteristics of the PUF, which are the result of random variations during its production. Any two PUFs will generate different outputs on a given input. Furthermore, it should not be feasible to replicate the behaviour of a PUF in software or hardware. Hence, the behaviour of the PUF of a device can be thought of as its fingerprint. For an overview of the use of PUFs in the IoT, see [47].

There are several protocols that employ PUFs to perform authentication and key exchange between a low power device and a server (e.g. [48]–[50]), or between two low power devices with the help of a trusted third party (e.g. [50]). The main advantage of these protocols is that they can function even on devices with extremely limited computational power and memory. As a downside, these protocols require either the active involvement of a trusted central server during key exchange, or a separate setup phase for every IIoT device with each server it needs to communicate with.

C. SUMMARY

All the solutions discussed above, with the exception of some protocols using PUFs, depend on having a trusted central server that negotiates trust between the parties of the network. To protect this central server from compromise, it should be sufficiently separated from the other IT in the smart factory. Of the solutions mentioned above, certificateless protocols and public key infrastructures do not need this central server to be connected to the network during regular operation. Among these, certificateless schemes promise to be simpler and potentially place lower requirements on the PLC hardware.

Beyond cryptographic considerations, the goal of securing the interconnection in smart factories needs collaboration between different disciplines. Information systems, such as MES, that are the backbone of smart factory operations must be designed from the ground up with security in mind. Given what we have learned from analyzing the literature on IIoT security and cryptographic protocols, the following additional questions arise:

- Are these specialized cryptographic schemes, in particular the certificateless protocols, efficient enough to run on low power legacy PLCs?
- How can these cryptographic solutions be applied to improve industrial cybersecurity?
- Is secure interconnection in smart factories a socio-technical concern rather than a purely technical venture?

V. A CASE STUDY

To understand the operation, structure, technology, and challenges of a smart factory, we use the example of the Smart Production Lab (Smart Lab) of Aalborg University (a learning cyber-physical factory). This exploratory case study allows studying the connection between MES and PLCs in an IIoT environment. Based on the example, we check the feasibility of using certificateless schemes and can propose a design for securing the data exchange between MES and PLCs.

A. SMART LAB SETUP

The Smart Lab of Aalborg University is a "small Industry 4.0 factory" [51], which is based on the cyber-physical factory by the Festo company. Festo is a leading industrial control and automation company, based in Germany. The automated production line of the Smart Lab has PLCs and is capable of being integrated with third-party IIoT devices. It is a learning lab with an assembly line that manufactures mock mobile phones by performing various operations, such as assembly, drilling, etc. For our study, we analyze its control domain and its network architecture, as shown in Fig. 8. The network can either operate fully wired or employ wireless communication between the PLCs and the MES. The fully automated assembly line is a discrete manufacturing facility and includes:

- Five production modules with two stations each;
- An MES, installed on a single computer, is the high-level process control and orchestrates overall production;
- A Festo CECC-LK PLC on each station of each production module;
- Switches which connect the PLCs and the MES computer using ethernet cables;
- In the case of wireless operation, a wireless multi-access gateway (MAGW) on each module and on the MES computer, which tunnel ethernet traffic over Wi-Fi or Long-Term Evolution (LTE) [52].

The cyber-physical factory, with its modular manufacturing systems, is meant for studying Industry 4.0 enablers. It fits the definition of the IIoT system by Boyes [1], in that it consists of networked PLCs which control a physical process, and which exchange real-time control information with an MES through the OPC Unified Architecture (OPC UA) protocol. Furthermore, the lab connects to an IIoT cloud platform by KUKA, which can be accessed through a web service.

During operation, the products are placed on carriers, which are transported through the production line on conveyor belts. During the process, the data exchange between the MES and the PLCs on the stations is as follows:

1) When a carrier with a product arrives at a station, the PLC at the station identifies the carrier via RFID and sends the carrier ID to the MES.
2) The MES then responds to the PLC with instructions on which actions should be performed on the product.
3) When the action has been performed, the PLC informs the MES about the completion.
4) Once the carrier can continue to the next station, the MES notifies the PLC, which sends the carrier on its way.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

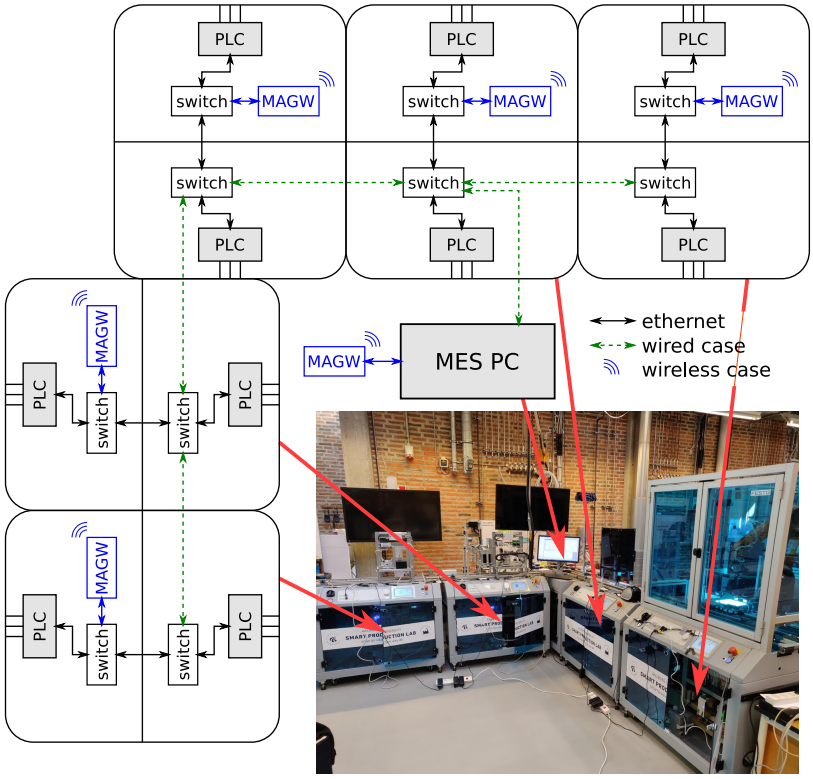

FIGURE 8. The network layout of the Smart Lab [52]. The green arrows represent ethernet cables that are used in wired operation. The blue elements are present only in wireless operation.

