TU Delft

Delft University of Technology

Exploiting Ripple20 to Compromise Power Grid Cyber Security and Impact System Operations

Subramaniam Rajkumar, Vetrivel; Stefanov, Alexandru; Musunuri, Shyam; de Wit, Johan

Publication date
2021

Document Version
Accepted author manuscript

Published in
CIRED 2021 Proceedings

Citation (APA)
Subramaniam Rajkumar, V., Stefanov, A., Musunuri, S., & de Wit, J. (2021). Exploiting Ripple20 to Compromise Power Grid Cyber Security and Impact System Operations. In *CIRED 2021 Proceedings*

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

EXPLOITING RIPPLE20 TO COMPROMISE POWER GRID CYBER SECURITY AND IMPACT SYSTEM OPERATIONS

Vetrivel S Rajkumar[1*], Alexandru Stefanov[1], Shyam Musunuri[2], Johan de Wit[3]

[1] Delft University of Technology, Delft, The Netherlands
[2]Siemens A.G, Nuremberg, Germany
[3] Siemens Nederland N.V, The Hague, The Netherlands
** V.SubramaniamRajkumar@tudelft.nl*

Keywords*: Cyber Security, Cyber Threats, Cyber Attacks, Cascading Failures, Blackout*

Abstract

Driven by power grid digitalisation, tighter coupling between the cyber and physical layers has introduced cyber security threats. This paper elucidates the emergence and possible consequences of recently identified Information Technology (IT) / Industrial Internet of Things (IIoT) vulnerabilities, i.e., Ripple20, and the threats it poses to power grid cyber security. In this paper, we investigate advanced cyber attack tactics and techniques to exploit Ripple20 and IEC 61850 vulnerabilities through various attack vectors. The presented cyber-physical attack scenarios focus on gaining unauthorised access from pole-mounted reclosers in MV networks to the control centre and substation Operational Technology (OT) systems. Subsequently, the aforementioned vulnerabilities are exploited to maliciously disconnect embedded generation, block substation protection functionality, and cause busbar faults. We then experimentally demonstrate the impact of such advanced cyber attacks on power system operation that initiate cascading failures and cause a blackout. Recommendations and mitigation techniques for advanced cyber threats in the OT domain of distribution system operators are also provided.

1 Introduction

The electrical power system is undergoing a digital transformation with the integration of more digital services in the Operational Technology (OT) domain. This transition has given rise to Industry 4.0 and increased Industrial Internet of Things (IIoT) presence in power grids. The rapid IIoT developments have introduced risks and cyber security concerns. Cyber attacks on power grids have emerged as a sophisticated modern-day threat with wide-ranging ramifications. Such scenarios are no longer fictitious, as demonstrated by the cyber attacks conducted on the power grid in Ukraine in 2015 and 2016 [1], [2]. The former attack resulted in a power outage in the distribution network, directly affecting nearly 225,000 customers [1]. Hence, cyber security is an issue of serious concern to utilities.

