ERENO: An Extensible Tool For Generating Realistic IEC–61850 Intrusion Detection Datasets

Silvio E. Quincozes[1], **Célio Albuquerque**[1],
Diego Passos[1], **Daniel Mossé**[2]

[1] Universidade Federal Fluminense - UFF

[2]Universidade de Pittsburgh - PITT

sequincozes@id.uff.br

{celio, dpassos}@ic.uff.br, mosse@pitt.edu

Resumo. *Os Sistemas de Detecção de Intrusão (IDSs) são componentes essenciais para lidar com ataques às redes baseadas na norma IEC–61850. No entanto, empregar IDSs em tais redes é um desafio. Uma questão importante é a falta de dados representativos e realistas sobre ataques aos protocolos IEC–61850. Neste trabalho, propomos uma ferramenta extensível que simula o tráfego da rede da subestação de forma realista para produzir atributos representativos. Como prova de conceito, uma linha de transmissão brasileira foi simulada, gerando-se datasets com 4,4 GB, incluindo 7 tipos de ataque. Os resultados com atributos propostos revelam um ganho de desempenho de IDS baseados em aprendizado de máquina que evoluiu de 52,24% para 99,46%.*

Abstract. *Intrusion Detection Systems (IDSs) are an essential component to deal with attacks that target the electric grid substations networks based on the IEC–61850 standards. However, employing IDSs in such scenarios is challenging. A key issue is a lack of representative and realistic data about attacks that target IEC–61850 networks. In this work, we propose an extensible tool that simulates the substation network traffic to produce representative features. As proof of concept, we simulated an existing Brazillian transmission line and generated more than 4.4GB of data containing seven attack types. Our results show that the proposed features increase the intrusion detection performance of machine learning algorithms from 52.24% to 99.46%.*

1. Introduction

Digital substations are a key component of reliable future smart grids. The IEC–61850 standards propose a set of communication protocols to define how Intelligent Electronic Devices (IEDs) can communicate in digital substations. However, there is a range of vulnerabilities that may compromise the IEC–61850 communication protocols and cause improper functioning of the power system. Therefore, Intrusion Detection Systems (IDSs) have become an essential component of safeguarding substations from malicious activities. However, having efficient IDSs for IEC–61850 networks is still challenging, especially due to the lack of available data about the existing attacks targeting their protocols.

1.1. Motivation

Cyberattacks on communication systems in digital substations are not only considered one of the main threats by researchers in the field [Hong and Liu 2019] but also present real threats that have already been witnessed by people from many countries around the world [Patel 2017, Radoglou Grammatikis and Sarigiannidis 2019].

Until the beginning of 2000, Supervisory Control and Data Acquisition (SCADA) system networks were assumed to be electronically isolated from the rest of the networks and, therefore, the industry's focus was on the physical security of the network [Patel 2017]. In 2010, *malware Stuxnet* attacked Iran's nuclear program [Radoglou Grammatikis and Sarigiannidis 2019]. *Stuxnet* specifically targeted the Iranian Programmable Logic Controller (PLC) and caused fast-spinning centrifuges to separate. According to Patel *et al.* [Patel 2017], this was one of the main incidents caused by cyber-attacks that prompted a perception of the urgent need to provide security in the communication network of SCADA systems, including digital substations.

In the United States (US), computer systems were compromised by more than 150 cyber attacks between 2010 and 2014. Between 2011 and 2014, utilities reported 362 instances of attacks that caused power outages [Hong and Liu 2019, Radoglou Grammatikis and Sarigiannidis 2019]. In 2016, an alert was issued about coordinated cyber attacks on 35 Ukrainian substations: more than 225,000 people were left without electricity [Hong and Liu 2019]. Information security vulnerabilities are continually growing. The US National Vulnerabilities Database (NVD) [NIST 2021] registered a growth from 6,447 vulnerabilities in 2016 to 20,138 vulnerabilities in 2021.

