Security Challenges in Control Network Protocols: A Survey

Anna Volkova, Michael Niedermeier, Robert Basmadjian, and Hermann de Meer

Abstract—With the ongoing adoption of remotely communicating and interacting control systems harbored by critical infrastructures, the potential attack surface of such systems also increases drastically. Therefore, not only the need for standardized and manufacturer-agnostic control system communication protocols has grown, but also the requirement to protect those control systems' communication. There have already been numerous security analyses of different control system communication protocols; yet, these have not been combined with each other sufficiently, mainly due to three reasons: First, the life cycles of such protocols are usually much longer than those of other Internet and communication technologies, therefore legacy protocols are often not considered in current security analyses. Second, the usage of certain control system communication protocols is usually restricted to a particular infrastructure domain, which leads to an isolated view on them. Third, with the accelerating pace at which both control system communication protocols and threats against them develop, existing surveys are aging at an increased rate, making their re-investigation a necessity. In this paper, a comprehensive survey on the security of the most important control system communication protocols, namely Modbus, OPC UA, TASE.2, DNP3, IEC 60870-5-101, IEC 60870-5-104, and IEC 61850 is performed. To achieve comparability, a common test methodology based on attacks exploiting well-known control system protocol vulnerabilities is created for all protocols. In addition, the effectiveness of the related security standard IEC 62351 is analyzed by a pre- and post-IEC 62351 comparison.

Index Terms—Control systems, Network protocols, Network security

I. Introduction: Control Networks in the Change of Time

THE need to take fast and cost effective decisions in a global market pressures service providers to enhance their infrastructures using remotely accessible control networks. A prime example of such networked control systems are Supervisory Control and Data Acquisition (SCADA) systems, used to operate and monitor a wide portion of industrial facilities and processes, often distributed over large geographic areas. To be able to signal and control such systems, the previous isolation of SCADA systems has been more and more reduced. Company networks and later on even remote access were allowed to control SCADA systems using telecontrol technologies. Due to the fast development of Information and Communications Technology (ICT), and particularly networking technology, the adoption of the Internet and a need to remotely control systems from anywhere around the world, consequently the complete isolation (i.e. an "air-gap") between control and potentially publicly accessible networks became illusionary [1].

Standard computer systems and their security measures adapted and grew to match the new requirements of this interconnected world. In contrast, most control systems were developed in the 1970s and designed to match the lifetime of the devices they were controlling, which would easily have a lifecycle of some 30 years. As most techniques in control systems—including hardware, software and networking—were therefore designed long before network security was perceived to be a requirement, challenges rapidly began to develop. Unfortunately, it took a long time for researchers and industrial stakeholders—until worldwide attacks on control systems (e.g., [2], [3] and [4]) became more prevailing—to realize the importance of network security. Two examples of such control system security incidents are described below:

- Attack on Maroochy Water Services, Australia. In 2000, a former employee of the Maroochy Water Services in Australia gained access to the water pumping SCADA system and released tons of sewage water into parks, rivers and residences. The damage to the company and the environment was enormous. The employee, who helped install the SCADA system in this area, exploited the lack of security policies and defense mechanisms to launch a series of attacks against different pumping systems of the company. He disguised his actions as normal malfunctions that needed to be physically repaired. The culprit was only arrested by chance, when he was stopped by a police patrol [2].
- Attack on public tram system in Lodz, Poland. In 2008, a teenager was able to hack the SCADA system controlling the public tram system in Lodz, Poland. He gained full access to the system, which had no security measures implemented and controlled the trains with a self-built remote control, which was able to send signals to the Remote Terminal Units (RTUs) controlling the junctions. Several trains were derailed and passengers were hurt during this attack [4].

The persistent challenge control system networks have been facing is that they inherit security problems from outside networks, putting industrial production, environmental integrity and human safety at risk [5]. One of the foremost weaknesses exploited in industrial control networks are vulnerabilities in the communication protocol standards

A. Volkova, M. Niedermeier, R. Basmadjian, and H. de Meer are with the Computer Networking Lab, Department of Computer Science and Mathematics, University of Passau, 94032 Passau, Bavaria, Germany, e-mail: {name.surname}@uni-passau.de.

and implementations [6], [7], [8]. However, up till now, no comprehensive analysis regarding the vulnerabilities and attacks of the most well-known control system protocols has been realized.

A. Research Objective

Looking at control system communication protocols (CSCPs), one can notice that there have been a broad and long lasting series of such protocols which were often developed a long time ago. To this regard, there have been several survey works in literature (see Section II) that tackled specific protocols from different perspectives. What is currently lacking is a single methodology that describes those protocols by looking at the problems from multiple dimensions. In this paper, we propose such a methodology as our research objective which allows us, based on a unified adversary model, to qualitatively describe and structurally classify communication protocols for control systems based on their threat levels. Our work provides the following contributions:

1) We propose a unified methodology to analyze the security of the most relevant CSCPs from the IEC 62351 standard's perspective.
2) We carry out a security assessment of CSCPs by considering pre- and post-implementation of the IEC 62351 standard.
3) We compose a fine-granular adversary model and attack scenarios that are essential in the context of Industrial Control Systems (ICSs).
4) We provide general protection measures as well as several security recommendations to improve the IEC 62351 standard and CSCPs.
5) We review well-known enhanced versions of legacy CSCPs and analyze them in the context of real life scenarios.

B. Structure

The remainder of this paper is structured as follows: Section II illustrates related work. Section III elaborates on the seven most important as well as five enhanced legacy CSCPs and describes general requirements and challenges of control network protocols. In Section IV, the adversary model considered in this paper is addressed. The security methodology and the protocol analysis are covered in Section V. The paper is concluded in Section VI, and future research directions are pointed out in Section VII.

II. Related work

The research area around control system protocols and their security challenges have been investigated for several decades already. The previous related work can be classified into three different types of contributions:

- Generic surveys, which covered general attack possibilities on a high abstraction level (Section II-A),
- Control system security analysis covering a single or a few protocols at most (Section II-B), or
- Security research which focuses only very specific types of attacks (Section II-C).

In the following, prominent examples of all three types of articles are discussed.

A. Overview-type Related Work

Dzung et al. provide a survey including security goals in control networks, possible attack vectors, and security solutions to mitigate them [9]. The survey gives a detailed overview of the current goals and challenges in control networks as well as partially in CSCPs, however, no further analysis of the protocols regarding their vulnerabilities is provided. Mohagheghi et al. show a detailed survey regarding both legacy CSCPs and their challenges as well as future trends in control systems in [10]. The paper mainly compares legacy protocols to the newer IEC 61850 standard, but does not put a major focus on security challenges. Johnson explores the weaknesses of SCADA-based systems in [11]. Also, several methods and tools are proposed to augment SCADA security. An overview of SCADA systems' components and the protocols Distributed Network Protocol (DNP3), IEC 60870-5, as well as IEC 60870-5-101 is given by Alsiherov et al. in [12]. Furthermore, the security standard 62351 is briefly introduced and security measures on the transport and network layer are discussed; security features of CSCPs are however not part of the paper. An overview of incidents related to missing SCADA security with a clear classification of attacks and the impact of incidents are given in [2] by Miller et al.. Robinson presents an adversary model as well as an overview on threat actors for SCADA systems in general and discusses security breaches in CSCPs [13]. The paper delivers security recommendations for ICSs in general. The risks to SCADA and ICS as well as the methods used by attackers to exploit vulnerabilities in those systems are investigated in [14] by Bartmann and Carson. The paper additionally covers mitigation strategies for the discussed threats. While the analysis is covering many attack vectors and threats, it does not focus on CSCPs specifically; in contrast, the focus is set to mitigation strategies ranging from (physical) tamper detection to network security.

Instead of giving an abstract overview of overarching problems in ICSs, SCADA, and/or CSCPs in general, our survey covers detailed attack scenarios for the most relevant CSCPs and gives concrete information regarding the expected impact of attacks. Also, mitigation strategies are provided.

B. Protocol-specific Related Work

Michalski et al. perform an in-depth analysis of the Telecontrol Application Service Element 2 (TASE.2) protocol in [15]. This covers both a detailed analysis of TASE.2 and its intended goals and functions, as well as possible security challenges and mitigation strategies. Schwarz and Börcsök investigate the security of Open Platform

Communications (OPC) Unified Architecture (UA) both on the application and communication layer in [16], which includes a fine-granular description of the protocol itself as well as its current challenges. In [17], Krotofil et al. provide a survey of selected state-of-the-art control system security methods. While there are several security-related research papers cited, the work mainly revolves around the Modbus protocol and DNP3. Drias et al. analyze control systems and their security requirements in general without applying a specific focus. Regarding the CSCPs, again Modbus and DNP3 are briefly investigated [18]. A testbed-based approach to study and simulate the various available techniques for securing and protecting SCADA systems against a wide range of cyber attacks is discussed in [19]. The developed testbed is then used to analyze Denial of Service (DoS) and compromised Human Machine Interface (HMI) attacks on the Modbus and DNP3 protocols. While the testbed-based approach in [19] offers a realistic scenario for the security assessment of SCADA systems, both the discussion of the adversary model as well as the analysis of security flaws within CSCPs are very brief. East et al. present a taxonomy of attacks on DNP3 [20]. The attacks are classified based on targets (control center, outstation devices and network/communication paths) and threat categories (interception, interruption, modification and fabrication). The attack taxonomy clarifies the nature and scope of threats to DNP3. In [21], Lee et al. analyze DNP3 and its existing security enhanced variants DNPSec and DNP3 Secure Authentication (SA). In addition, a new secure version of DNP3 named DNP3 Authenticated Encryption is developed and compared to DNP3, DNPSec, and DNP3 SA. Pidikiti et al. discuss a wide range of vulnerabilities and subsequent attacks on the IEC 60870-5-101 and IEC 60870-5-104 protocols in [22]. Matoušek provides an overview of IEC 60870-5-104 in [23] with a detailed description of the protocol's Application Protocol Control Information (APCI) and Application Service Data Unit (ASDU) formats. Additionally, the security challenges currently present in IEC 60870-5-104 are analyzed. An analysis on vulnerabilities in the Modbus and International Electrotechnical Commission (IEC) 61850 protocols is the topic of [24]. For both protocols, two different types of attacks are assessed: flawed/missing cryptographic protection and memory corruption vulnerabilities. In [25], an evaluation method for SCADA cyber security based on testbeds is presented. The proposed test environment reflects the real control and supervision substation of an electricity generation and distribution control system. Special focus is placed on the analysis of the overall behavior of both the IEC 60870-5-104 and IEC 61850 protocols. Similar to [19], the paper offers a testbed-focused approach, which however restricts its scenarios regarding both the type of attackers and the investigated protocols.

If not stated otherwise, the difference between our survey and the aforementioned work is that they only cover one or two CSCPs, while our survey investigates the seven most widely used CSCPs as well as three enhanced versions of Modbus and two of DNP3 and compares them using a unified methodology. Therefore, this difference is not explicitly stated for each related work.

C. Attack-specific Related Work

Maynard et al. present Man-in-the-Middle (MitM) attacks on the IEC 60870-5-104 protocol in [26]. Address Resolution Protocol (ARP) spoofing based MitM attacks on the Modbus and DNP3 protocols are investigated by Yang et al. in a cyber-security testbed which contains SCADA software and communication infrastructures [27]. Apart from that, future plans on implementing intrusion detection and prevention technology to address cyber-security issues in SCADA systems are presented. Both papers offer a deep investigation of a single attack, however, their contribution is limited due to the specialized focus.

In comparison, our survey covers multiple attacks that threaten all three main security goals (confidentiality, integrity, availability). Tables I and II offer an overview of the currently existing work and the research areas covered. It is noted here that not all entries in Tables I and II are explicitly addressed in this section due to space restrictions. To give a more comprehensive overview however, further related work is included in Tables I and II.

III. Control Network Protocols: Overview, Requirements and Challenges

In this section, we first give an overview of the most relevant CSCPs, and then present their requirements in terms of security and performance. This section is concluded by illustrating the implementation challenges of CSCPs in ICSs.

