Smart Grid Security Challenges and Approach at Substation Level Automation

Mladen Sverko [1]*, Darko Etinger* [1]*, Nikola Tankovic* [1]

[1] *Juraj Dobrila University of Pula*

Zagrebacka ul. 30, 52100 Pula, Croatia

ABSTRACT

This paper identifies the emerging cybersecurity issues of the smart grid ICT component in the implementation of control and monitoring systems at the substation level. The attack surface originates from a local network across different levels of interoperability, communication (data) model standard, and digital data collection. Given the level of complexity and overall exposure, the system is vulnerable to numerous cyber threats, resulting in significant consequences for system stability and availability. Since there is no absolute security or ultimately safe methods of cyber threat protection, an appropriate approach must be applied that will focus on prevention from the very design of the system, regular operation, and maintenance. In this paper, we propose a set of security measures that can be applied to elevate the security at the substation level.

Keywords: Smart Grid, Cybersecurity, Substation Automation, Control and Monitoring Systems, Power Distribution

INTRODUCTION

A smart grid must perform real-time monitoring and data analysis, tune itself to achieve optimal performance, and anticipate issues that may result in blackouts affecting entire regions. Numerous cyber-attack vulnerabilities should be analyzed and addressed considering all aspects of substation crucial to the overall smart grid. In cases of Stuxnet and Night dragon, attacks resulted in a substantial impact on the system, causing severe damage (Langner, 2011; Evans, 2011). With the emergence of new threats in the energy sector and targeted ransomware attacks, new diagnostic methods of machine learning are being considered (Oya and Omote, 2019). Such trends have resulted in general recommendations for industrial control systems related to security program development and deployment, risk assessment, and security architecture (Stouffer *et al.*, 2015), followed by guidelines emphasizing security engineering in the system lifecycle process (Ross, McEvilley and Oren, 2016). Recently these issues were addressed within a comprehensive document in the cyber-physical security system (Rashid *et al.*, 2019). As solutions implemented at the substation level of the ICT layer generally evolve in the direction of Internet-based technologies, this increases vulnerabilities and raises appropriate design principles.

The paper is organized as follows: the second section analyzes existing approaches in cybersecurity at the substation level, then design a model of the ICT layer, and single out critical assets and critical threats relevant to the smart substation. The third section proposes a holistic approach to cyber-security at the substation level, including the design approach to supervisory control and data acquisition (SCADA) system development. The final section concludes the paper.

RELATED WORK AND METHODOLOGY

It is common practice for researchers to implement various testbeds, primarily based on simulation software. In (Vellaithurai, Biswas and Srivastava, 2015), authors developed a testbed with a monitoring system layer, communication layer, and energy management layer to test the Aurora attack. Fig. 1 shows the smart substation ICT layer model based on the above testbed and substation models used in vulnerability assessment for SCADA system (Ten, Liu and Manimaran, 2008), with the addition of network and SCADA redundancy components. DNS and web servers are added to comply with the growing trend of internet-based SCADA systems development (Fazlollahtabar, 2021). The presented smart substation model shares a similar concept with other research related to Industrial control systems (ICS) and smart grid cybersecurity (Vellaithurai *et al.*, 2015; Sun, Hahn and Liu, 2018; Ullrich *et al.*, 2016; Wang *et al.*, 2018; Amin *et al.*, 2021; Zhang *et al.*, 2016) and can help define critical assets across the network layers. Liu *et al.* (2017) considers a malicious attack on bus and transmission line protection systems and use various Markov chain, Petri net, and Bayesian net methods (Vellaithurai *et al.*, 2015).

