Threat Scenario Generation for IEC104 Cyber Defense

Heinrihs Kristians Skrodelis, Bernhards Blumbergs, Andrejs Romanovs

Threat Scenario Generation for IEC104 Cyber Defense

Heinrihs Kristians Skrodelis
Dept. of Modeling and Simulation
Riga Technical University
Riga, Latvia
ORCID: 0000-0002-6453-5982

Bernhards Blumbergs
Laboratory for Cyber Resilience
Nara Institute of Science of Technology
Nara, Japan
ORCID: 0000-0001-9679-6282

Andrejs Romanovs
Dept. of Modeling and Simulation
Riga Technical University
Riga, Latvia
ORCID: 0000-0003-1645-2741

***Abstract*— The Industrial Control Systems (ICS) that govern critical infrastructure are increasingly targeted by cyber threats, particularly through communication protocols such as IEC 60870-5-104 (IEC104). This research paper focuses on enhancing the cybersecurity of ICS utilizing the IEC104 protocol, which is pivotal in Europe's critical infrastructure. Through a comprehensive literature review of previous IEC104 attacks, the study establishes a detailed understanding of the threat landscape. This foundational knowledge is utilized to develop realistic threat scenarios, which are developed for generating a labeled dataset for training machine learning models aimed at attack detection and prevention. The research methodology includes a thorough analysis of historical attack vectors. The outcomes are expected to significantly contribute to the robustness of critical infrastructure against cyber threats.**

Keywords—Industrial Control Systems, IEC 60870-5-104, cybersecurity, threat scenarios, critical infrastructure, cyber attacks

I. INTRODUCTION

ICS play a crucial role in the operation and management of critical infrastructure, such as power plants, water treatment facilities, and transportation systems. IEC104 protocol is a widely used communication standard in powergrid supervision and automation, which makes it an attractive target for cyber attackers. Ensuring the security of ICS is of paramount importance, as successful attacks can have direct consequences on public safety, the environment, and the economy. In recent years, machine learning (ML) techniques have emerged as a promising approach to improve ICS cybersecurity by detecting and preventing cyber attacks. However, the development of effective ML solutions requires robust datasets, which necessitate the creation of realistic threat scenarios [1]. This research serves as a crucial first step in this process by developing a sophisticated threat scenario, enabling the generation of comprehensive datasets necessary for training ML-based security solutions.

The decision to concentrate on IEC104 in this study stems from its extensive deployment in critical infrastructure networks across Europe, coupled with a noticeable uptick in cyber threats aimed at this specific protocol. Safeguarding systems that utilize IEC104 is not merely a technical hurdle but also a societal necessity. Successful cyber-attacks on such systems could have devastating impacts, jeopardizing public safety, environmental well-being, and economic stability.

However, the existence of IEC104 itself represents a limitation, constituting a significant research gap. This recognition underscores the importance of our study in addressing this limitation and contributing to a comprehensive understanding of the vulnerabilities and potential mitigations associated with IEC104 in critical infrastructure networks.

The primary contributions of this research are:

• Comprehensive analysis of past attacks on IEC104 to support realistic threat scenario generation.

• Development of threat scenarios tailored for IEC104 based ICS environments to create a labeled dataset suitable for training ML models.

The research methodology comprises several key phases. First, we analyze past attacks on IEC104 systems. After that, we carefully describe the profile of possible attacker. Lastly, we create a detailed attack scenario.

In research [2] authors tested the hypothesis that IEC-60780-5-104 has a lot of spontaneous communications which are not possible to include in simulated traffic. The results showed that emulated datasets are prone to simple and regular patterns and there is a room for improvement of emulated datasets, such as more detailed and complicated system configurations or adding random events to the process simulators.

In the current cybersecurity landscape, time has become the new currency for both defenders and attackers. As studies indicate, prompt detection and swift response can drastically minimize the damage caused by a security breach. Moreover, the adoption of ML and automation has proven to be a cost-effective strategy [3]. However, it is crucial that the response not only be quick but also correct, as false positives need to be minimized as much as possible. Therefore, a well-constructed threat scenario is needed to assure that realistic datasets are acquired to ensure defenses are both effective and efficient.

