Maximilian Eibl, Martin Gaedke. (Hrsg.): INFORMATIK 2017,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2017 973

Interoperability and Security Challenges of Industrie 4.0

Venesa Watson[1], Asmaa Tellabi[2], Jochen Sassmannshausen[3] and Xinxin Lou[4]

Abstract: Industrie 4.0 (I4.0) is the fourth industrial revolution, which will see the digital transformation of manufacturing, through the integration on Industrial Internet of Things (IIoT), Data and Services, and the convergence of Information Technology (IT) and Operational Technology (OT). With any such transformation, there exists challenges that must first be addressed for a successful outcome. For I4.0, these are interoperability and security, which respectively arise from the interconnection of devices from different manufacturers and/or with different communication protocols; and the interconnection of networks with competing critical and non-critical traffic, and the increased access to initially isolated networks. This paper presents an overview of standards, such as IEC 62443, the ISO 27000 series, IEC 62541 Open Connectivity Unified Architecture (OPC UA) and Time Sensitive Networks (TSN) (IEEE 1722-2016), which addresses these challenges.

Keywords: Industrie 4.0, IIoT, Interoperability, Security, IEC 62443, ISO 27000, OPC UA, TSN

1 Introduction

Industrie 4.0 (I4.0) is defined as the fourth industrial revolution, characterized by a technological evolution from embedded systems to information-driven cyber-physical systems. This requires the digital transformation of manufacturing, through innovation accelerators such as Industrial Internet of Things (IIoT), Services and Data; and the convergence of Information Technology (IT) and Operational Technology (OT), to realize smart decentralized manufacturing, self-optimizing systems, connected factories and a digital supply chain [II16] [IS16a] [Mc15]. The I4.0 infrastructure sees both the interconnection of devices that are from different manufacturers and/or have different protocols, and the interconnection of networks that have varying functional requirements. These interconnections enable increased access to systems that initially had restricted access, and increased instances of shared networks, where critical and non-critical data will compete for access. Standards from the IEC, IEEE, ISO and the Working Group for I4.0, seek to address these security and interoperability challenges. A selection of these standards are discussed concerning their suitability for I4.0.

[1]University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, venesa.watson@uni-siegen.de
[2] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, asmaa.tellabi@uni-siegen.de
[3] University of Siegen, Faculty of Science and Engineering, Chair for Data Communication Systems, Hölderlinstraße 3, Siegen, 57068, jochen.sassmannshausen@uni-siegen.de
[4]Bielefeld University, Department of Computer Networks and Distributed Systems, Universitätsstraße 25, Bielefeld, 33615, xlou@techfak.uni-bielefeld.de

doi:10.18420/in2017_100

2 Security and Interoperability for Industrie 4.0

Communication standards, such as IEC 62541 (Open Connectivity Unified Architecture (OPC UA)) and IEC 61850 (Communication Networks and Systems in Substations), are used to facilitate interoperability. In fact, OPC UA is recommended for implementing the communication layer of the Reference Architectural Model for Industrie 4.0 (RAMI 4.0), which is the framework for I4.0 [Mc15] [OP16]. Concerning I4.0 security, standards must address securing data exchanges, and should consider the different requirements for IT and OT.

In addition to interoperability, IEC 62541 addresses the security of data exchanges [IE15b]. IEEE 1722-2016 similarly addresses interoperability and security. For instance, it uses the globally-accepted Ethernet standard, which is then extended to support simultaneous transmission of both critical and non-critical data, among other security mechanisms; and is currently undergoing testing to fulfil the interoperability requirement, as is observed with the emerging OPC UA over TSN protocol [AB16] [TE16] [TT15]. Also considered is IEC 62443 (Industrial Communication Networks – Networks and System Security), which is a multi-part standard that comprehensively addresses security in the process and automation industry. This high-level security standard is partially based on the established generic security standard, ISO/IEC 27000 series. IEC 62443 is internationally recognized, and is touted as the central standard for security in I4.0 [TU17]. However, ISO 27000 series is preferred for small to medium-scale operators.