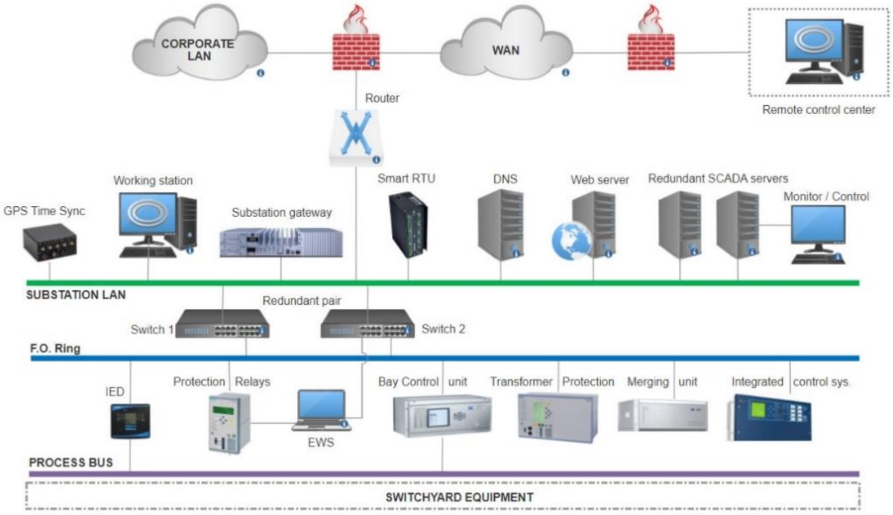

Figure 1. Model of substation ICT layer

Even if intelligent electronic device (IED) components are considered as critical assets under attack, the SCADA system is defined as a possible source of malware. In the case of an external attack, firewall and network switch residing on substation LAN are on the attack path. According to the vulnerability assessment proposed in Ten, Liu and Manimaran (2008), several penetrating substation networks are recognized with a SCADA system, VPN, and firewall as critical assets. It was concluded that the vulnerability scenario for each substation depends, among other things, on predefined firewall rule sets and security system policies. The research included three substation-level models under internal and external attack. In a state-of-the-art cybersecurity survey Sun, Hahn and Liu (2018) have noted that a commercial-grade firewall contains predefined rules that can conflict in many cases. However, as a core component, SCADA has been recognized as a primary target.

Critical Assets analysis

By analyzing the critical assets for the type of attack, the affected layer of substation network and source of the attack addressed in the previous section, the following critical assets are identified as specific for the defined SAS model. (1) Virtual Private Network (VPN) can raise the level of protection by providing a secure virtual environment for all connected devices, but that environment is as safe as the weakest node on the network. Furthermore, devices connected to LAN substations via VPN can also connect to their local LAN and depend on local security policies. If those are located on a compromised local network, they can quickly become an entry point for an external attack on LAN substations. (2) Firewall generally acts as a router that controls network traffic flow between networks that use different security measures. Cyberattacks gradually moved from the lower layers of network traffic to the application layer, reducing the firewall's overall efficiency. It can still be effective on the application layer, but if an attacker can deceive the filter and present itself as an allowed packet, it will pass through. In the case of a firewall implemented between corporate and substation networks, the goal is to provide data while protecting access to the system. (3) IEC 61850 Protocol shown on Fig. 2 presents structured data object model with well-defined semantics where data is organized by functions.

