Holistic attack methods against power systems using the IEC 60870-5-104 protocol

János Csatár, Péter György, and Tamás Holczer

***Abstract*—IEC 60870-5-104 is a widely used protocol for telecontrol in European power systems. However, security was not a design goal when it was originally published: This protocol lacks built-in security features such as encryption, integrity protection, or authentication. In this paper, we describe novel types of attacks against the protocol in a holistic way. Therefore, we also enumerate the possible entry points of the threat actors and demonstrate a new technique, where the malicious actor can precisely target the attack. These methods are demonstrated both on simulated environment and actual devices and compared with already published methods.**

***Index Terms*—IEC 60870-5-104, Attack, Security, Power system**

I. INTRODUCTION

As power systems became more interconnected and increasingly complex, the operation of it started to rely more and more on automation, remote sensing and control in favor of efficiency and reliability. This escalated to a point where the usage of information and communication technologies (ICT) became an essential part of power system operation; today's large power systems are already unable to function properly without ICT. Thus, it is a cyber-physical system where the process of physical power transmission and distribution is closely intertwined with communication. Since power systems have their own special needs, some industry specific communication protocols exist. One of these is IEC 60870-5 series standard, and its companion standard IEC 60870-5-104 [1] for TCP/IP based communication (abbreviated as IEC 104 further on). It was designed to transmit timestamped counters, measurement values, status signals and control commands or set-points and is widely used in some countries for SCADA control centers handling the operation of the power system; both on transmission and distribution levels. Cyber security was not a priority at the early days of power system digitization - and so core IEC 104 standard is lacking security measures. A security extension is given for 60870-5 based protocols in IEC 62351 [2] series standard incorporating - among others - standard TCP/IP security measures. Subsequently, supplemental information on implementation is now part of the IEC 60870-5 series (60870-5-7). However, two main challenges hinder the universal use of the more secure version.

- First, it requires hardware level support.
  - Several legacy equipment and software component exist due to the long life cycle that is usual in power systems.
  - Legacy support means coexistence of insecure and secure versions of IEC 104.
- The second challenging factor is increased complexity regarding a number of factors.
  - Installation and maintenance of more secure systems means increased effort, for example: managing role based access, certificate authorities, keys, etc.
  - Monitoring and validating traffic on the network becomes less straightforward and more time/resource consuming.
  - Debugging and investigation of malfunction becomes a multi level task.
  - The communication itself becomes more resource intensive - it involves overhead and so introduces latency and heavier network load.

But even in a fully IEC 62351 compliant system, security measures can still have vulnerabilities, which exposes the *core IEC 104* communication flow. The newer, paradigm changing IEC 61850 series standard is currently still more focused on substations than control centers; even some guideline exist in the IEC 61850 series how to map objects to other lower level communication protocols for usage beyond substations, like IEC 104.

Summing the above, IEC 104 will remain in operation for the coming years. It is mainly used between remote terminal units (RTU) and supervisory control and data acquisition (SCADA) systems. Since it is based on TCP/IP, an ICT infrastructure is needed, that is generally multipurpose and handles other types of traffic (e.g. remote access, configuration, network monitoring, etc.). At the same time, the SCADA system itself can be even geographically spread out; it is usual that the backup system is located at a different site.

The last few years showed that well resourced and sophisticated, power system targeted attacks can happen, like the two Ukrainian attacks in 2015 and 2016 [3], [4]. The case with SolarWinds [5], or log4j [6] pointed out that no system or component of a system can be considered completely secure as a vulnerability may be introduced by third party components. Even the communication provider of critical services can be attacked as we have seen recently in Portugal [7]. [8] shows a comprehensive survey of the topic. Compromising

J. Csatár is with the Department of Electric Power Engineering, Budapest University of Technology and Economics (e-mail: csatar.janos@vik.bme.hu).

P. György is with Ukatemi Ltd (e-mail: peter.gyorgy@ukatemi.com).

T. Holczer is with the Department of Networked Systems and Services, Budapest University of Technology and Economics (e-mail: holczer@crysys.hu).

This work was partially performed in the frame of the FIEK 16-1-2016-0007 project, implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the FIEK 16 funding scheme.

even part of a power system's IEC 104 communication could give substantial control to an attacker. All this makes the cybersecurity investigation of IEC 104 based communication flow a current research topic.

The focus of the research was put on the creation of a comprehensive attack scenario against a system using IEC 60870-5-104. To do so we:

1) enumerated the possible attack surfaces, where the attack can begin,
2) created a new, sophisticated way of packet injection into a live connection,
3) proposed how the communication nodes could be identified with open-source intelligence (OSINT) and other data by the adversary.

Furthermore, we demonstrated the effective use of the proposed packet injection attack on both simulated and real equipment.

The remainder of the paper is structured in the following way: We give a short overview of IEC 104 for the reader's convenience in Section II and discuss the related work afterwards. In Section IV we give an overview of possible entry points of an attack in case of power systems. The known and proposed new attacks against IEC 104 are described in details in Section V. The problem and a promising solution of precisely targeting such an attack is analysed in Section VI. Finally we conclude our paper in Section VII.

II. Overview of the IEC 60870-5-104 protocol

The IEC 60870-5-104 (IEC 104) is part of the IEC-60870 protocol family and is widely used for power systems in Europe (DNP3 is more widely used for the same purpose in North America). IEC 104 defines network access using TCP for IEC 60870-5-101.

The IEC 104 messages (Application Protocol Data Unit, APDU) are divided into two parts:

- APCI (Application Protocol Control Information) - Message header
- ASDU (Application Service Data Unit) - Message body

An APDU can contain a single APCI or an APCI and an ASDU. Generally, the length of the APCI is 6 bytes. In the remainder of this section, we will introduce the basics (from our point of view) of IEC 104 APDUs. These basics are necessary to understand why and how does some protocol-specific attacks operate. An in-depth analysis of IEC 104 was published in [9], which describes the protocol in more detail from every aspect.

A. Application Protocol Control Information

Each APCI (Application Protocol Control Information) starts with a start byte with value 0x68, followed by the 8-bit length of APDU (Application Protocol Data Unit) and four 8-bit control fields(CF).

The frame format is determined by the two last bits of the first control field. The standard defines three frame formats, I-format, U-format, and S-format. The S and I format stores the sequence numbers about the messages sent. If this counter is invalid, then the connection is terminated. Figure 1 shows the structure of different frames.

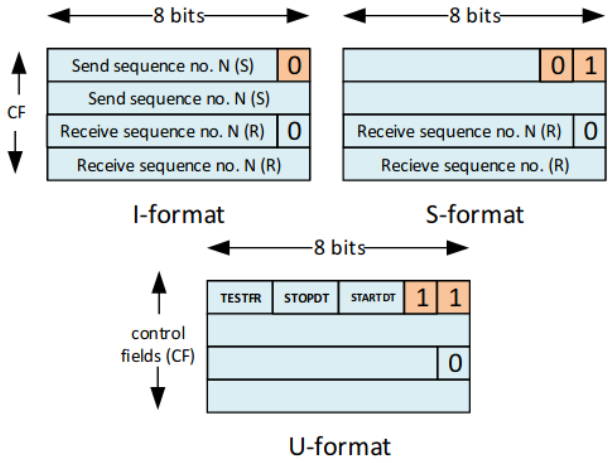

Fig. 1. The frame formats of APCI [9]

B. Application Service Data Unit

The ASDU contains two main sections:

- Data Unit Identifier
- Payload

The ASDU starts with a type of identification, which specifies the command. It also stores the originator's address, the addressee's address (ASDU address), the information object address, and the information element (value).

