Attacking IEC-60870-5-104 SCADA Systems

Panagiotis Radoglou-Grammatikis*, Panagiotis Sarigiannidis*, Ioannis Giannoulakis†
Emmanouil Kafetzakis†, Emmanouil Panaousis‡
* University of Western Macedonia, Kozani, Greece
† Eight Bells Ltd, Nicosia, Cyprus
‡ University of Surrey, Guildford, UK

***Abstract*—The rapid evolution of the Information and Communications Technology (ICT) services transforms the conventional electrical grid into a new paradigm called Smart Grid (SG). Even though SG brings significant improvements, such as increased reliability and better energy management, it also introduces multiple security challenges. One of the main reasons for this is that SG combines a wide range of heterogeneous technologies including Internet of Things (IoT) devices as well as Supervisory Control and Data Acquisition (SCADA) systems. The latter are responsible for monitoring and controlling the automatic procedures of energy transmission and distribution. Nevertheless, the presence of these systems introduces multiple vulnerabilities because their protocols do not implement essential security mechanisms such as authentication and access control. In this paper, we focus our attention on the security issues of the IEC 60870-5-104 (IEC-104) protocol, which is widely utilized in the European energy sector. In particular, we provide a SCADA threat model based on a Coloured Petri Net (CPN) and emulate four different types of cyber attacks against IEC-104. Last, we used AlienVault's rik assessment model to evaluate the risk level that each of these cyber attacks introduces to our system to confirm our intuition about their severity.**

***Index Terms*—SCADA security, Threat modelling, OSSIM, Coloured Petri Net, IEC-60870-5-104, Smart Grid**

I. Introduction

With the advent of the Internet of Things (IoT), the traditional electrical grid is transformed into a new paradigm called Smart Grid (SG) which combines Information and Communication (ICT) services with the conventional operations of the energy generation, transmission and distribution. According to [1], SG will probably be the largest example of the IoT technology, providing multiple benefits for both end-users and utility companies. Using SGs, the utility companies have the ability to monitor and control remotely all processes concerning the normal operation of the electrical grid, thus enhancing their overall business model. On the other side, energy consumers can monitor their energy consumption, resulting in more economical pricing and improving energy management.

Although SG offers multiple benefits, it also introduces significant cybersecurity challenges [2]. In particular, SG constitutes a large-scale network consisting of various heterogeneous technologies such as IoT and legacy systems making cybersecurity a complex problem to address. For instance, the constrained computing resources of IoT devices like smart meters hinder the adoption of conventional security measures such as asymmetric encryption mechanisms. Moreover, the vast amount of data generated by the various interconnections makes it more difficult to establish appropriate access control rules and policies. In the context of SG, the cyber attacks mainly aim at compromising the *availability* of systems and secondly their *integrity* and *confidentiality*. For instance, the various kinds of Denial of Service (DoS) attacks can disrupt the network functionality, thus resulting in disastrous consequences, such as power outage and blackouts. On the other side, the False Data Injection (FDI) attacks can compromise the data of smart meters, while the Man-in-the-Middle (MiTM) attacks compromise the data privacy.

An integral part of SG is the Supervisory Control and Data Acquisition (SCADA) systems that are responsible for monitoring and controlling automatic operations taking place in a transmission or a distribution substation [3]. The significant role of these systems, their constrained computing resources, as well as their legacy nature, making them an attractive target of cyber attackers. A successful cyber attack against SCADA systems may lead the adversary to control and affect the energy transmission and distribution functions. A characteristic example is the Stuxnet worm, which targeted the Iranian nuclear programme [4]. In addition, in 2015, Russian cyber attackers attacked a Ukrainian substation resulting in the power outage for more than 225,000 people [5].

There are many international communication standards utilized for the operation of SCADA systems. The most well-known are Modbus, Distributed Network Protocol (DNP3), Profinet, IEC-60870-5 and IEC-61850. In this paper, we focus on the security of the IEC-60870-5-104 [6] (i.e., IEC-104) protocol. In 1995, the International Electromechanical Commission (IEC) was released the IEC-60870-5-101 (i.e., IEC-101) protocol, which defines essential telecontrol messages between a logic controller and a controlling server. Six years later, IEC-104 was proposed. This combines the application messages of IEC-101 with the Transmission Control Protocol/Internet Protocol (TCP/IP), which itself introduces multiple security challenges. Thus, IEC-104's functionality is based on TCP/IP which itself presents various vulnerabilities. Moreover, the application data is exchanged without any authentication mechanism, i.e., as plaintext.