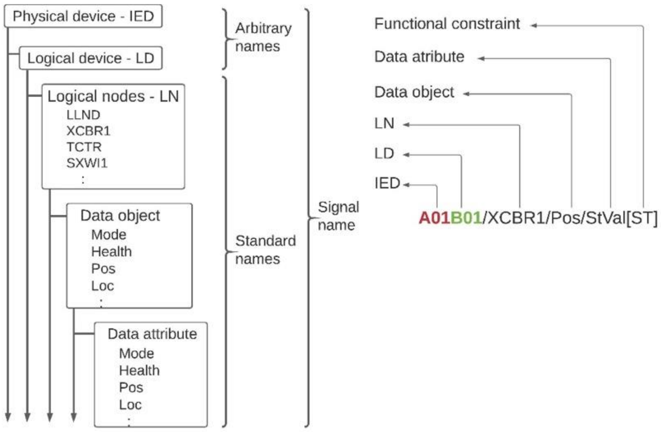

Figure 2. IEC 61850 Protocol Data Model

Some of the key benefits of the IEC 61850 standard comes from several types of configuration files structured to comply with formal XML-based configuration language, i.e., System configuration language (SCL), allowing more straightforward design and configuration of devices. Combined, they contain complete system specifications, configuration, descriptions, and communication parameters. As helpful as this is from the perspective of users and development engineers, the same data is of great benefit to attackers if they can be easily accessed on substation LAN. Considering that any signal exchanged on the local network is standardized in a way that clearly shows to which device and function it belongs, an attacker can, with relatively little effort, get an accurate real-time image of the entire system. (4) Cloud Solutions. There is no reason for SAS to resign cloud flexibility and not use cloud-based firewalls (Ullrich *et al.*, 2016). However, cloud firewalls are relatively new solutions, and the current infrastructure implies a physical firewall as part of SAS. By connecting to a cloud located outside the subnet LAN, the firewall allows traffic in both directions, which raises additional issues. First, the IP address to which we connect to cloud services can change as cloud services move between different data centers. IP address changes are problematic from the perspective of access control lists (ACLs), commonly known as packet filters, where filtering is done by IP addresses that can no longer be trusted. Second, if the firewall has domain-based rules, an attacker can still subscribe to the same cloud service, thereby sending packets from an approved source.

Relevant Types of Threats

Among significant number of cyber-threats affecting power grids (Langner, 2011; Evans, 2011), following can be considered as relevant (1) False Data Injections Attack (Wang *et al.*, 2018). The idea behind FDI is a faulty display of data coming from switchyard equipment over IDE on the process bus. By presenting the standard range/state data as critical (or opposite), we can force the operator's reaction in favor of the attacker. Through the FDI attacks, the smart grid can undergo load redistribution attacks, economic attacks, or misleading energy attacks (Amin *et al.*, 2021). (2) False Command Injections Attack (Zhang *et al.*, 2016) is more direct by generating a control signal sent to the IEDs without operator action. The consequence of both attacks is a change in the grid topology. In the structured IEC 61850 data model, the signal name reveals its function and destination device. Once an attacker has penetrated the system and analyzed network traffic on subnet LAN by capturing Manufacturing Message Specification protocol (MMS), it is not hard to understand which signal needs to be forged. (3) Distributed Denial of Service (DDoS) attack sends multiple requests and paralyzes the communication network by producing mass invalid data packages (Zhang *et al.*, 2020). In terms of the attack on substation ICT, it comes as an auxiliary attack to mask the previous two.

PROPOSED CYBERSECURITY MEASURES

Given the previously identified critical assets and relevant threats, the following essential elements of a holistic cybersecurity approach are proposed (1) Security by design. Zero trust user access and identity security architecture must be implemented (Mir and Ram Kumar, 2020) together with implementation of iteratively updated Zero trust security model (Mir, Rashid and Kumar, 2021). In general, the parametrization-over-programming principle should be followed in HMI development. Automated procedures should be defined managing alarming and reporting for remote locations in order to provide efficient operations (Mohani *et al.*, 2020). Combined with hardware and software redundancy, virtualization of SCADA servers, WEB servers, and workstations will provide a good prerequisite for fast system restore. (2) Advanced attack detection methods has more chance of success by using methods based on ML algorithms, in which modern approaches combine different techniques (Stouffer *et al.*, 2015). Some of the advanced countermeasures are defined in four phases of the Intelligence Led Penetration Testing (CBEST) framework, i.e. his implementation to the SCADA environment (Kaniewski, Jahankhani and Kendzierskyj, 2021). In this regard we suggest implementation of additional vulnerable virtual SAS elements that will serve as decoy for the attacker (Choo, Goh and Guo, 2021) which has already penetrated into the system and is pivoting the network laterally in search for vulnerable nodes. (3) Firewall and unidirectional gateway. As explained in Stouffer *et al.* (2015) unidirectional gateways permit data flow in one direction but are physically unable to send data back into the source network. When it comes to separating networks, a unidirectional gateway should replace a firewall to minimize all forms of external cyber-threats. On the other hand, firewall could be made more efficient in attack detection and prevention if enhanced by industrial grade Single Board Computer (SBC) as suggested by Choo, Goh and Guo (2021). (4) Data encryption at the local network level is a desirable measure to protect sensitive configuration files that are part of the IEC 61850 standard. Blocking access to this type of content will make it difficult for an attacker to gain insight into system functionality and grid topology.

Fig. 3 summarizes above the proposed cyber security measures in a holistic approach. to the design, operation and maintenance of ICT layer in relation to the prevention and protection of cyber threats.