A. Overview

The CSCPs analyzed in this survey are selected based on two requisites. First, the chosen protocols need to be of major importance within the sector of industrial control systems. Second, only standard protocols (and their security-enhanced variants) are considered in this survey, proprietary solutions are omitted. The chosen protocols (Modbus, OPC UA, TASE.2, DNP3, IEC 60870-5-101, IEC 60870-5-104, and IEC 61850) all fulfill these prerequisites [45], [46], [47]. Fig. 1 depicts an overview of the aforementioned seven protocols and the enhanced variants of Modbus and DNP3 (marked in green) as well as the protocols they are derived from. The letters located to the right of each marked node represent the International Organization for Standardization (ISO)/Open Systems Interconnection (OSI) layers covered by the respective protocol. The letters are abbreviations of: A $\rightarrow$ application layer, T $\rightarrow$ transport layer, N $\rightarrow$ network layer, DL $\rightarrow$ data link layer, and P $\rightarrow$ physical layer. Note that in the rest of this section while presenting the message structure of specific protocols, we use the following semantics in the corresponding figures: The width of each message is

	Modbus	Modbus-F2009	Modbus-S2015	Modbus-A2018	OPC UA	TASE.2
Overview	[10], [28], [17], [18], [29], [30]	[28]	[29]	[30]	[9], [31], [16]	[9], [15], [10]
Confidentiality violation	[28], [24], [27], [29], [30]	[28]	[29]	n/a	[16]	[15]
Integrity violation	[28], [24], [29], [30]	[28]	[29]	n/a	[16]	[15]
Availability violation	[28], [19], [24], [29], [30]	[28]	[29]	n/a	[16]	[15]

TABLE I
Classification of related work (part 1)

	DNP3	DNPSec	DNP3 SA	IEC 60870-5-101	IEC 60870-5-104	IEC 61850
Overview	[32], [10], [20], [12], [17], [18], [33], [34], [35]	[32], [21]	[36], [37], [21], [38]	[12]	[23]	[9], [10], [39], [40], [41], [14]
Confidentiality violation	[32], [20], [27], [33], [35]	[21]	[42], [21], [35]	[22]	[22], [25]	[24], [39], [40], [43]
Integrity violation	[32], [20], [33], [34], [35]	[21]	[42], [21], [35]	[22]	[22], [26], [25]	[24], [44], [39], [40], [43], [41]
Availability violation	[32], [20], [19], [33] , [35]	[21]	[42], [21], [35]	[22]	[22]	[24], [44], [39], [40], [43]

TABLE II
Classification of related work (part 2)

of 1 Byte (demonstrated only in Fig. 3, whereas for the other figures it is eliminated to save space). Furthermore, whenever the size of a specific field of a message is longer than 4 Bytes, we present the undefined field size with "...", such as for Data in Fig. 3.

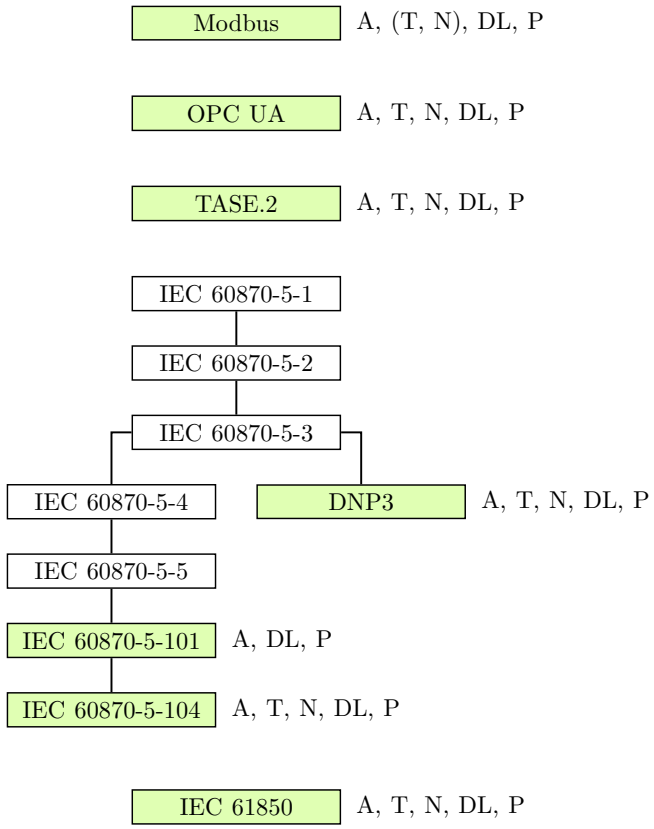

Fig. 1. Protocol overview and ISO/OSI layer coverage

1) Modbus: The Modbus protocol was developed and published by Modicon in 1979 and is foremost used in process automation. Modbus is still widely used, mainly because it is an open standard and has a simple structure. The responsibility for the maintenance and further development of the protocol lies with the Modbus organization. Modbus defines two different transmission methods: First, Modbus serial, which is used for communication via serial interfaces such as RS232 and RS485. Second, Modbus Transmission Control Protocol (TCP)/Internet Protocol (IP), which supports communication over a TCP/IP network. Two different transmission modes are defined for Modbus serial transmissions:

- Modbus RTU, for binary data encoding,
- Modbus American Standard Code for Information Interchange (ASCII), which encodes the data using an ASCII character set in the form of readable character strings.

Modbus works according to the master/slave principle. A master can communicate with one or more slaves. Only the slave explicitly addressed by the master may return data to the master. The protocol supports only binary and 16-bit values, which are read by the master in blocks. Neither quality markings nor time stamps are supported. Fig. 2 shows the ISO/OSI layer structure of the Modbus protocol, whereas Fig. 3 depicts the structure of a Modbus serial message.

There have been attempts to secure the Modbus protocols over time, e.g. in [28] (referred to as Modbus-F2009 from here on), [29] (referred to as Modbus-S2015 from here on), and [30] (referred to as Modbus-A2018 from here on). Modbus-F2009 only offers integrity and authentication, while Modbus-S2015 and Modbus-A2018

7	Modbus application layer	
6	n/a	
5	n/a	
4	n/a	TCP (RFC 793)
3	n/a	IP (RFC 791)
2	n/a	RFC 894
1	RTU (binary encoding) ASCII (ASCII encoding) RS232 (V.24), RS485	Ethernet (IEEE 802.3)

Fig. 2. ISO/OSI layer structure of Modbus protocol

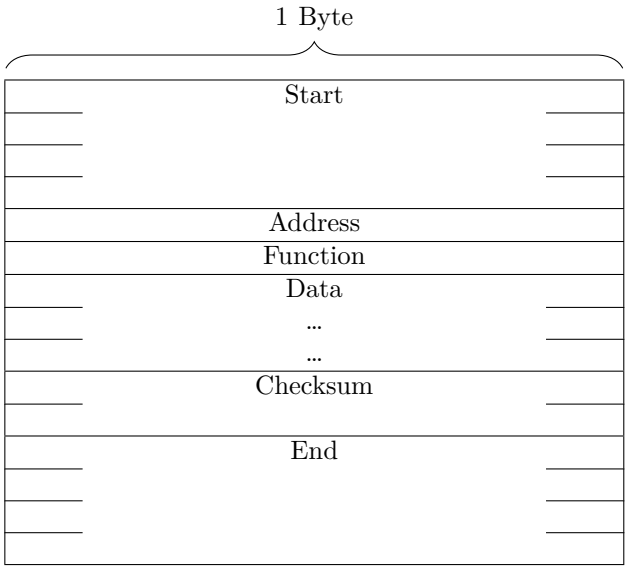

Fig. 3. Modbus message structure

provide confidentiality, integrity and authentication by applying well-known network security methods, such as symmetric and asymmetric cryptography, authentication, and replay protection mechanisms. More precisely, the Modbus successors have the following properties:

- Modbus-F2009. Rivest, Shamir and Adleman (RSA) signatures and Secure Hash Algorithm (SHA)-2 hashing are used to provide security.
- Modbus-S2015. Both RSA signatures and SHA-2 hashing are employed, similar to Modbus-F2009. However, in addition, Advanced Encryption Standard (AES) encryption is used for confidentiality.
- Modbus-A2018. A challenge-response authentication mechanism and AES encryption are employed to secure the protocol.

In the further analysis, the original Modbus protocol as well as its secure modifications are investigated.

2) OPC/OPC UA: OPC was first released in 1996 by the OPC Foundation, at the time by the name "Object Linking and Embedding for Process Control". The OPC protocol is today widely used in process automation, most notably to interconnect process data to HMI devices.

OPC employs a client/server principle, where a client (master) can access one or more servers (slaves). A server acts as data provider for the clients that obtain the data. OPC defines a number of interfaces serving various purposes, which are named in the following:

- Data Access (DA). This interface is the most well-known and is used to access process data.
- Alarm and Event (AE). The AE interface supplements the DA and is used to transmit events and alarms.
- Historical Data (HD). A supplement to the DA interface, which can transfer historical data.
- DA XML. Based on the DA interface, this relatively new interface uses eXtensible Markup Language (XML) for encoding DA content.

The latest development of the OPC standard is OPC UA, which was released in 2006 and combines the previous technologies from OPC DA, AE and HD. It is a pioneering standard for Industry 4.0 and Internet of Things (IoT). In contrast to most other CSCPs, the TCP/IP-based, service-oriented protocol offers both encryption and user authentication mechanisms. The most striking difference between OPC UA and its predecessors though is that it no longer is a Microsoft Windows® exclusive protocol, but is available on numerous operating systems as well as on-chip solutions. The ISO/OSI stack of OPC UA is depicted in Fig. 4, and the message structure of OPC UA binary is shown in Fig. 5.

7	UA Application	
6	UA Binary	UA XML
5	UA TCP UA Secure conversation	SOAP/HTTP WS Secure conversation
4	TCP (RFC 793)	
3	IP (RFC 791)	
2	MAC (IEEE 802.3)	
1	Ethernet (IEEE 802.3)	

Fig. 4. ISO/OSI layer structure of OPC UA protocol

3) TASE.2/ICCP/IEC 60870-6: The TASE.2 (which is similar to IEC 60870-6 and Inter-control Center Communications Protocol (ICCP)) is a standard used for wide-area communication between control centers in the electric power transmission network, which was standardized in 1997 by the IEC. It enables the exchange of time-critical information between control systems via Wide Area Network (WAN) and Local Area Network (LAN). Its scope is similar to that of OPC, but is—unlike early versions of OPC—not tied to a particular operating system.

The standard by itself does not address authentication or encryption (these services may be provided by lower protocol layers, though). TASE.2 relies on Manufacturing Messaging Specification (MMS), its core functions are specified as sets of so-called "Conformance Blocks", such as, e.g., periodic system data, device control, etc. The ISO/OSI layer structure of TASE.2 is given in Fig. 6. Its message structure is depicted in Fig. 7.

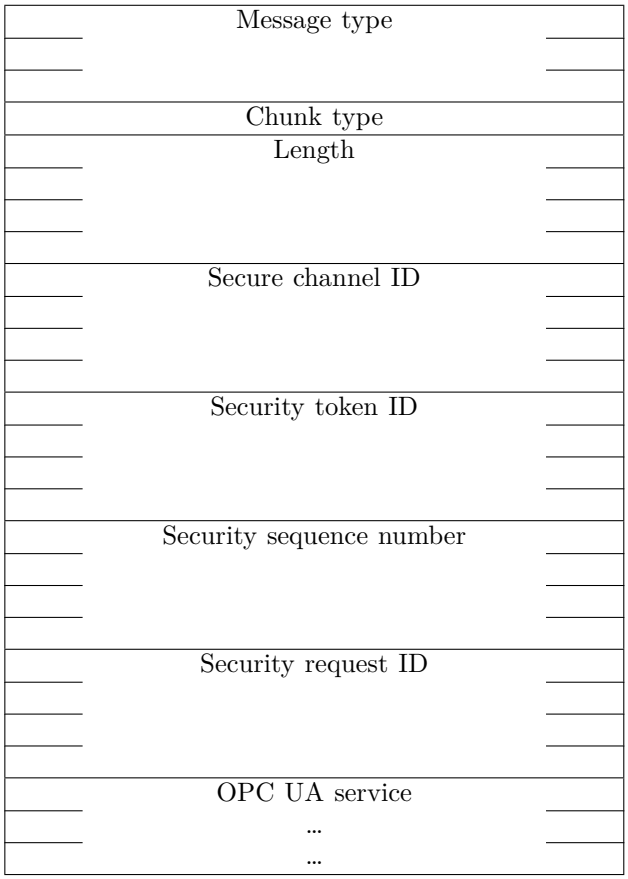

Fig. 5. OPC UA message structure

7	TASE.2, MMS ISO 9506, ISO 8650 ACSE		
6	ISO 8823/8825, ASN.1, BER, ISO/IEC 8824.1		
5	Connection oriented session, ISO/IEC 8327		
4	ISO/IEC 8073 TP4	RFC 1006 ISO/IEC 8073 TP0 over TCP	RFC 1070 ISO/IEC 8073 TP4 over UDP
3	CLNP - ISO/IEC 8473	IP (RFC 791)	
2	ISO/IEC 8802-2 LLC		
1	ISO/IEC 8802.3		

Fig. 6. ISO/OSI layer structure of TASE.2 protocol

4) DNP3: The DNP3 protocol is developed for communication with telecontrol substations and other Intelligent Electronic Devices (IEDs). It is especially tailored for the usage in energy-related SCADA systems and is widely adopted by North American power system utilities. The development was originally carried out by the Harris company, which in 1993 turned the development and maintenance over to the DNP3 User Group, an association of users and suppliers of the protocol.

Originally, the DNP3 protocol was developed for use on slow, serial communication links. However, during the development of DNP3, support for communication via TCP/IP networks was also implemented. In contrast to similar protocols, such as IEC 60870-5-101, DNP3 has a very powerful user layer (a layer on top of the ISO/OSI application layer, containing user data), which allows the data to be decoded even without implicit parameters. DNP3 has a variety of ways to display information objects and provides a high degree of interoperability on the user layer. This is achieved at the cost of increased complexity, which in turn requires a high implementation and testing effort.