The ASDU and the information object address (IOA) are used as selectors. The ASDU address is a two-byte long address field that specifies the recipient device. The IOA is a three-byte long address, and it determines which objects are affected by the command.

The operators need to know both the ASDU address and the IOA to send messages. The ASDU addresses and the IOAs of the devices are not publicly accessible. The values are assigned by the architects of the power grid and may differ for each power grid.

As Figure 2 shows, the ASDU address and the IOA are used to identify which element is affected by the message. Even though there are multiple devices with the same IOA, only one gets the message.

There are 127 different messages used in IEC 104, both monitoring and control are covered. When a server receives a command from the client, it responds based on the requests (acknowledgment for control commands, values of sensors for monitor commands). Figure 3 shows the structure of the ASDU.

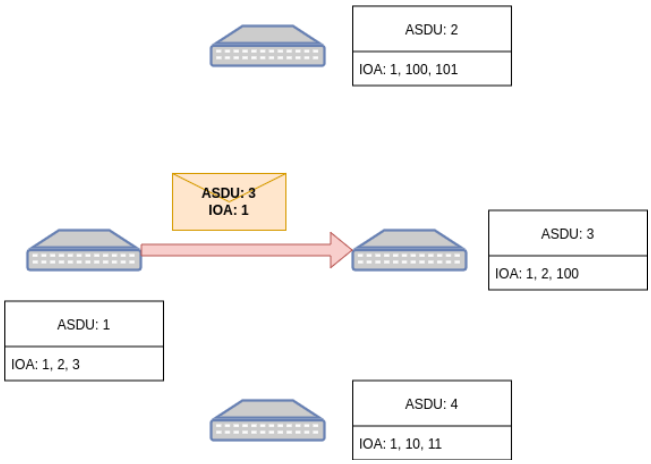

Fig. 2. IEC 60870-5-104 message identifiers.

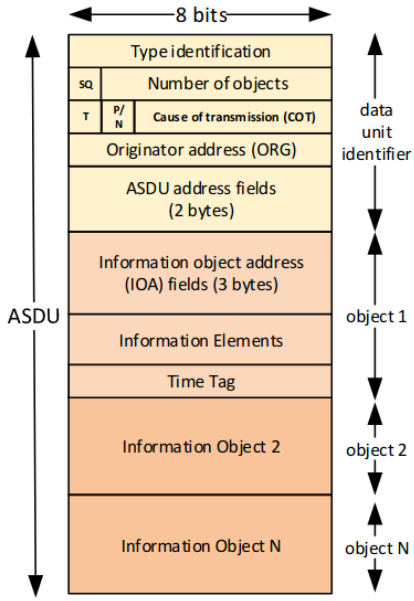

Fig. 3. The structure of ASDU [9].

It can be seen from this brief introduction, that this protocol does not provide any cryptographic protection for the messages being sent. This property enables different kinds of attacks described in Section V.

III. Related work

The IEC-60870 series is a widely researched and used protocol family, especially the IEC-60870-5-104 (IEC 104) protocol. Research usually focuses on how the protocol can be used efficiently, but the security aspects of the protocol are also studied. Most of the security-oriented research focuses on anomaly and attack detection in IEC 104 networks [10], [11], [12], [13], [14].

These detection mechanisms usually rely on deep packet inspection or data and time correlation. [14] compares different learning algorithms for anomaly detection and concludes that no unsupervised algorithm works perfectly alone. [13] focuses on detection of denial of service attacks based on machine learning. The paper shows by experiments that decision trees are suitable for DoS detection. In [10] shows that in some cases the Rule Learner classifier algorithm works well. [11] shows that timing anomalies in IEC 104 traffic can be detected efficiently if the anomaly is persistent or at least one hour long. Shorter timing anomalies are hard to detect. [12] proposes a traditional rule based algorithm that can efficiently detect known attacks. Recent reviews [15], [16] compares the different machine learning methods for anomaly detection in SCADA systems. Some of these methods can be used to detect attacks against the IEC 104 protocol. Apart from the detection, there is also a paper about hardening of the protocol [17].

Not just the defense side of the topic was researched, but multiple papers were published about attack vectors, and flaws in the protocol [18], [19], [20] and against systems that use IEC 104 [21], [22], [23]. Also, some exciting attack scenarios against power grid control infrastructure contain steps against the IEC 104 protocol [24]. During our research, we used the attacks described in these papers as inspiration. Furthermore, we tried to make them more sophisticated, and we even came up with new ideas that can be used in an attack scenario. In the following, we introduce the most relevant papers and position our current work.

Multiple flaws and attack vectors are described in [18] including unauthorized access, denial of service, and man-in-the-middle (MitM) attacks. As mentioned in the analysis of the IEC 104 protocol, it does not provide authentication. Therefore somebody with communication opportunities with the server can also use the services provided by IEC 104 and act as a legitimate IEC 104 client. The lack of authentication can result in devastating attacks because even with little technical knowledge, an attacker could cause severe harm to the network.

The authors of [18] tried two different attacks to cause a denial of service on the IEC 104 server. They tried flooding the server with commands which can be used to confuse the operator. The other attack was a TCP SYN DoS attack. The idea is the same as in a typical SYN DoS attack, they sent SYN packets to the IEC 104 server, and it responded with SYN-ACK, which the initiator of the communication did not handle. Using this attack, they could significantly increase the hardware and network usage of the device. Because the devices used in an IEC 104 network usually have minimal hardware resources, this attack can be efficiently used to cause a denial of service.

The authors also simulated a MitM attack, where they achieved the MitM position using ARP poisoning. They used ettercap[1] for carrying out ARP poisoning. Furthermore, ettercap filters were used to isolate and drop every IEC 104 packet, therefore terminating the communication of the legitimate parties. The authors of [18] used the OpenMUC implementation of the protocol to demonstrate these attacks.

[1] https://www.ettercap-project.org/

A similar ARP poisoning based MitM attack is analysed in [25].

A good overview of possible attacks can be found in [26] against the target protocol. The attacks are grouped into reconnaissance, attacks causing operational failures and attacks causing denial of service states. The effect of the different attacks is validated in a Hardware-In-the-Loop (HIL) Digital Station environment.

In the previous attack scenario, the authors assumed that the attacker already penetrated the SCADA system. [19] describes how this penetration can be done and used to inject IEC 104 packets into the system. The paper describes the necessary steps for a successful attack, like penetration, discovery, and injection.

From our point of view, the packet injection is an exciting step, but in that paper, they successfully injected commands to an IEC 104 server in a new session and not in an established session. To achieve it, they used a custom made tool to reset the session of the legitimate party (probably an operator) and initiated a new connection. Through the freshly built connection, they could issue IEC 104 commands to the server and control the grid that way. This kind of attack can be easily detected contrary to our proposed attack described in Section V.