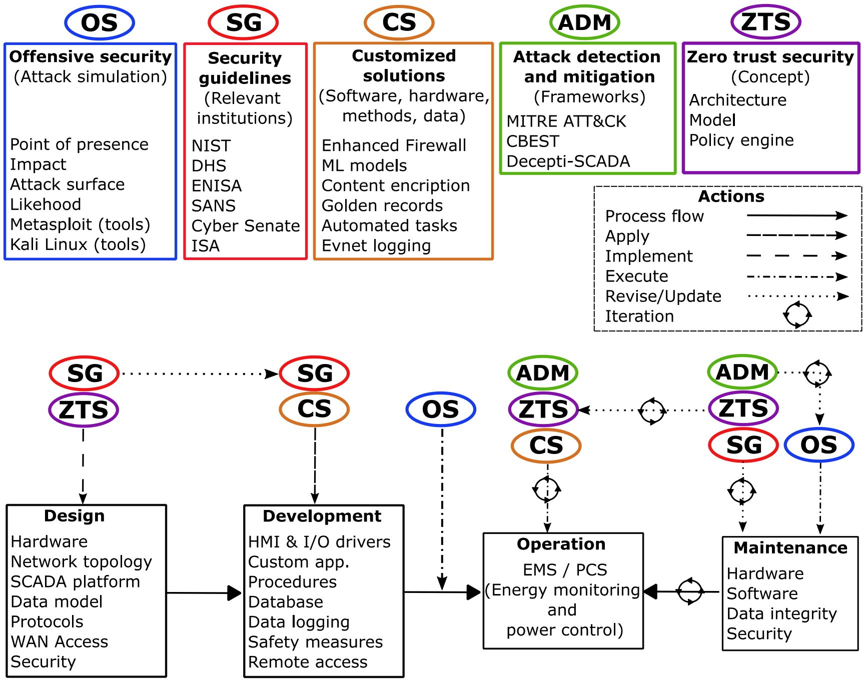

Figure 3. Cybersecurity holistic approach to SAS ICT layer

The proposed approach results in continuous attention to multiple aspects of cyber security from the early stages of project inception through operation and maintenance with the implementation of iterative and chained activities using updated models, frameworks and recommendations.

CONCLUSIONS AND LIMITATIONS

Model of ICT layer relevant to the smart substation based on existing testbed solutions has been used for analyzing critical assets proceeding from related works of vulnerability assessment, cybersecurity survey, and functional requirements for the development of cybersecurity protection systems. Substation-specific critical assets have been defined across the network layers, including physical devices, industry-specific protocols, and remote connections. We singled out the most relevant types of cyber-threats with the potential to paralyze the communication network or change the grid topology. Given the critical assets and relevant cyber-threats, we have proposed a holistic approach to cyber-security at the substation level. Proposed measures should be applied at the level of system design and development, data modeling, cybersecurity protection, operation and maintenance. Our analysis excluded users as a potential critical asset which, if included, would address an additional set of cybersecurity issues in the form of security awareness, access control, norms, and defense procedures. These issues significantly impact cybersecurity and, therefore, defense strategies should address them accordingly.

REFERENCES

Amin, M. *et al.* (2021) ‘CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review’, *IEEE Access*, pp. 38571–38601. doi: 10.1109/ACCESS.2021.3063229.

Choo, C. P. L., Goh, W. L. and Guo, H. (2021) ‘Security Development with an Industrial Device for SCADA System’, *IRC-SET 2020*, pp. 717–730. doi: 10.1007/978-981-15-9472-4_61.

Evans, S. (2011) *‘Night Dragon’ cyber attacks hit global energy companies - Tech Monitor*. Available at: https://techmonitor.ai/techonology/software/night-dragon-cyber-attacks-hit-global-energy-companies-100211 (Accessed: 17 January 2022).

Fazlollahtabar, H. (2021) ‘Internet of Things-based SCADA system for configuring/reconfiguring an autonomous assembly process’, *Robotica*, pp. 1–18. doi: 10.1017/S0263574721000758.

Kaniewski, J., Jahankhani, H. and Kendzierskyj, S. (2021) ‘Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector’, *Advanced Sciences and Technologies for Security Applications*, pp. 1–20. doi: 10.1007/978-3-030-72120-6_1.

Langner, R. (2011) ‘Stuxnet: Dissecting a cyberwarfare weapon’, *IEEE Security and Privacy*, 9(3), pp. 49–51. doi: 10.1109/MSP.2011.67.