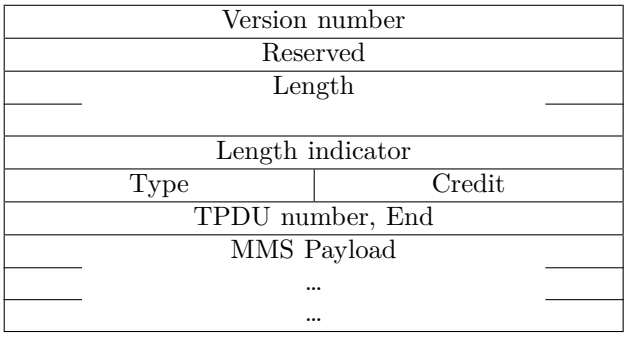

Fig. 7. TASE.2 message structure

Unlike IEC 60870-5-101, the protocol has a transport layer that allows a fragmented transmission of large amounts of data. This benefits the protocol when communicating over TCP/IP, because the entire bandwidth of the network can be effectively utilized. Another advantage over IEC 60870-5-101 is the possibility to request an acknowledgment from the other side on the user layer. As a result, a substation can remove the data from the buffer depending on whether these have been acknowledged by the destination.

The data link layer is based on IEC 60870-5-1 and IEC 60870-5-2, similar to IEC 60870-5-101. However, only a balanced mode is used, which is intended only for full-duplex point-to-point connections. Since DNP3 is also used in semi-duplex networks, a collision avoidance mechanism exists. The ISO/OSI layer structure of DNP3 is depicted in Fig. 8, while the message structure of DNP3 is visible in Fig. 9.

7	DNP V3.0 Data object library DNP V3.0 Data application layer	
6	n/a	
5	n/a	
4	DNP V3.0 Transport and network functions	TCP/UDP
3		IP
2	DNP V3.0 data link layer, IEC 60870-5-2 (balanced), IEC 60870-5-1 (FT 3)	RFC 894
1	RS232 (V.24)	Ethernet (IEEE 802.3)

Fig. 8. ISO/OSI layer structure of DNP3 protocol

Similar to the Modbus protocol, it is noteworthy that several attempts were made to secure DNP3 already, the most well-knowns being the DNPSec [32] and DNP3 SA (which is part of the Institute of Electrical and Electronics

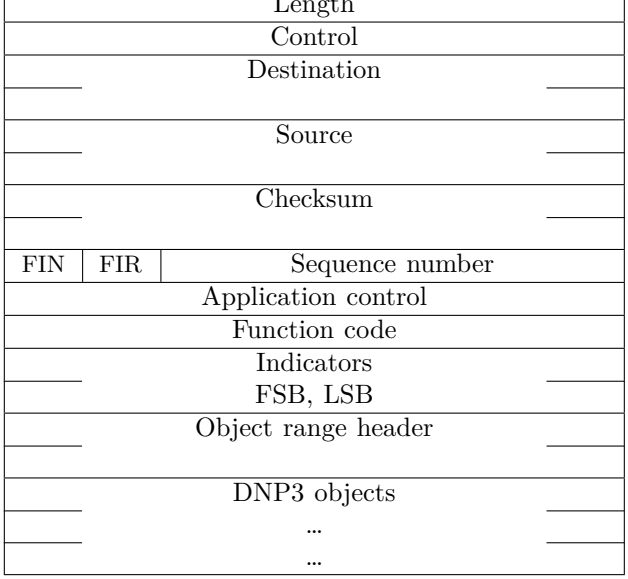

Fig. 9. DNP3 message structure

Engineers (IEEE) 1815-2012 standard [48]) [36] protocols, offering the following security features:

- DNPSec. The DNPSec protocol employs Triple Data Encryption Standard (3-DES) and Hash-based Message Authentication Code (HMAC) SHA-1 to provide security.
- DNP3 SA. In contrast to DNPSec, no encrytion is used. Integrity and authentication are provided by Challenge-response HMAC/Galois Message Authentication Code (GMAC) and SHA-2 hashing.

It needs to be noted at this point that the cryptographic algorithms employed in DNPSec (3-DES and SHA-1) are considered broken by now and are insecure against sophisticated attacks [49], [50]. Therefore, during the security analysis in Section V-C, the security features of DNPSec are regarded as ineffective against attacks. In the following, the original DNP3 protocol as well as both DNPSec and DNP3 SA are included in the security analysis of this paper.

5) IEC 60870-5-101: The IEC 60870-5-101 protocol is an international standard and was released by IEC in the early 1990s. The protocol was widely used in the field of power systems and is still used very frequently today. It is based on the so-called Enhanced Performance Architecture (EPA) and, according to the OSI layer model, this protocol only defines the physical, data link, and application layers.

IEC 60870-5-101 is mainly used on relatively slow transmission media using the asynchronous V.24 interface. The use of the X.24/X.27 interface with baud rates of up to 64000 bit/s, which is also defined in the standard, is hardly used in practice. The IEC 60870-5-101 standard is a "companion standard" and is supplemented by several others, as depicted in Fig. 1:

- IEC 60870-5-1: Different frame formats are defined here, whereby only the format FT1.2 is used for IEC 60870-5-101.
- IEC 60870-5-2: Defines the transfer methods of the data link layer.
- IEC 60870-5-3: Describes the basic structure of the user data.
- IEC 60870-5-4: Defines the encoding of information elements.
- IEC 60870-5-5: Describes basic functions of the user layer.

The IEC 60870-5-101 was significantly extended and specified in the year 2001 by a second amendment. Interoperability between devices from different manufacturers is ensured by means of a so-called "interoperability" list, the structure of which is defined in the standard. The original standard left much room for interpretation, leading to many implementations that are not necessarily compatible with each other.

A great advantage of IEC 60870-5-101 is the robustness of the data link and the simple structure of the application layer. The focus was placed on performance during the definition. To achieve this, certain information required to decode the data is not sent. The decoding of the data is only possible with correctly set parameters such as size of the information object address, size of the ASDU address, etc. In practice, the matching of parameters between components with the help of the interoperability list is easily possible and does not represent a major challenge.

A major disadvantage however are the gaps in the definition of the protocol, which often lead to problems. Particularly with respect to line redundancy, many different implementations exist, which require project-specific clarifications. Fig. 10 shows the ISO/OSI layer structure of IEC 60870-5-101, Fig. 11 shows the IEC 60870-5-101 message structure.

7	IEC 60870-5-101 Companion standard, IEC 60870-5-5, IEC 60870-5-4, IEC 60870-5-3	
6	n/a	
5	n/a	
4	n/a	
3	n/a	
2	Balanced, IEC 60870-5-2, IEC 60870-5-1 (FT 1.2)	Unbalanced, IEC 60870-5-2, IEC 60870-5-1 (FT 1.2)
1	RS232 (V.24)	X.24/X.27

Fig. 10. ISO/OSI layer structure of IEC 60870-5-101 protocol

6) IEC 60870-5-104: The IEC 60870-5-104 protocol is an international standard and was released in 2000 by the IEC. As the name of the standard "network access for IEC 60870-5-101 using standard transport profiles" suggests, the protocol is deeply linked with IEC 60870-5-101. IEC 60870-5-104 allows communication between the control center and the substation via a standard TCP/IP network.

Start				
Length				
Length (copy)				
Start				
RES	PRM	FCB ACD	FCV DFC	Function code
Link address field (0, 1, or 2 bytes)				
Type identification				
SQ	Number of objects			
T	P/N	Cause of transmission		
Originator address (optional)				
ASDU address fields (1 or 2 bytes)				
Information object address fields (1, 2 or 3 bytes)				
Object information				
Checksum				
End				

Fig. 11. IEC 60870-5-101 message structure

The TCP protocol is especially used for connection-oriented and secure data transmission.

IEC 60870-5-104 limits the information types and configuration parameters defined in IEC 60870-5-101 so that not all IEC 60870-5-101 functions are also supported by IEC 60870-5-104. Among others, IEC 60870-5-104 does not support short time stamps; also, the sizes of the individual address elements are permanently set to maximum values. In practice, however, manufacturers often place the IEC 60870-5-101 application layer on the IEC 60870-5-104 transport profile without taking its limitations into consideration. This can lead to problems with devices which strictly adhere to the standard. Interoperability between devices from different manufacturers is ensured by means of the so-called "interoperability list", the structure of which is defined in the standard.

The main advantage of IEC 60870-5-104 is communication over a standard network, which allows simultaneous data transmission with several devices and services. Otherwise, the advantages and disadvantages of IEC 60870-5-101 apply to IEC 60870-5-104, too. Fig. 12 depicts the ISO/OSI layer structure of IEC 60870-5-104, Fig. 13 shows the IEC 60870-5-104 message structure.

7) IEC 61850: IEC 61850 is the latest standard for communication networks and systems in substations and encompasses a large variety of concepts including 10 parts, depicted in Fig. 14.

Apart from the first two parts covering the introduction and glossary, parts 3, 4, and 5 of the standard start by identifying the general and functional requirements for substation communication. In order to assist the configuration

7	IEC 60870-5-104 Companion standard, IEC 60870-5-5, IEC 60870-5-4	
6	n/a	
5	n/a	
4	TCP (RFC 793)	
3	IP (RFC 791)	
2	PPP (RFC 1661/1662)	RFC 894
1	X.21	Ethernet (IEEE 802.3)

Fig. 12. ISO/OSI layer structure of IEC 60870-5-104 protocol

Start
Length
Control fields
ASDU as in IEC 60870-5-101
...
...

Fig. 13. IEC 60870-5-104 message structure

of all components from a system level perspective, a XML-based Substation Configuration Language (SCL) is defined in IEC 61850-6. It allows to define the relationships between the substation automation system and the substation itself. To provide information regarding its configuration, each device in the system must provide a SCL file. One of the main architectural novelties introduced by IEC 61850 is an abstract definition of its data items, which first allows the creation of data items and services that are agnostic regarding their underlying protocols. Second, these abstract items can be mapped onto any underlying protocol. While the definition of abstract data items is covered in IEC 61850-7, the specific mapping onto Generic Object Oriented Substation Events (GOOSE), MMS or SV is included in IEC 61850-8 and IEC 61850-9, respectively. IEC 61850-10 defines a conformance test with the numerous protocol definitions and constraints defined in the document.

While the standard covers the needs of the station automation regarding communication structures and the

1	Introduction and overview
2	Glossary of terms
3	General requirements
4	System and project management
5	Communication requirements for functions and device models
6	Configuration language for communication in electrical substations related to IEDs
7	Basic communication structure
8	Specific communication service mapping – MMS
9	Specific communication service mapping – SV
10	Conformance testing

Fig. 14. Parts of IEC 61850

7	TimeSync SNTP	SV	GOOSE	GSSE ACSE ISO/IEC 8649, 10035	MMS ISO 9506 ACSE ISO/IEC 8649, 8650	
6	n/a	n/a	ASN.1, BER ISO/IEC 8824.1	ISO/IEC 8649, 10035 ASN.1, BER ISO/IEC 8824.1	ISO/IEC 8822,8823 ASN.1, BER ISO/IEC 8824.1	
5	n/a	n/a	n/a	ISO/IEC 9548	ISO/IEC 8326, 8327	
4	UDP/IP	n/a	n/a	ISO/IEC 8602	ISO/IEC 8073	TCP/IP (RFC 1006)
3	IP (RFC 791)	n/a	n/a	ISO/IEC 9542	ISO/IEC 8473	IP (RFC 791)
2	RFC 894	VLAN (IEEE 802.1Q), CSMA/CD (IEEE 802.3)		IEEE 802.2 LLC		RFC 894
1	IEEE 802.3					

Fig. 15. ISO/OSI layer structure of IEC 61850 protocol

	Modbus	Modbus-F2009	Modbus-S2015	Modbus-A2018	OPC UA	TASE.2
Authentication	✗	Signature	Signature	Challenge-response	Password-based, X.509, WSS	✗
Authorization	✗	✗	✗	✗	✗	✗
Integrity	✗	SHA-2	SHA-2	Checksum	Signature	✗
Confidentiality	✗	✗	Encryption	Encryption	Encryption	✗

TABLE III
Overview and comparison of protocol features (part 1)

	DNP3	DNPSec	DNP3 SA	IEC 60870-5-101	IEC 60870-5-104	IEC 61850
Authentication	✗	HMAC	Challenge-response	✗	✗	✗
Authorization	✗	✗	✗	✗	✗	✗
Integrity	✗	SHA-1	SHA-2	✗	Checksum	Checksum
Confidentiality	✗	Encryption	✗	✗	✗	✗

TABLE IV
Overview and comparison of protocol features (part 2)

object-related data model, it is generally designed to also support many other automation applications. The basic principles are retained and supplemented by sector-specific data models, e.g. for communication, monitoring and control of wind power plants or hydroelectric power stations. Unlike IEC 60870-5-104, IEC 61850 is only defined for the station bus. From a technical point of view, however, IEC 61850 is also suited for process data transmission between stations and network control systems. This allows a complete system architecture from the process to the station control system and the grid control point without requiring the application of gateways. The IEC 61850 ISO/OSI layer structure is visible in Fig. 15, Fig. 16 shows the IEC 61850 message structure.

B. Protocol Security Overhead

In the protocol overview, several modernized variants of Modbus and DNP3 are discussed. It needs to be noted here, however, that the increased security realized within the discussed protocol variants comes at the prize of performance, mainly due to en-/decryption and signature procedures used. While the performance overhead incurred due to such security measures is commonly not a major issue, within the context of control systems, there are often real time performance requirements (see Section III-D). Therefore, in this section, a brief overview regarding the performance overheads of the enhanced variants of the Modbus or DNP3 protocol, respectively, is given.