In this paper, we investigate the security of IEC-104, by emulating four cyber attacks based on a theoretic threat model which adopts a Coloured Petri Net (CPN). We also assessed the risk, that each of these cyber attacks poses to the system, using the AlienVault's risk assessment model and real-world

data values from the Common Weakness Enumeration (CWE) category system.

The rest of this paper is organized as follows. Section II discusses relevant works on IEC-104 security. Section III provides a background on SCADA systems, IEC 60870-104 security and Petri nets. Section IV describes a CPN-based threat model for SCADA systems. In Section V, we present the implementation of four different attack types against IEC-104 and we determine their associated risk level. Finally, Section VI concludes this paper by summarizing its main contributions and discussing ideas for future work.

II. Related Work

In [7] E. Hodo et al. present an anomaly-based Intrusion Detection System (IDS) for a SCADA simulated environment which utilizes the IEC-104 protocol. The authors create their own dataset which includes passive Address Resolution Protocol (ARP) poisoning attacks, DoS attacks and replay attacks that replace legitimate packets with malicious ones. Based on this dataset and utilizing the Waikato Environment for Knowledge Analysis (WEKA) tool, they evaluated multiple machine learning algorithms, such as Naive Bayes IBk, J48, Random Forest, OneR, RandomTree and DecisionTable. J48 and DecisionTable scored the best accuracy.

In [8], Y. Yang et al. provide signature and specification rules for the IEC-104 protocol, by using the Snort IDS [9]. After studying the security of the specific protocol, the authors deployed attack signatures and specification rules for the following attacks: 1) unauthorized read commands, 2) unauthorized reset commands, 3) unauthorized remote control and adjustment commands, 4) spontaneous packets storm, 5) unauthorized interrogation commands, 6) buffer overflows, 7) unauthorized broadcast requests and 8) IEC-104 port communication. The difference between the attack signatures and specifications is that the former compares monitored data with known cyber attack patterns, while the latter compares monitored data with normal behavior patterns.

In [10], Y. Yang et al. also provide a specification-based IDS for the IEC-104 protocol. The core of their system is named Detection State Machine (DSM) and its functionality is based on Finite State Machines (FSM) methodology. More detailed, the operation of IEC-104 is determined through the correlations of FSM. In contrast to the traditional FSM-based systems, their implementation applies a set of alarms that are capable of distinguishing the protocol malfunctions. To deploy and demonstrate their methodology, the authors employ the Internet Traffic and Content Analysis (ITACA) software [11]. Concerning, the evaluation results, the authors argue that the True Positive Rate (TPR) and False Positive Rate (FPR) of their IDS are calculated at 100% and 0% respectively.

Undoubtedly, all works mentioned above provide useful information and methodologies concerning the IEC-104 security. Our paper intends to complement these works, by 1) providing a threat model based on CPN for the SCADA system, 2) implementing four cyber attacks against IEC-104 and 3) deriving their risk levels using the AlienVault's risk assessment model.

III. Background

A. SCADA systems

SCADA systems mainly consist of 1) a Master Terminal Unit (MTU), 2) logic controllers, 3) communication interfaces and 4) a Human Machine Interface (HMI). MTU is a server which communicates with the logic controllers that in turn monitor the operations of the industrial environment by detecting and preventing possible malfunctions and anomaly states. Examples of logic controllers are Programmable Logic Controllers (PLC) and Remote Terminal Units (RTU). The communication interfaces refer to the industrial protocols utilized for the communication between MTU and logic controllers. Finally, HMI is a Graphical User Interface (GUI) application which is installed in MTU and used by a system operator to transmit commands to logic controllers and receive data from them. In this work, we focus on SCADA systems consisting of PLC controllers that in turn consist of: 1) Processor, 2) Input Modules, 3) Output Modules, 4) Communication Module, 5) Memory Module and 6) Power Supply. In particular, the Processor unit is the core of PLC, which has been programmed to implement various logic functions and send commands to the Output Modules based on the data received by the Input Modules. The Input and Output Modules denote the field devices in an industrial environment, such as sensors, motors and valves. Furthermore, it is clear that PLC needs some communication ports to exchange data with MTU or other PLCs and industrial modules. The Communication Modules of PLC are usually compatible with Recommended Standard (RS) 232, RS 233, RS 485, Ethernet and Wi-Fi. Finally, the Power Supply unit provides power to the Processor and the other modules.