A very detailed description of MitM attacks is presented in [20]. The authors of the paper tried two different attacks that required MitM position: replay attack and packet modification attack. In the replay attack, the attacker captured a packet containing an IEC 104 C_CS_NA_1 and replayed it without modification. This attack did not work as the sequence numbers in the TCP header were incorrect, resulting in packet drop and an alert in the Snort anomaly detection system. The second attack was more successful than the first one. This attack starts by waiting for a good message, capturing and modifying it (dropped the original packet), and forwarding the modified version. With this attack, they could control the power grid or cause false alarms for the operators. However, they needed valid packets to alter them in their own needs.

The authors of [21], [22], [23] did not focus on the IEC 104 protocol. Instead, they investigated what the possible effects of malicious NTP messages on a system using IEC 104 are. Some of the attacks may even affect IEC-62351 compliant systems (which proposes security improvements for the standard IEC 104) because it relies on NTP as well.

In [21] the authors reviewed if malicious time settings can be propagated across the entire network, and the results showed that IEC clients and servers started to use the malicious time in their ASDU messages. This behavior can be abused to de-synchronize control loops, and it even affects logging mechanisms in the system.

[22] focuses on causing de-synchronize just by manipulating the packet process rate of the NTP synchronization server's queue. This attack may be used to undermine the QoS of the communication.

In [23] the authors showed that in some cases, when the clock of communicating parties is not synchronized, it can even result in DoS attacks.

There are newer protocols to support the communication needs of power grids. One is the IEC 61850 [27] with security extensions defined in IEC 62351 [28]. However, these extensions are not flawless either. The authors in [29] showed three weaknesses in the protocol. The security mechanism of IEC 62351 can also be applied to the protocol in the focus of this paper, the IEC 104. This was demonstrated in a laboratory setup in [30] as well.

The security of power systems is a well-studied field, two great surveys are [31], [32]. A recent paper focusing on the security of substations using IEC 104, among other protocols, can be found in [33]. Readers interested in a greater picture of cyber-physical systems security are encouraged to check the survey in [8].

We used techniques from the previously mentioned papers and improved them to achieve better and stealthier attacks during our research. We first executed some of the attacks described in the previous papers. Preliminary results of this experiment were published in [34] by us. Then we moved to designing new attacks. We designed a new way that can be used for DoS attacks as well. Furthermore, we developed the packet injection attacks by injecting packets into an established session without resetting the original connection and without relying on valid packets. This method is far harder to detect because the communicating parties generate no log messages, and no invalid messages are sent, which could trigger the alert of an IDS system.

Before introducing our attack toolkit, we describe the potential entry points of a system in the next section.

IV. ENTRY POINTS OF ATTACKS

In this section we highlight some key concepts of attack surfaces complementing our main topic. The basics and current state regarding operation of power system control and IT solutions can be found in literature (e.g. [35], [36], [37])

Reliability is of main concern in every aspect of power system operation. Fault of a single element must be withstood without any disturbance (n-1 principle), be it a transmission line or a server. There is always a fallback procedure: the other transmission lines can take the extra load, a spare server jumps in. This mindset challenges the implementation of cyber-security measures. For example, an adaptive firewall cannot block traffic that is yet unknown - or else it can lead to emergency situations. This can also be exploited: a spare system or communication link can be quietly targeted and, at the right moment, locking out the primary system creates an automatic fallback to the infected system. Reliability also means that one cannot simply shut down or restart a critical system element, making it a harder and slower process to recover from an incident. The recovery process may also require significant human resource and time, especially if a black-out situation was created. This means that restoration of power supply can take several hours if no permanent damage or change was introduced to the system. If physical damage was done (e.g. circuit breakers), it can take weeks until the system could operate again in normal - n-1 withstanding - state.

Operation of power systems span across huge geographic areas involving multiple companies and personnel in different domains. The larger the system the larger the attack surface is, that malicious attackers might leverage. Generally there are several regulations that require making certain data publicly available which makes some areas of open source intelligence unavoidable (tenders, network development plans, transparency reports, press releases, etc.). Not only this, but the potential damage a successful attack can inflict makes power systems an attractive target. Figure 4 shows the typical areas where IEC 104 are used in system operations - focusing on SCADA systems.

Some example of potential weaknesses:

- Utilities must have periodic data exchange (schedules, measurements, grid models)
  - Corporate internal firewall - the interface must acquire data from operational databases inside SCADA systems
  - Data exchange process - corrupting or injecting false data
  - Using the sheer knowledge of the exchanged data can be leveraged at other attacks.
- Utilities have remote access to substations and sites
  - Suppliers' system - a vendor can have direct access to equipment and or software
  - Physically infiltrating a substation and attacking the control center from there - it can be easier than it sounds, considering a distant, unmanned substation, away from any settlement.
- Utilities rely on third parties
  - Equipment manufacturers or software developers can be leveraged - supply chain attack
  - Service providers - it can be e.g. ICT infrastructure as a service

From the many possibilities, some general key entry points can be pinpointed:

- The SCADA (Supervisory Control and Data Acquisition) system itself, which could potentially provide a complete control over the system. Due to this, it is one of the most protected system regarding perimeter defense. At the same time, it provides a relatively big attack surface due to required communication over a large geographic area.
- Several interfaces for the SCADA system are required to, for example, fulfill data exchange responsibilities and to keep the database up-to-date with a geographic information system (GIS). The attack surface here is twofold. On one hand, an attacker can inject false data into the external system, which could even have an impact that prevents the SCADA system operating. On the other hand, an attacker can exploit vulnerabilities of the several interfaces.
- Utility business process applications plays an important role in efficiency and organized operations. For example, a schedule from the power system market or a planned maintenance serve as a baseline of the network's planned state.
- Network equipment (routers, firewalls) is the backbone of most of the systems utilities have. At the same time, network equipment is typically used everywhere, not just in power systems. They tend to be cheaper and more accessible for hackers and security researchers. Therefore zero-day vulnerabilities are discovered in these much more often than in other pieces of equipment.
- RTU (Remote Terminal Unit) is the data concentrator for several equipment and provides protocol translation, routing and switching functionalities. These are found in every substation, and generally the primary and spare systems come from a different vendors. They even have primary and backup communication link that are physically independent from each other.
- Substation equipment connects to RTU and thus provides another way into the system. The attack surface is larger than that of RTUs, because there are usually two RTUs in a substation, while there are tens, hundreds of other equipment from several manufacturers.

The amount of equipment, cooperating parties and geographic distance coupled with the interdependence of physical and cyber space make the systematic listing of entry points and a complete risk assessment especially challenging. The general frameworks could be partly used with the electric power system like ISO 27000 series standard (e.g., 27019 for ICS in energy sector) or IEC 62443. In North America NIST also creates standards and guidelines - among others - for risk assessment (e.g. NIST SP 800-30) and for security of industrial control systems (e.g. NIST 800-82). A holistic and generalized framework that fits every purpose does not exist, however, the concepts and definitions could be extended and used to secure critical infrastructure systems. [38] shows an example for creating a combined approach for cyber-physical systems.

V. USE CASES FOR ATTACKS AGAINST IEC 104

This section will introduce the attack vectors, the test environment, and the real-world devices used for evaluating the different attacks. We designed multiple attack scenarios based on our understanding of the protocol. Furthermore, we also tried attacks described in other papers, which were introduced in Section III.