Both industry and academia are concerned about information security in electrical substations. They consider this is one of the main concerns about smart grids. The provision of security and robustness in this domain is limited, due to the computing capacity of the equipment, which does not support the mechanisms used to protect traditional networks. Therefore, the employment of IDSs to enable responding to attacks will play a vital role in ensuring the correct functioning of electrical substations.

2. Research Problem

Deploying IDSs serves to identify malicious activities and mitigate the attacker's actions. Whereas IDSs are already widely deployed in traditional Information Technology (IT) systems, they are still in a premature stage in IEC–61850 networks. As these networks rely on specific protocols, such as Generic Object Oriented Substation Event (GOOSE) and Sampled Values (SV), they are vulnerable to novel attacks that explore their particularities; attacks include: replay [Hong et al. 2014], message injection [Yoo and Shon 2015], masquerade [Ustun et al. 2019], and DoS [Hoyos et al. 2012]. Thus, the IEC–61850-based IDSs require signatures from all these attack classes to enable a robust detection (*e.g.,* the machine learning-based IDS need data to perform training, testing, and assessment of their performance; the rule-based IDS need data for extracting detection rules; and, the anomaly-based IDS need data to assess their detection ability).

To support the IEC–61850-based IDSs, our research problem focuses on the lack of available datasets for intrusion detection in communication systems and networks in the context of electrical substations. To create an effective dataset, attack signatures should be built by considering realistic data, including electrical samples from SV and proper response of GOOSE protocols. Furthermore, it is clear that, to represent the realistic traffic behavior inside a substation or of a transmission line between two or more substations, both normal operation and transmission line faulty scenarios must be considered. In both situations, a variety of updated attack classes, as well as legitimate activities, must be considered. Building a robust IDS requires not only the availability of data that includes realistic attack scenarios but also the identification of which features are more representative for detecting each attack class. Therefore, extraction, enrichment, and selection of features are also necessary for robust intrusion detection.

3. Goals

Aiming at robustness and resilience in IEC–61850 digital substations, our key goals are to support the training, evaluation, and testing of IDSs. Thus, our main goal is to create an extensible tool for generating realistic and representative IEC–61850 datasets with different types of intrusions. Furthermore, we aim at proposing a novel feature selection method based on metaheuristics to perform feature selection on the generated dataset. Our specific goals are the following:

- The study of the current attack scenarios targeting IEC–61850 systems and the state-of-art IDSs solutions;
- The proposal of a novel taxonomy for the IEC–61850-based IDSs aspects;
- The reproduction of normal and faulty scenarios through simulations, based on the modeling of a real transmission line between two substations to generate and log realistic electrical samples;
- An extensible tool for generating realistic GOOSE and SV traffic features, based on realistic electrical signals and inclusion of state-of-art attacks targeting these protocols;
- A set of 8 public IEC–61850 datasets to support the training, testing, and evaluating of IDSs;
- Algorithms and methods to extract, enrich and select representative features from electrical and computer networks domains to maximize the results of IDSs.

4. Obtained Results and Contribution

Our main contribution is in the development of the Efficacious Reproducer Engine for Network Operations (ERENO). ERENO is an open-source framework for generating IEC–61850 datasets with representative features — extracted both from substation communication protocols and the electric domain — for detecting different types of intrusions. As an additional contribution and as a proof-of-concept, we present a suite of realistic IEC-61850 datasets that model 8 use cases, namely traffic for 7 common attacks and 1 for normal network traffic. Finally, we also present a novel taxonomy for the IEC–61850-based IDSs aspects. Our main contributions are summarized as follows:

- We introduced a novel methodology for simulating both normal and faulty scenarios on power grids through the PSCAD [1], reproducing a real transmission line;
- We presented a study of the current attack scenarios targeting IEC–61850 systems;
- We proposed the ERENO tool to generate realistic GOOSE and SV traffic features, taking as input the modeled real scenario in PSCAD;
- We identified and extracted the features of the electrical and computer network domains that are correlated with malicious actions. We also composed novel enhanced features;

[1] Available at `https://www.pscad.com/software/pscad/overview`.