More recently, nineteen zero-day vulnerabilities were discovered by a cybersecurity firm JSOF in a widely used industrial TCP/IP stack, dubbed Ripple20 [3]. The identified vulnerabilities are present in the network stack of embedded and IIoT equipment across a wide range of sectors such as healthcare, manufacturing, energy, etc. They are known to affect millions of devices from multiple major vendors, amplified by the supply chain factor, resulting in a *'ripple'* effect. The complete damaging effects of these vulnerabilities are not yet fully known. In particular, one of the identified vulnerabilities, i.e., Common Vulnerabilities and Exposure (CVE) 11896, is of serious concern. A successful exploitation of this critical CVE can result in arbitrary Remote Code Execution (RCE) by an adversary, leading to compromised operation of the targeted device. The exploitation of such vulnerabilities through sophisticated means can give rise to Advanced Persistent Threats (APTs) against the targeted system. It is a cause for worry that power system field equipment, particularly in the OT domain from multiple vendors have already been confirmed to be vulnerable to Ripple20 [3]. Keeping these facts in mind, this work seeks to emphasise how Ripple20 may serve as a sophisticated cyber attack vector against power grids, with dangerous implications, by exploiting zero-day vulnerabilities. Hence, the specific contributions of this paper are as follows. 1) Discuss the emergence of Ripple20 vulnerabilities and study their threats to power grid cyber security. We investigate advanced cyber attack tactics and techniques to exploit Ripple20 and IEC 61850 vulnerabilities through various attack vectors. The cyber-physical attack scenarios presented in this paper focus on gaining unauthorised access from pole-mounted reclosers in MV networks to the control centre and substation IT-OT systems. Subsequently, the Ripple20 and IEC 61850 vulnerabilities are exploited to maliciously disconnect embedded generation, disable substation protection, and cause busbar faults. 2) We experimentally demonstrate the impact of such attack scenarios on power system operation that can initiate cascading failures and cause a blackout. 3) We recommend the need for equipment manufacturers in the energy supply chain to follow latest cyber security standards and guidelines and inform system operators of current implementations and shortcomings. Consequently, this may aid in the timely detection and mitigation of emergent cyber threats against the power system.

2 Ripple20 Vulnerabilities and Cyber Threats

The power grid OT system architecture supported by IIoT is shown in Fig. 1. This comprises of three levels, i.e., bay, station, and control centre. In addition, we also consider the IIoT for pole-mounted reclosers in the MV distribution

networks that communicate with the control centre via a Wide Area Network (WAN) using IEC 104. Within the substation, an Ethernet-based Local Area Network (LAN) enables communication amongst the station controller, servers, and Human Machine Interface (HMI). A dedicated gateway ensures connectivity between the substation and control centre's Supervisory Control and Data Acquisition (SCADA) system, using protocols such as IEC 104. At the bay level, a dedicated fibre ring connects the station controller with Bay Control Units (BCUs) and other Intelligent Electronic Devices (IEDs) through IEC 61850. It is to be noted that some devices from certain vendors, located at the station and bay levels, i.e., printers, switches, and IEDs are confirmed to be affected by Ripple20 [3].

2.1 Ripple20 Vulnerabilities

Ripple20 is a collection of nineteen zero-day vulnerabilities discovered within a widely used networking stack found in embedded and IIoT equipment. Of these nineteen vulnerabilities, this paper focuses on CVE-2020-11896, which has a severity score of 10 out of 10 [3]. This clearly indicates its alarming threat, as a successful exploitation may lead to malicious remote code execution.

CVE-2020-11896 is a critical vulnerability in the Treck TCP/IP stack, wherein an attacker can achieve RCE by sending carefully crafted User Datagram Protocol (UDP) packets to an open port on the target IIoT device. A successful exploit of this vulnerability requires support of IP fragmentation with IP tunnelling on the target device. However, even if this is not the case, the target device is still vulnerable to Denial of Service (DoS) attacks [3]. The root cause for this vulnerability stems from an incorrect packet trimming procedure of fragmented packets in the Treck TCP/IP stack. This can result in a heap or buffer overflow that can subsequently be exploited to achieve malicious RCE. As indicated in [3], the steps to achieve this are summarised as follows: (i) UDP packets are sent to the target device at a high rate to ensure a non-empty socket queue, (ii) maliciously fragmented UDP packets are injected to exploit the vulnerability through IP tunnelling, (iii) incorrect packet trimming will result in improper buffer allocation on the heap of target device, subsequently overflown through 'tfcopypacket' function within the Treck stack. This last memory allocation contains shellcode to achieve malicious remote code execution. Thus, a write-what-where attack strategy is realised through a successful exploitation of the vulnerability [3]. This represents a serious threat to the OT system and IIoT devices in distribution networks, where attackers can take control of IEDs and execute malicious code to manipulate substation monitoring and control and disable power grid protection.