B. IEC 60870-5-104 Security

The functionality of IEC-104 is based on the TCP/IP which exhibits a number of security issues. Although the IEC 62351 [12] standard provides solutions and guidelines that enhance the security of IEC-101 and IEC-104, the industrial nature of the SCADA systems using these protocols hinders their immediate upgrade. Consequently, besides the weaknesses of the TCP/IP, a severe security issue of IEC-104 is that the data at the application layer is transmitted without integrating encryption mechanisms, thus making it possible the execution of traffic analysis and MiTM attacks. In addition, many commands of the protocol, such as reset command, interrogation commands, read commands, etc. do not integrate authentication mechanisms, thereby resulting in unauthorized access. This vulnerability is crucial, since a cyber attacker possesses the ability to control PLCs and possibly, the overall operation of an automation substation, thereby generating disastrous consequences.

TABLE I
TRANSITIONS OF SCADA SYSTEM BASED ON A COLORED PETRI NET.

Transition Number	Flow Type	Source Place	Destination Place	Transition Description
1	Power Supply Flow	Power Supply	Processor	The power supply component provides power to the processor
2	Power Supply Flow	Power Supply	Input Modules	The power supply component provides power to the input modules
3	Power Supply Flow	Power Supply	Output Modules	The power supply component provides power to the output modules
4	Data Flow	Input Modules	Processor	The input modules transmit signals data to the processor
5	Commands Flow	Processor	Output Modules	The processor handles the input signals provided by the input modules and transmits control commands to the output modules
6	Data Flow	Processor	Memory	The processor stores some control data to the memory
7	Data Flow	Processor	Communication Module	The processor passes the control data to the communication module
8	Data Flow	Communication Module	MTU	The control data is sent to MTU via the communication module
9	Data Flow	MTU	Communication Module	The communication module receives control data from the MTU
10	Commands Flow	MTU	Communication Module	The receives control commands from the MTU

C. Petri Nets

Petri nets have been used successfully to describe various synchronous and asynchronous physical phenomena as well as communication processes, by depicting the information flows among the various elements [13]. The architecture of a Petri net is commonly composed of the following elements: *1) Place*, *2) Transition*, *3) Connection* and *4) Token*. A *Place* is an elliptical node which usually denotes a device or component sending data to another device (or component). *Transition* is a rectangular and intermediate node between the *Connection* of two *Places*, where *Connection* is depicted by a directed arrow. Finally, *Token* depicted by a black circle denotes the type of information transmitted between two *Places*. These elements cooperate with each other to depict the various information flows taking place in an environment, by satisfying necessarily the following rules: *1) all Connections must be directed*, *2) a Connection can only exist between a Place and a Transition*, *3) Connections between Places are not allowed*, *4) Connections between Transitions are not allowed* and *5) a Place can hold one or more Tokens*.

CPN is an extension of Petri Nets, where different types of information flows can be described, utilizing different *Tokens* called *Tokens Colour*. In this paper, we will use three *Tokens Colour*. The first one is illustrated by a yellow triangle and denotes the power flows transmitted by the Power Supply to the other components of PLC. The second *Token Colour* is depicted by a blue circle and implies the data flows exchanged by the various components and systems. Finally, the last *Token Colour* is depicted by an orange square, which in turn denotes the command flows.

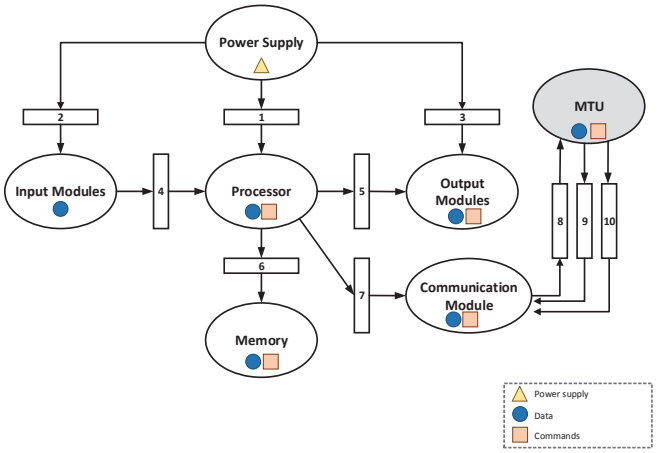

Fig. 1. CPN-based SCADA Architecture.