The Smart Lab is a modular manufacturing system, where the manufacturing line consists of several modules comprising controllers and machine tools [51]. This kind of setup, enabled by IIoT, supports reconfigurability in a factory, which is required to meet future market demands for high product variety and short product life cycles [53]. However, the two security concerns in this scenario can be:

1) During the steps listed above, an attacker could interfere with the data exchange by performing a man-in-the-middle attack and, for example, halt production or cause it to create the wrong product, as mentioned in [54].
2) To provide security in such modular systems, it must be possible to quickly establish secure connections between the MES and IIoT devices that are newly added to the production line. This is crucial to enable plug and play of IIoT devices in a smart factory.

B. CRITERIA FOR ASSESSING SECURE INTERCONNECTION

We assess our solution for secure interconnection based on the following two criteria.

1) Resistance to network sniffing and man-in-the-middle attacks between MES and PLCs

While there are many attacks an adversary can attempt after gaining access to the factory network, we focus on an attacker who reads the data transferred between the MES and a PLC of the Smart Lab or tries to insert themselves between the two, intercepting and potentially modifying all the data. This is in light of a 2016 study [54], in which a penetration test was conducted on the Smart Lab to determine its weakness to various attacks. The test was conducted on-site, from the internal network of the Smart Lab, focusing on the data exchange between the MES and PLCs. At that time, the lab was set up with only the default security configuration and was found to be weak in many ways. Among others, a port scan revealed many open ports on some of the network devices, including unsecure services like Telnet and File Transfer Protocol. Network sniffing found much of the traffic to be unencrypted and to include information about the network and its devices that would be useful for further attacks. The paper also mentions the possibility of conducting a man-in-the-middle attack via, say, Address Resolution Protocol spoofing, which would allow an attacker to modify data and commands exchanged between the MES and PLCs. Thus, the paper demonstrates the need for strong encryption and authentication of the data exchange between the MES and PLCs.

While these considerations assume that an attacker has access to the factory network, we stress that they are relevant even in case of a remote attacker. This is because after first having compromised a local device over the Internet, the attacker is then able to carry out further attacks from within

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

the network. An example for this is the TRITON attack in Saudi Arabia, in which the attackers first gained access to the IT systems of a petrochemical plant, and from there were able to move on to the OT network and finally infect safety systems [55].

2) Suitability for PLCs with low processing power and memory

We note from the literature we reviewed in Section II that the PLCs used in factories tend to have low computational power, and the same is true in the case of the Smart Lab. Hence, when choosing a cryptographic solution, we need to ensure that the PLCs are capable of running it, as otherwise expensive new hardware would need to be bought. Modularity allows connections with various IIoT devices and it is highly likely that some of them will be low power devices.

C. PROCEDURE TO CHECK THE FEASIBILITY OF A CRYPTOGRAPHIC SOLUTION

We check the feasibility of certificateless schemes for data exchange between MES and PLCs because some of the schemes have low computational power and memory requirements with an uncomplicated key exchange process. (We will elaborate on this in Section VI). The feasibility was checked in two steps:

1) Hardware feasibility: We choose a certificateless key exchange scheme with an open-source implementation and for which benchmarks exist [45] and compare the specifications of the PLCs used in the Smart Lab to the requirements of the scheme and the hardware used in the benchmarks.
2) Network feasibility: To check the feasibility of the implementation of such a scheme in the Smart Lab, we consider how the protocol fits into the existing network architecture.

D. SUMMARY

The Smart Lab presents a case example for a smart factory because it is built around the *Festo CP Factory*, allowing the addition and removal of modules, while integrating relevant Industry 4.0 technologies [51]. In its default configuration, it is highly vulnerable to cyberattacks from anyone who gains access to its network. Based on this, we discuss the design considerations in the following section.

VI. DESIGN CONSIDERATIONS & DISCUSSION

While previous studies on IIoT security did attempt to close the gap of integrating cryptographic schemes with an MES and PLCs, we follow the systems thinking approach, which studies the problem within the context of a larger system (a smart factory). This is beneficial because we will then be able to understand how a security implementation can interrelate with an information system like MES and how it should perform over time.

A. DESIGN REQUIREMENTS FOR SECURE INTERCONNECTION IN INDUSTRY 4.0

Industry 4.0 has smart factories that are reconfigurable. So far, the Smart Lab served its purpose of giving requirement specifications for a cyber-physical factory, which is synonymous to a smart factory. But the real-life case of a smart factory will need to consider the business requirements for Industry 4.0. Industry 4.0 sets out a vision for manufacturers to match future market requirements by manufacturing goods with high product variety and shorter product life cycles. Apart from the obvious requirements, such as wireless communication, the following should also be considered:

1) Low cost of hardware such as PLCs;
2) Exploiting IIoT opportunities to support a high degree of product variety in manufacturing;
3) Low implementation complexity in terms of reuse of existing IT systems (such as MES), especially for small scale manufacturers.

B. DETERMINING SECURITY REQUIREMENTS FOR A SMART FACTORY: USING QFD METHOD ON SMART LAB

To further distill the design requirements, we use the QFD method, which consists of a design tool called the House of Quality. QFD is a popular technique to enhance the quality of a system to be designed by identifying important design requirements. QFD was first developed in Japan in the 60s for the industrial engineering domain and gained popularity among other fields, such as software engineering, military applications, educational services, etc., since it is a structured and interdisciplinary technique.

We use the case of the Smart Lab to smoothly translate the high-level requirements of a cyber-physical factory into low-level security requirements for a cryptographic solution and to gauge their relative importance. Based on the *percent of importance* of each design characteristic, we prioritize the design characteristics of secure interconnection between MES and PLCs of the automated production line. We conduct the QFD in two phases (Fig. 9). In the first house (Fig. 10), the relationship matrix shows how much each design characteristic contributes to achieving a given design requirement. The correlation matrix, which is the *roof* of the house, presents whether the design characteristics synergize or conflict with each other. The second house (Fig. 11) works in the same manner.

Security assessment for a smart factory:

We use two phases in our QFD matrix to gather the requirements for secure interconnection in a smart factory (see Fig. 9). They are:

1) In the first house, QFD leads to matching up the design requirements of interconnection in smart factories with the design characteristics for security.
2) In the second house, the design characteristics for security are used to deduce the low-level requirements for the selection of a cryptographic scheme.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

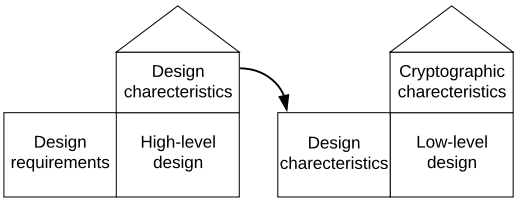

FIGURE 9. The two phases of QFD.