II. RELATED WORK

Due to the mostly proprietary nature of SCADA network protocols, there is a lack of openly available datasets. This section discusses ongoing initiatives in creating datasets for ICS, with a focus on the utilization of the IEC104 protocol. To effectively combat cybersecurity threats, it is imperative for security researchers to have access to non-sensitive, yet authentic datasets that mirror real-world environments. These datasets are crucial for enhancing and evaluating the efficacy of defensive strategies.

In pursuit of relevant data, we conducted a systematic search using keywords such as "IEC104 dataset," "SCADA dataset," and "ICS dataset," which yielded a limited number of results. Among the datasets discovered, Westring et.al. [4] is notable for its inclusion of 12 distinct network attacks targeting the IEC104 protocol. These attacks were executed

within a virtual testbed environment, providing a controlled setting for analysis. However, the labeled dataset is constrained in scope, with each attack's packet capture (PCAP) file comprising approximately of a small number of 6000 packets.

Radoglou-Grammatikis et.al. [5] published a labeled dataset that is particularly focused on cybersecurity threats related to the IEC104 protocol, including DoS and unauthorized commands. This dataset is comprised of 12 different cyberattacks, with each corresponding packet capture (.pcap) containing at least 60000 packets. This larger dataset offers a more extensive foundation for testing and improving intrusion detection systems in the context of SCADA environments, making it a valuable addition to the limited datasets.

Maynard et.al. [6] published a dataset with IEC104 MITM and reconnaissance attacks, but it is not labeled. This dataset adds to the available resources by providing specific examples of MITM attacks and reconnaissance activities targeting the IEC104 protocol.

Additionally, a recent study by Arifin et.al. [7] introduced a dataset featuring three attacks, including port scan, brute force, and DoS. However, this dataset lacks detailed information on the testbed construction, revealing only that it's a physical testbed, and the attacks are carried out using the Kali Linux operating system.

The entirety of the executed attacks took place within virtual environments and is considered a signifcant drawback. In this reasearch, authors aim to develop a dataset rooted in actual systems. Results presented by Al-Hadhrami et.al. [8] show that traffic attributes which exist in emulated datasets may be not valid in real datasets. The ultimate objective is to integrate this dataset into a real-world environment rather than a simulated one. Hence, the need for a real dataset is even more emphasized. Consequently, none of the existing datasets align with the specific needs of our research.

III. Attacks on SCADA Systems

The literature review section offers a summary of prior studies concerning IEC104 attack patterns. This examination assists in pinpointing areas where existing research may be lacking and lays the groundwork for our own investigation. We carried out the literature review by conducting a comprehensive search for scientific articles and industry reports, employing a snowball approach with keywords "IEC104 cyberattacks" and "ICS/SCADA cyber attacks".

In SCADA systems, malicious attackers primarily aim to either disable the system or cause damage to the system by transmitting malformed data or commands, leading to communication disruptions or malfunction. The vulnerability of IEC104-based SCADA systems is heightened due to their interconnected nature within smart grids and their reliance on unencrypted protocols [9]. The communication channel between the Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) is particularly vulnerable to attacks in SCADA networks as they are considered as a trusted environment. This is where protocols such as IEC101 and IEC104 are utilized for data acquisition and control [10].

The research by Rakas et.al. [11]presents a summary of 26 studies conducted on evaluating SCADA intrusion detection systems through simulated attacks. These studies used various testbeds, datasets, and attack simulations, including real systems controlling electric power supply. The datasets used range from real traffic recordings to synthetic and experimental datasets. The most commonly used simulated attacks across the studies are denial of service (DoS) attacks, reconnaissance, protocol specification violation, man-in-the-middle (MITM) attacks, and SCADA-specific attacks.

Kaspersky report [12] presents a brief overview of key incidents in industrial cybersecurity in 2023, with a focus on notable events within the power and energy sectors.

One notable incident involved Aker Solutions, a Norwegian service provider for the energy industry, whose Brazilian subsidiary, CSE Mechanical and Instrumentation, fell victim to ransomware. The attackers, claiming access to the company's IT systems, encrypted digital files, and locked access to data. Similarly, ABB, a Swedish-Swiss electrical equipment manufacturer, experienced a ransomware attack, with the Black Basta ransomware group targeting its Windows Active Directory. Notably, ABB terminated VPN connections to prevent further spread. In India, Madhya Pradesh Power Management Company Limited (MPPMC) faced a ransomware attack, leading to immediate actions following government guidelines. Qulliq Energy Corporation in Canada and Hitachi Energy in Japan also encountered cyberattacks affecting their systems, with the latter experiencing data theft through a zero-day vulnerability.