IV. THREAT MODELLING

A. CPN-based SCADA Architecture

Fig. 1 depicts the transformation of a SCADA system described by subsection III-A into a CPN. The components of PLC, as well as MTU, consist of the various Places of CPN. Concerning the possible Transitions, Table I, explains them in detail, utilizing the following labels: Transition Number, Flow Type, Source Place, Destination Place and Transition Description. The Connections, as illustrated in Fig. 1, are all directed. Finally, three Tokens Colour are utilized; the first one is depicted by a *yellow triangle* denotes the *power supply flows*. These flows are directed by the Power Supply to the other components of PLC. The second Token Colour is illustrated by a *blue circle* and indicates the *data flows*. Data flows are defined between 1) Input Modules and Processor, 2)

Processor and Memory System, 3) Processor and Communication Module, 4) Communication Module and MTU. Finally, the last Token Colour is depicted by an *orange rectangle* and implies the *command flows*. Command flows are located between 1) Processor and Output Modules and 2) MTU and Communication Module. Based on this CPN-based SCADA architecture, in the next subsection, we identify the potential threats per transition.

B. CPN-based Threat Model

Table II presents the threat model for IEC-104 SCADA systems, based on CPN of Fig. 1. In particular, we have classified the possible threats into two categories: 1) Physical Attacks and 2) cyber attacks. The first category denotes the case where the attacker has physical and direct access to the industrial environment, by destructing possible components or changing the corresponding interfaces between them. For each transition, the corresponding physical attacks are described by Table II. The second class denotes those attacks where the adversary cannot access the physical devices, but he/she exploits the system vulnerabilities of IEC-104 to perform the various malicious actions. In particular, we have identified four possible categories of cyber attacks against IEC-104: 1) Unauthorised Access, 2) MiTM attacks, 3) DoS attacks and 4) Traffic Analysis attacks. Specific examples of these attacks are emulated in the next section. As in the case of the physical attacks, for each transition, Table II determines the corresponding cyber attacks.

V. Attack Emulation and Risk Assessment

The purpose of this section is twofold. We first emulate the the cyber attacks determined by our threat model and second, we identify their risk level by using the Alienvault's risk assessment model adopted by AlienVault OSSIM [14].

A. Testbed

Fig. 2 illustrates the testbed used for emulating the aforementioned cyber attacks against the IEC-104 protocol. In particular, the device with IP address 192.168.1.8 plays the role of a PLC using the IEC TestServer software. The latter emulates IEC-104 and its user interface consists of three panels, which accordingly include settings for its operation, active commands and various information about its connections. The device with IP address 192.168.1.7 emulates an MTU which communicates with the previous device utilizing the QTester104 software. The graphical interface of QTester104 is also divided into three panels. The first panel comprises various settings about its operation. The lower left panel displays messages, such as errors, new connections and disconnections regarding the communication between PLC and MTU. Finally, the lower right panel displays specific information of the aforementioned communication, including the Information Object Address (IOA), the type of command, its value, the Cause of Transmission (CoT), possible flags, the number of packets received by PLC and time information.