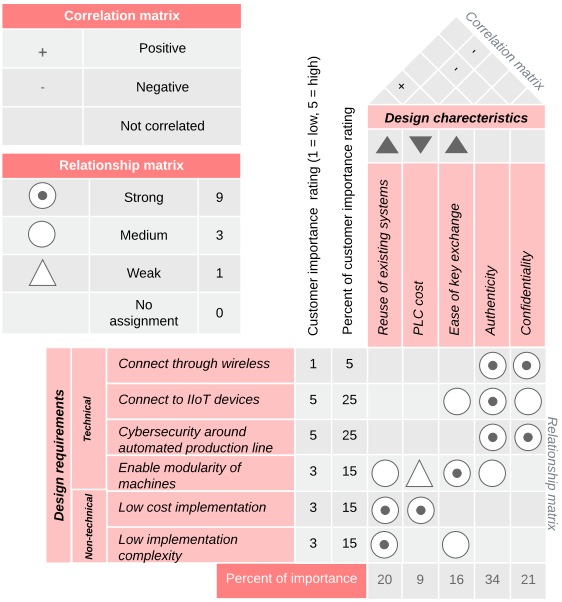

FIGURE 10. The first QFD house.

First house based on the case of the Smart Lab:

We choose the following design requirements, which adhere to the smart factory competencies: a wireless connection, connecting to IIoT devices, cybersecurity around an automated production line, modularity of machines, low cost of implementation, and low complexity of implementation. Our chosen design requirements are: the use of the existing PLCs and MES, the costs of the PLCs, the ease of key exchange, authenticity, and confidentiality. We include integrity under authenticity for the purpose of our QFD analysis, since they are closely related concepts that are usually achieved simultaneously by the same protocol, and would give almost identical evaluations.

We discuss the rows of the first house (Fig. 10) individually:

1) Connect through wireless: Authenticity and confidentiality are crucial requirements for wireless communication due to its higher vulnerability to attacks. This is a particularly important point as future factories might use 5G.
2) Connect to IIoT devices: This is a core requirement for smart factories. Authenticity is a crucial requirement for this because it prevents sabotage of the manufacturing process.
3) Cybersecurity around automated production lines: Cybersecurity is required to prevent sabotage of manufacturing orders and theft of competitive production information. Authenticity and confidentiality are crucial requirements for this.
4) Enable modularity of machines: Reconfigurable manufacturing systems enable flexibility and support production that is high in variety with short product life cycles. To enable this level of modularity, it is crucial that devices can readily exchange shared keys whenever they need to connect to a new peer.
5) Cost and complexity of implementation: The ability to employ low-cost PLCs and to reuse the existing infrastructure greatly assists in reducing cost and complexity.

From the calculated importance of the design characteristics, we conclude that authenticity is the most important design target for secure interconnection in smart factories. This matches with the idea that an attacker can do the most damage to a factory by disrupting and manipulating the production process.

Second house for cryptographic considerations:

To ensure that cryptography-based security solutions adhere to design targets, we chose the following cryptographic characteristics: processing time required (time required to execute the protocol on the given hardware), memory requirements (random-access memory (RAM) needed for executing the protocol), communication complexity (the amount of data needing to be transferred during the execution of the protocol), resistance to computational attacks (e.g., breaking encryption by only analyzing the encrypted data stream), resistance to infrastructure compromise (if, e.g., a central server is hacked into), and connection without third party involvement (no involvement of a central server during the key exchange between two machines).

The rows of the second house (Fig. 11) are discussed below:

1) Reuse of existing PLCs and MES: Low requirements on the hardware of PLCs make it more likely that legacy PLCs can be used. In the case of our Smart Lab, the existing PLCs appear to be capable of using certificateless cryptosystems.
2) Low cost of the PLCs: Low requirements of a cryptosystem can enable the use of cheaper PLCs.
3) Ease of key exchange: Key exchange is faster and easier if the processing and communication requirements are lower. It is furthermore helpful if the key exchange can be carried out by only these two devices. For the Smart Lab, third party involvement would mean the inclusion of an entirely new server in the network,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

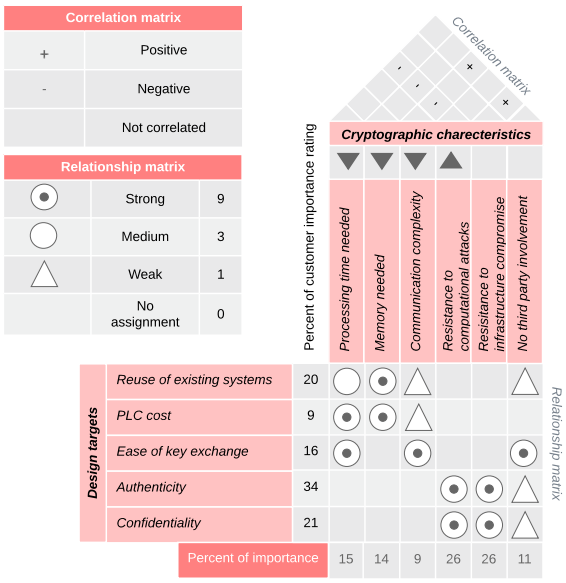

FIGURE 11. The second QFD house.

which we want to avoid.

4) Authenticity and Confidentiality: Evidently, to fulfil these requirements, the cryptographic scheme must be resistant to computational attacks. It is also helpful if the compromise of certain devices in the network does not allow the attacker to break the cryptography in other parts.

From the calculated relative importance of the cryptographic characteristics, we see that resistance to different kinds of attacks is the most important aspect. This is not surprising, since having vulnerable cryptography would defeat the purpose. The next most important are low requirements on memory and computation time. We conclude that the cryptographic protocols should be efficient, but not at the cost of security.

C. REQUIREMENTS FOR SECURE IT/OT CONNECTION

We address the security concerns raised in Section V-A by checking the feasibility of a cryptographic solution in the case of the Smart Lab, as described in Section V-C.

Hardware requirements:

To verify that certificateless schemes can satisfy the requirements for low power in the Smart Lab, we look for a certificateless cryptographic scheme which is targeted at low power devices and which has an implementation that allows us to deduce the concrete hardware requirements. The LiKe certificateless key exchange scheme [45] has an implementation available on GitHub[1]. Below we compare the requirements of LiKe to the specifications of the Festo CECC-LK PLCs [56] used in the Smart Lab:

[1] `https://github.com/pietrotedeschi/like-iot` (accessed May 26, 2020)

1) The LiKe protocol requires 13594 bytes of read-only memory and 960 bytes of RAM, which is well within the capabilities of the CECC-LK PLC, which has 2 MB of permanent storage and 16 MB of RAM.
2) In the benchmarks using OpenMote-b devices [57], the LiKe key exchange is reported to take around 340 ms for an 80-bit security level. Since the OpenMote-b has a clock speed of 32 MHz, which is less than the 400 MHz reported for the CECC-LK PLC, we expect that the PLCs should be able to complete the key exchange in a reasonable time. However, a direct comparison is impossible here, since the OpenMote-b contains hardware acceleration features for cryptographic operations, which speed up the key exchange.