Given the involvement in and advantages for I4.0, ISO 27000 series (specifically 27001, 27002 and 27019), IEC 62443, IEC 62541 and IEEE 1722-2016 have been selected for further discussion. An overview for each is provided in the following subsections.

2.1 ISO 27000 Series Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary

The ISO/IEC 27000 series assist organizations keep information assets secure. Bringing information security deliberately under overt management control is a central principle throughout the ISO/IEC 27000 standards. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS). On the other hand, ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing or maintaining ISMS. TR 27019:2013 provides guiding principles based on ISO/IEC 27002 for information security management applied to process control systems as used in the energy utility industry. While the previous standards focused exclusively on information system in business the aim of ISO/IEC TR 27019:2013 is to extend the ISO/IEC 27000 set of standards to the domain of process control systems and automation technology.

2.2 IEC 62443 Industrial Communication Networks – Network and System Security

IEC 62443 is an important standard that covers security in industrial systems. It was developed by the ISA99 committee of the International Society of Automation and the working group 10 of the IEC Technical Committee 65. The standard consists of four main parts, which are further divided into several parts. Currently, some parts are still under development. The scope of IEC 62443 is very wide and covers aspects like policy management, security requirements and component requirements. The standard addresses both system suppliers as well as end users who operate an industrial automation system [IS16b]. Parts of IEC 62443 have a similar scope like the IEC 27000-series of security standards. For example, IEC 62443 also describes aspects like security program management or security risk analysis. Overall, IEC 62443 is not a technical standard like IEC 62541 or IEC 61850 that give detailed guidance of how systems and protocols have to be modelled. Instead, the standard gives a more comprehensive overview of security requirements, security risks that have to be countered, and how products have to be developed to meet certain security requirements. IEC 62443 also provides a model of an industry automation control system and further introduces different zones that cover different areas of the system with the same security requirements. Security analysis of a system can be done on a high level or zone-specific approach [IE15a]. In addition, IEC 62443 introduces security requirements and security levels that help to evaluate and to define certain security measures in a system [IE15c]. IEC 62443 is also applicable beyond Industry automation systems, as demonstrated by the European standardization organization CEN-CENELEC-ETSI in their identification of certain parts of IEC 62443 that can be used to increase security in power system automation [CC14].

2.3 IEC 62541 Open Connectivity Unified Architecture (OPC UA)

OPC UA is a multi-part standard that supports interoperability to allow different devices to communicate. OPC UA facilitates communication through sending messages between OPC UA Clients and Servers. A security model is defined in part 2 [IE15b] to provide security for this communication, whilst part 7 [IE15g] contains security profiles, to address security needs for configurations with lowest security needs to those with highest security needs. The security features provided includes controls to authenticate users and OPC UA clients and servers, preserve the integrity and confidentiality of communication between the clients and servers, and to verify device functionality [IE15b] [IE16a]. OPC UA offers flexibility to vendors to implement these controls as needed, seeking mainly to provide support for their implementation, such as key management services for cryptographic controls [IE16a]. OPC UA also offers flexibility in its applicability to different environments, as demonstrated in [OP16]. For instance, its

applicability to the nuclear context is demonstrated by AREVA. Realizing the potential of OPC-UA in sensors, AREVA started integrating these into monitoring instruments (SIPLUG®) for mountings and their associated electric drives (Fig 1.). This solution allows direct access to SIPLUG® data by AREVA reporting and trend monitoring system, an advantage for the nuclear industry. This use of OPC UA facilities the monitoring of critical systems in remote environments, without negatively affecting the availability of the system [OP16]. As OPC UA is an open standard, SIPLUG® is discoverable by other OPC UA-capable devices. In addition to integrated security, OPC UA also provides historian data collection, which is useful for data-driven analyses.