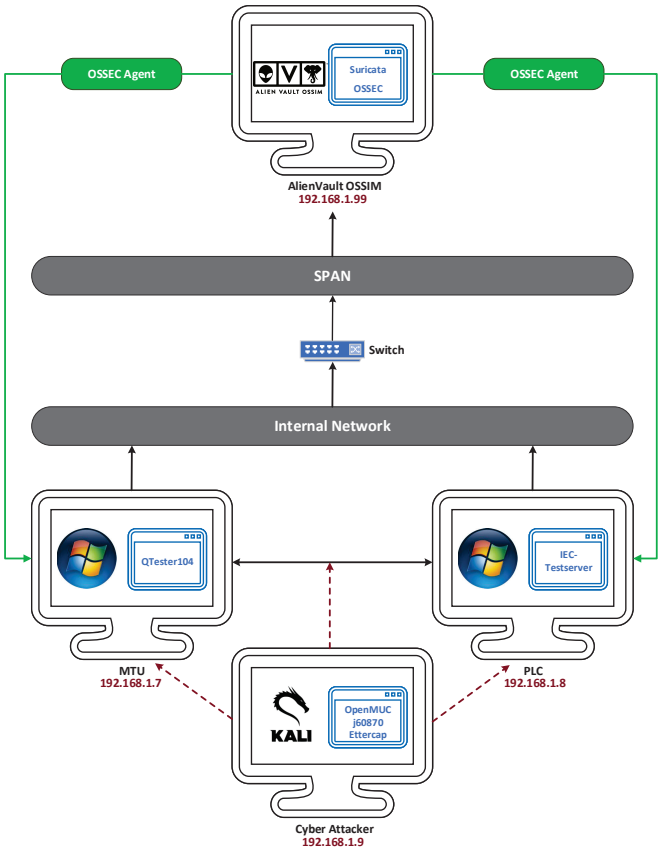

Fig. 2. Testbed for emulating cyber attacks against IEC-104.

The machine carrying Kali Linux and IP address 192.168.1.9 emulates the cyber attacker. The specific device is going to be used to perform the cyber attacks utilizing preinstalled penetration testing tools, such as Ettercap and hping, as well as the OpenMUC j60870 software in order to transmit unauthorized commands to PLC. In particular, OpenMUC j60870 was developed based on Java and it includes only two protocol commands: 1) Interrogation command (C_IC_NA_1) and 2) Clock Synchronization command (C_CS_NA_1). For the purposes of the paper, we further extended its capabilities by integrating the Read command (C_RD_NA_1), the Reset command (C_RP_NA_1) and the Counter Interrogation command (C_CI_NA_1).

Finally, the device with the IP 192.168.1.99 corresponds to the AlienVault OSSIM which undertakes to monitor and protect PLC and MTU. OSSIM constitutes a System Information and Event Management (SIEM) system integrating multiple security tools and correlation mechanisms capable of detecting possible anomalies and providing overall protection. Concerning our testbed, OSSIM was configured to monitor and control efficiently the communication between PLC and MTU. In particular, we firstly determined MTU and PLC as assets of OSSIM. Secondly, we deployed the corresponding policies for these assets. Next, we activated the availability monitoring agents for these assets, by employing the Nagios tool. Next, we enabled and configured appropriately both Host Intrusion

TABLE II
THREAT MODEL FOR IEC 60870-5-104 SCADA SYSTEMS.

	Attacks on Power Supply Flows	**Attacks on Control Data Flows**	**Attacks on Control Command Flows**
Transitions	1, 2, 3	4, 6, 7, 8, 9	5, 10
Physical Attacks	1) Physical disruption or malicious modification of the connections 1, 2 and 3. 2) Physical destruction or malicious modification of the Power Supply, Processor, Input Modules and Output Modules.	1) Physical disruption or malicious modification of the connections 4, 6, 7, 8 and 9. 2) Physical destruction or malicious modification of the Processor, Input Modules Output Modules, Memory, Communication Module and MTU. 3) Physical malicious programming of the Processor 4) Physical violation of MTU of the SCADA system.	1) Physical disruption or malicious modification of the connections 5 and 10. 2) Physical destruction or malicious modification of the Processor, Output modules, Communication Module and MTU. 3) Physical malicious programming of the Processor 4) Physical violation of MTU of the SCADA system.
Cyber attacks	1) Unauthorised access to Processor 2) Unauthorised access to Input Modules 3) Unauthorised access to Output Modules	1) Unauthorised access to Input Modules 2) Unauthorised access to Processor 3) Unauthorised access to Output Modules 4) MiTM attack between Input Modules and Processor 5) MiTM attack between Output Modules and Processor 6) DoS attacks 7) MiTM attack between Communication Module and MTU 8. Traffic Analysis Attack	1) Unauthorised access to Processor 2) Unauthorised access to Output Modules 3) MiTM attack between Communication Module and MTU 4) DoS attacks 5. Traffic Analysis Attack

Detection System (HIDS) and Network Intrusion Detection System (NIDS) tools, called OSSEC and Suricata, respectively. For this process, we utilized and adjusted the rules of [8]. Finally, Suricata should be able to monitor the whole network traffic. To this end, OSSIM was configured to employ a SPAN (Switch Port Analyzer) port.