- Modbus-F2009. Fovino et al. state that in their test scenarios, the protocol causes a performance overhead of 291% at maximum and 12% at minimum (relative to the original Modbus protocol) [28].
- Modbus-S2015. To the best of our knowledge, there is currently no information available regarding the performance overhead incurred by the usage Modbus-S2015. However, it is expected that the overhead is at least as high as with Modbus-F2009, as both employ signatures and SHA-2, and, in addition, Modbus-S2015 uses encryption.
- Modbus-A2018. According to [30], the Modbus-A2018 protocol variant leads to a performance overhead of 500% at maximum and 0% at minimum (relative to the original Modbus protocol).
- DNPSec. To the authors' knowledge, there is no quantitative performance evaluation available investigating the DNPSec protocol. However, Lee et al. provides a qualitative estimation of the performance overhead, which is considered as "high" [21].

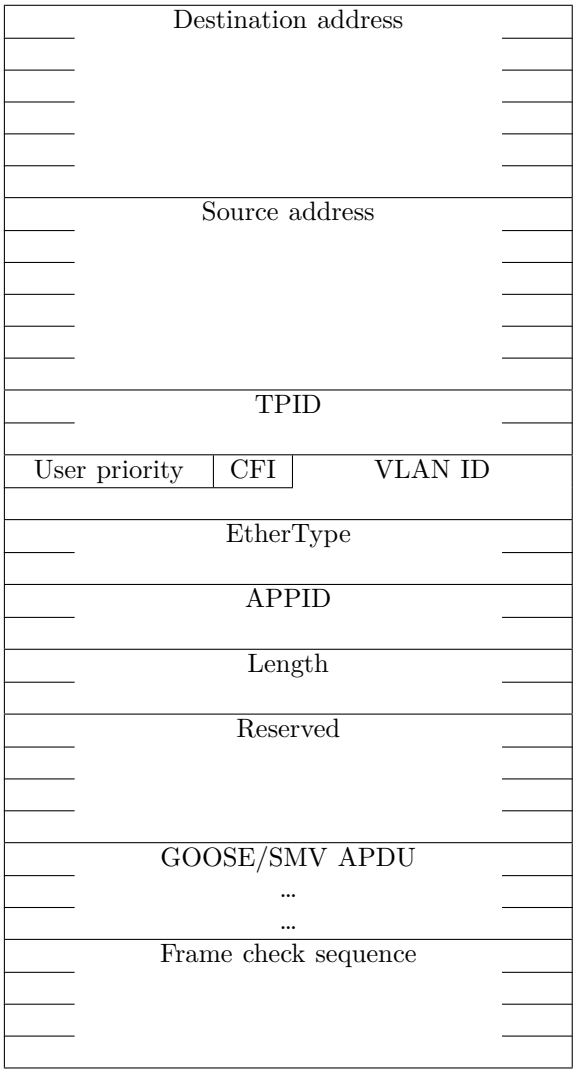

Fig. 16. IEC 61850 message structure

- DNP3 SA. Similar to DNPSec, [21] states that the performance overhead is considered "medium". However, the performance of DNP3 SA also depends on the usage of the non-aggressive or aggressive mode (further information available in IEEE 1815-2012).

C. Requirements

For the above-described CSCPs applied in the industrial context, three basic security requirements need to be considered in addition to the corresponding protocol's performance as this has a significant impact to the practicability of the proposed solution. Next, we give the exact definition of the security requirements considered in this paper, which are based on the ones illustrated in the technical specification report IEC 62351-1:

- Confidentiality. Prevention of unauthorized access to information by individuals, entities or processes.
- Integrity. Prevention of unauthorized modification or altering of information.
- Availability. Prevention of denial of service and insurance of authorized and continuous access to information.

While all of these aforementioned security goals do exist in the context of ICSs, it is noteworthy that their importance gets reordered. The most important goal in ICSs is availability, followed by integrity and confidentiality, in contrast to the usual CIA order.

Regarding performance, control systems have real-time requirements where decisions need to be taken quickly (within seconds) and any fraction of downtime period of the system could result in investment and reputation losses as well as environmental disasters. An application scenario can be found within the context of smart grids, where ICT plays an eminent role especially in demand/response schemes. Here real-time constraints are present as the decisions on how resources are controlled have a drastic impact on the overall system behavior. In this context, the major objective is to match energy generation and consumption. If such a balance is not met, it jeopardizes the stability of the grid which leads to brown- and blackouts.

D. Challenges

Control system's security has been a wide-spread topic in the ICT community in the last years, in particular with regard to CSCPs. This development was only fostered by several successful attacks in the past receiving public attention, e.g. [51], [4], [2]. While the development of control system communication standards is accelerating, the current situation with control systems is often coined by a discrepancy between old and new.

Numerous challenges can be highlighted in implementing security requirements within the context of networked control systems (e.g. SCADA) in practice. As previously mentioned, hardware/software and networking for such systems were designed and developed back in the 1970s, which consequently results in limited processing, storage and communication bandwidth. As a matter of fact, the conventional security measures devised within the context of ICT and networking technologies become extremely challenging to be implemented in control systems. Exchanging these legacy parts would either be connected to high costs due to revenue loss during transition time or not be possible at all because of custom builds often working with code written by operators no longer working for the company. What's worse, these legacy control systems were often designed in a time where security concerns were dangerously neglected. Additionally, control systems are used in wide-spread industrial sites which necessitates the physical intervention of personnel and results in difficulty in implementing key management, certificate revocation and other security measures. Finally, although security measures in wireless systems were improved in the last decade, wireless technologies are still not widely used in control systems due to extremely noisy environment (e.g. power systems) that might perturb the corresponding signal.

This derives the conclusion that control systems have specific requirements, which have to be considered while thinking of security strategies. Often, these requirements cause conflicts and contradictions between well-known protection methods and a functional control system. To get an overview, the most important requirements of control systems are listed below:

- Legacy constraint. Often control systems consist of legacy components with low bandwidth, little computational power and/or limited storage space [52]. Some even are not supported any more by their vendors with updates or patches. This often is due to the long lifecycle of control system products, which can be up to 30 years. A change of these components will often result in high costs or revenue loss due to downtime which companies are not willing to accept.
- 24/7 constraint. Control systems, which supervise critical infrastructures need to be operational all time. Even a short downtime can cause huge monetary or reputation damage or even endanger human lives (e.g. blackouts) [53].
- Real-time constraint. In industrial control systems, the devices have to react as quickly as possible to commands given by the operator through a control system. Often, if a critical state is reached, the decision has to be made in a matter of seconds. This means that low latency and efficient use of bandwidth are critical for these systems [53].

IV. Adversary Model

An adversary model is a common method to summarize assumptions about the nature, significance and resources of persons and organizations tending to perform malicious activities and cause harm to the system [54]. The adversary model is developed to describe the capabilities of a potential attacker, indicate the threats and attack scenarios. Nowadays, due to the diversity of possible attacks and interests of different actors, it is especially important to investigate the threat landscape precisely. This section presents a collaborative overview on threat actors and discusses their features. In general, adversaries, also defined as threat actors, can be classified as outsiders, having no authorized access to telecontrol systems, and insiders, i.e. legal entities with a certain set of permissions in the targeted system. This approach is used, for example, in [55].

According to IEC 62351-1 part 5.2.3, eight classes of potential threat actors can be distinguished. This classification is however incomplete, until corresponding threat levels are assigned. Here, a threat level is a qualitative measure of potential impact, which occurs if an adversary completes its attack successfully. Moreover, the standard presents viruses and worms as a separate threat actor. This makes the model incoherent, since viruses and worms need to be considered as tools, not threat actors themselves. Furthermore, depending on the type of virus or worm and the targeted element(s) of the system, different threat levels are required. As a result, this class of threat actors is not considered in this paper. In the following, the threat actors investigated in the analysis (Section V-C) are listed:

- Unskilled and skilled outsiders. Outsiders with various level of hacking skills are common adversaries which system defenders are facing. Usually these actors have no ideology except the curiosity to break the security of a system. Unskilled outsiders are usually able to detect reachability of hosts in control networks and use common tools for penetration testing, but do not have any special knowledge regarding CSCPs. Skilled outsiders in addition possess enough experience in breaking telecontrol systems and network security. This makes it rational to attach different threat level to outsiders depending on their skills.
- Industrial espionage. Not only persons but entire organizations may be interested in breaking control network security. Resulting availability problems may lead to customers changing their provider; also, sensitive information can be stolen. Organizations have enough resources to employ high skilled professionals, but have to work secretly not to disclose their illegal activities.
- Trusted insiders. One of the most common threats are malicious insiders that can have low hacking skills, but hold enough information about systems' architecture and maintenance. Potential harm depends on the position and security clearance of the insider. Malicious administrators, as a worst case scenario, have enough knowledge to ruin security systems as well as the whole critical infrastructure causing catastrophic damage.
- Terrorist groups. Nowadays terrorist and hacker groups are becoming one of the most dangerous actors in cyberspace. These organizations aim to perform attacks on critical infrastructures in order to present their ideology and personal beliefs [13]. Potential damage depends on the resources such a group has access to. Several terrorist and hacker groups get support from their nations and interested organizations. Nevertheless, highly skilled professionals are usually employed by terrorist groups or join it on their own.
- National states, foreign intelligence services. According to [13], the most powerful actors in critical infrastructures' security are hostile nations and their intelligence services. Having almost unlimited resources, hostile nations can hire skilled professionals to damage critical infrastructures such as power, water and industry to influence the current political situation. These attacks can cause loss of citizens' lives. Another common motivation is espionage and collection of information about national infrastructures for future purposes. Moreover, national cyber security services are interested in testing their possibilities to gain access to another nation's resources.

Table V presents an overview of the adversary model

Class name	Threat level	Motivation	Impact	Resources	Level of hacker skills	Typical attacks (see Section V)
Unskilled outsider	0	Curiosity	Low to minimal	Heavily bounded resources	Low	Detection of network devices, network exploration, eavesdropping
Skilled outsider	1	Money, personal problems	Low to medium	Usually bounded resources	Medium to high	Eavesdropping, information theft, replay attacks, exploitation of a software and hardware vulnerabilities
Industrial espionage	2	Interests of organization, financial harm	High	Usually uses bounded resources in order not to disclose activities	High	Information theft, denial of service
Trusted insiders	3	Personal problems, treason	Low to high	Uses resources of targeted system and access level	From low to highest depending on access level	Information and credentials theft, log tampering
Hacktivists, Terrorists	4	Ideology	Highest	Almost unbounded computational power	Highest	DDoS, disruption of the whole system, virus attacks
States, Foreign intelligence services	5	National interests	Highest	Unbounded computational power	Highest	Information theft, DDoS, disruption of the whole system, virus attacks

TABLE V
Adversary Model

described above. It defines a set of major properties for each of the defined adversaries:

- Threat level. A qualitative marker which allows to distinguish different classes of adversaries based on their overall potential impact, if an adversary completes its attack successfully.
- Motivation. Summarizes assumptions about possible stimulus.
- Impact. A qualitative marker which describes potential damage (data, human, or environmental), similar to ISO 31000/IEC 61508 [56].
- Resources. Summarizes assumptions about computational power available to the adversary.
- Level of hacker skills. Summarizes assumptions regarding the professional knowledge possessed by the adversary.
- Typical attacks. Provides examples of possible security breaches, which are later discussed in Section V.

The set of properties is not exhaustive, more properties can be defined to complete the adversary information, such as necessity of the physical access, requirement of the specific hardware, and sustainability of the deployed security measures to the malicious activity.

V. Potential Security Breaches in Control System Communication Protocols

This section covers attacks related to CSCPs. The origin of the vulnerabilities for most of the protocols is the lack of basic confidentiality, integrity and authentication mechanisms for data communication. Lack of confidentiality and integrity leads to unwanted access to and possible modification of data transmitted over the channel. At the same time, lack of authentication is a reason of the unquestioning acceptance of all the commands received by RTUs. Attacks are classified based on the security requirements they violate. For some interaction attacks, such as replay or MitM, several classes are possible.

A. IEC 62351 Standard Overview

The scope of the IEC 62351 standard is to provide power systems with the relevant end-to-end security information for their control operations. For this purpose, the main objective is to propose development of standards for security of the communication protocols defined by IEC TC57, especially for the IEC 60870-5, IEC 60870-6 and IEC 61850 series [57]. To this end, the standard is divided into 13 parts:

- Part 1: Introduction to the standard.
- Part 2: Glossary of terms.
- Part 3: Security for profiles including TCP/IP.
- Part 4: Security for profiles including MMS.
- Part 5: Security for profiles including IEC 60870-5.
- Part 6: Security for IEC 61850 profiles.
- Part 7: Security through network and system management.
- Part 8: Role-based access control.
- Part 9: Key management.
- Part 10: Security Architecture.
- Part 11: Security for XML files.
- Part 12: Resilience and security for power systems.
- Part 13: Guidelines on security topics to be covered in standards.