The attacks were tested in a small simulator consisting of virtual machines and the OpenMUC [39] implementation of the IEC 104 protocol. The topology can differ for the scenarios, but it always had one IEC 104 server, one client, and at least one attacker.

The attacks are available for everyone wanting to reproduce our results. The attack scripts are publicly available on GitHub[2]. To make reproducing easier, we used Docker containers, and each attack scenario has a detailed step-by-step description. The topology of the attack is depicted on Figure 5.

[2]https://github.com/CrySyS/IEC-104-Attacks

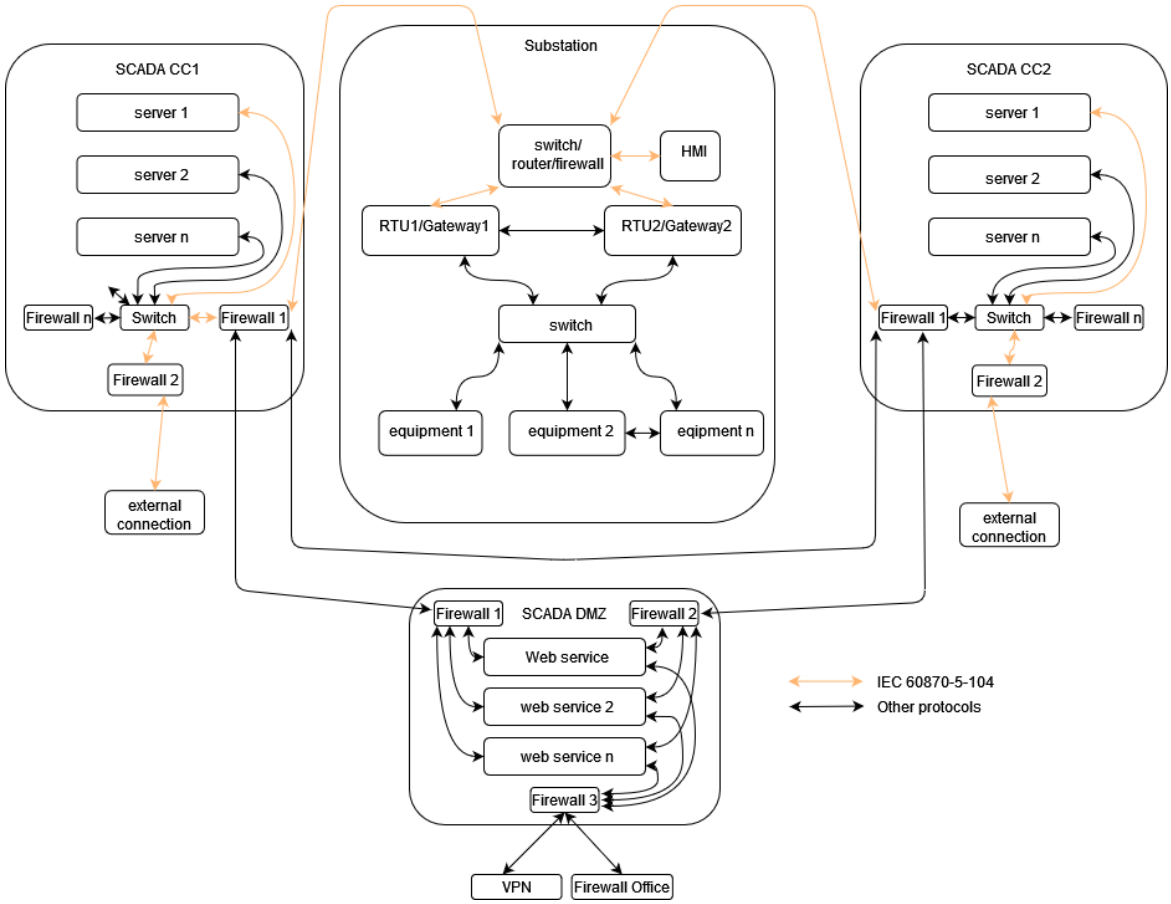

Fig. 4. Generalized communication scheme of the power system control, highlighting usage of IEC 60870-5-104.

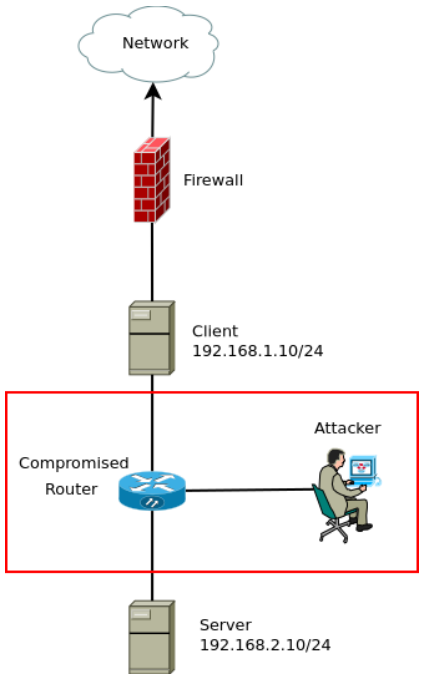

Fig. 5. The topology of the testbed.

As soon as we successfully attacked the purely software-based simulator, we also tested it on real devices, which included:

- an Opal-RT OP5707 based real-time simulator system. It can conduct hardware-in-the-loop simulation, which plays an important role in power system research, including communication-related studies.
- an Infoware RTU (MAB V2[3]). It is a piece of industrial-grade equipment produced by a local firm and is used widely in the power system of Hungary.
- a CitectSCADA based HMI by Schneider (Aveva). It is also a popular choice for substations' local HMI needs.
- a newer and an older version of EuroProt+ protection equipment by Protecta.

The most important attacks against the protocol are the following.

A. Unauthorized access

The protocol does not support authentication by design. Therefore if an attacker can connect to an IEC 104 server, they can execute arbitrary IEC 104 command on the server.

[3]http://www.infoware-zrt.hu/intelligens-rendszerek-mabv2-es-mab3-gwy-iranyitastechnikai-rendszer

We tried this attack against the OpenMUC implementation of the protocol and on two real devices (Infoware RTU, OpalRT simulator). As expected, none of them implemented extra authentication alongside the protocol. In the following, we will not discuss this attack because it is already explained in detail in [18].

B. ASDU address field starvation

The idea of the attack is to use up every possible ASDU address field of the IEC 104 network. Since the ASDU address field is stored on 2 bytes, 65535 (actually 65533 since 0 and 65535 are not used) different addresses can be used. To deplete the address pool, the attacker must initiate connections to the IEC 104 server without closing the previously established connection. In theory, after the address pool becomes depleted, the server will not accept new connections.

The attack was carried out in the testbed with two attackers, one server, and one client. The OpenMUC implementation of the protocol can handle only 100 connections simultaneously. After reaching the limit, no new connections could be made to the server.

The attack was successful against real devices as well. The OpalRT simulator and the Infoware RTU could handle only a single connection. Therefore if an attacker could connect to the device, the operators could not interact with the server. This attack was also tested against two Protecta devices. Both could handle nine parallel connections. When all of them are acquired by an attacker, the operator would have no means of controlling the device. The small number of parallel connections can be easily exploited to prevent the operator from connecting to the server.