A common theme across the described cyberattacks is the prevalence of ransomware. In most of the cases, the organizations faced a threat where malicious actors gained unauthorized access to their IT systems, encrypted digital files, and demanded a ransom for the restoration of access or the prevention of data leaks.

In the MITRE ATT&CK framework tailored for ICS [13], various 'techniques of attack' are systematically organized under a series of 'tactics for attack.' These tactics define the sequential stages involved in a cyber-attack and are officially categorized as: Initial Access, Execution, Discovery, Collection, Inhibit Response Function, Impair Process Control, and Impact. To enrich the scope of our study, we will employ a tabular structure to classify all documented attacks found in both academic literature and industry publications. Furthermore, we will identify whether each attack is specifically targeting the IEC104 protocol or has a wider applicability. Although there are other versions of the MITRE ATT&CK framework, such as the Enterprise edition, these are only pertinent to the initial phases of an ICS attack. Given that our research assumes the attacker has already breached the network, such frameworks will not be considered in our analysis.

A. Past Attack Scenarios

In our research, we conducted a comprehensive analysis of various attacks documented in both scientific literature and industry reports. Our objective was to illuminate the range of threats targeting the IEC104 protocol and to identify associated attack vectors. Through this investigation, we identified 14 attack scenarios. These scenarios are summarized in Table 1, along with their corresponding MITRE ATT&CK IDs.

Scenario 1: In the Industroyer attack, also known as Crash Override, a sophisticated malware targeted Ukraine's power grid in 2016. This unprecedented cyber warfare disrupted the electricity distribution network in Kyiv. Industroyer exploited

vulnerabilities in power grid protocols, communicating directly with switches and circuit breakers. It used a range of payload components to map the network, decompile firmware, reprogram settings, and execute commands, all while disrupting telecommunications services. [14], [15], [16].

Scenario 2: The Triton incident, also called Trisis, occurred in 2017 at a Saudi petrochemical plant. Attackers exploited a zero-day vulnerability to target Schneider Electric's Triconex Safety Instrumented System. Their aim was to reprogram the controls, potentially causing a catastrophic incident. However, their actions inadvertently triggered a shutdown, revealing their presence [15], [17]

Scenario 3: LockerGoga, a ransomware incident in 2019, targeted industrial and manufacturing companies, with Norsk Hydro suffering significant losses. LockerGoga infiltrated networks via phishing emails or vulnerabilities, encrypting files and changing user passwords. Attackers manually deployed the ransomware, carefully selecting their targets [18]

Scenario 4: The REvil or Sodinokibi ransomware affected JBS Foods in 2021, leading the company to pay a ransom of 11 million dollars. Attackers exploited phishing or software vulnerabilities, escalated access rights to administrative privileges, and encrypted files. A ransom note demanded payment in cryptocurrency for a decryption key [19]

Scenario 5: The Conficker incident in 2008 targeted millions of systems globally by exploiting vulnerabilities in Windows OS. This malicious worm propagated using weak passwords and unpatched flaws. It formed a botnet, restricted cybersecurity access, and updated itself through complex peer-to-peer (P2P) methods, causing substantial damage [20]

Scenario 6: In the Maroochy Water Breach of 2000, a disgruntled ex-employee attacked sewage systems by exploiting vulnerabilities in wireless SCADA controls. Over two months, the attacker issued commands that released raw sewage into public areas while manipulating alarm parameters to avoid detection. This incident is a landmark case in cybercrime due to its scale and sophisticated techniques [21]

Scenario 7: The Bad Rabbit ransomware attack in 2017 targeted organizations in Russia and Ukraine. Attackers used vulnerabilities in the Server Message Block protocol (SMB) to spread their ransomware. Masquerading as an Adobe Flash installer, Bad Rabbit encrypted victims' data files and demanded a ransom for decryption. It also employed powerful exploits to spread laterally across networks [22].

Scenario 8: The EKANS ransomware, also known as Snake, emerged in 2019, specifically targeting industrial control systems. It disrupted processes by forcibly halting multiple operations and encrypting files, causing serious production shutdowns and financial losses [23].