- We implemented 8 use cases on the ERENO tool to generate 7 attack classes and one class of benign normal traffic;
- We made the ERENO–IEC–61850 dataset publicly available[2]. The dataset was generated by the ERENO tool, also publicly available[3]; and
- We proposed the GRASP-FS, a novel implementation of the GRASP metaheuristic for the feature selection.

We assessed our dataset with the J48 classification algorithm. The Accuracy (Acc), Precision (Pr), Recall (Rc), and F1-Score (F1) results are detailed in Table 1. These metrics reveal that the proposed feature enrichment generated more valuable GOOSE (`GS++`) and SV (`SV++`) features. They resulted into a 99.52% F1 to multi-class intrusion detection and 99.46% F1 to the most challenging attack (*i.e.,* masquerade attacks). With the basic GOOSE features (G), these F1 were 72.84% and 52.24%, respectively. Therefore, very significant improvements were observed. Our traffic generation solution can not only generate attack signatures, but also improves their detection by providing representative features for machine learning algorithms.

Features	**Multi-class**				**Masquerade (UC03)**			
	Acc	**Pr**	**Rc**	**F1**	**Acc**	**Pr**	**Rc**	**F1**
`GS`	95.23%	75.98%	75.22%	72.84%	94.78%	43.87%	64.55%	52.24%
`GS & SV`	97.18%	83.62%	84.45%	82.20%	95.68%	51.01%	60.31%	55.27%
`GS++ & SV`	98.29%	86.72%	89.66%	87.22%	97.06%	65.52%	70.65%	67.99%
`GS++ & SV++`	99.88%	99.76%	99.29%	99.52%	99.95%	99.70%	99.22%	99.46%

Tabla 1. Comparison between the protocol features and their enrichment.

Several other results are reported in the thesis document, as well as in the production reported in Section 5. Besides, there are novel works in progress that originated from this thesis. Some of them are being carried out by other students from both undergraduate and graduate level, from four different Brazilian federal universities. Thus, as an additional result, a novel research line was begun.

5. Publications

Along the development of this thesis, we documented each step of our study through academic articles published in international journals and national/international conferences. Part of our research had a direct contribution to this thesis (see Section 5.1). Another part comprises products that are not part this thesis, but study correlated themes; we included them here because they are indirect products of the doctoral research (see Section 5.2).

5.1. Production of the Thesis Direct Results

1. [Quincozes et al. 2022]: QUINCOZES, S. E., PASSOS, D., DE ALBUQUERQUE, C. V. N., MOSSE, D. An Extended Assessment of Metaheuristics-based Feature Selection for Intrusion Detection in CPS Perception Layer. **Annals of Telecommunications**, 2022.

[2] The ERENO tool is available at: `https://github.com/sequincozes/ereno`

[3] The ERENO-IEC-61850 dataset is available at: `https://www.kaggle.com/datasets/sequincozes/ereno-iec61850-ids`