C. TCP stream poisoning

The protocol uses TCP as the transport protocol. Therefore attacks targeting the TCP transport protocol can be used against the IEC protocol as well. An attacker who can inject packets in an active communication session can inject TCP packets with invalid checksums in the connection or inject a FIN or RST packet while impersonating a legitimate party of the communication to cause a denial of service. This attack was proven successful both in the simulator and in the case of real devices (between the Citect SCADA and the Infoware RTU, between the Opal-RT OP5707 and a RaspberryPi with OpenMUC) as well. TCP-based attacks will not be mentioned in the following because they are described in more detail in [18] and [19].

D. Modifying IEC 104 sequence numbers

Each participant of the communicating parties keeps a record of the number of received and sent messages. Upon a message is received, these sequence numbers are validated. In the case of correct sequence numbers, the message is processed. Otherwise, the message is dropped, and the connection is terminated due to the incorrect sequence numbers. Since the protocol does not define a mechanism to protect the integrity of the message header, this behavior can be abused by an attacker who can modify the messages of active connection to cause a denial of service.

To modify the IEC 104 sequence numbers, the attacker needs to be in a MitM position to inspect and modify forwarded packets. We used *iptables* and the *NetfilterQueue* [40] package of *Python* to move traffic forwarding from kernel-space to user-space. Since, at the time of writing this paper, the *set_payload* function of NetfilterQueue was not working, we dropped the original packet and sent out a forged one using *Scapy* [41].

This attack was carried out with success in the simulator and with real devices (between the Citect SCADA and the Infoware RTU, between the Opal-RT OP5707 and a RaspberryPi with OpenMUC) as well. To achieve MitM position, we used *bettercap* [42], a framework for carrying out ARP poisoning attacks.

E. Packet injection

The protocol does not define a mechanism for protecting the header or the body of the IEC messages. An attacker with man-in-the-middle capabilities can manipulate arbitrary packets of the communication. The attacker can even inject new packets into the communication. However, the attacker needs to be careful because the sequence numbers of the legitimate communicating parties will not match. To avoid the termination of the connection, the attacker needs to modify the sequence numbers to match the expectations of the destinations.

The setup used to inspect, modify or drop packets was the same as in V-D. Injecting a new packet to the communication and modification (in case of packet length changes) requires extra care because the TCP sequence numbers and the IEC 104 sequence numbers of the communicating parties will not match. Therefore to avoid the termination of the TCP session, it needs to be patched to match the receiver's expectations for all future packets as well. Therefore the attacker needs to keep a record of both session numbers on all of the attacked streams. The authors started to work on this topic and showed some preliminary results in [34]. This can results in a complete takeover of the communication, since the attacker can inject, modify or drop arbitrary packets without the possibility of trivial detection of the attack.

This attack was successful in the case of the simulator. Furthermore, it worked well in the case of real industrial devices (between the Citect SCADA and the Infoware RTU, between the Opal-RT OP5707 and a RaspberryPi with OpenMUC). To achieve MitM position, we used *bettercap* as in the previous attack.

The only remainder of an efficient attack is the targeting of the attack. The attacker knows what they want to achieve but does not know which ASDU address or IOA should be modified to achieve that goal. In the next section we show a method which can help the attacker in this question.

VI. TARGETING ATTACKS IN UNKNOWN ENVIRONMENTS

A. Introduction to the pairing based attack

Previously, we have shown numerous attacks against the IEC 104 protocol. These attacks included MitM attacks where

TABLE I
DATA COLLECTED AT THE MITM POSITION (LEFT) AND DATA COLLECTED FROM AUXILIARY SOURCE (RIGHT).

$IUID$	T_1	T_2	T_3
1000	8.7	11.2	9.3
2000	6.2	5.1	3.9

SID	T_1	T_2	T_3
A	5	5	4
B	8	12	10

the attacker could manipulate data transferred among the parties using IEC 104. However, the attacker could not decide what to manipulate because the pairing among real world identifiers (station IDs) and IEC 104 identifiers (ASDU Address; Information Object Addresses, IOA) is unknown. Therefore the attacker only could randomly set the values of different IOAs on different devices which could lead to harmful events, but not to full control.

In this part of the paper, we show how the attacker can learn the station ID-IOA pairs. The very same method can be used if the ASDU address is also unknown. In the following we will use the following nomenclature for the sake of simplicity:

SID: station ID, real world identifier of a data point known to the attacker

IUID: IEC 104 unique identifier unknown to the attacker, ASDU address and IOA pair

The revealed pairing can help the attacker to successfully compromise and take over the control of the system. The attacker can use the previously described MitM position to eavesdrop and learn the values set by the IEC 104 client. This way, one can learn the values assigned to each IUID (remember, the ASDU contains the ASDU address, the IOA and the value itself). The attacker can also periodically collect some auxiliary information (e.g. query some public web page, or utilize other acquired intelligence sources) to learn the values assigned to each SID. The different sources of auxiliary information is described in Section VI-B. Based on the auxiliary information and the information collected at the MitM position the attacker can build an error matrix to find the most likely pairing. This algorithm is presented in the following artificially small example.

Table I. represent the data learned through eavesdropping the IEC 104 communication at the MitM position and collecting the auxiliary sources at times T_1, T_2 and T_3. For the sake of simplicity, only two IDs are used in the example. In real life scenarios, the number of IDs are much higher; the robustness of the algorithm with higher station numbers is analyzed in Section VI-F.

The next step of our algorithm is to calculate the error of the different pairings which is the sum of squared differences for every possible pairing. The possible pairings are the following ($SID - IUID$): A-1000, A-2000, B-1000, B-2000.

Based on the time series presented earlier, the calculations for the first pair would be the following:

$$ERROR(A, 1000) = (8.7-5)^2 + (11.2-5)^2 + (9.3-4)^2 = 80.22$$

We can simply calculate the same error for every possible pair. The matrix of the errors can be represented as:

	A	B
1000	80.22	1.62
2000	1.46	88.06

The last step of the algorithm is to choose pairs which covers the matrix and calculate the total error. It can be done in two ways in this example:

- 80.22 + 88.06 (SID=A is paired to IUID=1000 and SID=B is paired to IUID=2000)
- 1.46 + 1.62 (SID=A is paired to IUID=2000 and SID=B is paired to IUID=1000)

Our goal is to find the lowest one, so the second one will be the correct. From this, we can learn that the most likely pairing in this case was A-2000 and B-1000. Generally finding the best pairing is not so obvious. Fortunately the well-known Hungarian algorithm [43] solves exactly this problem.

The steps of the algorithm are the following:

1) Collect n time series of IEC 104 communication for n different IUIDs
2) Collect n time series from auxiliary source for n different SIDs
3) Calculate an n-by-n matrix of squared differences of the time series
4) Find a minimal pairing based on the Hungarian algorithm
5) The result of the algorithm is the most likely IUID - SID pairing

We paired n IUID to n SID in the above example for the sake of simplicity. The very same algorithm can be used to pair n by m values ($n >= m$) if we have m SIDs to pair with n IUIDs.