2.*2 IEC 61850 Vulnerabilities*

IEC 61850 is a widely used standard for substation automation and protection [4]. It forms the very basis of digital substations, offering advantages such as interoperability and reduced equipment footprint. However, research has raised valid cyber security concerns of the standard and shown that its Sampled Values (SV) and Generic Object-Oriented Substation Event (GOOSE) protocols are susceptible to various cyber attacks. These include man-in-the middle, replay, and data modification attacks due to the lack of encryption and authentication mechanisms [5], [6]. The SV protocol is used to communicate measurements from the bay to digital protection relays via merging units.

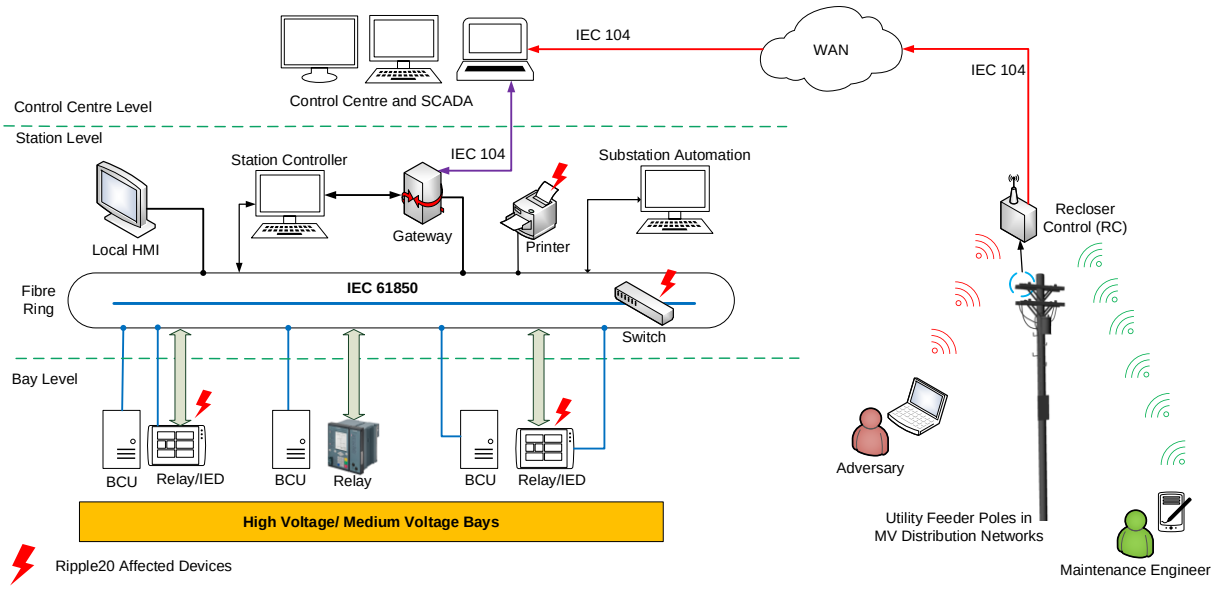

Fig. 1 OT-IIoT architecture for distribution systems

On the other hand, the GOOSE protocol is used to communicate critical substation events and messages between IEDs within a digital substation. Thereby, successful tampering of the former can lead to undesirable protection inhibition, while cyber attacks targeting the latter can lead to malicious opening of circuit breakers [6]. Hence, in this work we demonstrate the severity and dangerous consequences of cyber attacks exploiting Ripple20/IEC 61850 vulnerabilities.