Scenario 9: The NotPetya cyber attack in 2017, believed to be initiated by the Russian military, exploited vulnerabilities in Ukrainian tax software. Initially disguised as ransomware, it turned out to be a destructive wiper, spreading rapidly and causing billions of dollars in damages across various institutions [22], [24].

Scenario 10: The Stuxnet Worm attack in 2010, believed to be a US-Israel joint operation, targeted Iran's nuclear program. This advanced malware abused a set of zero day vulnerabilities and manipulated nuclear centrifuges, causing significant damage while remaining undetected. It is a landmark case due to its scale, sophistication, and successful targeting of national infrastructure [25].

Scenario 11: The BlackEnergy malware and KillDisk tool, used in high-profile cyberattacks in 2015, was notorious for deleting or overwriting data, incapacitating computers, rewriting BIOS code, and tampering with the Master Boot Record (MBR). Its impact was substantial, with the power outage at a Ukrainian substation drawing considerable attention[26]

Scenario 12: The Ryuk ransomware attack in 2019 was led by the hacker group Grim Spider. They targeted healthcare institutions, demanding exorbitant ransoms to decrypt data. Their tactics involved spear-phishing, exploiting vulnerabilities, and escalating privileges. Ryuk posed severe threats to critical infrastructure and operations [27].

Scenario 13: The CosmicEnergy tool is an advanced OT/ICS-oriented malware designed to disrupt electric power systems. It is known for its ability to infiltrate and manipulate critical infrastructure control systems. Cybercriminals employ it to compromise power distribution, which can lead to prolonged power outages [28]

Scenario 14: Industroyer.V2 is a variant of the original Industroyer malware, customized to target intelligent electronic devices within power grid operations. Its unique capabilities pose significant threats to electric power systems. Industroyer.V2 uses a variety of attack techniques to infiltrate and compromise ICS, causing widespread disruption [29].

TABLE I. PAST ATTACK SCENARIO ID'S

Scenario ID	MITRE ATT&CK IDs
1	T0800, T0801, T0802, T0803, T0804, T0805, T0806, T0807, T0809, T0813, T0814, T0815, T0816, T0827, T0829, T0831, T0832, T0837, T0840, T0846, T0855, T0881, T0884, T0888
2	T0820, T0821, T0834, T0843, T0845, T0846, T0849, T0853, T0857, T0858, T0868, T0869, T0871, T0872, T0874, T0880, T0885, T0890
3	T0827, T0828, T0829
4	T0828, T0849, T0853, T0863, T0869, T881, T0882, T0886
5	T0826, T0828, T0847
6	T0813, T0815, T0836, T0838, T0855, T0856, T0878, T0879
7	T0828, T0863, T0866, T0867
8	T0828, T0840, T0849, T0881
9	T0828, T0866, T0867
10	T0801, T0807, T0821, T0831, T0832, T0834, T0835, T0836, T0842, T0843, T0847, T0849, T0851, T0863, T0866, T0867, T0869, T0873, T0874, T0877, T0885, T0886, T0888, T0889, T0891
11	T0809, T0829, T0872, T0881
12	T0828

13	T0807, T0809, T0831, T0855
14	T0801, T0802, T0806, T0836, T0855, T0881, T0888

B. Attack Techniques

These scenarios demonstrate the breadth and complexity of cyberattacks on industrial control systems and critical infrastructure. By visually representing the technique IDs in Fig. 1 below, we can discern the historical prevalence of attack methods. Notably, a few distinctly stand out: T0828 (Loss of Productivity and Revenue), occurring in 7 out of 12 scenarios, T0881 (Service Stop) in 5 scenarios, and T0849 (Masquerading), T0855 (Unauthorized Command Message), and T0888 (Remote System Information Discovery) in 4 scenario instances each.