B. Methodology

Taking the constraints/challenges of Sections III-C and III-D into account, the three security requirements (i.e. confidentiality, integrity and availability) are satisfied through the combination of security management techniques and technologies. Among several, certificate and key management (e.g. authentication) together with encryption

(e.g. AES) are the most prominent countermeasures to the security threats discussed in Section V-C. It is worthwhile to note that security is an "end-to-end" requirement of control systems for the sake of ensuring authenticated access to sensitive equipment, authorized access to data and information on equipment failures. Due to this large spectrum, a "one size fits all" paradigm is not appropriate as each asset needs to be secured based on its required security level. To this end, a continuous security process cycle is proposed in the IEC 62351 standard, which consists of the following five steps: (1) security assessment, (2) security policy, (3) security development, (4) security training and (5) security audit. In this paper, we focus on the first step of this cycle for the purpose of our analysis and results. More precisely, the considered methodology consists of assessing assets by considering their security requirements and the probable risks of attack. For this purpose, we carry out the security assessment by studying the protocols without (pre) and with (post) the implementation of the IEC 62351 security standard. The end result of such a methodology is to qualitatively highlight the security improvements of IEC 62351 as well as to emphasize the missing parts of such a standard within an industrial context such as smart grid SCADA systems. The reason for using a qualitative analysis is the difficulty to extract real and exact numbers from industrial control systems due to confidentiality reasons. It is noteworthy that regarding the usage of IEC 62351 in the Modbus protocol, its application is possible theoretically (e.g. using Transport Layer Security (TLS) to secure Modbus TCP communication); however a technical realization may often be hardly achievable, due to resources' limitations present in legacy Modbus systems. In the upcoming analysis, an applicability of IEC 62351 on the Modbus protocol is assumed to be possible. For the OPC UA protocol, no application of the IEC 62351 security standard is considered, as OPC UA implements its own security features without relying on IEC 62351. Therefore, in the following, no pre-/post-IEC 62351 analysis is performed for OPC UA.

C. Analysis

1) Confidentiality Violation Attacks:

Detection of control system devices. The initial step of all communication-based attacks is the detection of devices in the network. For detecting control system devices two approaches can be considered – passive and active. A passive approach implies that an interface is being set up in promiscuous mode to subsequently monitor traffic. During active detection, packets are sent out from an attacker's device in order to obtain responses from control systems. The Application Protocol Data Units (APDUs) sent during active detection carry specific control commands which force target devices to answer with confirmation.

Measures, defined by IEC 62351: There are no comprehensive counter measures defined in the standard. General security recommendations are discussed in Section V-D.

In Table VI, the results for the device detection attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, Modbus-F2009, Modbus-S2015, Modbus-A2018, TASE.2, OPC UA, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	Modbus, Modbus-F2009, Modbus-S2015, Modbus-A2018, TASE.2, OPC UA, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850

TABLE VI
Vulnerability analysis results for device detection attack

Eavesdropping. Eavesdropping is an example of SCADA communication confidentiality violation. Because of the lack of inbuilt confidentiality protection, these attacks are easy to perform. Eavesdropping represents a common activity of outsiders with low hacking skills. By eavesdropping on the communications of control system devices, attackers can learn control commands while simply listening to the traffic, and log message exchanges between different nodes. As there usually are no encryption mechanisms specified for CSCPs, using an eavesdropping attack, adversaries can obtain a full image of the current system state. Detected traffic can be used later for more sophisticated attacks, such as replay and MitM.

Real case scenarios:

- Modbus, IEC 60870-5-101, IEC 60870-5-104. One of the most suitable methods to attack Modbus and IEC 60870-5-based protocols is by port mirroring, as described in [26]. To capture packets, an attacker has to configure a span port on network devices, so that all targeted traffic is retransmitted to the attacker's system. There are several ways how a span port can be configured, such as gaining administrative privileges on network devices for outsiders or direct access for insiders. Attackers require some experience in serial protocols' message exchange. Capturing of messages is a confidentiality violation and can lead to active attacks.
- TASE.2. By design, the TASE.2 protocol does not include any inbuilt security measures. The confidentiality of information transmitted over the TASE.2 connection is expected to be implemented by the underlying protocols.
- DNP3. For the scenario of DNP3, this type of attack was analyzed within a testbed setup by eavesdropping the network traffic between a slave IED and master gateway through ARP cache poisoning [33]. A side-effect of eavesdropping was the successful manipulation of the Media Access Control (MAC) addresses by the attacker, who altered the destination MAC address of the frame to the attacker's machine address. Whereas the forwarding of messages to the attacker's machine

does not have any further direct security implications except for a confidentiality violation, it however induced an increased delay in the communication, which in certain cases could be deemed dangerous, especially if fast reaction times are required.
- IEC 61850. Using an ARP spoofing approach, an adversary can launch a MitM attack on the MMS communications of IEC 61850. Based on this MitM attack, several kinds of attacks can further be launched, among others eavesdropping. An example scenario would be an adversary that wants to gather additional information by eavesdropping on the hijacked or tapped communication before carrying out further attacks. Such a scenario is described in [41].

Measures, defined by IEC 62351: The encryption applied by TLS through IEC 62351 is an effective mean to prohibit adversaries from accessing information through eavesdropping.

In Table VII, the results for the eavesdropping attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, Modbus-F2009, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	—

TABLE VII
Vulnerability analysis results for eavesdropping attack

Content Addressable Memory (CAM) table overflow attack. One of the possible confidentiality violation attacks which gain the possibility to eavesdrop on CSCPs with TCP/IP profile is the CAM table overflow attack [58]. Data link layer's switching devices process Ethernet frames based on MAC or hardware addresses. A CAM table maps the switch ports to the destination MAC addresses. As a result, frames are sent to the intended address on an individual basis. If an attacker triggers a CAM table overflow, it forces a switching device to act as a hub, i.e. broadcast Ethernet frames to all ports. Attackers can flood the CAM table with new MAC-port entries in order to fill up the device's memory. As a result, the target device is not able to function as intended and begins broadcasting Ethernet frames to all available ports. Having access to one of the ports, e.g. for external connections, attackers are able to listen and capture the traffic that flows through the switching device.

Real case scenarios: This attack exploits the functionality of Ethernet switches. Since there are several CSCPs in substation networks that use Ethernet switches to connect IEDs, all IEC substations are vulnerable to these attacks. Among these protocols are, among others, Modbus, DNP3, IEC 60870-5-104, and IEC 61850. Experiments with IEC 61850 are observed in [59].

Measures, defined by IEC 62351: There are no comprehensive counter measures defined in the standard. General security recommendations are discussed in Section V-D.

In Table VIII, the results for the CAM table overflow attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, Modbus-F2009, Modbus-S2015, Modbus-A2018, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	Modbus, Modbus-F2009, Modbus-S2015, Modbus-A2018, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850

TABLE VIII
Vulnerability analysis results for CAM table overflow attack

Masquerade attack. An ARP spoofing attack is an example of masquerading [58], [44]. This attack exploits the lack of verification and authentication support in CSCPs. ARP is a stateless protocol used to map an IP address to a physical machine address. The ARP cache is updated with new information each time a host receives a reply, whether a request was sent or not. ARP spoofing is a way to modify a target host's ARP cache with a forged entry to allow attackers to masquerade as a legitimate host and get access to traffic for further actions. Often ARP spoofing is used to launch further subsequent attacks, such as MitM, session hijacking, or DoS.

Real case scenarios:
- Modbus, IEC 60870-5-101, IEC 60870-5-104. Examples of successful utilization of ARP spoofing as a step for a MitM attack are presented in [26] and [27].
- DNP3, DNPSec. An eavesdropping attack was realized by Rodofile et al. in [33] within the context of DNP3, where the attacker intercepted the communication as a result of ARP cache spoofing. Due to the ineffective security measures in DNPSec, a similar attack can be realized.
- IEC 61850. As previously discussed, using ARP spoofing attacks, a masquerade attack is possible on IEC 61850, which is presented in [41].

Measures, defined by IEC 62351: There are no comprehensive measures defined in the standard. General security recommendations are presented in Section V-D.

In Table IX, the results for the masquerade attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, TASE.2, DNP3, DNPSec, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	Modbus, TASE.2, DNP3, DNPSec, IEC 60870-5-101, IEC 60870-5-104, IEC 61850

TABLE IX
Vulnerability analysis results for masquerade attack

Credential theft. Besides operator commands and system responses, typical data exchanges in critical infrastructures such as smart grid also include customer names, identification numbers, schedule information and location data. These data are sensitive since they may carry credentials that allow persons or organizations to gain access to the system. Credential-based attacks include several phases. In the first phase, an attacker abuses the low confidentiality protection of CSCPs to obtain sensitive information. This information can subsequently be used by an attacker to authenticate as a legal entity and compromise the whole system. As a result, these attacks can further lead to integrity and availability violations.

Real case scenarios:

- Modbus, Modbus-F2009, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104. Lack of encryption in CSCPs makes it easy for attackers to get information by simple eavesdropping and use it for further attacks such as user-to-root. A user-to-root attack allows to gain superuser privileges while starting as a normal user. Having superuser privileges, malicious outsider of low clearance level can rise to insider level and cause severe damage. The scope of damage to the infrastructure depends on the access rights assigned to the stolen credentials.
- IEC 61850. Besides the lack of encryption in IEC 61850 as in the other CSCPs, password cracking attacks can be performed on application level services such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP) and Telnet running on IEDs, as presented in [59] and [60].

Measures, defined by IEC 62351: Apart from basic authentication methods, IEC 62351-8 presents a Role-Based Access Control Model (RBAC) for power systems. This model ensures the security policy implementation by defining specific roles for users with different levels of trust. Being introduced in a system, an access model restricts the transmission of credentials over a network. However, the implementation of a sophisticated access model for each system is a time and money consuming process, preceded by a laborious and difficult designing phase. An example of static and dynamic role identification is discussed in [61]; furthermore, the authors emphasize that IEC 62351 does not provide means to enforce authorization rights in detail.

In Table X, the results for the credential theft attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, Modbus-F2009, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	Modbus, Modbus-F2009, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850

TABLE X
Vulnerability analysis results for credential theft attack

2) Integrity Violation Attacks:

Replay, alteration and spoofing attacks. Captured messages can be used for replay attacks, by which an attacker uses obtained messages to retransmit them with modifications or delay in order to trick the target device(s). By retransmitting messages without modification, an attacker is able to trigger pull requests from field devices and obtain enough information regarding their state and current measurement data. Replay attacks with modification of data (insertion, deletion, alteration) are even more dangerous, because they lead to integrity and availability violations. Modified messages can contain wrong data and commands. Furthermore, an attacker can drop initial packets in order to craft a new packet to be sent instead. By injecting his/her own command or data to a control system, an attacker can disturb normal system processes and provoke emergencies. As an example, an attacker can gain access to smart meters and inject control signals into the system. The aim of this replay attack may be to shut down the power supply to a certain area.

The lack of data link integrity in CSCPs additionally leads to an absence of non-repudiation and, as a result, to repudiation attacks. The system is unable to properly track users' activities, which allows potentially malicious actions to be taken while forging the origin of these actions. The goal of such attacks is usually to impersonate a legitimate user and exploit this impersonation to execute malicious actions on a system. Its usage can be extended to general data manipulation in the name of others. If such an attack is successful, the logging information cannot be used for forensic analysis later and needs to be considered invalid or misleading.

For example, an attacker can modify information, transmitted from RTUs to the administration subsystem, in order to create a misleading perception regarding the current state of the field devices. Furthermore, it's possible to impersonate commands and messages in order to make administrators think that malicious activities in the system originated from random device failures instead of a third party.

Real case scenarios:

- Modbus. The lack of authentication mechanisms in combination with no integrity checks makes the Modbus protocol highly susceptible to replay, alteration and spoofing attacks. It is possible for any attacker to impersonate a legitimate Modbus master, enabling the reuse of Modbus messages sent to or from slave devices. Due to the lack of integrity checks, the messages cannot only be resent, but also altered in any way required by an attacker. Similarly, messages may be spoofed, e.g. by impersonating a slave and sending arbitrary messages to its master.
- OPC UA. Even for the well-secured protocols, such as OPC UA, alteration attacks are taking place if the security means are implemented in the wrong way. Thus, failing to deactivate the security mode None can lead to a protocol downgrade attack and subsequently

lead to interception and alteration of messages.

- TASE.2. The absence of integrity measures in TASE.2 leads to easily realizable alteration attacks. Attackers are able to access the data in transmission and insert false information, which will be perceived by the control center as valid.
- DNP3. An address alteration attack can be achieved targeting DNP3. To this end, the attacker's objective is to intercept DNP3 frames and change their corresponding DNP3 destination addresses. Note that a DNP3 address is different from a MAC address. Changing the DNP3 destination address of a frame causes other devices to reply, or the intended device fails to receive the message. It was shown in [33] that such an attack has some practical limitations if the intention is to forward the frame from one device to another. More precisely, in order to be able to forward the frame to another device, a TCP connection needs to be established prior to the attack. As a matter of fact, this attack makes sense if there are more than one master configured on the slave device.
- IEC 60870-5-101. Integrity violation attacks are easy to perform in IEC 60870-5-101 environments. The reason for such a simplicity is the fact that the IEC 60870-5-101 protocol lacks data integrity features, such as strong checksum algorithms. As depicted in Figure 11, the checksum is implemented as a one byte field. As a result, one of the weakest links in this protocol is its one byte checksum that is not sufficient to provide message integrity. Overflow of the checksum byte is a trivial operation and an attacker can alter data values and the checksum field to perform undetectable modifications.
- IEC 60870-5-104. As shown in a simulated environment in [26], replay attacks on IEC 60870-5-104 can easily be performed. Packets are captured from the span port of the switch and replayed by using Kali Linux scripts. This experiment shows the simplicity of this attack and discusses the problem of its detectability in industrial networks, where the presence of stateful Intrusion Detection Systems (IDSs) for low-level devices is unlikely.
- IEC 61850. Cai et al. illustrate an attack on IEC 61850 based on the fact that SV, GOOSE, and MMS packets on most current smart substation network are transmitted in plain text via TCP/IP and Ethernet protocol [57]. The first attack is a GOOSE- and SV-based alteration attack which can compromise IEDs [39]. In [44], this attack is extended further by implementing it in a malware that can capture, alter and re-inject GOOSE messages into the network.