2.3 Cyber Attack Tactics and Techniques

The cyber attack tactics and techniques in this paper seek to gain unauthorised access to a digital substation and exploit Ripple20 and IEC 61850 vulnerabilities to maliciously disconnect embedded generation, block substation protection functionality, and cause busbar faults. These are mapped with the MITRE attack framework [7], as follows. 1) Initial Access: the cyber attack originates from the MV distribution network. Pole-mounted reclosers, commonly found on utility feeders in MV networks are typically used for protection and implementation of normal open points. They contain Recloser Controllers (RC) for configuration of protection settings and maintenance. Such RC units are also enabled with communication capabilities in the form of Ethernet, wireless (802.11/Bluetooth) or cellular radio. Wireless functionality allows ease of access for network technicians to the recloser unit for configuration and maintenance, without having to climb the pole. Advanced wireless attacks [8] exploiting the lack of multi-factor authentication and encryption mechanisms may allow an adversary to gain unauthorised access to the RC unit via its wireless access point. Furthermore, RCs communicate directly with the SCADA system in the control centre through protocols such as IEC 104, DNP3, and/or IEC 61850. The lack of physical security coupled with weak cyber security practices adopted by recloser manufacturers makes pole-mounted RCs viable gateways for adversaries into the control centre OT network. 2) Lateral Movement: the second tactic entails unauthorised access from the control centre OT to the substation. Real-world incidents such as the 2015 and 2016 cyber attacks in Ukraine have established the means and know-how to carry out such lateral movements [1], [2]. Hence, in this paper, we will assume the adversary carries out a similar attack tactic to gain access to the substation OT system. 3) Command and Control: once inside the substation, the adversary can carry out active network reconnaissance to identify possible target devices containing the Ripple20 vulnerabilities, i.e., printers, network switches, and IEDs. This can be achieved by monitoring TCP/IP stack signatures through open-source libraries such as ‘corelight’ used for Treck Ripple20 IIoT device discovery and exploit detection. Thereby, an attacker may identify a target printer directly connected the substation LAN. Subsequently, by supplying a carefully crafted UDP packet and exploiting CVE-2020-11896, the attacker may achieve a memory leak on the printer and gather information pertaining to the Ethernet switch between the bay and station levels. As the network switch is also affected by Ripple20, the CVE can again be exploited to take control of the switch. Consequently, it is possible to conduct network reconnaissance via the switch to monitor and capture critical IEC 61850 traffic. 4) Impact: in the final stages of the attack, the adversary can successfully exploit Ripple20 to execute malicious code on affected IEDs, which generate genuine IEC 61850 traffic. The executed code can spoof IED behaviour and fabricate malicious GOOSE and SV data frames. Such an attack vector is of alarming consequence as it can bypass the authentication and integrity solutions proposed by the IEC 62351-6 standard, aimed at securing IEC 61850. The spoofed GOOSE can disconnect circuit breakers, while fabricated SV can maliciously trip relays and/or disable IED protection functionality, as shown in our previous work [6].

2.4 Cyber Attack Scenarios

This section focuses on two cyber attack scenarios targeting both IEC 61850 and Ripple20. The former spoofs IEC 61850 SV to maliciously induce trip conditions. On the other hand, the latter exploits Ripple20 to inhibit protection device functionality, in addition to causing a busbar fault.

2.4.1 Cyber Attack Scenario 1: The SV protocol within the IEC 61850 defines the specific communication service for the exchange of fundamental system measurements, i.e., voltages and currents to IEDs and relays, digitised at the source through merging units. These measurements are used for substation protection and automation applications at sampling rates of 80 or 256 samples/cycle. Distributed energy resources such as PV plants and windfarms connected to the distribution network are equipped with interface protection that includes underfrequency and Rate of Change of Frequency (ROCOF). If the measured system frequency f_{meas} goes below specified threshold for a certain time duration t_{set}, the protection relay issues a trip command to the generator circuit breaker via GOOSE. Therefore, an adversary can capture legitimate SV traffic and process the instantaneous measurements to reconstruct the voltage waveform indicated in Fig. 2 as nominal. Based on this, the adversary can then fabricate a voltage waveform with the same amplitude but shifted in phase, as indicated in Fig. 2.