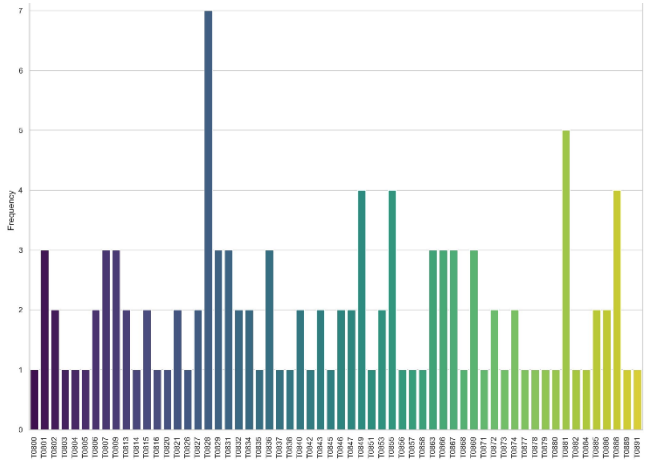

Fig. 1. Frequency of Technique IDs

Within the wide array of cyberattack scenarios analyzed, it is noteworthy that only a minority specifically targeted the IEC104 protocol, but it does not diminish its potential to inflict an incapacitating effect on European power grids. Specifically, only 3 out of the 14 scenarios discussed: Scenarios #1 (Industroyer attack), #13 (CosmicEnergy tool), and #14 (Industroyer.V2) were identified as having the IEC104 protocol as their direct focus. The original Industroyer attack compromised the Ukrainian power grid by exploiting protocol vulnerabilities, while CosmicEnergy and the evolved Industroyer.V2 malware posed sophisticated threats to industrial control systems through similarly specialized means.

In these 3 attacks, tactics mentioned at least 2 times were: T0801 (Block Command Message), T0802 (Block Reporting Message), T0806 (Brute Force I/O), T0807 (Denial of Control), T0809 (Data Destruction), T0831 (Manipulation of Control), T0855 (Unauthorized Command Message), T0881 (Service Stop), and T0888 (Change Operating Mode).

The descriptions of the real cases, employed methods and techniques, and identified tactics will serve as the foundation for IEC104 specific attack scenario development.

IV. The Setup

Most studies simulate network infrastructures and introduce a high level of artificiality due to the high equipment costs, required in-depth technical knowledge, and potential legal issues involved. Author's employ an environment consisting of real devices and industrial protocols, which provides a high novelty and significant contribution.

Fig. 2. ICS lab with stations [30]

The authors implement and execute the developed threat scenario in the industrial automation and control system (IACS) environment as described by Kelle [30]. This environment is developed and maintained by the Information Technologies Security Incident Response Institution of the Republic of Latvia (CERT.LV) and is a homogeneous representation of the Latvian national energy grid consisting of gas and electrical energy sectors. The environment is based on the actual devices, software components, and industrial communication protocols as used in the energy grids representing their operational processes as close to the real production OT environment as possible. The modular components are displayed in Fig. 2. and represents the following functional stations (in clockwise order as presented in the figure):

Station 1.1: represents the natural gas transmission lines, flow control, and supervisory management. This station relies on following communication protocols – RS232 serial bus, RS485 parallel bus, and Modbus and Modbus-TCP.

Station 1.2.: represents the natural gas distribution lines, flow control, and supervisory management. Functionality level and used protocols are similar to station 1.1., but varies from the hardware and their interconnectivity design perspective.

Station 2: represents the underground gas storage and extraction. This station depends on gas transmission and import station 1.1., and distribution station 1.2., to ensure the collection of gas and its extraction for use in electrical energy production. This station employs PROFIBUS and PROFINET industrial protocols.

Station 5: emulates the electrical energy production by the gas turbines. This station functions if there is a flow of gas from transmission or distribution network, or as long as there is gas in underground storage. This station uses the IEC104 protocol for supervision and control communications with the SCADA system.

Station 3: represents the electrical energy transmission grid (TSO), its supervision, and control and management. This station uses optical token ring for near-real time communications between the power relays with IEC-61850 protocol suite, and industrial Ethernet with IEC104 communications with SCADA system.

Station 4.1.: represents the electrical energy distribution grid (DSO), its supervision, and control and management. This station employs the same communication protocols as station 3 with a different set of devices used for automation, protection, and industrial Ethernet management. This substation is one of the electrical energy supply points for the gas storage station 2. In case both electrical supply points fail, the gas distribution and storage is halted, having a cascading impact on electrical energy production and the rest of the energy system.

Station 4.2: similarly to station 4.1., represents electrical energy transmission substation. Although conceptually similar, the stations 3, 4.1. and 4.2., use a different set of devices as used in real production environment and implements different communication topologies and engineering approaches for redundancy and failover protection. This station is one of the electrical supply points for the gas storage station 2.