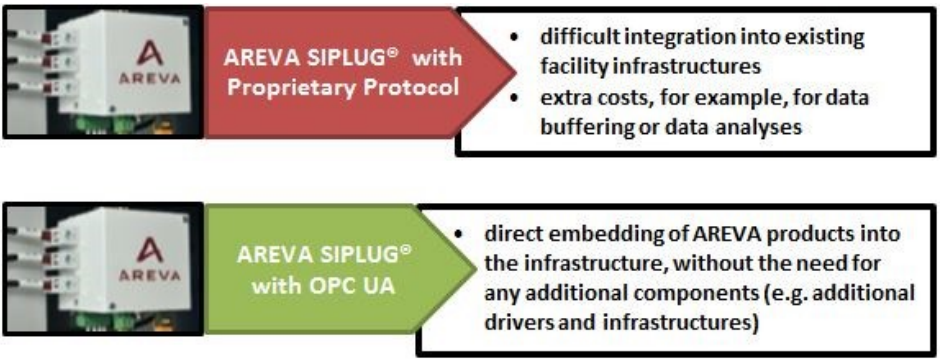

Fig. 1: AREVA SIPLUG® Interoperability with Proprietary Protocol versus with OPC UA.

2.4 IEEE 1722-2016 Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks

Defined by IEEE 1722-2016, TSN is a set of IEEE 802 Ethernet sub-standards that introduces real-time capabilities to the standard Ethernet [IE16b] [TT15]. In IEEE 1722-2016, consideration is given to the industrial context (industrial automation and control networks), where TSN is used to refer to industrial control and other application data streams that are not audio or video in nature [IE16b] [TT15]. TSN provides deterministic, real-time support for both industrial control and IIoT, with functionality that converges critical and non-critical traffic and multiple applications on one network, without the risk of collision to affect the delivery of the critical traffic; facilitates the integration of subsystems to the real-time control systems without network or equipment alterations; and provides more precise information on the source of network faults, to support faster diagnosis and repairs [TT15]. TSN provides competitive advantages for industrial networks, particularly in IIoT infrastructures, where time-critical communication and the protection against traffic congestion are essential requirements. TSN features can also be leveraged with standards for interoperability, such as OPC UA. In that, whilst OPC UA facilitates communication between the devices, TSN ensures a successful connection between these devices, and enables a real-time data communication. Efforts are still underway to improve TSN support of interoperability

for cross-platform communication. In fact, TTTech, with the Industrial Internet Consortium (IIC), recently recorded a successful interoperability of IEEE 802.1Qbu [TT17].

3 Interoperability with IEC 62541 and IEC 61850

3.1 Scope of Application

Both the IEC 62541 (OPC UA) [IE16a] and IEC 61850 (Communication Networks and Systems in Substations) [IE13] are standards with focus on communication and system modelling in automation scenarios. IEC 61850 is highly specialized to power system automation, whereas the OPC UA is an important standard in industry automation scenarios. The main differences between OPC UA and IEC 61850 will be described in the following sections.

3.2 Data Modelling

Both IEC 61850 and OPC UA use data models to represent physical processes and equipment, and applications can interact with the data model using specified services. The IEC 61850 data model is highly specialized to power system automation. IEC 61850-7-3 [IE10b] and IEC 61850-7-4 [IE10c] define data classes and logical nodes that represent certain functionalities, and can be understood as "building blocks" of which a system can be modelled. The original scope of IEC 61850 is automation of substations; therefore, the definition refers to equipment used in this scenario. Extensions like IEC 61850-7-410 [IE10c] and IEC 61850-7-420 [IE09] use the same data classes but define additional logical nodes that enable IEC 61850 to cover distributed energy resources and hydro-power-plants. In contrast, the OPC UA is used in industry automation with a high diversity of device types and highly specialized devices that have to be modelled. Therefore, the OPC UA data model is not as static as the IEC 61850 data model. IEC 62541-3 [IE15c] and IEC 62541-5 [IE15e] introduce the OPC UA approach of data modelling that allows the modelling of arbitrary complex systems. The user may define own objects types that can be instantiated (as nodes in the address space). Relationships between objects are described with references. For example, there is a reference type "HasComponent" that indicates that a certain node is also part of a node. Due to the generic approach, the IEC 61850 data model can be modelled with OPC UA [Ls11]. The opposite case is not possible.