Measures, defined by IEC 62351: Apart from designing a secure network environment, application level IEC 62351 can be used to mitigate this attack. The standard provides challenge-response mechanisms based on HMAC with pre-shared key [62]. These measures aim to ensure authentication and integrity for the IEC 60870-5-101/IEC 60870-5-104 protocols.

In case of 61850, depending on the traffic sent via IEC 61850 (GOOSE, SV, or MMS) and the respective required timing, different security measures are recommended by IEC 62351. For MMS, messages are expected to make use of TLS, therefore authentication, confidentiality as well as integrity can be achieved. In contrast, for GOOSE or SV, the extended Protocol Data Unit (PDU) containing a signature is used to guarantee both authenticity and integrity. Also, the standard suggests the usage of RSA signatures for authenticity and integrity of extended PDUs, which makes it unsuitable for time-critical applications (traffic allowing a 4 ms maximum response time), as RSA signatures are relatively expensive in terms of computation power required. Here, other techniques requiring a lower computational complexity, such as HMACs would need to suffice [63]. Both measures—if implemented correctly—can protect against replay, alteration and spoofing attacks. However, several attacks were discovered even after the introduction of IEC 62351:

The first is a replay attack on the GOOSE protocol, where previously sent legitimate messages can be injected again after the stNum value (32 bit) is reset to zero [40], [64]. According to the validation scheme employed in GOOSE, the receiver accepts a message that was recorded by an attacker shortly before the stNum reset and replayed shortly after. Besides this replay attack, a DoS can be achieved using the same exploit, because all legitimate subsequent messages after the injected one would be dropped until their respective stNum values exceed that of the replayed message.

Second, MMS messages are not entirely secured against integrity violations [65]. The security of MMS messages is described in IEC 62351-4 and offers two profiles targeting transport (T-Profile) and application security (A-Profile). The T-Profile covers the protection of information on the TCP/IP level using TLS. The A-Profile defines security measures to be taken on application layer. However, the authentication used in the A-Profile does not provide application layer message integrity, which makes the usage of the T-Profile mandatory to achieve integrity protection. Combining A-Profile and T-Profile therefore provides authentication, integrity protection and confidentiality on transport level and authentication on application level. This approach works fine; however only if the transport connection spans the same entities as the application connection. As soon as there is a difference in transport and application connection hops, security problems arise. An example may be a scenario in which a proxy is used. Here the T-Profile is terminated by the proxy, whereas the application connection may be established end-to-end, directly with the actual entity to be reached. Since IEC 62351-4 does not provide application level integrity, no end-to-end application level security is provided.

Third, a security loophole exists enabling replay attacks on the SV protocol, where a previously sent message can

be replayed to a different receiver. This attack requires that two or more SV clients are subscribed to the same data set of a logical node. For each communication relationship a separate control block with different parameter values exists. Specifically of interest for this attack is that the values for the smpRate (number of samples sent per second) may differ. If different subscribers are receiving messages at different rates, their smpCnt values diverge. This attack works by replaying a message originally sent to a subscriber with a higher smpRate (and therefore higher smpCnt value) to a subscriber with a lower smpRate (and therefore lower smpCnt value).

In Table XI, the results for the replay, alteration and spoofing attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, TASE.2, DNP3, DNPSec, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	IEC 61850

TABLE XI
Vulnerability analysis results for replay, alteration and spoofing attack

Man-in-the-Middle. A MitM attack is a form of attack where the communication between two users is either monitored or even modified by an unauthorized third party. Generally, the attacker first actively eavesdrops on a communication by intercepting a public key message exchange and retransmits this message while replacing the requested key with his/her own. This process is transparent to both original parties, i.e. they appear to communicate normally. Neither the sender nor the receiver recognizes that the communication partner is an attacker trying to access or modify the message before retransmitting it to the originally intended destination.

Real case scenarios:

- Modbus. The complete lack of integrity checks in the Modbus protocol enables any attacker who has access to the control system network to either eavesdrop on messages or even modify legitimate messages and fabricate new messages and send them to slave devices [66].
- DNP3. In [34], attack scenarios based on packet fabrication and modification were studied by analyzing the function codes present in data link and application layers respectively. A MitM attack use case was considered by modifying the function codes for the three different cases: request of Master Terminal Unit (MTU), response of RTU, solicited MTU to unsolicited RTU response. It was shown that by fabricating or modifying erroneous data function codes (e.g. read, select, operate) of a DNP3 request or response, serious impacts on the control system can be achieved.
- IEC 60870-5-101, IEC 60870-5-104. Maynard et al. discuss MitM for IEC 60870-5-104 in the power grid environment of LINZ STROM GmbH in [26]. The attack includes capturing of packets and further packet replacement. In order to force victim devices to accept crafted packets, a setup was created that was able to modify the checksum field. Yang et al. present MitM attacks on IEC 60870-5-104 based on ARP cache poisoning [27].
- IEC 61850. An attacker can use several layer 2 techniques to realize a MitM network attack [40]. An example is ARP cache poisoning, which was already described before. After a successful ARP poisoning, any traffic meant for the victim's IP address is sent to the attacker instead. There are several types of attacks that the attacker can produce based on the MitM attack, namely eavesdropping, alteration, injection, and DoS attacks, which are further described later in this listing.

Measures, defined by IEC 62351: IEC 62351-5 provides measures to ensure authentication and encryption, i.e. HMAC with a pre-shared key and different encryption recommendations. These recommendations can generally not be rated as strong enough [62], but still provide a sufficient level of protection against adversaries with low threat levels. However, the protection is not high enough to withstand high threat level adversaries.

In Table XII, the results for the Man-in-the-Middle attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, TASE.2, DNP3, DNPSec, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	—

TABLE XII
Vulnerability analysis results for Man-in-the-Middle attack

3) Availability Violation Attacks:

DoS/DDoS. DoS attacks have the purpose of causing damage by drastically limiting, even denying, access to specific resources, thus making them unusable to intended users [67]. These attacks usually cause detrimental effects on the availability of sensitive infrastructure. The most common scenario for CSCPs is as follows: A number of active processes running on the attacker's machine or compromised system devices flood the communication channel with traffic targeting one or several end nodes. As a result, the target node is slowed down and cannot guarantee further operation. Also, a loss of packets sent by other nodes is a common side effect of such an attack. The scope of damage depends mainly on the attacker's resources. In case of a DDoS attack—meaning the attacker(s) use a large number of traffic generators—the whole ICS cannot satisfy real-time constrains anymore. With a wide range of dedicated DoS software available, attackers can easily produce fake Modbus or IEC 60870 packets not serving a valid purpose and flood the network links with them.

Real case scenarios:

- Modbus. Modbus is lacking broadcast suppression, which leads to the possibility to send messages to all connected devices of a control network. This in turn offers an attacker an effective mean to create a DoS condition by flooding messages received by all serially connected devices [66].
- TASE.2. The availability of TASE.2 cannot be guaranteed in modern wide area networks, since the protocol completely relies on lower level communication protocols. The way the TASE.2 protocol stack is organized directly influences its security. Furthermore, interoperability problems may arise due to the different, vendors-specific implementations, which may influence the stable operation. In [68], potential attacks impacting availability based on traffic pattern analysis are discussed. The monitoring of traffic rates can pinpoint moments when systems are facing critical situations. The destruction of a communication channel at this point of time will therefore have a major detrimental impact. This attack is possible even if the TASE.2 traffic is encrypted.
- DNP3. Based on [33], DoS attacks were created by modifying the length field of a DNP3 payload, which also necessitated the recalculation of the Cyclic Redundancy Check (CRC) field, sent from slave IECs to the master device. As a side effect of this attack, the master device rejects the corresponding frame and consequently the required physical mechanism fails.
- IEC 60870-5-101, IEC 60870-5-104. SYN flooding is a generic example of DoS attack on CSCPs with TCP/IP profiles, such as IEC 60870-104 or Modbus. It uses resources of the TCP stack to overflow a server by sending an unbounded number of SYN packets and ignoring the SYN ACKs returned by the server. As a result, a server exceeds its resources waiting for the anticipated ACK that is expected to arrive from a legitimate client. Using a sufficient number of SYN packets forces the target server to refuse any further legitimate connections since the number of concurrently opened TCP connections is limited. This event is considered as DoS and leads to availability violation. IP fragmentation attacks are another common form of DoS attack on CSCPs based on TCP/IP. In this scenario, an attacker overbears the communication channels by abusing the datagram fragmentation mechanisms.
- IEC 61850. There are several types of DoS attacks that can be launched against an IEC 61850 network. A trivial DoS attack that exploits common services on IEDs is shown in [59]. As an example, it is assumed there are two services running on an IED (The first service is FTP on port 21, the second is Telnet on port 23). A DoS attack is then executed by opening multiple sessions on one of the services and keeping them idle. SYN flooding and buffer overflow attacks are two other types of DoS attacks that have been simulated and tested on IEC 61850 substation networks in [69]. SYN flood attacks are possible because some IEDs run services such as FTP, HTTP and Telnet for management purposes [69]. Buffer overflow attacks are done by overrunning buffer boundaries, leading to the memory space being overwritten while writing data to buffers. This attack is executed by transmitting malicious code into IEDs, which is possible due to both the vulnerability of IEDs and the unavailability of security measures for IEDs to detect malicious code [69]. Another DoS attack can be realized by sending a large number of GOOSE or SV messages to an IED so that it becomes overwhelmed and no longer able to respond to legitimate requests [39]. Moreover, a DoS can be realized by performing a GOOSE poisoning attack as proposed in [43]. The goal of the attack is to get the subscriber to accept GOOSE messages with a higher sequence number than the ones sent by the publisher. As a result, all GOOSE messages from the publisher will be considered outdated by the subscribers and the subscribers will only accept and process the GOOSE messages from the attacker. There are three variants of GOOSE poisoning attacks proposed in [43]. The three variants are high status number attack, high rate flooding attack, and semantic attack.

Measures, defined by IEC 62351: In [70], it is mentioned that IEC 62351 does not sufficiently cover DoS/DDoS attacks and they should be guarded against through implementation-specific measures.

In Table XIII, the results for the DoS/DDoS attack analysis are summarized.

Vulnerable protocols	
Pre-IEC 62351:	Modbus, Modbus-F2009, Modbus-S2015, Modbus-A2018, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850
Post-IEC 62351:	Modbus, Modbus-F2009, Modbus-S2015, Modbus-A2018, TASE.2, DNP3, DNPSec, DNP3 SA, IEC 60870-5-101, IEC 60870-5-104, IEC 61850

TABLE XIII
Vulnerability analysis results for DoS/DDoS attack

D. Security Recommendations

In the following, first, several general security recommendations are presented; second, enhancements to the IEC 62351 standard going beyond its current state are covered; third, security improvements to CSCPs are discussed.

1) General Protection Measures: As shown in Section V-C, protocol specific measures, defined by the IEC 62351 security standard, are not sufficient against existing threats. Detailed assessments are presented in [62] and [65]. Some attacks are not covered by the standard or protection measures are not effective by design. As a result, IEC 62351 is not a panacea for resolving all security challenges at hand. This section provides an overview of general network

security means to mitigate the impact from malicious activities.

Reliable network security remains the main requirement and allows to prevent unwanted access and exploration of the network, including the detection of network nodes. Since the idea of security by obscurity is not a workable solution, a proper design and implementation to secure the network perimeter is essential. A secure network perimeter includes grained firewalling, effective IDS or Intrusion Prevention System (IPS), depending on the network segment. Authentication, sophisticated access control and monitoring should be introduced for all network segments. Apart from the enforced network perimeter, redundant network services should be installed to ensure reliability.

Security measures should be applied not only to CSCPs and control network devices, but also to the switching and routing points. For example, one of the possible techniques to mitigate attacks on switching devices, such as CAM table overflow attacks, is to activate port security. It ensures that no MAC flooding of the switching device is possible, because the MAC address count will be limited by default to one. To relax this restriction for complex industrial networks, which require more flexibility, vendor-specific methods can be applied. Furthermore, the port can be configured to shut down or block MAC addresses that exceed a specified limit. Moreover, routing and switching security mechanisms allow to prevent several types of DoS attacks and attacks on IP-networking, such as IP fragmentation.