Station CTRL ST: Is the centralized SCADA workstation for visual HMI representation of the overall energy grid, its supervision and control. This MS WIndows workstation is based on Wonderware software and employs a set of drivers and wrappers to ensure the support for all employed supervisory protocols. This station allows duplex interaction with every station to ensure full supervisory control and data acquisition.

V. Final Scenario

Based on a thorough analysis of the most frequent techniques, as outlined in Table 1, we curated a selection that pertains exclusively to network activity, as system-related methods have no direct impact on network traffic. From the comprehensive array of techniques available, we pinpointed 18 techniques that are network-centric, encompassing *T0800, T0803, T0804, T0805, T0814, T0820, T0834, T0840, T0842, T0843, T0851, T0855, T0856, T0858, T0866, T0867, T0884*, and *T0888*. To refine the attack scenario while preserving specificity and relevance, we conducted an additional filter, prioritizing techniques based on their frequency of occurrence.

In all three cyberattacks targeting IEC104 (scenarios #1, #13, and #14), the incidents involved the following attack techniques, each occurring at least twice: *T0801* (Monitor Process State), *T0802* (Automated Collection), *T0806* (Brute Force I/O), *T0807* (Command-Line Interface), *T0809* (Data Destruction), *T0831* (Manipulation of Control), *T0855* (Unauthorized Command Message), *T0881* (Service Stop), and *T0888* (Remote System Information Discovery). It is noteworthy that all of these tactics, with the exception of *T0881* and *T0807*, are applicable to IEC104 network based IDS, while *T0807* and *T0881* is host-related and will not be considered in the subsequent scenario analysis.

By referencing Fig. 1, which illustrates all the techniques applied across various ICS scenarios, it becomes evident that three of these attacks consistently ranked among the top five most frequent ones. Specifically, *T0855*, *T0881*, and *T0888* emerged as the most prevalent also they were also identified as the most popular attacks in IEC104-specific incidents. The remaining two, *T0828* (Loss of Productivity and Revenue) and *T0849* (Masquerading), have unique characteristics. *T0828* is an outcome of the attack, where the specific attack technique is less crucial, while *T0849* involves file renaming—a task beyond the scope of network based IDS.

Delving deeper and examining the general ICS attacks (those distinct from the IEC104-specific incidents) that occurred at least three times, we've compiled the list presented in Table 2.

TABLE II. General Attack Applicability to IEC104

ICS MITRE ATT&CK ID	**IEC104 Applicability**
T0801 (Monitor Process State	Applicable
T0807 (Command-Line Interface)	Applicable, but host related
T0809 (Data Destruction)	Applicable, but host related
T0829 (Loss of View)	Applicable, but host related
T0831 (Manipulation of Control)	Applicable
T0836 (Modify Parameter)	Applicable
T0863 (User Execution)	Applicable, but host related
T0866 (Exploitation of Remote Ser-vices)	Applicable, but host related
T0867 (Lateral Tool Transfer)	Applicable, but host related
T0869 (Standard Application Layer Protocol)	Applicable

Many of the analyzed ICS attack techniques find limited relevance in the context of network based IDS development, as they mostly pertain to system processes like command-line execution and manipulation of files. Consequently, only 3 from the ICS attack techniques prove applicable to IEC104 within this scope: *T0831* (Manipulation of Control), *T0836* (Modify Parameter) and *T0869* (Standard Application Layer Protocol). With the integration of these 3 ICS attacks into the previously mentioned set of 5 IEC104 attack techniques, the comprehensive lineup is presented in Table 3.

This approach ensures that our scenario remains focused and effectively tailored to network-centric threats, encompassing both the most frequent attacks specific to IEC104 and other ICS protocols. While there might not be an abundance of IEC104 attacks, given its lesser popularity among threat actors, the inclusion of generic attacks, which could also be applicable to IEC104, becomes a notable aspect. This observation serves as a significant strength for our research, highlighting a research gap that needs attention. As attacks may potentially be executed, it underscores the necessity for proactive defenses to be in place.