3.3 Services

Both OPC UA and IEC 61850 provide services that allow clients to obtain information about the data model managed by the server, to read and write values and add/delete data

elements. Both standards support publisher-subscriber communication scenarios. The services are described in IEC 62541-4 [IE15d] and IEC 61850-7-2 [IE10a]. The services definitions are not protocol-specific, IEC 61850 calls the service definition the “Abstract Communication Service interface”. The service definitions are aligned with the data models and security concepts.

3.4 Communication Protocols

Both OPC UA and IEC 61850 realize the communication services with certain protocols. OPC UA provides a binary protocol and a XML-based protocol, which are both based on TCP/IP. IEC 62541-6 defines a “mapping” of data elements to these formats [IE15f]. IEC 61850-8-1 defines a mapping to the MMS protocol [IE11], which is currently the only supported protocol for client-server-communication. The planned extension, IEC 61850-8-2, will also introduce the XML based communication XMPP to realize the services defined in IEC 61850-7-2 [IE10a]. In contrast to OPC UA, IEC 61850-8-1 also provides real-time protocols designed for fast transmission of sensor data or event information. These protocols are used in process bus communication and are able to meet narrow time constraints (Round-trip-times of below 4ms). The protocol stack is also very lightweight - the application layer is based directly on the MAC layer. TCP/IP based protocols are not suitable for this purpose.

3.5 Security

The security concepts for IEC 61850 and OPC UA are similar and mainly focus on communication security. However, the OPC UA security approach is more “Bottom up” and included in the standard IEC 62541 as separate part (IEC 62541-2) [IE15b]. The service definitions of the OPC UA also provide services to build up a secure communication channel/session between client and server. The service definitions also include security relevant elements, i.e. an “authenticationToken”, which shall provide authentication of origin of requests. IEC 61850 service definitions do not cover security aspects explicitly as IEC 62541 does. The security measures for IEC 61850 are introduced separately by IEC 62351 and refer to the protocols that are used by IEC 61850. The IEC 61850-7-2 ACSI itself does not define services with security features. In general, security measures are protocol-specific. Both OPC UA and IEC 61850 introduce security on different levels, e.g. TLS on transport layer and mutual authentication on application layer (IEC 61850-8-1 with IEC 62351-3 and IEC 62351-4) or in case of OPC UA the establishment of a secure channel with a session on top of the secure channel. In contrast to IEC 61850 and IEC 62351, the OPC UA protocols for the Secure Channel and the Session are located on application level, the transport protocols can be OPC UA TCP or SOAP/HTTP (IEC 62541-6). Given this structure, the OPC UA communication security can be seen as more end-to-end than the IEC 61850-8-1 communication security realized with TLS and ACSE. However, end-to-end security can be possible with IEC 61850-8-2 and XMPP using techniques such as XML encryption

and XML signatures. In contrast to IEC 61850, the standard IEC 62541 provides detailed auditing mechanisms. Access Control is not covered by IEC 62541-2, whereas IEC 62351-8 introduces access control mechanisms for IEC 61850. However, both OPC UA and IEC 61850 mention the possibility to restrict access to data elements by making them only visible to certain clients.

4 Specific Security Considerations with OPC UA and TSN

The following subsections take a closer look at the security provisions and challenges of both OPC UA and TSN. Also discussed is an emerging protocol, OPC UA over TSN.

4.1 Security Considerations with OPC UA

OPC UA is made up of 13 parts, the first seven parts are related to the core specifications e.g. the concept, security model, address space model, services, information model, service mappings and profiles. The parts eight to thirteen are related to access type specifications like data access, alarms and conditions, programs, historical access, discovery and aggregates.