We note, however, that it is not possible to directly use the existing implementation of LiKe in the Smart Lab since it was developed for the OpenWSN network stack [58], which is not available for the Festo CECC-LK PLC. Hence a new implementation would be needed.

Since we are taking an abductive approach to this study, we consider implementation to be outside the scope for this paper. Our contribution is instead on the architectural requirements side. Finally, we stress that we do not specifically recommend the LiKe cryptosystem, as it is a recent proposal and has not yet been subject to sufficient scrutiny to be used in real-world applications. But it serves as an example to demonstrate that certificateless cryptosystems can satisfy the low power requirements for our Smart Lab.

Network requirements:

We assume the KGC to be running on a separate computer that is not connected to the Smart Lab network. Instead, each device that is to be part of the network is individually connected to the KGC for a short time during initialization. At that time, the KGC provides the device with a partial private key, which allows it to derive a proper private/public key pair. Once connected to the network, the device can use this key pair to securely exchange a shared secret key with other devices, without further involvement of the KGC or any other third party. Assuming that the chosen protocol is secure, this will prevent man-in-the-middle attacks, since an attacker cannot obtain a private/public key pair for the identity of another device and hence cannot impersonate it. The protocol works equally well whether the connection between the PLC and the MES server is achieved via an ethernet cable or wirelessly since the cryptographic protocol is independent of exactly how the data are physically sent from one device to another.

D. RECOMMENDATIONS FOR DESIGNING A SECURE SMART FACTORY

1) Security in the distributed control architecture

Distributed control is achieved in the automated production line by distributed information principles. To support this idea, the Level 3 architecture needs to be designed in a

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

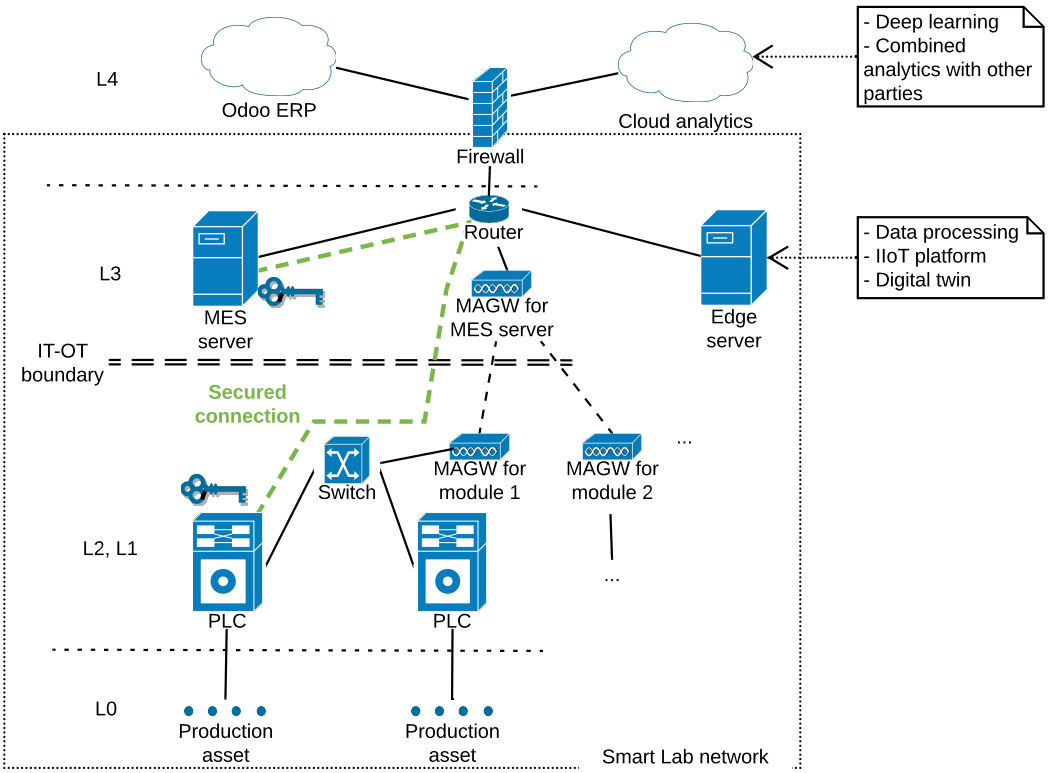

FIGURE 12. Proposed high-level architecture of secure data exchange between MES and lower levels (based on the Smart Lab).

manner in which some of the control decisions from MES are outsourced to the level below. Therefore, this paper works towards securing the link between Level 3 and below.

The smart factory of Industry 4.0 has cyber-physical systems communicating and coordinating over IIoT [15]. This type of distributed control architecture is supported by edge computing. It enables modular manufacturing systems, where modules with PLCs can be added to and removed from a production line. When a PLC is added, it potentially needs to establish connections with multiple new edge servers, and hence be able to promptly share secret keys with them. This calls for an uncomplicated key exchange protocol that can be executed without the active involvement of a third party.

The implementation of Industry 4.0 requires vertical and horizontal integration [13], [59]. In the industrial automation field, vertical integration refers to the integration of IT and OT systems from different levels of the ISA 95 hierarchy, and horizontal integration refers to the integration of IT systems used at different stages of the supply chain, both within and between enterprises. The concept of the IIoT goes beyond the extent of a single factory or company and can include different parts of a supply network. The horizontal integration of systems for data visibility among different parts of a supply network for example allows the manufacturer to quickly adjust to changes in demand further down the supply chain.

IT/OT integration is the first step to achieve the integration along vertical and horizontal value chains. Therefore, this paper addresses security when the IT and OT systems are integrated.

a: Integration of IIoT with the ISA 95 hierarchy

Digitalization is an enabler of smart factories, and IIoT interconnection is imperative to this. It involves a certain degree of decentralization of operations management but need not challenge the existence of well-established IT systems such as MES. A smart factory vision can be achieved with an agnostic approach where both the IT and OT domains converge to fulfill the common goals of improving operational efficiency. This means IT and OT are neither competing with each other nor replacing each other. We present the secure, digitalized, and interconnected IT/OT architecture for the Smart Lab in Fig. 12. Based on this architecture, the QFD analysis, and the feasibility considerations, we synthesize a generalized model for the systems in a smart factory using a certificateless key exchange protocol in Fig. 13. With this model, we also want to stress that the ISA 95 structure is still useful in a smart factory, where the Level 3 functionalities of ISA 95 should be hosted locally for reasons of security, latency, and resistance to network interruptions.