B. Auxiliary information sources

The pairing based attack requires an information source where the real station IDs (name of the variable) and related values can be found. Such an information source can be publicly accessible in many countries. These web pages display the current flows of different countries, stations or substations in near real time. Some examples are the following:

- Border crossing data per country and region: https://www.electricitymap.org
- EU detailed cross border physical flows and market data: https://transparency.entsoe.eu
- Real time electricity consumption and inter-regional flows from France: https://www.rte-france.com/en/eco2mix
- Hungarian Power System Actual Data: https://mavir.hu/web/mavir-en/hungarian-power-system-actual-data

The attacker can also use other private but not well protected information sources, like data series shared between different companies.

The finer the auxiliary information, the easier and more accurate the result is. In Section VI-F we show how the

accuracy of this information influences the results of the algorithm.

Transmission system (along with the transmission system operator - TSO) is most affected by this openness. The basic topology of the transmission system is relatively easy to reconstruct via satellite images, while for some regions it is even well known from publications (like the ENTSO-E materials in Europe). Generally, neighboring TSOs have a few connections with each other, thus - for example - the flows on the physical lines could be guessed from the data on energy exchange between countries. The transmission system has much less substations and transmission lines compared to the distribution system, which means that even little information defines the state of the system that adequately supplements the pairing algorithm.

C. Implementation of the attack

We have implemented the attack with 3 main parts, the IEC 104 eavesdropper, the auxiliary information collector (web crawler) and the SID-IUID match maker.

1) IEC 104 eavesdropper: The implementation of the eavesdropper is described in Section V. However in this particular case we only want to store the values of the IUIDs in time-series (time-IUID-value tuples). No modification or injection is needed in this phase.

2) The web crawler: The web crawler is similar to the IEC 104 eavesdropper as it downloads and stores the auxiliary information source in time-series (time-SID-value tuples).

3) The match maker: The match maker reads the stored data from the two sources and calculates the squared differences matrix. This matrix is the input of the Hungarian algorithm which calculates the pairs with the lowest error. The result is a list containing the SID-IUID pairs. The algorithm was implemented in Python using scipy and numpy.

D. Verification of the matching algorithm

The verification of the algorithm was done by testing it with many different cases. We could not use real life data in this research, therefore we wrote a Python script that generated numerous data series and also used a series from a simulator. We ran the algorithm on these artificial time-series and verified the results.

E. Generation of data series

The goal of this step is to generate data series that can be used for testing. We wanted to make the generated data series as realistic as possible, therefore the data was generated according to the following rules.

- The values of the stations are changing smoothly in real-life, therefore using plain random numbers would result in unrealistic scenarios. To avoid this, only the first value is random and the rest is generated using the ones before them.
- The publicly available web page nor the measurements themselves wouldn't represent accurate values in a real-life scenario, therefore some noise needs to be added to the data.
- The number of the values generated for each scenario is also random, therefore we can validate if it works properly with even a small amount of data available.

F. Test scenarios

We used a manually crafted test scenario (#5) and several artificially created base test cases (#1-#4) for performance evaluation. For the latter, the SID-IUID pairs are generated randomly for each test case. The results of the algorithm was compared to the ground truth. We ran millions of test cases with the following configurations.

Explanation of these constants are the following:

- CHANGE_RATE_MIN/CHANGE_RATE_MAX: A random number is generated in this interval, and the previous value is multiplied by it. This ensures that the values can only change smoothly.
- VALUE_COUNT_MIN/VALUE_COUNT_MAX: The number of values for each station is generated in this interval (length of test case).
- MIN_VALUE/MAX_VALUE: The value of the station is generated in this interval.
- ITERATION_COUNT: The number of test cases in the scenario.
- NOISE_MIN/NOISE_MAX: As mentioned earlier the website doesn't show accurate values, therefore the original value is multiplied by a number which is generated in the range of these numbers. This can be considered as quantization error.
- STATION_COUNT: The number of data points to pair.

The parameters of the five different scenarios are summarized on Table II.

TABLE II
PARAMETERS AND RESULTS OF THE SCENARIOS

Parameter	S1	S2	S3	S4	S5
CHANGE_RATE_MIN	0.8				n.a
CHANGE_RATE_MAX	1.2				n.a
VALUE_COUNT_MIN	10	10	10	20	20
VALUE_COUNT_MAX	20	50	50	20	192
MIN_VALUE	-1000				n.a
MAX_VALUE	1000				n.a
ITERATION_COUNT	10^6				
NOISE_MIN	0.7	0.8	0	0.9	0.85
NOISE_MAX	1.3	1.2	2	1.1	1.15
STATION_COUNT	13	13	13	100	13
Success rate	97.4%	99.9%	68.9%	100%	94.2%

1) Scenario 1: In this scenario, the size of the data series was between 10 and 20, which is considered a rather small sample size. The algorithm correctly determined the pairs in 974827 cases out of 1000000. This means that in this case, the algorithm had a success rate of 97.4%.

2) Scenario 2: In this scenario, we tested the effect of longer time series (10 to 50 values per station) with smaller noise. We expected to get better results than in the previous scenarios as more input data was used in the pairing phase. The algorithm correctly determined the pairs in 999282 cases out of 1000000. This means that a success rate of 99.9% was achieved.

3) Scenario 3: In this scenario, the noise rate was enormously large (in a real scenario, it would be less than 10%, here we have 100%), and the value count per station was between 10 and 50. The algorithm still determined the pairs correctly in 689448 cases out of 1000000. This means that in this case, the algorithm had a success rate of 68.9%.

4) Scenario 4: In this scenario, the algorithm correctly determined the pairs in 1000000 cases out of 1000000. This means that in this case, the algorithm had a success rate of 100%. In this scenario, the number of stations was greatly increased, but the run-time of the matching scaled linearly. This indicates that the algorithm is suitable for larger sets with reasonable running times. We think this scenario is the most realistic in terms of parameter selection.

5) Scenario 5: This scenario significantly differs from the previous ones. The values for this scenario was crafted manually to mimic real-life values. Creating a lifelike simulated environment is generally challenging, however, here the goal was to simply have a system which has the same correlation behavior as a real one: the different measurements on substations (i.e. a node in a graph) and on transmission lines (i.e. an edge in a graph) all have a dependency on each other. The strongest connection among these measurements comes from the physical properties of a network which is represented by load-flow calculation that is generally used for these purposes in the industry. A correlation - although to a much lesser extent - also could exist via the natural shape of load profiles; this approach is also widely used in the industry since decades. For this specific scenario, consumption and generation values were based on actual measurements and statistically created profiles. Moreover, a simulated network topology was used to estimate the current and voltage values for every time step with load-flow calculations. Thus, even the effect of one node on an other is also apparent. Also, a variety of load behaviour was represented (photovoltaic, wind, gas power plant; industrial, commercial and aggregated residential load). We created a single set of timeseries as a foundation and added random noise (to represent measurement uncertainty) just like with the other scenarios and used a variety of time periods to represent that an attacker starts to eavesdrop at a random time. The algorithm correctly determined the pairs in 942000 cases out of 1000000. This means that in this case, the algorithm had a success rate of 94.2%. It is important to note that there are periods when some values remain the same for some nodes, which makes pairing really hard for the algorithm (e.g. photovoltaic plants are typically not producing anything for several hours during the night resulting in long, indistinguishable sequences of zeros).