2. [Quincozes et al. 2021a]: QUINCOZES, S. E., PASSOS, D., DE ALBUQUERQUE, C. V. N., MOSSE, D. A survey on intrusion detection and prevention systems in digital substations. **Computer Networks**, v. 184, p. 1-13, 2021.
3. [Quincozes et al. 2021b]: QUINCOZES, S. E., PASSOS, D., DE ALBUQUERQUE, C. V. N., MOSSE, D., OCHI, L. S., SANTOS, V. F. On the Performance of GRASP-Based Feature Selection for CPS Intrusion Detection. **IEEE Transactions on Network and Service Management**, v. 19, p. 614-626, 2021.
4. [Quincozes et al. 2021c]: QUINCOZES, S. E., RANIERY, C., CERETTA, R., PASSOS, D., DE ALBUQUERQUE, C., MOSSE, D., Counselors network for intrusion detection. **International Journal of Network Management (IJNM)**, v. 31, n. 3, p. e2111, 2021.
5. [Quincozes et al. 2020a]: QUINCOZES, S. E., PASSOS, D., DE ALBUQUERQUE, C. V. N., MOSSE, D., OCHI, L. S. GRASP-based Feature Selection for Intrusion Detection in CPS Perception Layer. **In: IEEE 4th Conference on Cloud and Internet of Things (CIoT)**, p. 41-48, 2020.
6. [Quincozes et al. 2019b]: QUINCOZES, S. E., RANIERY, C., CERETTA, R., PASSOS, D., DE ALBUQUERQUE, C., MOSSE, D. A Counselors-Based Intrusion Detection Architecture. **In: Latin American Network Operations and Management Symposium (LANOMS)**. 2019.
7. QUINCOZES, S. E., PINHEIRO, J. L., PASSOS, D., DE ALBUQUERQUE, C. V. N., MOSSE, D. ERENO: A Framework for Generating Realistic IEC–61850 Intrusion Detection Datasets. Planned target: **Transactions on Dependable and Secure Computing**, expected to 2022 (under submission).

5.2. Production on Correlated Themes (during the thesis period)

6. DELFINO, W. O., QUINCOZES, S. E., VIEIRA, J. L., PASSOS, D. P., SAADE, M. D., ALBUQUERQUE, C.V.N., Fault Recovery on Software Defined Network. Planned target in 2022: **IEEE Access**.
7. QUINCOZES, S. E., QUINCOZES, V.E., KAZIENKO, J. F. An Extended Evaluation on Machine Learning Techniques for Denial-of-Service Detection in Wireless Sensor Networks. Planned target in 2022: **IEEE Internet of Things Journal**.
8. [Quincozes et al. 2021g] QUINCOZES, V. E., QUINCOZES, S. E., MANSILHA, R., KREUTZ, D., KAZIENKO, J. F. A Mobile Application for Scheduling Health Services on Demand.**Simpósio Brasileiro de Sistemas de Informação**, 2022.
9. [Soares et al. 2021]: ZOPELLARO, A. A., SOARES, L., MATTOS, D. P., PINHEIRO, P., QUINCOZES, S. E, ..., PASSOS, D., DE ALBUQUERQUE, C. V. N., et al. Enabling Emulation and Evaluation of IEC 61850 Networks With TITAN. **IEEE Access**, v. 9, p. 49788-49805, 2021.
10. [Zopellaro Soares et al. 2021]: ZOPELLARO, A., ..., QUINCOZES, S. E., ..., PASSOS, D., ALBUQUERQUE, C., et al. SDN-based teleprotection and control power systems: A study of available controllers and their suitability. **International Journal of Network Management (IJNM)**, v. 31, n. 3, p. e2112, 2021.
11. [Vieira et al. 2021]: VIEIRA, J. L., FERREIRA, V., BASTOS, I., QUINCOZES, S. E., ..., PASSOS, D., DE ALBUQUERQUE, C. V. N., et al. THANOS: Teleprotection Holistic Application for ONOS Controller. **In: International Symposium on Integrated Network Management (IM)**. IEEE, 2021. p. 818-823.