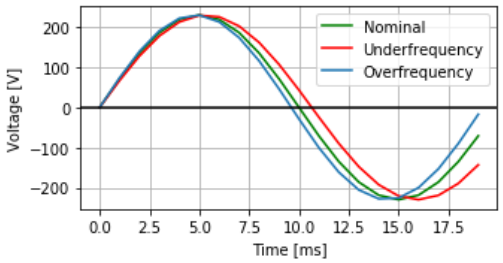

Fig. 2 Voltage waveforms for different frequency conditions

If recreated over multiple cycles, this results in a sustained artificial underfrequency condition. The fabricated waveform is sampled at the same rate and the resulting samples are encapsulated into spoofed SV data frames. These are injected via the network switch, targeting the underfrequency relay, causing it to trip. Therefore, by carefully manipulating the communicated SV measurements, relay trip commands are maliciously induced via GOOSE, causing embedded generation to trip on fabricated underfrequency conditions.

2.4.2 Cyber Attack Scenario 2: Substation interlocking schemes ensure that the control of any primary equipment does not lead to equipment damage or endanger workers. An example is to prevent the opening of a disconnector while the circuit breaker is closed. Consider a two-busbar single breaker arrangement with two feeder bays and a coupler, as depicted in Fig. 3. The software-based interlocking exchanges information between bay control units of the coupler and feeders. The coupler BCU informs the feeder BCUs when the coupler is closed. If this condition is met, disconnectors may always be operated in the feeder bays, even if the circuit breakers of the feeders are closed. Beside hardwiring, interlocking schemes within a digital substation can also be implemented through GOOSE. A successful attacker can spoof the GOOSE messages between the coupler and feeder BCUs by exploiting Ripple 20. More specifically, the adversary executes code on the coupler BCU and fabricates GOOSE data frames that indicate the coupler CB is closed, when in fact it is open. Subsequently, interlocking is made inactive, allowing feeder disconnectors to be opened while their CBs are closed.

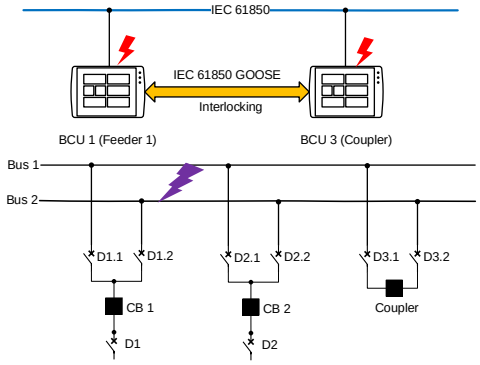

Fig. 3 Cyber attack targeting interlocking scheme

An attacker with access to bay level IEDs can exploit Ripple20 vulnerabilities to achieve a twofold objective. Firstly, the attacker executes remote code on the compromised BCUs to manipulate software-based interlocking schemes and put multiple relays out of service, disabling all protection functionality in the substation. Secondly, the attacker fabricates GOOSE messages to open disconnectors on load [6]. This inadvertent opening of a line disconnector on heavy load will result in an electric arc that can lead to sustained busbar faults.

3 Experimental Results

This section presents the simulation results for the two cyber attack scenarios carried out on the IEEE 39-bus test system, which includes two 345 kV/110 kV TSO-DSO interface substations at buses 30 and 5, as indicated in Fig. 4.

3.1 Cyber Attack Scenario 1

The generator at bus 30 represents a 100 MW PV power plant connected to the distribution network. The cyber attack targets the interface protection of the power plant exploiting IEC 61850 SV vulnerabilities to mimic a sustained underfrequency condition, as presented in Fig. 5. Hence, the frequency relay disconnects the PV plant leading to a loss of generation, which can impact transmission system operation.