The security model of OPC UA is specified in part 2 of the specification by OPC Foundation. One of the most important considerations in choosing a technology is security. OPC UA focus on securing the data exchanged between applications by implementing a sophisticated security model that ensures the authentication of clients, servers, and users and the integrity of their communication. It uses X.509 certificates and corresponding private keys. Digital certificates are electronic credentials issued by trusted entities that are used to verify the identities of individuals, computers, and further entities on a network. Digital certificates function in the same way as identification cards such as passports and drivers' licenses [KE17]. The data is transferred as follows: first, a secure channel is established to ensure confidentially by providing encryption, messages signatures to maintain integrity and application authentication using X.509 application instance certificates during the establishment of a secure communication connection [UN17]. Second, a secure session is established between server and client to guarantee user´s authentication and authorization. OPC UA uses symmetric and asymmetric encryption to achieve confidentiality as a security objective, including symmetric and asymmetric signatures to address integrity [KE17]. OPC UA also provides tracking information which is an essential fragment of a site cyber security management system through a clear auditing mechanism.

Secure data transfer between clients and servers in OPC UA is based on certificates issued by a certificate authority (CA). OPC UA client and server both have application instance certificates, which are sent to the other member of communication channel while establishing a secure channel. Both parties validate the received certificates from

CA. After the secure channel has been established, client starts to establish a session with server by sending its software certificate to server. After, the server authenticates the user; it authorizes the access to the requested objects. Sometimes HTTPS is used to create secure channels, however these channels do not provide application authentication. Software certificate can be installed on several hosts, describe the capabilities of the software product. An OPC UA Application installed on a single machine is called an Application Instance. Every instance must have its individual Certificate, used to identify itself when connecting to other applications. It is identified by a global unique URI. Server responds to this request by sending its own certificates and again both members validate received certificates from CA. Certificates authenticated in OPC UA are X.509 certificates. In field device level, verifying every received certificate from CA would cause an important delay to data transfer. Therefore, due to X.509 hierarchical nature it is possible for an automation system provider to act as CA. For example, PLC could act as CA for all the field devices connected to it [KE17].

The security profiles of OPC UA are specified in part 7 of the specification by OPC Foundation. There are three security profiles available in OPC UA: Basic128Rsa15, Basic256 and none. Basic128Rsa15 is a group of security algorithms that include aes128 for encryption, sha1 for authentication and rsa15 for key wrap. Similarly, basic256 consist of aes256 for encryption, sha1 for authentication and RsaOaep for key wrap. On the other hand, Security policy none is used in case the application does not need to use security certificates for encrypted communication - the security policy none means no need for certificates or user login [KE17].

OPC UA is built to be platform independent; in addition to that the communication is constructed into layers on top of the standard TCP/IP stack. Above the standard transport layers there are two additional layers, one that handles the session and the other to establish a secure channel between the client and server. The transport layer is made up of TCP/IP and on top of that SSL, HTTP or HTTPS. The Communication layer guarantees a secure communication channel also ensures the authentication of the end-points. This is based on X.509 certificates; it consists of three parts: a public key that is publically known, a private key that is known only to the application, and identity information that allow applications to know who possesses the certificate [KE17]. securely.

4.2 Security Considerations with TSN

One of the key benefits of TSN is that with the use of Ethernet, it has the advantage of deploying existing, compatible security standards and management features. To secure key TSN features and functions, Avnu Alliance (community responsible for certifying TSN and AVB standards) has identified security considerations that require interfacing with network-based security functions for authorizations, authentication and management [BS16]. The network-based security functions must guard against attacks such as Denial-of-Service (DoS), which target the time-critical function of TSN. Attacks