12. [Quincozes et al. 2021f]: QUINCOZES, V. E., QUINCOZES, S. E., et al. Identifica ISP: Autenticação Mútua entre Múltiplas Entidades para Serviços de Suporte Técnico Prestados por ISPs. **In: Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas (SBSeg)**. SBC, 2021. p. 26-33.
13. [Quincozes et al. 2021e]: QUINCOZES, V. E., QUINCOZES, S. E., KAZIENKO, J. F. **Livro de Minicursos da VII Escola Regional de Sistemas de Informação**, Capítulo 7. 1ed. Porto Alegre: SBC, 2021, p. 250-284.
14. [Quincozes et al. 2021d]: QUINCOZES, V. E., QUINCOZES, S. E., KAZIENKO, J. F. Avaliando a Sobrecarga de Mecanismos Criptográficos Simétricos na Internet das Coisas: Uma Comparação Quantitativa entre os Protocolos MQTT e CoAP. **In: Anais do XX Workshop em Desempenho de Sistemas Computacionais e de Comunicação.** SBC, 2021. p. 13-24.
15. [Uchôa et al. 2020]: UCHÔA, L., QUINCOZES, S. E., VIEIRA, J. L., PASSOS, D., DE ALBUQUERQUE, C. V. N., MOSSE, D. Analysis of smart grid fault recovery protocols. **In: IEEE/IFIP Network Operations and Management Symposium (NOMS)**. IEEE, 2020. p. 1-8.
16. [Borgiani et al. 2020]: BORGIANI, V. M., MORATORI, P., KAZIENKO, J. F., TUBINO, E. E., QUINCOZES, S. E. Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks Within Industrial Internet of Things. **IEEE Internet of Things Journal**, v. 8, n. 6, p. 4569-4578, 2020.
17. [Quincozes and Kazienko 2020]: QUINCOZES, S. E., KAZIENKO, J. F. Machine Learning Methods Assessment for Denial of Service Detection in Wireless Sensor Networks. **In: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT)**. IEEE, 2020. p. 1-6.
18. [Kreutz et al. 2020]: KREUTZ, D. L., MANSILHA, R.B., QUINCOZES, S. E., et al. Introducão a verificação automática de protocolos de seguranca com scyther. **Minicursos da XVIII Escola Regional de Redes de Computadores**, SBC, 2020.
19. [Quincozes et al. 2020b]: QUINCOZES, V. E., Temp, D., QUINCOZES, S.E., et al. Sistema para Autenticação entre Clientes, Técnicos e ISPs. **In: Anais da XVIII Escola Regional de Redes de Computadores.** SBC, 2020. p. 116-122.
20. [Quincozes et al. 2019c]: QUINCOZES, S. E., ..., PASSOS, D., DE ALBUQUERQUE, C. V. N., et al. Survey and Comparison of SDN Controllers for Teleprotection and Control Power Systems. **In: LANOMS**. 2019.
21. [Quincozes et al. 2019a]: QUINCOZES, S. E., TUBINO, E. E.; KAZIENKO, J. F., Mqtt protocol: Fundamentals, tools and future directions. **IEEE Latin America Transactions**, v. 17, n. 09, p. 1439-1448, 2019.
22. [Quincozes and Kazienko 2019]: QUINCOZES, S. E., KAZIENKO, J. F. Experimental evaluation of a secure and ubiquitous architecture for electronic health records retrieval. International **Journal of E-Health and Medical Communications (IJEHMC)**, v. 10, n. 4, p. 39-53, 2019.
23. [Junior et al. 2019]: JUNIOR, C. R., QUINCOZES, S. E., KAZIENKO, J. F., LegitimateBroker: Mitigando Ataques de Personificação em Broker MQTT na Internet das Coisas. **In: Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. SBC, 2019. p. 141-154.
24. [Quincozes et al. 2018]: QUINCOZES, S. E., et al. Avaliação de Conjuntos de Atributos para a Detecção de Ataques de Personificação na Internet das Coisas. **In: Anais Estendidos do VIII Simpósio Brasileiro de Engenharia de Sistemas**

Computacionais. SBC, 2018.

Thesis Availability

This thesis is available online at the following URL: `http://www.ic.uff.br/PosGraduacao/frontend-tesesdissertacoes/download.php?id=1042.pdf&tipo=trabalho`

References

Borgiani, V., Moratori, P., Kazienko, J. F., Tubino, E. R., and Quincozes, S. E. (2020). Toward a distributed approach for detection and mitigation of denial-of-service attacks within industrial internet of things. *IEEE Internet of Things Journal*, 8(6):4569–4578.