Liu, Xindong *et al.* (2017) ‘Power System Risk Assessment in Cyber Attacks

Considering the Role of Protection Systems', *IEEE Transactions on Smart Grid*, 8(2), pp. 572–580. doi: 10.1109/TSG.2016.2545683.

Mir, A., Rashid, I. and Kumar, K. R. (2021) 'An Augmented Smart Grid based SCADA Security Management System (SSMS) based on Zero-Trust Architecture'. doi: 10.4108/eai.27-2-2020.2303258.

Mir, A. W. and Ram Kumar, K. R. (2020) 'Zero Trust User Access and Identity Security in Smart Grid Based SCADA Systems', *Advances in Intelligent Systems and Computing*, 1383 AISC, pp. 716–726. doi: 10.1007/978-3-030-73689-7_68.

Mohani, S. S. *et al.* (2020) 'SCADA System Framework for Monitoring, Controlling and Data Logging of Industrial Processing Plants', *2020 International Conference on Computational Intelligence, ICCI 2020*, pp. 149–152. doi: 10.1109/ICCI51257.2020.9247645.

Oya, M. and Omote, K. (2019) *Early detection of remote access Trojan by software network behavior*, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer International Publishing. doi: 10.1007/978-3-030-14234-6_37.

Rashid, A. *et al.* (2019) *The Cyber Security Body of Knowledge*. CyBOK, University of Bristol. Available at: https://www.nationalarchives.gov.uk/ (Accessed: 17 January 2022).

Ross, R. S., McEvilley, M. and Oren, J. C. (2016) 'Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [including updates as of 1-03-2018]'. doi: 10.6028/NIST.SP.800-160.

Stouffer, K. *et al.* (2015) 'Guide to Industrial Control Systems (ICS) Security NIST Special Publication 800-82 Revision 2', *NIST Special Publication 800-82 rev 2*, pp. 1–157. Available at: http://industryconsulting.org/pdfFiles/NIST Draft-SP800-82.pdf.

Sun, C. C., Hahn, A. and Liu, C. C. (2018) 'Cyber security of a power grid: State-of-the-art', *International Journal of Electrical Power and Energy Systems*, 99, pp. 45–56. doi: 10.1016/j.ijepes.2017.12.020.

Ten, C. W., Liu, C. C. and Manimaran, G. (2008) 'Vulnerability assessment of cybersecurity for SCADA systems', *IEEE Transactions on Power Systems*, 23(4), pp. 1836–1846. doi: 10.1109/TPWRS.2008.2002298.

Ullrich, J. *et al.* (2016) 'The role and security of firewalls in cyber-physical cloud computing', *EURASIP Journal on Information Security Ullrich et al. EURASIP Journal on Information Security*, 2016, p. 18. doi: 10.1186/s13635-016-0042-3.

Vellaithurai, C. *et al.* (2015) 'CPIndex: Cyber-physical vulnerability assessment for power-grid infrastructures', *IEEE Transactions on Smart Grid*, 6(2), pp. 566–575. doi: 10.1109/TSG.2014.2372315.

Vellaithurai, C. B., Biswas, S. S. and Srivastava, A. K. (2015) 'Development and Application of a Real-Time Test Bed for Cyber–Physical System', *IEEE Systems Journal*, pp. 1–12. doi: 10.1109/jsyst.2015.2476367.

Wang, Z. *et al.* (2018) 'Power System Security under False Data Injection Attacks with Exploitation and Exploration Based on Reinforcement Learning', *IEEE Access*, 6, pp. 48785–48796. doi: 10.1109/ACCESS.2018.2856520.

Zhang, Y. *et al.* (2016) ‘Inclusion of SCADA Cyber Vulnerability in Power System Reliability Assessment Considering Optimal Resources Allocation’, *IEEE Transactions on Power Systems*, 31(6), pp. 4379–4394. doi: 10.1109/TPWRS.2015.2510626.

Zhang, Z. *et al.* (2020) ‘Pattern Analysis of Topological Attacks in Cyber-Physical Power Systems Considering Cascading Outages’, *IEEE Access*, 8, pp. 134257–134267. doi: 10.1109/ACCESS.2020.3006555.