2) IEC 62351 Improvement Recommendations: The current granularity and detail of the security specifications given in IEC 62351-3 leave room for standard-compliant systems not to uphold the required security. The key factor to remedy this security loophole is the specification of key management inside IEC 62351. Without a clearly defined key management policy, adversaries are able to undermine message confidentiality, integrity, as well as authentication. This—in turn—leads to further attacks.

Especially in the case of IEC 61850, it is expected that the standard may evolve beyond its current state to include, e.g., feeder and control center communication. Although other protocols covering communications beyond substations exist, the usage of IEC 61850 can improve these applications [10], e.g. by using the same logical nodes, or applying the same messaging techniques such as GOOSE and SV. Mohagheghi et al. state that an expanding of IEC 61850 to include control centers is technically possible, however likely to achieve questionable performance. Therefore, solutions which require additional work are to either provide a proxy server for IEC 61850 data in substations, or to map the IEC 61850 data model content to traditional CSCPs, such as DNP3 or IEC 60870-5 [10]. Moreover, the interoperability requirements imposed by IEC 61850-5 in combination with IEC 62351 allow a downgrade attack to be implemented. The underspecification in IEC 62351-3 leaves many security-relevant decisions to the system manufacturers, leading either to incompatibilities, or to choose the lowest common denominator of security as common ground. As [71] argues, there is a reasonable likelihood that the security flaws do not only exist for the combination of IEC 61850 with IEC 62351, but also in other communication protocols, such as IEC 60870 or DNP3.

Also, Fries et al. recommends to extend IEC 62351 to overcome the identified weaknesses by introducing security sessions for MMS connections in [65]. This requires changes in the IEC 62351-4 for security of MMS communication as currently only the MMS-initiated command has the appropriate ASN.1 structures to transport security information. Furthermore, to provide the required integrity protection, the current signature calculation in IEC 62351-4 needs to be revised [65].

3) CSCP Improvement Recommendations: To secure CSCPs based on TCP/IP, an often employed fix is to use TLS. While these protocols offer reliable security, they themselves are not without limitations, especially in the context of ICSs. Foremost, TLS suffers from the fundamental constrain that they can only be used in combination with reliable transport protocols (i.e., TCP), restricting their usage in ICS environments. In addition, they have performance overheads associated with them, cannot provide non-repudiation, and can only ensure channel security, in contrast to object security. Moreover, TLS does not provide protection against traffic analysis or DoS attacks based on connection resets, since the connection handling is done by a lower level protocol (i.e., TCP) [72]. Therefore, although the usage of TLS offers an easy to implement security benefit, future improvements need to focus on finding integral security extensions for CSCPs themselves, as partly demonstrated in, e.g., DNP3 SA.

VI. Conclusion

Current control systems are based on ICT devices and their ability to communicate and exchange information with each other by means of a well-defined network. An example of this can be found in the evolution of the traditional power grid to today's smart grid where energy planning is enabled through data monitoring and controlling of the distributed power generating resources.

Early on, these networks were typically realized using only proprietary solutions. However, the need for remote control and the advances in area of computer networks (e.g. Internet) led to the blending of traditional control networks with the modern Internet. In parallel, several network protocols were developed, each targeting specific requirements in order to achieve communication in control systems. On the one hand, the merge of control networks and the Internet contributed to managing control systems without being on site (which was highly required). On the other hand, however, control systems inherited the security vulnerabilities that only threatened the modern Internet before.

In this paper, we carried out a qualitative security analysis by studying the most broadly employed CSCPs: Modbus (and three of its variants), OPC UA, TASE.2, DNP3 (and two of its variants), IEC 60870-5-101, IEC 60870-5-104, and IEC 61850. To this end, we proposed a uniform methodology to perform the security analysis. First, we composed an adversary model and defined different attack scenarios; consequently, the vulnerable protocols were identified before and after applying the IEC 62351 security standard. In cases where IEC 62351 does not propose any (or no suitable) security solutions, recommendations were presented to protect against these vulnerabilities. It is worthwhile mentioning that in this paper, we focused on protocol vulnerabilities exploitable through network-based attacks.

However, there are also known hardware/software vulnerabilities in networking elements that continue to be exploitable. Here, remote attackers can discover the currently running version of the software and use known exploits to cause DoS or obtain access over a targeted node. Also, threats can emanate not only from the physical medium but from the control system devices themselves and the way networking functions are realized. Thus, powerful adversaries, such as funded organizations and hostile nations, have an ability to convince vendors to implement backdoors into hardware and software such as communication devices, administration and monitoring systems. These are hidden pieces of hardware/software usually used by vendors to provide remote support such as troubleshooting, software updates and patching. These backdoors can, however, also be used to obtain access to sensitive information as well as to cause DoS to critical system elements.

VII. Future Research Perspectives

After the careful analysis of the most prominent legacy and current CSCPs, several research orientations requiring further work are identified in this Section, which are organized into different topics.

A. IEC 62351: Challenges and Performance

The security standard IEC 62351 is currently partly unfinished as well as underspecified, as illustrated in Section V-D2. While the issue of underspecification is solvable by updating the standard using more fine-granular specifications for security solutions, challenges especially do exist in detecting currently unknown loopholes and interaction effects between different CSCPs in combination with IEC 62351. Finding and effectively solving such shortcomings will be an important future challenge worth investigating.

Apart from the future work required in the security of IEC 62351, it is also important to extensively test its impact on the achieved performance of CSCPs, as applicability is only achievable if Quality of Service (QoS) requirements can be upheld. To be able to guarantee that, extensive experimentation in numerous scenarios—and possibly subsequent optimizations—are required.

B. Standardization and Validation

Standardization is still a major topic in critical infrastructures overall, and in control systems and protocols in particular. This is mainly because of two reasons: First, standardization is directly connected to interoperability, enabling vendor-agnostic communication between devices. Second, standardization offers reliable security and a more focused, in-depth security development and analysis. Therefore, the identification of major future standards, as well as their rigorous security analyses will be important upcoming challenges.

While standardization defines the required specifications, it was shown in [73] that, for the use case of IEC 60870-5-104 protocol, not every device implementing the corresponding protocol, actually follows the specification. Hence, new rigorous methodologies and tools need to be devised for the sake of validating whether the devices implement correctly the corresponding standards' specifications.

C. Legacy Protocols: IoT and Further Improvements

The development of the security measures for CSCPs makes them more applicable for the further areas, such as IoT. For example, light-weight, open and compatible Modbus can serve as a control mean in non-industrial IoT systems.

Furthermore, although there are several security improvements available to legacy protocols, such as Modbus and DNP3, which were discussed in this survey, there is still no solution that fulfills all security requirements:

- Cremers et al. discuss that DNP3 SA still has several security issues. These include, among others, an improvable authentication properties for the Update Key Change messages, an unclear specification regarding the usage of Challenge SeQuence numbers (CSQs), and a missing deprecation of HMAC-SHA-1. A full list is given in [35]. These issues need to be addressed in future versions of the DNP3 SA protocol.
- In the case of DNPSec, it is highly recommended to update the protocol to employ recent and secure cryptographic algorithms, as 3-DES and SHA-1 are broken, as previously stated in Section III-A.

D. Performance Improvements for CSCPs

Maintaining an acceptable performance for the security means is another issue to be solved during design and development of secure CSCPs. This paper does not focus on the precise analysis of the limited applicability of security mechanisms to the industrial networks with special requirements and constrains. As an example, the performance of DNPSec makes it unsuited for the usage in resource constrained environments [21]. Further research in this direction may reveal the way effective and secure protocols can be designed.

Furthermore, the usage of signatures is an important security feature in CSCPs, allowing effective authentication and integrity protection. While RSA is currently often

used, finding/optimizing a signature scheme to improve performance to a real-time level is still an open issue.

In addition to the optimization of signature schemes, the key distribution within ICSs is a challenge that requires further research [74]. Most protocols using symmetric encryption schemes assume a secure channel to pre-establish shared keys and argue that a trusted certificate authority to establish a Public Key Infrastructure (PKI) cannot be safely assumed. While algorithms employing asymmetric schemes offer additional security benefits, they suffer from major performance drawbacks.

Apart from the aforementioned future research topics, only the first step of a security process (as defined in IEC 62351), namely the security assessment, is performed in this article. As future work, it would be interesting to analyze the impact of the assessment results on the rest of the process such as security policy, deployment, etc. Furthermore, security standards and requirements are likely to change and evolve in the future, so an ongoing contribution in this respect will be to update the presented security assessment based on the refined standards and requirements.

Acknowledgment

The research leading to these results was supported by the Bavarian Ministry of Economic Affairs and Media, Energy and Technology as part of the East-Bavarian Centre of Internet Competence project and Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) research grant #ME 1703/12-1, entitled Black-Start.

References

[1] M. Naedele, "Addressing IT Security for Critical Control Systems," in 40th Annual Hawaii International Conference on System Sciences, 1 2007, pp. 115–124.

[2] B. Miller and D. Rowe, "A Survey SCADA of and Critical Infrastructure Incidents," in Proceedings of the 1st Annual Conference on Research in Information Technology, ser. RIIT '12. New York, NY, USA: ACM, 2012, pp. 51–56. [Online]. Available: http://doi.acm.org/10.1145/2380790.2380805

[3] W. Yusheng, F. Kefeng, L. Yingxu, L. Zenghui, Z. Ruikang, Y. Xiangzhen, and L. Lin, "Intrusion Detection of Industrial Control System Based on Modbus TCP Protocol," in IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), 3 2017, pp. 156–162.

[4] The Register. (2008) Polish Teen Derails Tram After Hacking Train Network. Online: accessed 18.04.2017. [Online]. Available: http://www.theregister.co.uk/2008/01/11/tram_hack/

[5] J. A. Crain and S. Bratus, "Bolt-On Security Extensions for Industrial Control System Protocols: A Case Study of DNP3 SAv5," IEEE Security and Privacy Magazine, vol. 13, no. 3, pp. 74–79, 5 2015.

[6] T. H. Morris and W. Gao, "Industrial Control System Cyber Attacks," in Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research, ser. ICS-CSR 2013. UK: BCS, 2013, pp. 22–29. [Online]. Available: http://dl.acm.org/citation.cfm?id=2735338.2735341

[7] I. N. Fovino, A. Coletta, A. Carcano, and M. Masera, "Critical State-Based Filtering System for Securing SCADA Network Protocols," IEEE Transactions on Industrial Electronics, vol. 59, no. 10, pp. 3943–3950, 10 2012.

[8] B. Babu, T. Ijyas, P. Muneer, and J. Varghese, "Security Issues in SCADA based Industrial Control Systems," in 2nd International Conference on Anti-Cyber Crimes, 3 2017, pp. 47–51.

[9] D. Dzung, M. Naedele, T. P. V. Hoff, and M. Crevatin, "Security for Industrial Communication Systems," Proceedings of the IEEE, vol. 93, no. 6, pp. 1152–1177, 6 2005.

[10] S. Mohagheghi, J. Stoupis, and Z. Wang, "Communication Protocols and Networks for Power Systems – Current Status and Future Trends," in 2009 IEEE/PES Power Systems Conference and Exposition, 3 2009, pp. 1–9.

[11] R. E. Johnson, "Survey of SCADA Security Challenges and Potential Attack Vectors," in International Conference for Internet Technology and Secured Transactions, 11 2010, pp. 1–5.

[12] F. Alsiherov and T. Kim, "Research Trend on Secure SCADA Network Technology and Methods," WSEAS Transactions on Systems and Control, vol. 5, no. 8, pp. 635–645, Aug. 2010.

[13] M. Robinson, "The SCADA Threat Landscape," in Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research. BCS, 2013, pp. 30–41.

[14] T. Bartman and K. Carson, "Securing Communications for SCADA and Critical Industrial Systems," in 69th Annual Conference for Protective Relay Engineers, 4 2016, pp. 1–10.

[15] J. T. Michalski, A. Lanzone, J. Trent, S. Smith, and J. Michalski, "Secure ICCP Integration Considerations and Recommendations," Sandia National Laboratories, Tech. Rep., 2007.

[16] M. H. Schwarz and J. Börcsök, "A Survey on OPC and OPC-UA: About the Standard, Developments and Investigations," in XXIV International Conference on Information, Communication and Automation Technologies, 10 2013, pp. 1–6.

[17] M. Krotofil and D. Gollmann, "Industrial Control Systems Security: What is happening?" in 11th IEEE International Conference on Industrial Informatics, 7 2013, pp. 670–675.

[18] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of Cyber Security for Industrial Control Systems," in International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, 8 2015, pp. 1–8.

[19] M. Mallouhi, Y. Al-Nashif, D. Cox, T. Chadaga, and S. Hariri, "A Testbed for Analyzing Security of SCADA Control Systems (TASSCS)," in Innovative Smart Grid Technologies 2011, 1 2011, pp. 1–7.

[20] S. East, J. Butts, M. Papa, and S. Shenoi, A Taxonomy of Attacks on the DNP3 Protocol. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 67–81. [Online]. Available: https://doi.org/10.1007/978-3-642-04798-5_5

[21] D. Lee, H. Kim, K. Kim, and P. D. Yoo, "Simulated Attack on DNP3 Protocol in SCADA System," in The 31th Symposium on Cryptography and Information Security, 2014.