G. Evaluation

The previous test scenarios showed that the algorithm works well even with extreme configurations. Scenario 4 was closest to reality in terms of complexity. In that case, the algorithm had a success rate of 100%. The data values were as realistic as possible in Scenario 5, and that scenario also succeeded over 94% of the cases. Therefore we affirm that this approach can be used to match SIDs to IUIDs. The speed of the algorithm is also acceptable, Scenario 4 had the longest run-time, but it still took less than 1 second to calculate one case. We argue that the described algorithm can be successfully used as an early phase of an attack, where the target IUIDs can be discovered. The algorithm should run only once after a long data collection phase so the running time of the algorithm is not so important.

As the results show, the pairing works very well, but a successful attack chain requires many steps described in this paper. First, the attacker needs to access the network where the IEC communication is used (the possible entry points are analysed in Section IV). Then the attacker needs to get in a position where they can eavesdrop on the IEC server and client (in this step, the attacker gathers identifier and value pairs, the possible methods are introduced in Section V). Meanwhile, eavesdropping on the transmission, the attacker also needs to find a reliable data source where the station's values and names are present. After the attacker has gathered enough information, they can run the Hungarian algorithm to find the correct SID and IUID pairs as described in this section. When the pairing is done, the attacker can start various attacks against the power grid to control it as they desire. With this knowledge, masquerading and precisely targeting the attack becomes feasible. For example, the adversary could open circuit breakers without the system operators knowing it, thus leaving specific areas without power. Or, the adversary could remain hidden until it modifies the network enough to cause a large scale blackout.

The risk of the whole scenario can be analysed based on the DREAD scoring system [44], where the components of the risk are Damage potential, Reproducibility, Exploitability, Affected users, and Detectability. The scoring systems uses High, Medium and Low scores. The Damage potential of the scenario is high as physical damage even causing fire at the substation is probable. The Reproducibility of the attack is medium as special knowledge of power systems and network protocols are also required at the same time. The Exploitability is Medium as a vulnerable entry point must be found at the beginning, but after that the attack is straightforward. The number of Affected Users can be very high as a blackout around a substation can affect thousands of people. The attack can be detected relatively easily as it creates different anomalies in the operation. A well-configured anomaly detector can detect it and trigger an alarm. This means that the risk coming from the detectability is low. A successful attack scenario can violate all components of the CIA objectives: the Confidentiality of identifiers used inside the substation is violated by the pairing. The Integrity of the commands and measured values is affected by the selective modification of the IEC 104 messages, while the Availability of the power system might be violated by selectively opening and closing circuit breakers.

If someone wants to avoid such attacks, a systematic approach must be used. It starts with the application of the risk assessment frameworks discussed in Section IV and the realization of countermeasures mentioned in the frameworks and in Section III.

VII. SUMMARY

In this paper, we analyzed the security of the IEC 104 protocol. We showed existing attacks against the protocol and also designed new attack vectors. To supplement, we published our attack scripts to make it possible for everyone to reproduce our attacks.

We assembled a realistic attack scenario in a holistic approach comprising the following parts:

- We enumerated the possible entry points a threat actor can use to access IEC 104 communication.
- We showed and created new techniques which can result in man in the middle position for the attacker and showcased the operation with actual equipment.
- By collecting traffic from the attacked network and from auxiliary sources we demonstrated how the real identity of the information object addresses can be revealed.

By leveraging the demonstrated methods, one can get into a position from where taking over the entire telecontrol system is straightforward.

In the future, we will focus on extending the framework with advanced false packet creation methodologies which can increase the chance that the attack itself could remain hidden. This involves synchronised packet injection at multiple places that produces a consistent state of the network. It would also be interesting to test our attack scenario in a real deployment (especially the accuracy of the pairing), but it is challenging to persuade a TSO to let us access their internal systems.

REFERENCES

[1] "IEC 60870-5-104, part 5-104: Transmission protocols – network access for iec 60870-5-101 using standard transport profiles," 2006.

[2] "IEC 62351, power systems management and associated information exchange - data and communications security," 2021.

[3] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[4] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. IEEE, 2017, pp. 1–8. [Online]. Available: DOI: 10.1109/CPRE.2017.8090056

[5] L. Constantin, "Solarwinds attack explained: And why it was so hard to detect," 2020. [Online]. Available: https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

[6] F. Wortley, C. Thompson, and F. Allison, "Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package," 2021. [Online]. Available: https://www.lunasec.io/docs/blog/log4j-zero-day/

[7] E. Burke, "Targeted cyberattack takes out Vodafone Portugals," 2022.

[8] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29 775–29 818, 2021. [Online]. Available: DOI: 10.1109/ACCESS.2021.3058403

[9] P. Matoušek, "Description and analysis of iec 104 protocol," *Faculty of Information Technology, Brno University of Technology, Tech. Rep, 2017*. [Online]. Available: https://www.fit.vut.cz/research/publication/11570

[10] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated IEC-60870-5-104 traffic," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–7. [Online]. Available: DOI: 10.1145/3098954.3103166

[11] C.-Y. Lin and S. Nadjm-Tehrani, "Timing patterns and correlations in spontaneous SCADA traffic for anomaly detection," in *22nd International Symposium on Research in Attacks, Intrusions and Defenses ({RAID} 2019)*, 2019, pp. 73–88. [Online]. Available: https://www.usenix.org/conference/raid2019/presentation/lin

[12] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. Wang, "Intrusion detection system for IEC 60870-5-104 based SCADA networks," in *2013 IEEE power & energy society general meeting*. IEEE, 2013, pp. 1–5. [Online]. Available: DOI: 10.1109/PESMG.2013.6672100

[13] M. A. S. Arifin, D. Stiawan, J. Rejito, M. Y. Idris, R. Budiarto et al., "Denial of service attacks detection on scada network iec 60870-5-104 using machine learning," in *2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*. IEEE, 2021, pp. 228–232. [Online]. Available: DOI: 10.23919/EECSI53397.2021.9624255

[14] M. Anwar, A. Borg, and L. Lundberg, "A comparison of unsupervised learning algorithms for intrusion detection in iec 104 scada protocol," in *2021 International Conference on Machine Learning and Cybernetics (ICMLC)*. IEEE, 2021, pp. 1–8. [Online]. Available: DOI: 10.1109/ICMLC54886.2021.9737267

[15] S. V. B. Rakas, M. D. Stojanović, and J. D. Marković-Petrović, "A review of research work on network-based scada intrusion detection systems," *IEEE Access*, vol. 8, pp. 93083–93108, 2020. [Online]. Available: DOI: 10.1109/ACCESS.2020.2994961

[16] O. A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, S. Rimer, and K. O. A. Alimi, "A review of research works on supervised learning algorithms for scada intrusion detection and classification," Sustainability, vol. 13, no. 17, p. 9597, 2021. [Online]. Available: DOI: 10.3390/su13179597

[17] P. Matoušek, O. Ryšavỳ, and M. Grégr, "Increasing visibility of IEC 104 communication in the smart grid," in *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*, 2019, pp. 21–30. [Online]. Available: DOI: 10.14236/ewic/icscsr19.3

[18] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis, and E. Panaousis, "Attacking IEC-60870-5-104 SCADA systems," in *2019 IEEE World Congress on Services (SERVICES)*, vol. 2642. IEEE, 2019, pp. 41–46. [Online]. Available: DOI: 10.1109/SERVICES.2019.00022