The IIoT living within the ISA 95 structure could mean that the Level 3 (MES) becomes more distributed. This goes hand in hand with factories adopting edge computing (see II-B), where most of the data are collected and processed

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

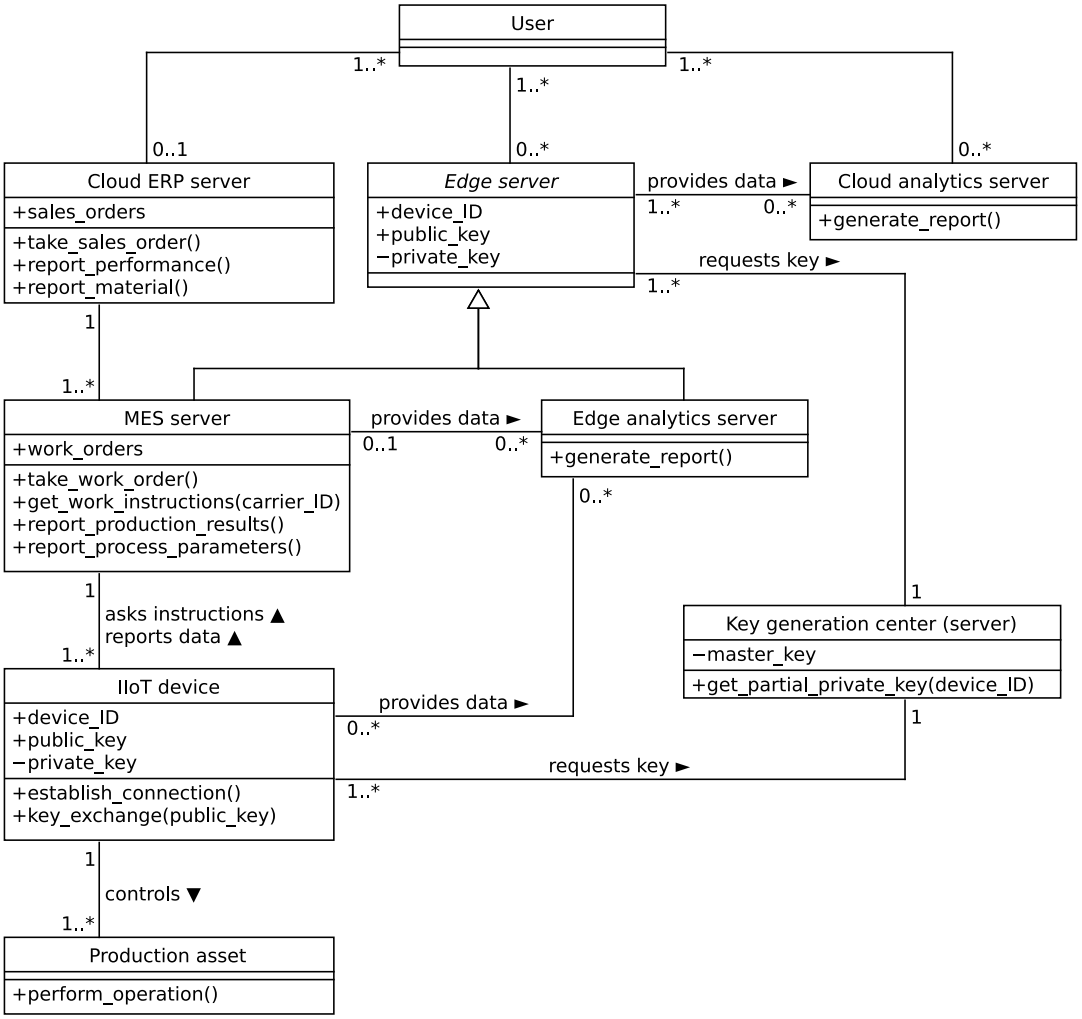

FIGURE 13. UML class diagram of the proposed architecture for a smart factory, describing the entities as well as the relationships between them.

on servers near the point of production. For this reason and because of the need for modularity, the number of IT/OT connections will increase. These connections can for example be secured by using certificateless cryptographic protocols as we present in this paper.

Traditionally, industrial automation and control systems were secured from outside attacks by keeping them separated from Level 4 (i.e., ERP) and the Internet. This can mean setting up a firewall or *demilitarized zone* between Level 4 and the lower levels [1]. However, this goes counter to the vision of interconnection in the IIoT, because IIoT allows breaking the traditional hierarchical control architecture [22]. Instead, IIoT enables a distributed control architecture, so that additional focus needs to be placed on security within industrial control systems. In some modern cases, demilitarized zones might not be applicable at all, as some standard MES solutions are offered as a module of ERP where the common server is hosted on the cloud. Therefore, the security challenges are of a different nature, in that the cloud infrastructure is a particularly valuable target from the point of view of an attacker. We recommend however not completely abandoning the idea of separating different zones: The PLCs and other low power devices should not be directly connected to the Internet, since this would expose them to attack. Instead, they should only connect to the MES or edge servers within the site, which may do initial data processing, and in turn connect to, e.g., a cloud server, as we show in Fig. 12. The edge servers tend to have more computational power and are thus better able to securely connect to the Internet using established methods like TLS. Although this introduces a level of indirection that may affect the responsiveness, this can be ameliorated if the most time-sensitive computations are conducted on edge servers. Even so, it is still important to secure the IT/OT connections, as attackers may get access to the shop floor network.

b: Applying cryptography on low power OT devices

It is well known that it is difficult to integrate a diverse range of OT devices, often with low processing power and memory, into traditional security systems. For example, Roman [38]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2020.3035963, IEEE Access