[22] D. S. Pidikiti, R. Kalluri, R. K. S. Kumar, and B. S. Bindhumadhava, "SCADA Communication Protocols: Vulnerabilities, Attacks and Possible Mitigations," CSI Transactions on ICT, vol. 1, no. 2, pp. 135–141, 6 2013. [Online]. Available: https://doi.org/10.1007/s40012-013-0013-5

[23] P. Matoušek, "Description and Analysis of IEC 104 Protocol, Technical Report no. FIT-TR-2017-12," Faculty of Information Technology, Brno University of Technology, Tech. Rep., 2017.

[24] J. L. Rrushi, SCADA Protocol Vulnerabilities. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 150–176. [Online]. Available: https://doi.org/10.1007/978-3-642-28920-0_8

[25] J. Jarmakiewicz, K. Maślanka, and K. Parobczak, "Development of Cyber Security Testbed for Critical Infrastructure," in International Conference on Military Communications and Information Systems, 5 2015, pp. 1–10.

[26] P. Maynard, K. McLaughlin, and B. Haberler, "Towards Understanding Man-in-the-Middle Attacks on IEC 60870-5-104 SCADA Networks," in Proceedings of the 2nd International Symposium on ICS & SCADA Cyber Security Research. BCS, 2014, pp. 30–42.

[27] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Q. Yao, B. Pranggono, and H. F. Wang, "Man-in-the-Middle Attack Testbed Investigating Cyber-Security Vulnerabilities in Smart Grid SCADA Systems," in International Conference on Sustainable Power Generation and Supply. IET, 2012, pp. 1–8.

[28] I. N. Fovino, A. Carcano, M. Masera, and A. Trombetta, "Design and Implementation of a Secure Modbus Protocol," in Critical Infrastructure Protection III, C. Palmer and S. Shenoi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 83–96.

[29] A. Shahzad, M. Lee, Y.-K. Lee, S. Kim, N. Xiong, J.-Y. Choi, and Y. Cho, "Real Time MODBUS Transmissions and Cryptography

Security Designs and Enhancements of Protocol Sensitive Information," Symmetry, vol. 7, no. 3, pp. 1176–1210, 2015. [Online]. Available: http://www.mdpi.com/2073-8994/7/3/1176

[30] E. Ádámkó, G. Jakabóczki, and P. T. Szemes, "Proposal of a Secure Modbus RTU Communication with Adi Shamir's Secret Sharing Method," International Journal of Electronics and Telecommunications, vol. 64, no. 2, pp. 107–114, 2018.

[31] R. Huang, F. Liu, and P. Dongbo, "Research on OPC UA Security," in 5th IEEE Conference on Industrial Electronics and Applications, 6 2010, pp. 1439–1444.

[32] M. Majdalawieh, F. Parisi-Presicce, and D. Wijesekera, "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework," in Advances in Computer, Information, and Systems Sciences, and Engineering, K. Elleithy, T. Sobh, A. Mahmood, M. Iskander, and M. Karim, Eds. Springer Netherlands, 2006, pp. 227–234.

[33] N. Rodofile, K. Radke, and E. Foo, "Real-Time and Interactive Attacks on DNP3 Critical Infrastructure Using Scapy," in 13th Australasian Information Security Conference, 2015.

[34] C. Singh, A. Nivangune, and M. Patwardhan, "Function Code Based Vulnerability Analysis of DNP3," in IEEE International Conference on Advanced Networks and Telecommunications Systems, 2016.

[35] C. Cremers, M. Dehnel-Wild, and K. Milner, "Secure Authentication in the Grid: A Formal Analysis of DNP3: SAv5," in European Symposium on Research in Computer Security, 2017.

[36] G. Gilchrist, "Secure Authentication for DNP3," in 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 7 2008, pp. 1–3.

[37] R. Amoah, "Formal Security Analysis of the DNP3-Secure Authentication Protocol," 2010.

[38] R. Amoah, S. Camtepe, and E. Foo, "Securing DNP3 Broadcast Communications in SCADA Systems," IEEE Transactions on Industrial Informatics, vol. 12, no. 4, pp. 1474–1485, 8 2016.

[39] J. Hong, C. C. Liu, and M. Govindarasu, "Detection of Cyber Intrusions using Network-based Multicast Messages for Substation Automation," in Innovative Smart Grid Technologies 2014, 2 2014, pp. 1–5.

[40] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A Review of Security Attacks on IEC61850 Substation Automation System Network," in Proceedings of the 6th International Conference on Information Technology and Multimedia, 11 2014, pp. 5–10.

[41] B. Kang, P. Maynard, K. McLaughlin, S. Sezer, F. Andrén, C. Seitl, F. Kupzog, and T. Strasser, "Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations," in 2015 IEEE 20th Conference on Emerging Technologies Factory Automation (ETFA), 9 2015, pp. 1–8.

[42] I. A. Siddavatam and F. Kazi, "Security Assessment Framework for Cyber Physical Systems: A Case-study of DNP3 Protocol," in 2015 IEEE Bombay Section Symposium (IBSS), 9 2015, pp. 1–6.

[43] N. Kush, M. Branagan, E. Foo, and E. Ahmed, "Poisoned GOOSE: Exploiting the GOOSE Protocol," in Australasian Information Security Conference, U. Parampali and I. Welch, Eds. Auckland University of Technology, Auckland: Australian Computer Society, Inc., 1 2014, pp. 17–22. [Online]. Available: https://eprints.qut.edu.au/66227/

[44] J. Hoyos, M. Dehus, and T. X. Brown, "Exploiting the GOOSE Protocol: A Practical Attack on Cyber-Infrastructure," in IEEE Globecom Workshops, 12 2012, pp. 1508–1513.

[45] A. Shahzad, "The SCADA Review: System Components, Architecture, Protocols and Future Security Trends," American Journal of Applied Sciences, vol. 11, pp. 1418–1425, 08 2014.

[46] D. Kang and R. J. Robles, "Compartmentalization of Protocols in SCADA Communication," International Journal of Advanced Science and Technology, 2009.

[47] European Union Agency for Network and Information Security, "Communication Network Dependencies for ICS/SCADA Systems," European Union Agency for Network and Information Security, Tech. Rep., 2017.

[48] IEEE 1815-2012, "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," Institute of Electrical and Electronics Engineers, Standard IEEE 1815-2012, 2012.

[49] T. Radu and S. Mircea, "Evaluation of DES, 3 DES and AES on Windows and Unix Platforms," in International Joint Conference on Computational Cybernetics and Technical Informatics, 5 2010, pp. 119–123.

[50] M. Stevens, "New Collision Attacks on SHA-1 Based on Optimal Joint Local-Collision Analysis," in Advances in Cryptology – EUROCRYPT 2013, T. Johansson and P. Q. Nguyen, Eds. Springer Berlin Heidelberg, 2013, pp. 245–261.

[51] M. Abrams and J. Weiss, "Malicious Control System Cyber Security Attack Case Study Maroochy Water Services," The MITRE Corporation, Applied Control Solutions, Tech. Rep., 2008.

[52] A. Saxena, O. Pal, and Z. Saquib, Public Key Cryptography Based Approach for Securing SCADA Communications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 56–62. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-19542-6_10

[53] L. Pièrre-Cambacédès and P. Sitbon, "Cryptographic Key Management for SCADA Systems-Issues and Perspectives," in International Conference on Information Security and Assurance (isa 2008), 4 2008, pp. 156–161.

[54] C. W. Ten, G. Manimaran, and C. C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, vol. 40, no. 4, pp. 853–865, 7 2010.

[55] A. A. Cardenas, T. Roosta, and S. Sastry, "Rethinking Security Properties, Threat Models, and the Design Space in Sensor Networks: A Case Study in SCADA Systems," Ad Hoc Networks, vol. 7, no. 8, pp. 1434–1447, 11 2009. [Online]. Available: http://dx.doi.org/10.1016/j.adhoc.2009.04.012

[56] IEC SC 65A, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," International Electrotechnical Commission, Standard IEC 61508, 2010.

[57] J. Cai, Y. Zheng, and Z. Zhou, "Review of Cyber-Security Challenges and Measures in Smart Substation," in International Conference on Smart Grid and Clean Energy Technologies, 10 2016, pp. 65–69.

[58] T. J. O'Connor, "Detecting and Responding to Data Link Layer Attacks," SANS Institute, Tech. Rep., 2010.

[59] U. K. Premaratne, J. Samarabandu, T. Sidhu, R. Beresh, and J. C. Tan, "An Intrusion Detection System for IEC61850 Automated Substations," IEEE Transactions on Power Delivery, vol. 25, no. 4, pp. 2376–2383, 10 2010.

[60] ——, "Security Analysis and Auditing of IEC61850-Based Automated Substations," IEEE Transactions on Power Delivery, vol. 25, no. 4, pp. 2346–2355, 10 2010.

[61] A. Nagarajan and C. D. Jensen, "A Generic Role Based Access Control Model for Wind Power Systems," Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 1, no. 4, pp. 35–49, 2010.

[62] R. Schlegel, S. Obermeier, and J. Schneider, "Assessing the Security of IEC 62351," in Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research. British Computer Society, 2015, pp. 11–19.

[63] F. Hohlbaum, M. Braendle, and F. Alvarez, "Cyber Security Practical Considerations for Implementing IEC 62351," 2010.

[64] M. Strobel, N. Wiedermann, and C. Eckert, "Novel Weaknesses in IEC 62351 protected Smart Grid Control Systems," in IEEE International Conference on Smart Grid Communications (SmartGridComm), 11 2016, pp. 266–270.

[65] S. Fries, H. J. Hof, and M. Seewald, "Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments," in Fifth International Conference on Internet and Web Applications and Services. IEEE, 2010, pp. 135–142.

[66] E. D. Knapp and J. T. Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Elsevier Science, 2014.

[67] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring Internet Denial-of-Service Activity," ACM Transactions on Computer Systems, vol. 24, no. 2, pp. 115–139, 2006.

[68] G. Dán, H. Sandberg, M. Ekstedt, and G. Björkman, "Challenges in Power System Information Security," IEEE Security & Privacy, vol. 10, no. 4, pp. 62–70, 2012.

[69] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion Detection of NSM Based DoS Attacks Using Data Mining in Smart Grid," Energies, vol. 5,

no. 10, pp. 4091–4109, 2012. [Online]. Available: http://www.mdpi.com/1996-1073/5/10/4091

[70] F. Cleveland, "IEC 62351 Security Standards for the Power System Information Infrastructure," IEC TC57 WG15, Tech. Rep., 2012.

[71] J. G. Wright and S. D. Wolthusen, "Limitations of IEC 62351-3's Public Key Management," in IEEE 24th International Conference on Network Protocols (ICNP), 11 2016, pp. 1–6.

[72] J. H. Graham and S. C. Patel, "Security Considerations in SCADA Communication Protocols," Intelligent Systems Research Laboratory, Department of Computer Engineering and Computer Science, University of Louisville, Tech. Rep., 2004.

[73] M. Kerkers, J. Chromik, A. Remke, and B. Haverkort, "A Tool for Gererating Automata of IEC60870-5-104 Implementations," in 19th International GI/ITG Conference on Measurement, Modelling and Evaluation of Computing Systems, 2018.

[74] C. L. Beaver, D. R. Gallup, W. D. Neumann, and M. D. Torgerson, "Key management for scada (sand2001-3252)," Sandia National Laboratories, Tech. Rep., 2002.

Anna Volkova owns a diploma in information systems security from Peter the Great St. Petersburg Polytechnic University and a Master of computer science focusing on information security from University of Passau. She contributed in more than 5 network security, Software-Defined Networking (SDN) security and smart grid security research projects the last three years.

Michael Niedermeier is working as a research associate at the Chair of Computer Networks and Computer Communications and at the Institute of IT Security and Security Law (ISL) at the University of Passau since 2009. His main research areas focus on novel dependability enhancements, security and functional safety in distributed systems such as the smart grid. He scientifically contributed to EU EFRE SECBIT, EU FP7 SEC-2013.2.5-4 HyRiM, and the East-Bavarian Centre of Internet Competence supported by Bavarian Ministry of Economic Affairs and Media, Energy and Technology. Moreover, he was an active member of both the EURO-NF and EINS networks of excellence.

Robert Basmadjian holds a Ph.D. from University of Toulouse on data replication. After completing his doctorate, in 2009 he joined University of Passau as a postdoctoral fellow, where his main research interests are large-scale energy management systems (Smart Grid), and performance modeling of computing systems (queuing theory). He has more than 25 scientific publications in the respective fields. He was a scientific and technical contributor to EU FP7 FIT4Green and ALL4Green projects related to Demand Response in data centers as well as to H2020 Electrific project. Moreover, he was an active member of WG 2 and 3 of COST ACTION 804, EURO-NF and EINS.

Hermann de Meer has been appointed as Full Professor of computer science at the University of Passau, Germany, since 2003. He is heading the Computer Networking Lab and co-heading the Institute of IT Security and Security Law (ISL). His interests of research include network virtualization, digitization of energy systems, IT security of critical infrastructures, and distributed control and optimization. He received his PhD from University Erlangen-Nuremberg, Germany, in 1992, and his habilitation from Hamburg University, Germany. He is member of the ACM and of the GI (Gesellschaft für Informatik) and fellow of the DFG (Deutsche Forschungsgemeinschaft).