Hong, J. and Liu, C. (2019). Intelligent electronic devices with collaborative intrusion detection systems. *IEEE Transactions on Smart Grid*, 10(1):271–281.

Hong, J., Liu, C., and Govindarasu, M. (2014). Detection of cyber intrusions using network-based multicast messages for substation automation. In *Innovative Smart Grid Technologies (ISGT)*, pages 1–5. IEEE.

Hoyos, J., Dehus, M., and Brown, T. X. (2012). Exploiting the goose protocol: A practical attack on cyber-infrastructure. In *2012 IEEE Globecom Workshops*, pages 1508–1513. IEEE.

Junior, C. R., Quincozes, S., and Kazienko, J. (2019). Legitimatebroker: Mitigando ataques de personificação em broker MQTT na internet das coisas. In *Anais do XIX Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais*, pages 141–154. SBC.

Kreutz, D. L., Mansilha, R. B., Quincozes, S. E., Jenuário, T. S., and Chervinski, J. O. (2020). Introducão a verificação automática de protocolos de seguranca com scyther. In *Minicursos da XVIII Escola Regional de Redes de Computadores (ERRC)*, chapter 3, pages 43–68. Sociedade Brasileira de Computação.

NIST (2021). National Institute of Standards and Technology: National Vulnerability Database (NVD).

Patel, S. (2017). *IEC-61850 Protocol Analysis and misc Intrusion Detection System for SCADA Networks using Machine Learning*. PhD thesis, University of Victoria.

Quincozes, S., Emilio, T., and Kazienko, J. (2019a). Mqtt protocol: Fundamentals, tools and future directions. *IEEE Latin America Transactions*, 17(09):1439–1448.

Quincozes, S. E., Albuquerque, C., Passos, D., and Mosse, D. (2021a). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, 184:107679.

Quincozes, S. E., dos Santos, C. R. P., Nunes, R., de Albuquerque, C. V. N., Passos, D. G., and Mosse, D. (2019b). A counselors-based intrusion detection architecture. In *Latin American Net. Op. and Management Symp. (LANOMS)*.

Quincozes, S. E. and Kazienko, J. F. (2019). Experimental evaluation of a secure and ubiquitous architecture for electronic health records retrieval. *International Journal of E-Health and Medical Communications (IJEHMC)*, 10(4):39–53.

Quincozes, S. E. and Kazienko, J. F. (2020). Machine learning methods assessment for denial of service detection in wireless sensor networks. In *6th World Forum on IoT (WF-IoT)*, pages 1–6. IEEE.

Quincozes, S. E., Kazienko, J. F., and Copetti, A. (2018). Avaliação de conjuntos de atributos para a detecção de ataques de personificação na internet das coisas. In *Anais Estendidos do VIII Simpósio Brasileiro de Engenharia de Sistemas Computacionais*. SBC.

Quincozes, S. E., Mosse, D., Passos, D., Albuquerque, C., Ochi, L. S., and dos Santos, V. F. (2021b). On the performance of grasp-based feature selection for cps intrusion detection. *IEEE Transactions on Network and Service Management*.

Quincozes, S. E., Passos, D., Albuquerque, C., Mossé, D., and Ochi, L. S. (2022). An extended assessment of metaheuristics-based feature selection for intrusion detection in cps perception layer. *Annals of Telecommunications*, pages 1–15.

Quincozes, S. E., Passos, D., Albuquerque, C., Ochi, L. S., and Mosse, D. (2020a). GRASP-based Feature Selection for Intrusion Detection in CPS Perception Layer. In *2020 4th Conference on Cloud and Internet of Things (CIoT)*, pages 41–48. IEEE.

Quincozes, S. E., Raniery, C., Ceretta, R., Albuquerque, C., Passos, D., and Mosse, D. (2021c). Counselors network for intrusion detection. *International Journal of Network Management*, 31(3):e2111.