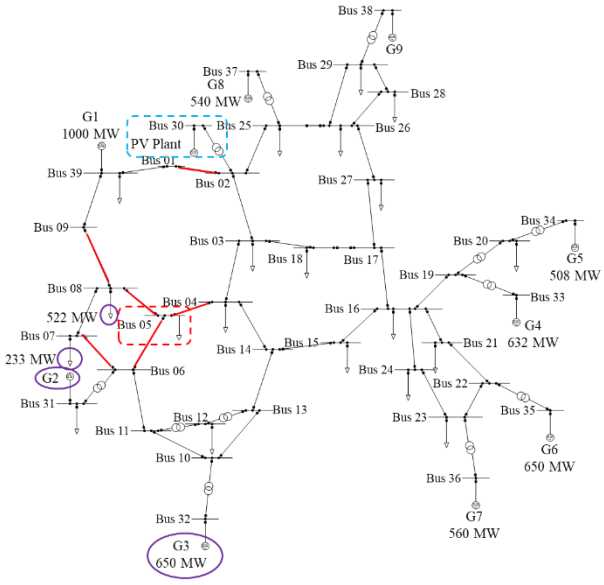

Fig. 4 IEEE 39-bus test system

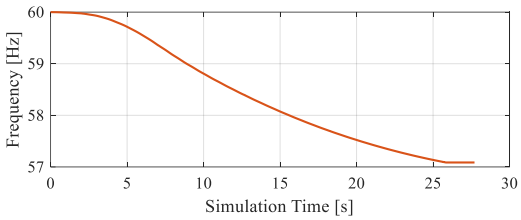

Fig. 5 Attack scenario 1: fabricated underfrequency condition

3.2 Cyber Attack Scenario 2

The cyber induced busbar fault shown in Fig. 6 is permanent in nature as substation protection is disabled. Line 06-07 is then tripped by distance protection. As the busbar fault is not cleared yet, generation continues feeding into the fault. Consequently, generators 2 and 3 are disconnected on ROCOF as it exceeds the setting of 2 Hz/s over 500 ms, as seen in Fig. 7. Lines 04-05, 05-06, 05-08 are then tripped by distance protection, which clear the fault, thereby disconnecting the entire substation. Next, lines 01-02 and 08-09 are disconnected by distance protection, leaving one area unsupplied. This causes a drop in system frequency, activating underfrequency load shedding. In summary, the cyber attack on the distribution substation causes cascading failures in the transmission system, culminating in a power outage of nearly 750 MW.

4 Conclusions and Recommendations

This paper discusses the emergence of Ripple20 vulnerabilities and threats to compromise power grid cyber security and impact system operation. We present how Ripple 20 vulnerabilities can be exploited to penetrate critical OT networks and compromise IIoT and OT devices in substations. Consequently, adversaries may carry out advanced cyber

attacks, induce cascading failures, and cause a blackout. This is of alarming consequence, considering the increasing trend of cyber attacks on critical infrastructures.