can also exploit the time/clock synchronization protocols, such as Precision Time Protocol (PTP) and Time Division Multiple Access (TDMA) mechanism, both used by TSN. [TG09] and [Py14] identified network attacks against PTP, in an industrial context (substation automation), some of which the TSN integrated features to protect against. There are no integrated controls for interruption of message exchange attack and selective packet delay. TDMA provides guaranteed bandwidth, absence of collisions, and bounded and predictable latency collisions. TSN uses the TDMA features to split time into repeating cycles, to allow convergence of critical and non-critical information on one network [BE16] [Tm15]. Time slots in these cycles are reserved for critical data streams, and require synchronization between the internal clocks for the network devices, to be maintained [BE16]. Attacks against these time slots and the clock synchronization can disrupt the transmission of critical data. In wireless deployments, especially, TDMA is susceptible to DoS attacks caused by jamming [Tm15]. Other network security threats, as identified in [Mt14], include Layer 2/3 DoS attacks, performance attacks, and network reconnaissance through exploitation of the time protocol.

Both [Py14] and [TG09] provided proposals to address the PTP attacks, however, some of these proposals have limitations that can allow attackers to bypass the controls through the exploitation of a different attack path. Additionally, these proposals require further analysis, to identify potential drawbacks of implementing controls such as: (1) the clock drift correction of islanded nodes, to preserve clock synchronization; (2) layer 2 security mechanisms such as Media Access Control Security (MACsec) and Ingress Filtering and Policing, which respectively used to authenticate, encrypt and preserve the integrity of the data streams between the network participants, and verify data integrity; (3) increasing the level of encryption in the packets, to preserve message integrity; Defense in Depth and Diversity network access layer security mechanisms, to harden TSN at routers and switches; (4) adding a handshake mechanism for additional master clock verification; and (5) using encrypted tunnels, to secure the communication between master and slave clocks [BE16] [Py14].

The controls implemented to secure TSN must protect against network security attacks, whilst also preserving the critical real-time functions and features of TSN. In that, these controls themselves must have real-time capabilities. Otherwise, the introduced latency can cause time-sensitive end-device applications to enter a safe shutdown state immediately [BE16].

4.3 OPC UA TSN (OPC UA over TSN)

OPC UA TSN represents the combination of the IEEE TSN Ethernet standard and the publisher/subscriber extended OPC UA protocol, which supports the standardization of communication in industrial automation for IT and OT integration, a basic requirement for realizing IIoT and I4.0 [TE16]. For this, the OPC UA publisher/subscriber (extended) protocol was referenced instead of the client/server model presented in IEC 62541.

[IN16] states that is because the client/server architecture OPC UA standard is not ideal in fulfilling the requirements for implementing IIoT and I4.0. As such, the OPC Foundation is in the process of standardizing OPC UA Publisher/Subscriber as an additional communication model [IN16]. The TSN specification covers the data link layer (Layer 2) and the physical layer (Layer 1), whilst the OPC UA covers higher layers in the OSI model [Rm16]. Combining TSN with OPC UA provides advantages for the automation architecture: the real-time, deterministic network capabilities for I4.0 can be realized, along with the required manufacturer- and platform-independent, interoperable network devices. With the widely-used Ethernet providing the backbone, in conjunction with an international standard for interoperability, this new architecture provides a flexible, future-proof network, that delivers scalability and low maintenance cost [IN16]. Development, testing and implementation is being driven by a group of leading automation and information technology suppliers, as they envision it as the solution for achieving "*an open, unified, standards-based and interoperable IIoT solution for deterministic and real-time peer-to-peer communication between industrial controllers and to the cloud*" [AB16].

The AREVA SMARTEST R&D Project will also consider these protocols, with the aim of contributing to an overall improvement in security for I&C. For instance, this project will: (1) use the protocols for comprehensive modelling and analysis; (2) involve preparation of security tests that will be applicable for OPC UA enabled devices from multiple vendors; and (3) provide products with OPC UA interfaces, like AREVA SIPLUG®, so that overall interoperability solution costs are reduced by up to 90%.