B. Attacks Emulation

In the following, we summarise the attacks we emulated as part of our testbed. For each attack, we describe its purpose and a high-level view of how it is undertaken.

IEC-104 Packet Flooding Attack. This attack constitutes a kind of DoS which aims at flooding MTU with specific IEC-104 command packets in order to mainly generate a possible malfunction to MTU, confuse the system operator or even disrupt the operation of MTU. To emulate this attack, we configured PLC to transmit the single point information command (M_SP_NA_1) to MTU per second. The functionality of MTU was not affected by this attack. Nevertheless, If there were more PLCs, it is likely that MTU would present certain malfunction. Moreover, it is noteworthy that OSSIM was not able to detect the attack, since this action does not violate any security rules of Suricata and OSSEC.

TCP SYN DoS Attack. The TCP SYN Attack is a usual DoS attack that the cyber attacker continuously transmits to PLC several SYN packets without remaining the corresponding answers (SYN+ACK). To emulate this attack, we utilized the pre-installed hping tool of Kali Linux. During the specific attack, the Central Processing Unit (CPU) usage rate increased 23%, while the memory utilization rate increased by 12%. Accordingly, the network utilization rate increased by 4.81%. This attack did not disrupt the communication between PLC and MTU. Nevertheless, it should be noted that in a real environment where PLC is characterized by constrained computing resources, this attack may be more successful. Furthermore, if there were more cyber attackers, the effect of the attack would be different. Finally, it should be noted that OSSIM successfully detected this attack.

Unauthorized Access. Normally, an unauthorized user should not be able to communicate with PLC; however, as mentioned before IEC-104 does not provide any authentication mechanism. To emulate this attack, we modified appropriately the IP address of the cyber attacker; hence he/she is not considered as a member of the network. Subsequently, we utilized the OpenMUC j60870 software to transmit the following commands: 1) Read command (C_RD_NA_1), 2) Reset Process command (C_RP_NA_1) and 3) Counter Interrogation command (C_CI_NA_1). OSSIM detected all of these actions.

MiTM IEC 60870-5-104 Isolation Attack. We carried out a MiTM attack in which the cyber attacker aims at isolating and dropping the IEC-104 network traffic between PLC and MTU. To this end, we performed an ARP poisoning attack utilizing the Ettercap software. In addition, we developed and enabled an Ettercap filter which isolates and drops the IEC-104 packets between PLC and MTU. As in the previous cases, OSSIM timely recognized the attack.

C. Risk Assessment For IEC 60870-5-104

In the following, we are using a use case, to derive the overall risk level that each attack type, implemented as part of our

TABLE III
RISK ASSESSMENT VALUES

Threat	CWE Vulnerability	Threat Occurrence	Impact
DoS Attacks	Allocation of Resources Without Limits or Throttling (CWE-770)	8.65	3.5
Traffic Analysis Attacks	Cleartext Transmission of Sensitive Information (CWE-319)	7.834	2.5
MiTM Attacks	Missing Encryption of Sensitive Data (CWE-311)	6.793	3.5
Unauthorized Access	Improper Access Control (CWE-284)	9.4	3.5

testbed, introduces. The definition of the final expected risk is in line with AlienVault's risk assessment model [14]: $Risk = (Asset\ Value \times Event\ Priority \times Event\ Reliability)/25$, where each security event is related to the detection of the threat that inflicts this risk. *Asset Value* (ranging between 0-5) is assigned by each organization and implies how significant an asset is. In our testbed, there are two assets: 1) MTU and 2) PLC whose value is equal to 5, since they are crucial for the normal operation of a SCADA system. *Event priority* (ranging between 0-5) is determined by the expected impact of this threat, while *event reliability* (ranging between 0-10) is determined by the probability of the threat occurring.

We have used *impact*, *threat occurrence* values from the case study presented in [15] to initialize *Event Priority* and *Event Reliability* respectively. These values were computed by using real-world data from the Common Weakness Enumeration (CWE) category system for software weaknesses and vulnerabilities. Table III presents these values for each of the identified attacks of our testbed implementation.