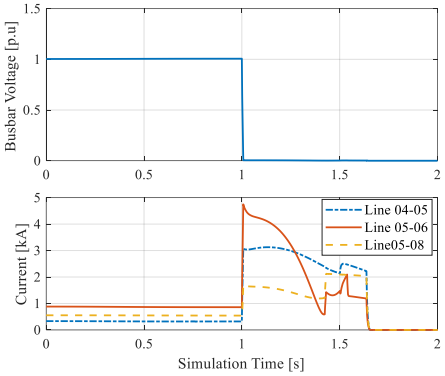

Fig. 6 Cyber-physical attack resulting in a busbar fault

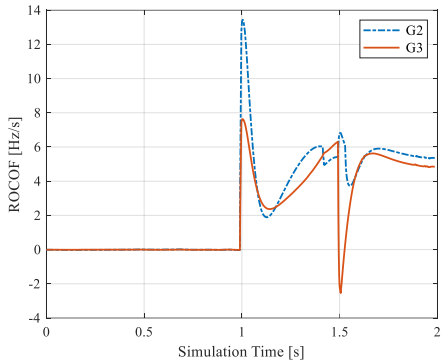

Fig. 7 Generation trip on abnormal ROCOF

Table 1 Cascading failures in attack scenario 2

No	Time [s]	Event
1	0s	Start of simulation.
2	1 s	Cyber attack results in a permanent busbar fault, as substation protection is disabled.
3	1.4 s	Line 06-07 from neighbouring substation is tripped due to distance protection.
4	1.5 s	Generators 2 and 3 are disconnected due to abnormal ROCOF conditions.
5	1.6 to 1.7 s	Lines 04-05, 05-06, and 05-08 are tripped by distance protection, clearing the fault.
6	1.8 to 3.3 s	Lines 01-02 and 08-09 are disconnected by distance protection, leaving one area unsupplied.
7	5 to 7 s	Drop in system frequency activates underfrequency load shedding in increments of 5.9, 6.5 and 6.7 %.
8	20 s	End of simulation. Cyber attack results in a loss of load of 750 MW.

It is recommended that system operators deploy SCADA in the cloud as a backup to traditional SCADA systems. This can ensure redundancy, while offering enhanced resilience against cyber threats. We also recommend the adoption of the IEC 62351-6 standard to ensure authentication and message integrity of end-to-end devices within digital substations. Additionally, DSOs must keep track of up-to-date security policies and procedures, especially processes and tools for authentication and revise them periodically. This can minimise the risk of major cyber-related threats. The increased risk of supply chain attacks includes non-native components with open-source software and networking stacks that may contain multiple loopholes. Hence, we call for a generic procedure to periodically validate the cyber security of such software and stacks, adopted across multiple industry sectors.

Possible mitigation measures to prevent the discussed attack tactics include ensuring encryption and authentication access for feeder poles containing RC units with communication capabilities. The system should be regularly audited for cyber security, as per policy mandated regulations. To prevent techniques such as lateral movement, security controls such as firewalls must be kept up to date. Furthermore, deployment of intrusion detection and Security Information and Event Management (SIEM) systems can also help in prevention of lateral movement. To mitigate command and control actions, authentication mechanisms through IEC 62351-6 must be implemented within substations, in addition to screening and validation of software and networking stacks currently in use. In conclusion, we are witnessing an increase in awareness and mitigation of vulnerabilities and threats originating from supply chain risks in the energy domain, mainly driven by vendors, consultants, and new technology adoption by utilities.

5 Acknowledgement

This work is part of the DeSIRE program of the 4TU Centre for Resilience Engineering.

6 References

[1] R. Lee et al, “Analysis of the Cyber Attack on the Ukrainian power grid,” Electricity Information Sharing and Analysis Center (E-ISAC) Tech Report, pp. 1–26, Mar 2016.

[2] R. Lee et al, “Modular ICS Malware,” Electricity Information Sharing and Analysis Center (E-ISAC) Tech Report, pp. 1–27, Aug 2, 2017.

[3] M. Kol and S. Oberman, “CVE-2020-11896 RCE and CVE-2020-11898 Info Leak,” JSOF Inc. White Paper, pp. 1-27, June 2020. Accessed: Feb 07, 2021. [Online]. Available: https://www.jsoftech.com/wpcontent/uploads/2020/06/JSOF_Ripple20_Technical_Whitepaper_June20.pdf

[4] International Electrotechnical Commission. Communication Networks and Systems for Power Utility Automation - Part 5: Communication Requirements for Functions and Device Models. IEC 61850-5, 2013.

[5] T. A. Youssef et al, "IEC 61850: Technology Standards and Cyber-Threats," in *Proc IEEE Int Conf on Environment and Elect Engg*, Florence, Italy, Jun 2016, pp. 1–6.

[6] V. S. Rajkumar et al, "Cyber Attacks on Power System Automation and Protection and Impact Analysis," in *Proc IEEE PES Innovative Smart Grid Tech Conf Europe*, The Hague, Netherlands, 2020, pp. 247-254.

[7] MITRE ATT&CK. MITRE Corp. Accessed: Feb 07, 2021. [Online]. Available: https://attack.mitre.org/

[8] A. Lonzetta et al, “Security Vulnerabilities in Bluetooth Technology as Used in IoT,” *J. Sens. Actuator Net.*, vol. 7, no. 3, p. 28, Jul 2018.