5 Conclusion

To successfully realize the I4.0 architecture, challenges to security and interoperability must be sufficiently addressed. This complex architecture features interconnections of devices and networks, which require communication standardization to support cross-platform communication, and security controls to preserve confidentiality, integrity, and especially, availability. The standards, IEC 62443, IEC 62541, ISO 27000 series and IEEE1722-2016, addresses these challenges, however, additional testing and extensions are necessary to qualify the recommendations of these standards as sufficient and efficient based on IIoT and I4.0 requirements. For instance, features and functions implemented to guard against cyber-attacks must not impede time-critical communication. As well, controls must be implemented to guard against identified attacks. It is envisioned that the continued work of standardization bodies and invested organizations, will provide additional guidelines to address this function versus interoperability and security dilemma. The AREVA SMARTEST project aims to also contribute to the on-going effort of 'smart' testing and 'smart' security, to ensure reliable and resilient systems.

Acknowledgements

Some of the addressed cybersecurity related topics are being elaborated as part of AREVA GmbH's participation in the "SMARTEST" R&D (2015-2018) with German University partners, partially funded by German Ministry BMWi.

References

[AB16] ABB: Leading automation and information technology suppliers drive OPC UA TSN for unified IIoT communication to the controller level, abb.com/cawp/seitp202/288CCF9454F992B9C1258074002D93EC.aspx, accessed: 25/07/2017.

[BE16] Belden: Cyber security for TSN in modern automation networks, wireless.electronicspecifier.com/around-the-industry/cyber-security-for-tsn-in-modern-automation-networks, accessed: 25/05/2017.

[BS16] Baehren, F.; Stanton, K.: Avnu Alliance: Compliance & Interop for the Common Parts of TSN/AVB, standards.ieee.org/events/automotive/2016/d2_05_baehren_avnu_certified_time_sensitive_networking_1.01.pdf, accessed: 25/05/2017.

[CC14] CEN-CENELEC-ETSI: Smart grid coordination group. Smart grid information security,energynetworks.org/assets/files/electricity/engineering/Standards/SGCG%20Reports%20071014/SGCG_WGSGIS_Sec0078_INF_ReportforComments.pdf, accessed 22/06/2017.

[IE09] IEC 61850-7-420 Communication networks and systems in substations - Part 7-420: Basic communication structure - Distributed energy resources logical nodes.

[IE10a] IEC 61850-7-2 Communication networks and systems in substations - Part 7-2: Basic communication structure for substation and feeder equipment - Abstract communication service interface (ACSI).

[IE10b] IEC 61850-7-3 Communication networks and systems for power utility automation - Part 7-3: Basic communication structure - Common data classes.

[IE10c] IEC 61850-7-4 Communication networks and systems for power utility automation - Part 7-4: Basic communication structure - Compatible logical node classes and data object classes.

[IE11] IEC 61850-8-1 Communication networks and systems in substations - Part 8-1: Specific communication service mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3.

[IE13] IEC 61850-1 Communication networks and systems in substations – Part 1: Introduction.

[IE15a] IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-2: Security risk assessment and system design.

[IE15b] IEC 62541-2 OPC Unified Architecture – Part 2: Security Model.

[IE15c] IEC 62541-3 OPC Unified Architecture – Part 3: Address Space Model.

[IE15d] IEC 62541-4 OPC Unified Architecture – Part 4: Services.

[IE15e] IEC 62541-5 OPC Unified Architecture – Part 5: Information Mode.

[IE15f] IEC 62541-6 OPC Unified Architecture – Part 6: Mappings.

[IE15g] IEC 62541-7 OPC Unified Architecture – Part 7: Profiles. Switzerland: IEC.

[IE16a] IEC 62451-1 OPC Unified Architecture – Part 1: Overview and Concepts.

[IE16b] IEEE 1722-2016: IEEE Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks.

[II16] IIC: Industrial Internet of Things Volume G4: Security Framework., iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf, accessed: 22/05/2017.

[IN16] Industrial.softing.com: Implementing Deterministic OPC UA Communication, industrial.softing.com/uploads/softing_downloads/OPCUAPublisherSubscriber_W_EN_160407_100.pdf, accessed: 25/05/2017.