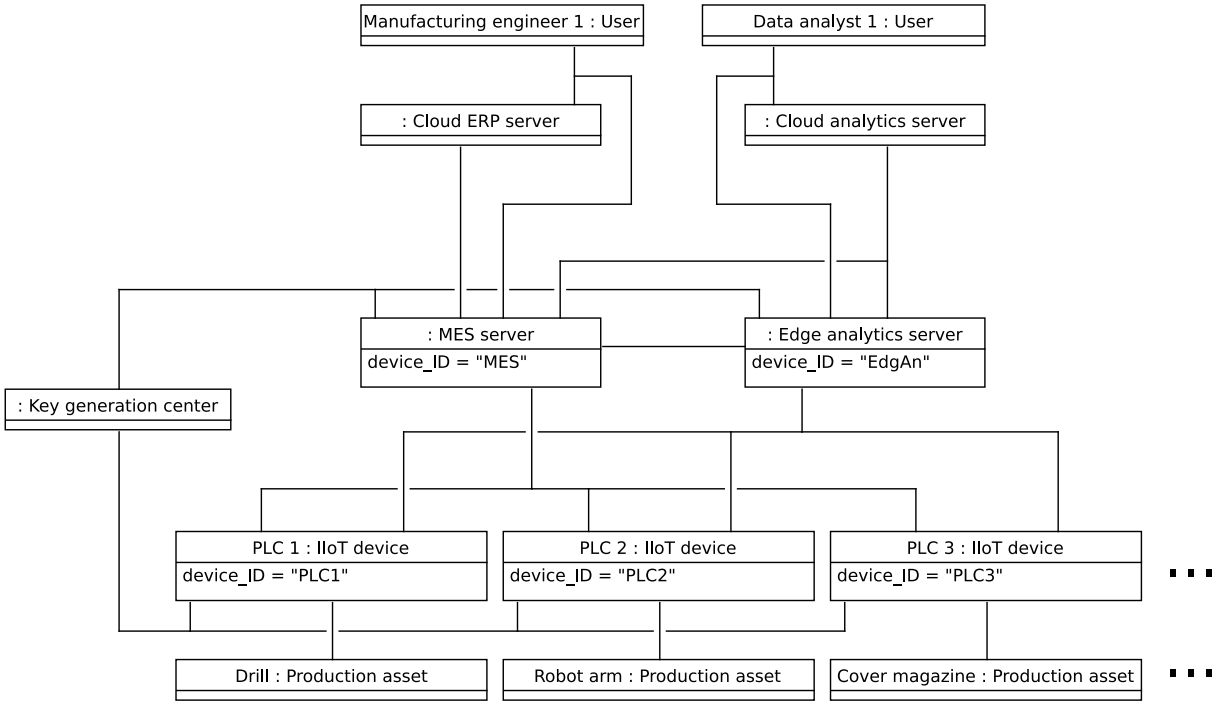

FIGURE 14. UML object diagram of the instantiated architecture (Fig. 13) for the Smart Lab.

writes:

> "These current security mechanisms, based on traditional public key infrastructures will almost certainly not scale to accommodate the IoT's amalgam of contexts and devices."

Boyes [1] mentions the difficulty of using strong encryption with IIoT devices which have constrained processing power and memory. Yu [22] also mentions this issue with regard to establishing shared secret keys between low power devices. We address this issue by considering cryptographic protocols, particularly certificateless protocols, that are suited for low power devices and involve less management overhead than does a public key infrastructure. We check their feasibility in the example of the Smart Lab. To illustrate how a certificateless key exchange scheme could fit into the Smart Lab, we give an instantiation of the proposed model of Fig. 13 for the Smart Lab in Fig. 14.

We have addressed research question Q1 by giving architectural and cryptographic recommendations for securing the (wired or wireless) connection from the MES to the PLCs in an IIoT context. We have used the Smart Lab as a basis for our inquiry. Q2 was also addressed by considering the Smart Lab to derive the requirements for secure IT/OT connectivity on the design and cryptographic levels using QFD.

2) Future work in standardization

The devices used in a factory may be from different vendors, so we believe that future work should develop standardized and open protocols to secure the interconnection between them. Any standardized solution for security in a distributed control architecture should be able to run on legacy systems. This requires that a secure smart factory can be developed on top of existing equipment and does not require new infrastructure. This becomes easier if the vendors of the PLCs consider security needs and design their PLCs to be powerful enough to run standardized protocols. ISA has also been addressing the issue of industrial cybersecurity in the ISA/IEC 62443 standard [60] due to the increase of both intra and inter-organization interconnectivity. The OPC UA standard also includes a security model [23], [61]. We recommend that such standards be followed.

In this paper, we present a technological solution for securing the IT/OT link. However, cybersecurity issues extend beyond the technical realm and are rather a socio-technical concern. For example, an attacker can gain access to MES or OT systems by using social engineering techniques, such as phishing or tailgating. A manufacturing enterprise must counteract cyberattacks by not only exclusively focusing on technological solutions but also by training the employees in security protocols.

3) Developing the design principle of secure interconnection

As discussed in Section II-A, MES is critical for Industry 4.0 and IIoT-connected MES enables smart factories. Since security concerns must drive MES design, we develop a design principle for smart factories with MES.

Principle of security: MES connecting to OT devices should be able to verify the identity of the device and establish an authenticated and encrypted connection in an ad-hoc manner, and vice-versa, ideally without involving a

third party. This principle facilitates IIoT interconnection by mitigating the risk of cyber-attacks that disrupt production by exploiting the increased connectivity between MES and OT.

Owing to the recommendations we present in this paper, bringing security to the interconnection in smart factories need not be an expensive project, nor should it prevent manufacturers from exploiting IIoT opportunities. It can be achieved by reusing existing system capabilities with efficient cryptography.

VII. CONCLUSIONS

We studied the smart factory design principle of interconnection and reviewed studies on security in the IIoT concerning Level 3 of ISA 95, and learned that the literature highlights vulnerabilities around the OT architecture. We determined that the IT/OT link (such as the data exchange between the MES and PLCs) is a weak point in a factory as far as cybersecurity is concerned.

Driven by the need to secure the IT/OT link with appropriate cryptographic protocols and infrastructure, especially in the case of modular manufacturing systems, we listed some of the security challenges faced by the IIoT. By focusing on the data exchange between an MES and a PLC, we gave an overview of types of cryptographic schemes that are tailored to the low power and real-time nature of the IIoT. A feasibility study was done based on the Smart Lab (an Industry 4.0 learning factory) to assess if certificateless cryptographic schemes can be applied in a smart factory context (with wireless, low-cost, and low power requirements). However, there is currently no consensus on how to secure the IT/OT connection. Due to this gap in knowledge, we deduce that cryptography in manufacturing is not a popular academic topic yet and existing cryptographic schemes for the IIoT need further cryptanalytic scrutiny.