[19] Q. S. Qassim, N. Jamil, M. Daud, N. Ja'affar, S. Yussof, R. Ismail, and W. A. W. Kamarulzaman, "Simulating command injection attacks on IEC 60870-5-104 protocol in SCADA system," *International Journal of Engineering & Technology*, vol. 7, no. 2.14, pp. 153–159, 2018. [Online]. Available: DOI: 10.14419/ijet.v7i2.14.12816

[20] P. Maynard, K. McLaughlin, and B. Haberler, "Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA networks," in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014)* 2, 2014, pp. 30–42. [Online] Available: DOI: 10.14236/ewic/ics-csr2014.5

[21] A. Baiocco and S. D. Wolthusen, "Causality re-ordering attacks on the IEC 60870-5-104 protocol," in *2018 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2018, pp. 1–5. [Online]. Available: DOI: 10.1109/PESGM.2018.8586010

[22] J. Wright and S. Wolthusen, "Time accuracy de-synchronisation attacks against IEC 60870-5-104 and IEC 61850 protocols," in *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2019, pp. 1–5. [Online]. Available: DOI: 10.1109/ISGT.2019.8791558

[23] A. Baiocco and S. D. Wolthusen, "Indirect synchronisation vulnerabilities in the IEC 60870-5-104 standard," in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2018, pp. 1–6. [Online]. Available: DOI: 10.1109/ISGTEurope.2018.8571604

[24] J. Jarmakiewicz, K. Parobczak, and K. Maślanka, "Cybersecurity protection for power grid control infrastructures," *International Journal of Critical Infrastructure Protection*, vol. 18, pp. 20–33, 2017. [Online]. Available: DOI: 10.1016/j.ijcip.2017.07.002

[25] D. Deb, S. R. Chakraborty, M. Lagineni, and K. Singh, "Security analysis of mitm attack on scada network," in *Machine Learning, Image Processing, Network Security and Data Sciences: Second International Conference*, MIND 2020, Silchar, India, July 30-31, 2020, Proceedings, Part II 2. Springer, 2020, pp. 501–512. [Online]. Available: DOI: 10.1007/978-981-15-6318-8_41

[26] L. Erdődi, P. Kaliyar, S. H. Houmb, A. Akbarzadeh, and A. J. Waltoft-Olsen, "Attacking power grid substations: An experiment demonstrating how to attack the scada protocol iec 60870-5-104," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: DOI: 10.1145/3538969.3544475

[27] R. E. Mackiewicz, "Overview of IEC 61850 and benefits," in *2006 IEEE Power Engineering Society General Meeting*. IEEE, 2006, pp. 8–pp. [Online]. Available: DOI: 10.1109/PSCE.2006.296392

[28] S. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2019. [Online]. Available: DOI: 10.1109/TII.2019.2956734

[29] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016, pp. 266–270. [Online]. Available: DOI: 10.1109/SmartGridComm.2016.7778772

[30] M. G. Todeschini and G. Dondossola, "Securing IEC 60870-5-104 communications following IEC 62351 standard: lab tests and results," in *2020 AEIT International Annual Conference (AEIT)*, 2020, pp. 1–6. [Online]. Available: DOI: 10.23919/AEIT50178.2020.9241101

[31] W.-W. Li, W.-X. You, and X.-P. Wang, "Survey of cyber security research in power system," *Power System Protection and Control*, vol. 39, no. 10, pp. 140–147, 2011.

[32] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer networks*, vol. 57, no. 5, pp. 1344–1371, 2013. [Online]. Available: DOI: 10.1016/j.comnet.2012.12.017

[33] S. Hussain, J. H. Fernandez, A. K. Al-Ali, and A. Shikfa, "Vulnerabilities and countermeasures in electrical substations," *International Journal of Critical Infrastructure Protection*, p. 100406, 2021. [Online]. Available: DOI: 10.1016/j.ijcip.2020.100406

[34] P. György and T. Holczer, "Attacking IEC 60870-5-104 protocol," in *Proceedings of the 1st Conference on Information Technology and Data Science*, 2020, pp. 140–150. [Online]. Available: http://ceur-ws.org/Vol-2874/paper13.pdf

[35] M. S. Thomas and J. D. McDonald, *Power System SCADA and Smart Grids*. CRC press, 2017. [Online]. Available: DOI: 10.1201/b18338

[36] K. Siozios, D. Soudris, D. Anagnostos, and E. Kosmatopoulos, *IoT for Smart Grids: Design Challenges and Paradigms (Power Systems)*. Springer, 2019. [Online]. Available: DOI: 10.1007/978-3-030-03640-9

[37] S. K. Khaitan, C.-C. Liu, and J. D. McCalley, *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015. [Online]. Available: DOI: 10.1007/978-3-662-45928-7

[38] S. C. Matta, A. M. Shaaban, C. Schmittner, A. Pinzenöhler, E. Szalai, and M. Tauber, "Risk management and standard compliance for cyber-physical systems of systems," *Infocommunications Journal*, vol. 13, no. 2, pp. 32–39, 2021. [Online]. Available: DOI: 10.36244/ICJ.2021.2.5

[39] "IEC 60870-5-104," https://www.openmuc.org/iec-60870-5-104/, 2019.

[40] "NetfilterQueue," https://pypi.org/project/NetfilterQueue/, 2017.

[41] "Scapy," https://scapy.net/, 2021.

[42] "bettercap," https://www.bettercap.org/, 2021.

[43] H. W. Kuhn, "The hungarian method for the assignment problem," *Naval research logistics quarterly*, vol. 2, no. 1-2, pp. 83–97, 1955. [Online]. Available: DOI: 10.1002/nav.3800020109

[44] J. Meier, *Improving web application security: threats and countermeasures*. Microsoft press, 2003.

János Csatár received the Ph.D. degree in Electrical Engineering from the Budapest University of Technology and Economics (BME) in 2019. Since 2019 he has been working as an assistant professor in the Smart Power Laboratory (SPL), Department of Electrical Power Engineering, Budapest University of Technology and Economics. Fields of interest: His research interest for the PhD was power system modeling with a special focus on distribution system. Recently his research interest focuses on hardware-in-the-loop simulation, co-simulation and interdependence of power systems and communication networks.

Péter György holds a Master's degree from the Budapest University of Technology and Economics (BME), which he obtained in 2022. He has actively participated in Capture The Flag competitions since 2019 as a member of the c0r3dump team. In 2021, Péter joined Ukatemi Technologies Plc, where he currently serves as the leader of the penetration testing team. Fields of interest: Péter focused his research on identifying vulnerabilities through black-box fuzzing during his Master's program. However, his current interests primarily revolve around network penetration testing and exploring various facets of web security.

Tamás Holczer received the Ph.D. degree in Computer Science from the Budapest University of Technology and Economics (BME) in 2013. Since 2013 he has been working as an assistant professor in the Laboratory of Cryptography and System Security (CrySyS), Department of Telecommunications, Budapest University of Technology and Economics. Fields of interest: In the past his research interests and his Ph.D. dissertation were focused on the privacy problems of wireless sensor networks and ad hoc networks. Lately he is working on the security aspects of cyber physical systems. The research topics include: security of industrial control networks, honeypot technologies in embedded systems, network monitoring and intrusion detection in industrial networks, and security aspects of intra-vehicular networks.