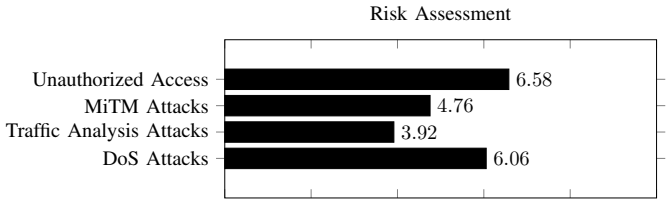

Fig. 3. Risk assessment values for the various IEC-104 attacks.

Fig. 3 depicts that *Unauthorized Access* and *DoS attacks* introduce the highest risk levels among the other two cyber threats modelled; *Traffic Analysis* and *MiTM*. This confirms our intuition that accessing as well as interrupting pose the highest risks to critical infrastructures such as a SCADA system. On the other hand, traffic analysis and any kind of MiTM introduce a fair amount risk as they can be the first step towards getting access to the system.

VI. CONCLUSIONS

The security of SCADA systems is crucial for the overall protection of smart grid. The protocols used by these systems present various security issues, since they usually combine the TCP/IP transform capabilities with legacy application messages. In this paper, we focused on IEC-104 and we provided a threat model for it. We also emulated and evaluated four critical cyber attacks against IEC-104. In our future work, we aim to develop an IDS which will be capable of identifying possible anomalies and zero-day attacks against IEC-104 communications. The proposed system will be integrated into OSSIM utilizing the jailbreak interface. Moreover, the proposed IDS will apply machine learning and statistical analysis techniques on TCP/IP network flows and it will keep statistics (e.g., number of packets, bytes) for each IEC-104 packet, by monitoring the IEC-104 transactions based on Common Address of ASDU (CoA), IOA and CoT.

REFERENCES

[1] S. Tan, D. De, W. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 397–422, Firstquarter 2017.

[2] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[3] Y. Lopes, N. C. Fernandes, and K. Obraczka, "Smart grid communication: Requirements and scada protocols analysis," in *2018 Simposio Brasileiro de Sistemas Eletricos (SBSE)*, May 2018, pp. 1–6.

[4] C. Baylon, *Lessons from Stuxnet and the Realm of Cyber and Nuclear Security: Implications for Ethics in Cyber Warfare*. Cham: Springer International Publishing, 2017, pp. 213–229.

[5] A. Hansen, J. Staggs, and S. Shenoi, "Security analysis of an advanced metering infrastructure," *International Journal of Critical Infrastructure Protection*, vol. 18, pp. 3 – 19, 2017.

[6] P. Matoušek, "Description and analysis of iec 104 protocol," Faculty of Information Technology, Brno University o Technology, Tech. Rep., 2017.

[7] E. Hodo, S. Grebeniuk, H. Ruotsalainen, and P. Tavolato, "Anomaly detection for simulated iec-60870-5-104 trafiic," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ser. ARES '17. New York, NY, USA: ACM, 2017, pp. 100:1–100:7. [Online]. Available: http://doi.acm.org/10.1145/3098954.3103166

[8] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for iec 60870-5-104 based scada networks," in *2013 IEEE Power Energy Society General Meeting*, July 2013, pp. 1–5.

[9] W. Park and S. Ahn, "Performance comparison and detection analysis in snort and suricata environment," *Wireless Personal Communications*, vol. 94, no. 2, pp. 241–252, May 2017. [Online]. Available: https://doi.org/10.1007/s11277-016-3209-9

[10] Y. Yang, K. McLaughlin, S. Sezer, Y. B. Yuan, and W. Huang, "Stateful intrusion detection for iec 60870-5-104 scada security," in *2014 IEEE PES General Meeting — Conference Exposition*, July 2014, pp. 1–5.

[11] J. Hurley, A. Munoz, and S. Sezer, "Itaca: Flexible, scalable network analysis," in *2012 IEEE International Conference on Communications (ICC)*, June 2012, pp. 1069–1073.

[12] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of iec 62351," *Journal of Information Security and Applications*, vol. 34, pp. 197 – 204, 2017.

[13] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 741–749, 2011.

[14] AlienVault, "Alienvault ossim documentation," https://www.alienvault.com/documentation/.

[15] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decision Support Systems*, vol. 86, pp. 13–23, 2016.