TABLE III. FINAL ATTACK SCENARIO

No.	MITRE ID	Technique Name	Tactic
1	T0888	Remote System Information Discovery	Discovery
2	T0801	Monitor Process State	Collection
3	T0802	Automated Collection	Collection
4	T0869	Standard Application Layer Protocol	Command and Control
5	T0806	Brute Force I/O	Impair Process Control
6	T0836	Modify Parameter	Impair Process Control
7	T0855	Unauthorized Command Message	Impair Process Control
8	T0831	Manipulation of Control	Impact

The attack simulation will follow the MITRE ATT&CK steps, starting from the point where the attacker has successfully infiltrated the network. Our simulation will begin with the Discovery stage, adhering to the logical sequence of tactics. The techniques are arranged systematically in accordance with the framework. Specifically, the final two techniques belong to the Impact tactic, representing the ultimate consequences of the attacks. Although these last techniques will not simulated, it is acknowledged that the overall scenario results would involve these impacts and potentially more.

VI. CONCLUSIONS AND FUTURE WORK

In this study, we have demonstrated the importance of real-world datasets over simulated ones for the evaluation of IDS in industrial automation and control systems (IACS). By simulating a threat scenario for a Latvian national energy grid, using real devices and industrial protocols, we have highlighted the deficiencies of emulated datasets, which often generate overly simplistic and regular data patterns. These limitations underscore the pressing need for the development of more intricate and dynamically updated datasets that can adequately represent the complexities of real world systems.

Our findings emphasize that real world data achieves higher accuracy and complexity, thereby offering a more reliable basis for testing and evaluating IDS. The integration of detailed configurations and random events into simulated network infrastructures holds the potential to enhance dataset realism.

This research also can serve as a guideline for generating threat scenarios applicable to various network protocols. By conducting thorough literature reviews of previous attacks, assigning appropriate MITRE ATT&CK framework IDs, and selecting the most frequent and applicable attack vectors, researchers can generate more relevant and diverse threat scenarios.

REFERENCES

[1] H. K. Skrodelis and A. Romanovs, "Synthetic Network Traffic Generation in IoT Supply Chain Environment," in 2022 63rd International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2022 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ITMS56974.2022.9937126.

[2] C.-Y. Lin and S. Nadjm-Tehrani, "A Comparative Analysis of Emulated and Real IEC-104 Spontaneous Traffic in Power System Networks," 2021, pp. 207–223. doi: 10.1007/978-3-030-69781-5_14.

[3] O. Nikiforova, A. Romanovs, V. Zabiniako, and J. Kornienko, "Detecting and Identifying Insider Threats Based on Advanced Clustering Methods," IEEE Access, vol. 12, pp. 30242–30253, 2024, doi: 10.1109/ACCESS.2024.3365424.

[4] E. Westring, A. Fundin, C.-Y. Lin, T. Gustafsson, and S. Nadjm-Tehrani, "RICSel21: A dataset with network attacks targeting IEC-60870-5-104 in SCADA systems." [Online]. Available: www.rics.se

[5] P. Radoglou-Grammatikis et al., "Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach," IEEE Trans Industr Inform, vol. 18, no. 3, pp. 2041–2052, Mar. 2022, doi: 10.1109/TII.2021.3093905.

[6] P. Maynard, K. McLaughlin, and S. Sezer, "An Open Framework for Deploying Experimental SCADA Testbed Networks," 2018. doi: 10.14236/ewic/ICS2018.11.

[7] M. A. S. Arifin, D. Stiawan, Susanto, J. Rejito, Mohd. Y. Idris, and R. Budiarto, "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, Oct. 2021, pp. 228–232. doi: 10.23919/EECSI53397.2021.9624255.

[8] Y. Al-Hadhrami and F. K. Hussain, "Real time dataset generation framework for intrusion detection systems in IoT," Future Generation Computer Systems, vol. 108, pp. 414–423, Jul. 2020, doi: 10.1016/j.future.2020.02.051.

[9] R. Kalluri, L. Mahendra, R. K. Senthil Kumar, G. L. Ganga Prasad, and B. S. Bindhumadhava, "Analysis of Communication Channel Attacks on Control Systems—SCADA in Power Sector," Lecture Notes in Electrical Engineering, vol. 487, pp. 115–131, 2018, doi: 10.1007/978-981-10-8249-8_11.