Quincozes, S. E., Soares, A., Oliveira, W., Cordeiro, E., Lima, R., Saade, D., Ferreira, V., Lopes, Y., Vieira, J., Uchôa, L., et al. (2019c). Survey and comparison of SDN controllers for teleprotection and control power systems. In *Latin American Net. Op. and Management Symp. (LANOMS)*.

Quincozes, V. E., Quincozes, S. E., and Kazienko, J. F. (2021d). Avaliando a sobrecarga de mecanismos criptográficos simétricos na internet das coisas: Uma comparação quantitativa entre os protocolos MQTT e CoAP. In *Workshop em Desempenho de Sist. Comp. e de Comunicação*, pages 13–24. SBC.

Quincozes, V. E., Quincozes, S. E., and Kazienko, J. F. (2021e). Desvendando a camada de aplicação na internet das coisas: Teoria, prática e tendências. In *Livro de Minicursos da VII Escola Regional de Sistemas de Informação (ERSI-RJ)*, chapter 7, pages 250–284. Sociedade Brasileira de Computação.

Quincozes, V. E., Quincozes, S. E., Kreutz, D., and Mansilha, R. B. (2021f). Identifica isp: Autenticação mútua entre múltiplas entidades para serviços de suporte técnico prestados por isps. In *Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 26–33. SBC.

Quincozes, V. E., Quincozes, S. E., Kreutz, D., Mansilha, R. B., and Kazienko, J. F. (2021g). A mobile application for scheduling health services on demand. In *Simpósio Brasileiro de Sistemas de Informação (SBSI)*, pages 818–823. IEEE.

Quincozes, V. E., Temp, D., Quincozes, S. E., Kreutz, D., and Mansilha, R. B. (2020b). Sistema para autenticação entre clientes, técnicos e isps. In *ERRC*, pages 116–122. SBC.

Radoglou Grammatikis, P. I. and Sarigiannidis, P. G. (2019). Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access*, pages 46595–46620.

Soares, A. A. Z., Soares, L. F., Mattos, D. P., Pinheiro, P. H., Quincozes, S. E., Ferreira, V. C., Apostolo, G. H., Carrara, G. R., Moraes, I. M., Albuquerque, C., et al. (2021). Enabling emulation and evaluation of iec 61850 networks with titan. *IEEE Access*, 9:49788–49805.

Uchôa, L., Quincozes, S., Vieira, J. L., Passos, D., Albuquerque, C., and Mosse, D. (2020). Analysis of smart grid fault recovery protocols. In *Net. Op. and Management Symp. (NOMS)*, pages 1–8. IEEE.

Ustun, T. S., Farooq, S. M., and Hussain, S. S. (2019). A Novel Approach for Mitigation of Replay and Masquerade Attacks in Smartgrids Using IEC 61850 Standard. *IEEE Access*, 7:156044–156053.

Vieira, J. L., Ferreira, V. C., Bastos, I. V., Quincozes, S. E., de Oliveira Delfino, W., dos Santos, Y. d. R., Lopes, Y., Passos, D., Albuquerque, C. V., Moraes, I. M., et al. (2021). Thanos: Teleprotection holistic application for onos controller. In *Int. Symp. on Integrated Net. Manag. (IM)*, pages 818–823. IEEE.

Yoo, H. and Shon, T. (2015). Novel approach for detecting network anomalies for substation automation based on IEC 61850. *Multimedia Tools and Applications*, 74(1):303–318.

Zopellaro Soares, A. A., Lucas Vieira, J., Quincozes, S. E., Ferreira, V. C., Uchôa, L. M., Lopes, Y., Passos, D., Fernandes, N. C., Monteiro Moraes, I., Muchaluat-Saade, D., et al. (2021). Sdn-based teleprotection and control power systems: A study of available controllers and their suitability. *International Journal of Network Management*, 31(3):e2112.