[IS16a] i-Scoop: Industrie 4.0: the fourth industrial revolution – guide to Industrie 4.0, i-scoop.eu/Industrie-4-0/#Industrie_40_definition_the_digital_transformation_of_Industrie_and_the_fourth_industrial_revolution, accessed: 22/05/17.

[IS16b] International Society of Automation - The 62443 series of standards, isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf, accessed: 29/05/2017.

[KE17] Kepware: How OPC UA protects your data, info.kepware.com/blog/how-opc-ua-protects-your-data, accessed: 22/06/2017.

[Ls11] Lehnhoff, S.; Mahnke, W.; Rohjans, S.; Uslar; M.: IEC 61850 based OPC UA Communication - The Future of Smart Grid Automation. In: 17th Power Systems Computation Conference, Sweden, 2011.

[Mc15] Mosch, C.: RAMI 4.0 and Industrie 4.0 component, mv.vdma.org/en/-/rami-4-0-und-industrie-4-0-komponente, accessed: 22/05/2017.

[Mt14] Mizrahi, T.: Security Requirements of Time Protocols in Packet Switched Networks, tools.ietf.org/html/rfc7384#page-7, accessed: 25/05/2017.

[OP16] OPC Foundation: Unified Architecture: Interoperability for Industrie 4.0 and the Internet of Things, opcfoundation.org/wp-content/uploads/2016/05/OPC-UA-Interoperability-For-Industrie4-and-IoT-EN-v5.pdf, accessed: 22/07/2017.

[Py14] Pathan, Y., Dalvi, A., Pillai, A. and Patil, D. (2014), Analysis of selective packet delay attack on IEEE 1588 Precision Time Protocol. Available at: colorado.edu/itp/sites/default/files/attached-files/team_7_-_arun_ravindran_pillai_-_apr_25_2014_433_pm_-_group_7_final.pdf.

[Rm16] Rowe, M., Time-Sensitive Networks Find New Applications, eetimes.com/author.asp?section_id=36&doc_id=1330816, accessed: 25/05/2017.

[TE16] Technik-medien.at: OPC UA TSN | Foundation for Industrial IoT and Industrie 4.0., technik-medien.at/wp-content/cache/page_enhanced/technik-medien.at//2016/11/27/opc-ua-tsn-grundsteinlegung-fuer-industrial-iot-und-industrie-4-0//_index.html_gzip, accessed: 25/05/2017.

[TG09] Tournier, J.; Goerlitz, O.: Strategies to Secure the IEEE 1588 Protocol in Digital Substation Automation. In: The Fourth International CRIS Conference on Critical Infrastructures, IEEE, Linkoping, Sweden, pp.1-8, 2009.

[Tm15] Tiloca, M.; De Guglielmo, D.; Dini, G.; Anastasi, G.; Das, K.: JAMMY: a Distributed and Dynamic Solution to Selective Jamming Attack in TDMA WSNs. IEEE Transactions on Dependable and Secure Computing, 08/15, (In Press), 2015.

[TT15] TTTech: IEEE TSN (Time-Sensitive Networking): A Deterministic Ethernet Standard, tttech.com/technologies/deterministic-ethernet/time-sensitive-networking/, accessed: 25/05/2017.

[TT17] TTTech: TTTech Successfully Completes First Interoperability Testing of TSN Preemption Standard, tttech.com/news-events/newsroom/details/tttech-successfully-completes-first-interoperability-testing-of-tsn-preemption-standard/, accessed: 25/05/17.

[TÜ17] TÜEV NORD CERT GmbH: Industrial IT Safety and Security for Control and Communications Systems Industry 4.0, tuev-nord.de/fileadmin/Content/TUEV_NORD_DE/pdf/PDB_Zertifizierung_nach_IEC_62443_EN_WEB.pdf, accessed: 21/06/17.

[UN17] Unified Automation: C++ Based OPC UA Client/Server SDK Documentation, documentation.unified-automation.com/uasdkcpp/1.5.3/html/L2ServerSdkSecurity.html#L3ServerSdkSecurityAA, accessed: 22/06/17.