With this paper, we tried to raise awareness of the pressing issue of industrial cybersecurity around the IIoT. Based on the results from the QFD assessment, we provided recommendations on how to design a secure smart factory from an information systems perspective. While we used the Smart Lab for this, users can repeat the assessment and obtain scores based on their priorities to document design considerations for bringing security to their smart factory. We formulated a design principle for information systems security (see VI-D3) to uphold the vision for modular manufacturing systems in manufacturing enterprises. We have also deduced that the structure of ISA 95, where there is a separation of Level 3 functionalities from the business domain, is compatible with and indeed helpful for security in smart factories. We therefore recommend considering the structure of ISA 95 for the purpose of security and modularity.

We conclude that designing security for a smart factory is a socio-technical challenge and securing the link between MES and PLCs in the IIoT can be a step toward it.

ACKNOWLEDGMENT

We thank Hjalte Nielsen, the technician of the Smart Production Lab of Aalborg University, Denmark, for providing information on the PLCs used in the Lab.

REFERENCES

[1] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial internet of things (IIoT): An analysis framework," *Computers in Industry*, vol. 101, no. April, pp. 1–12, 2018.

[2] S. Jeschke, C. Brecher, H. Song, and D. B. Rawat, *Industrial Internet of Things*. Berlin: Springer-Verlag, 2017.

[3] T. Vilarinho, B. A. Farshchian, J. Floch, and B. M. Mathisen, "A communication framework for the internet of people and things based on the concept of activity feeds in social computing," in *Proceedings—9th International Conference on Intelligent Environments, IE 2013*, 2013, pp. 1–8.

[4] F. J. N. De Santos and S. G. Villalonga, "Exploiting local clouds in the Internet of Everything environment," in *Proceedings—23rd Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2015*, 2015, pp. 296–300.

[5] ISA95, Enterprise-Control System Integration. Accessed on Aug. 18, 2020. [Online]. Available: https://www.isa.org/isa95

[6] N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet Dossier," Tech. Rep., 2011.

[7] O. Morariu, C. Morariu, and T. Borangiu, "Policy-based security for distributed manufacturing execution systems," *International Journal of Computer Integrated Manufacturing*, vol. 31, no. 3, pp. 306–317, 2018.

[8] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the Industrial Internet of Things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, dec 2015, pp. 795–800.

[9] N. Tuptuk and S. Hailes, "Security of smart manufacturing systems," *Journal of Manufacturing Systems*, vol. 47, no. February, pp. 93–106, apr 2018.

[10] R. Paes, D. C. Mazur, B. K. Venne, and J. Ostrzenski, "A Guide to Securing Industrial Control Networks: Integrating IT and OT Systems," *IEEE Industry Applications Magazine*, vol. 26, no. 2, pp. 47–53, 2020.

[11] G. Avoine, S. Canard, and L. Ferreira, "IoT-friendly AKE: Forward Secrecy and Session Resumption Meet Symmetric-key Cryptography," in *European Symposium on Research in Computer Security*. Springer-Verlag, 2019, pp. 463–483.

[12] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably Secure and Lightweight Certificateless Signature Scheme for IIoT Environments," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3701–3711, 2018.

[13] H. Kagermann, W. Wahlster, and J. Helbig, "Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Final report of the Industrie 4.0 Working Group," 2013.

[14] D. Zuehlke, "SmartFactory—Towards a factory-of-things," *Annual Reviews in Control*, vol. 34, no. 1, pp. 129–138, 2010.

[15] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2016-March. IEEE, 2016, pp. 3928–3937.

[16] M. Demartini, F. Tonelli, L. Damiani, R. Revetria, and L. Cassettari, "Digitalization of manufacturing execution systems: The core technology for realizing future smart factories," in *Proceedings of the XXII Summer School "Francesco Turco" – Industrial Systems Engineering*, 2017, pp. 326–333.

[17] S. Mantravadi and C. Møller, "An overview of next-generation manufacturing execution systems: How important is MES for industry 4.0?" *Procedia Manufacturing*, vol. 30, pp. 588–595, 2019.

[18] B. Scholten, *The Road to Integration: A Guide to Applying the ISA-95 Standard in Manufacturing*. International Society of Automation, 2007.

[19] B. Koerber, H. Freund, T. Kasah, and L. Bolz, "Leveraging industrial software stack advancement for digital transformation," *Digital McKinsey*, 2018.

[20] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, oct 2016.

[21] B. Chen, J. Wan, L. Shu, P. Li, M. Mukherjee, and B. Yin, "Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges," *IEEE Access*, vol. 6, pp. 6505–6519, 2018.

[22] X. Yu and H. Guo, "A survey on IIoT security," in *Proceedings—2019 IEEE VTS Asia Pacific Wireless Communications Symposium*. IEEE, 2019, pp. 1–5.

[23] V. Watson, A. Tellabi, J. Sassmannshausen, and X. Lou, "Interoperability and Security Challenges of Industrie 4.0," in *Informatik 2017, Lecture Notes in Informatics (LNI)*, 2017.

[24] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, "A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities," *IEEE Communications Surveys & Tutorials*, 2020.

[25] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and Its Countermeasures," in *Proceedings—2018 IEEE Global Conference on Wireless Computing and Networking*. IEEE, 2018, pp. 124–130.

[26] E. Bajramovic, D. Gupta, Y. Guo, K. Waedt, and A. Bajramovic, "Resilience in Security and Crises through Adaptions and Transitions," in *Informatik 2019, Lecture Notes in Informatics (LNI)*, no. September, 2019, pp. 571–584.

[27] K. Sha, W. Wei, T. A. Yang, Z. Wang, and W. Shi, "On security challenges and open issues in Internet of Things," *Future Generation Computer Systems*, vol. 83, pp. 326–337, 2018.

[28] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on internet of things security: Requirements, challenges, and solutions," *Internet of Things*, p. 100129, 2019.

[29] H. A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A comprehensive IoT attacks survey based on a building-blocked reference model," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, pp. 355–373, 2018.

[30] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," *IEEE Access*, vol. 8, pp. 88 892–88 932, 2020.

[31] J. Sengupta, S. Ruj, and S. D. Bit, "A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[32] L. Zhou, K.-H. Yeh, G. Hancke, Z. Liu, and C. Su, "Security and Privacy for the Industrial Internet of Things: An Overview of Approaches to Safeguarding Endpoints," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 76–87, sep 2018.

[33] Y. Zhang and X. Huang, "Security and Privacy Techniques for the Industrial Internet of Things," in *Security and Privacy Trends in the Industrial Internet of Things*. Springer-Verlag, 2019, pp. 245–268.

[34] T. Gebremichael, L. P. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, "Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges," *IEEE Access*, vol. 8, pp. 152 351–152 366, 2020.