[10] D. Deb, S. R. Chakraborty, M. Lagineni, and K. Singh, "Security Analysis of MITM Attack on SCADA Network," Communications in Computer and Information Science, vol. 1241 CCIS, pp. 501–512, 2020, doi: 10.1007/978-981-15-6318-8_41.

[11] S. V. B. Rakas, M. D. Stojanovic, and J. D. Markovic-Petrovic, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems," IEEE Access, vol. 8, pp. 93083–93108, 2020, doi: 10.1109/ACCESS.2020.2994961.

[12] "H1 2023 – a brief overview of main incidents in industrial cybersecurity | Kaspersky ICS CERT." Accessed: Apr. 29, 2024. [Online]. Available: https://ics-cert.kaspersky.com/publications/reports/2023/10/05/h1-2023-a-brief-overview-of-main-incidents-in-industrial-cybersecurity/

[13] MITRE, "ICS Techniques." Accessed: May 20, 2024. [Online]. Available: https://attack.mitre.org/techniques/ics/

[14] Dragos Inc., "Analysis of the Threat to Electric Grid Operations".

[15] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems," in 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, Sep. 2020, pp. 1537–1543. doi: 10.1109/ETFA46521.2020.9212128.

[16] ESET, "WIN32/INDUSTROYER A new threat for industrial control systems," 2017.

[17] A. Di Pinto, Y. Dragoni, and A. Carcano, "TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, Its Communications and Its OT Payload".

[18] A. Adamov, A. Carlsson, and T. Surmacz, "An analysis of lockergoga ransomware," 2019 IEEE East-West Design and Test Symposium, EWDTS 2019, Sep. 2019, doi: 10.1109/EWDTS.2019.8884472.

[19] "REvil, A Notorious Ransomware Gang, Was Behind JBS Cyberattack, The FBI Says : NPR." Accessed: Apr. 29, 2024. [Online].

Available: https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says

[20] S. Shin, G. Gu, N. Reddy, and C. P. Lee, "A Large-Scale Empirical Study of Conficker," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 676–690, Apr. 2012, doi: 10.1109/TIFS.2011.2173486.

[21] J. Slay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in Critical Infrastructure Protection, Boston, MA: Springer US, pp. 73–82. doi: 10.1007/978-0-387-75462-8_6.

[22] A. S. Petrenko, S. A. Petrenko, K. A. Makoveichuk, and P. V. Chetyrbok, "Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), IEEE, Jan. 2018, pp. 945–949. doi: 10.1109/EIConRus.2018.8317245.

[23] Dragos Inc., "EKANS Ransomware and ICS Operations | Dragos Dragos." Accessed: Apr. 29, 2024. [Online]. Available: https://www.dragos.com/blog/industry-news/ekans-ransomware-and-ics-operations/

[24] R. A. Lika, D. Murugiah, S. N. Brohi, and D. Ramasamy, "NotPetya: Cyber Attack Prevention through Awareness via Gamification," in 2018 International Conference on Smart Computing and Electronic Enterprise (ICSCEE), IEEE, Jul. 2018, pp. 1–6. doi: 10.1109/ICSCEE.2018.8538431.

[25] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society, IEEE, Nov. 2011, pp. 4490–4494. doi: 10.1109/IECON.2011.6120048.

[26] McAfee Labs, "Analyzing KillDisk Ransomware, Part 1: Whitelisting | McAfee Blog." Accessed: Apr. 29, 2024. [Online]. Available: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/analyzing-killdisk-ransomware-part-1-whitelisting/

[27] CIS, "Security Primer – Ryuk." Accessed: Apr. 29, 2024. [Online]. Available: https://www.cisecurity.org/insights/white-papers/security-primer-ryuk

[28] Proska Ken, Zafra Daniel, and Lunden Keith, "COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises | Mandiant." Accessed: Apr. 29, 2024. [Online]. Available: https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response

[29] Zafra Daniel and Leong Raymond, "INDUSTROYER.V2: Old Malware Learns New Tricks | Mandiant." Accessed: Apr. 29, 2024. [Online]. Available: https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks

[30] R. Kelle and B. Blumbergs, "FURTHERING INDUSTRIAL CONTROL SYSTEM INTRUSION DETECTION SYSTEMS' ADVANCEMENT BY ANALYZING THE IEC 60870-5-104 PROTOCOL & ITS TRAFFIC," 2023.