[35] A. R. Hevner, "A three cycle view of design science research," *Scandinavian Journal of Information Systems*, vol. 19, no. 2, p. 4, 2007.

[36] C. Alcaraz, "Secure Interconnection of IT-OT Networks in Industry 4.0," in *Advanced Sciences and Technologies for Security Applications*, 2019, pp. 201–217.

[37] D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," in *Second International Conference on Sensor Technologies and Applications*. IEEE, 2008, pp. 839–844.

[38] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[39] B. Neuman and T. Ts'o, "Kerberos: An authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 33–38, sep 1994.

[40] Sigfox. Accessed on Feb. 19, 2020. [Online]. Available: https://www.sigfox.com/

[41] *LoRaWAN™ 1.1 Specification*, LoRa Alliance, 2017.

[42] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Proceedings of CRYPTO 84 on Advances in Cryptology*. Berlin: Springer-Verlag, 1985, p. 47–53.

[43] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in *International conference on the theory and application of cryptology and information security*. Springer, 2003, pp. 452–473.

[44] M. Ma, D. He, N. Kumar, K.-K. K. R. Choo, and J. Chen, "Certificate-less Searchable Public Key Encryption Scheme for Industrial Internet of Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 759–767, 2018.

[45] P. Tedeschi, S. Sciancalepore, A. Eliyan, and R. Di Pietro, "LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 621–638, jan 2020.

[46] Y. Zhang, R. H. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and Robust Certificateless Signature for Data Crowdsensing in Cloud-Assisted Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 5099–5108, 2019.

[47] A. Babaei and G. Schiele, "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges," *Sensors*, vol. 19, no. 14, p. 3208, 2019.

[48] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[49] M.-D. Yu, M. Hiller, J. Delvaux, R. Sowell, S. Devadas, and I. Verbauwhede, "A lockdown technique to prevent machine learning on PUFs for lightweight authentication," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 2, no. 3, pp. 146–159, 2016.

[50] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1327–1340, 2017.

[51] O. Madsen and C. Møller, "The AAU Smart Production Laboratory for Teaching and Research in Emerging Digital Manufacturing Technologies," *Procedia Manufacturing*, vol. 9, pp. 106–112, 2017.

[52] R. S. Mogensen, S. Barbera, I. Rodriguez, G. Berardinelli, A. Fink, R. Marcker, S. Markussen, T. Raunholt, T. Kolding, and G. Pocovi, "Implementation and trial evaluation of a wireless manufacturing execution system for industry 4.0," in *IEEE Vehicular Technology Conference*, 2019, pp. 0–7.

[53] H. P. Wiendahl, H. A. ElMaraghy, P. Nyhuis, M. F. Zäh, H. H. Wiendahl, N. Duffie, and M. Brieke, "Changeable Manufacturing—Classification, Design and Operation," *CIRP Annals—Manufacturing Technology*, vol. 56, no. 2, pp. 783–809, 2007.

[54] A. H. Knudsen, M. A. M. Sørensen, T. D. Villumsen, and J. M. Pedersen, "How we hacked an automated production line," in *9th Annual International CMI Conference Smart Living, Cyber Security and Privacy*, 2016.

[55] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The first ICS cyber attack on safety instrument systems," in *Proc. Black Hat USA*, 2018, pp. 1–26.

[56] *Festo Controller CECC*, Festo AG & Co. KG, 2014.

[57] *Open Mote B*, Industrial Shields, 2019.

[58] T. Watteyne, X. Vilajosana, B. Kerkez, F. Chraim, K. Weekly, Q. Wang, S. Glaser, and K. Pister, "OpenWSN: a standards-based low-power wireless development environment," *Transactions on Emerging Telecommunications Technologies*, vol. 23, no. 5, pp. 480–493, aug 2012.

[59] PwC, "Industry 4.0: Building the digital enterprise," 2016. [Online]. Available: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

[60] International Society of Automation, "Quick Start Guide: An Overview of ISA/IEC 62443 Standards: Security of Industrial Automation and Control Systems," 2020. [Online]. Available: https://gca.isa.org/hubfs/ISAGCA Quick Start Guide FINAL.pdf

[61] M. D. Wolfgang Mahnke, Stefan-Helmut Leitner, *OPC Unified Architecture*. Berlin: Springer-Verlag, 2008.

SOUJANYA MANTRAVADI is a Ph.D. student in industrial engineering and information systems. She has a bachelor's degree in mechanical engineering from JNTU Hyderabad, India (2011) and an M.S. from KTH Royal Institute of Technology, Sweden (2015). She completed her masters thesis while interning for Alstom in Paris and has worked as Research Analyst at Mordor Intelligence, as Trainee at the Paul Scherrer Institute (ETH Domain), and as an Engineer at Amada. She is currently employed as a Research Assistant at Aalborg University funded by MADE Digital project and is collaborating externally with the University of Cambridge for her Ph.D.

RETO SCHNYDER received the B.S. and M.S. degrees in mathematics, and his Ph.D. in cryptography and number theory, from the University of Zurich, Switzerland in 2012, 2013, and 2017, respectively. Since 2018, he has been a Postdoctoral Researcher at the Department of Mathematical Sciences, Aalborg University, Denmark. His research interests include finite fields, secret sharing, and secure multiparty computation, in particular designing protocols on the basis of algebraic number theory. He has been teaching bachelor courses in algebra for two years and supervised student projects in applied algebra.

CHARLES MØLLER (born 1962) is a full professor in enterprise systems and process innovation at the Center for Industrial Production at the Department of Materials and Production, Aalborg University. He is researching the interplay between operations and information systems from the perspectives of both technology and organization. His research interests include ERP/MES systems, IT/OT integration, virtual factories, and Smart Production. He is currently engaged in the Danish platform, Manufacturing Academy of Denmark (MADE) where he is primary investigator in digital supply chains, smart factories, and value chain execution and optimization. He holds an M.S. (EE) from the Technical University of Denmark and a Ph.D. in industrial engineering from Aalborg University.

THOMAS DITLEV BRUNOE was born in Aalborg, Denmark in 1980. He received his M.S. in industrial management in 2004 from Aalborg University, Denmark, where he also received his Ph.D. degree in product configuration in engineer-to-order companies in 2008. He has worked in industry for six years, and has been with Aalborg University since 2010, where he is now an associate professor. He is the author of more than 130 peer reviewed scientific papers. His research interests include changeable manufacturing, reconfigurable manufacturing systems, product and process modelling, product configuration, mass customization, and information systems development.