A Blueprint for Cyber Security of Brownfield Substations in Power Systems using IEC 62443

Rajkumar, Vetrivel S.; Musunuri, Shyam; Stefanov, Alexandru; Bruijns, Siem; Wit, Johan de; Klaar, Danny; Louh, Amadou; Thoen, Arnaud; Palensky, Peter

Publication date
2022

Document Version
Final published version

Published in
Proc. CIGRE Paris Session 2022

Paper ID – 0348 Session 2022
D2 - Information Systems & Telecommunication
PS 2/ Cybersecurity Techniques, Technologies,
and Applications for Securing Critical Utility Assets

A Blueprint for Cyber Security of Brownfield Substations in Power Systems using IEC 62443

Vetrivel S. Rajkumar[*1], Shyam Musunuri[2], Alexandru Stefanov[1], Siem Bruijns[3], Johan de Wit[4], Danny Klaar[3], Amadou Louh[5], Arnaud Thoen[5], Peter Palensky[1]

[1]Delft University of Technology, [2]Siemens AG, [3]TenneT TSO BV
[4]Siemens Nederland NV, [5]Stedin NV
[1,3,4,5]The Netherlands, [2]Germany

***V.SubramaniamRajkumar@tudelft.nl**

SUMMARY

Increased power grid digitalisation and the transition to cyber-physical power systems raises questions, especially regarding vulnerabilities, cyber threats, and secure operation of the power system. It is well recognised that Information and Communication Technologies (ICTs) are vulnerable to cyber attacks. As a result, the beginning or middle of the life cycle of utility critical infrastructures pose serious cyber security threats. This is because for some of the equipment, the concept of cyber security may be very limited or non-existential, e.g., segregation of critical assets. Furthermore, existing substation infrastructures comprise of a combination of heterogeneous, co-existing smart and legacy technologies. When these are upgraded with newer technologies such as Internet of Things (IoT) sensors, this gives rise to significant cyber security challenges that must be addressed. Accordingly, cyber security and resilience aspects are crucial for further digitalisation and modernisation of the power system. The IEC 62443 3-3, 4-2, and 2-4 are a set of standards that specifically address these issues. The standards serve as a cornerstone for a secure-by-design and defence in depth approach. The security level of substation Operational Technologies (OT) infrastructure needs to be upgraded, incorporate latest cyber security developments, and minimise the risk of cyber attacks and threats. The upgrades whilst being critical, are non-trivial to perform, as power grid OTs have extremely high uptime requirements with little to no time for patching or security related activities. This presents system operators with challenges for the implementation of up-to-date cyber security practices. The most critical aspect to understand and improve the cyber security of a substation is knowledge about the actual and target security levels. Hence, in this paper, we consider typical brownfield OTs of substations and propose an iterative method to calculate the actual and target cyber security levels. Furthermore, we propose a blueprint to enhance cyber security of electrical substations by minimising the gap between the actual and target security levels through a set of countermeasures. The iterative method involves a step-by-step approach to calculate the substation security levels based on IEC 62443. The proposed method can be adopted for different substation architectures to determine the target security level of a substation. Moreover, the proposed blueprint provides crucial know-how of hardening of OT systems and secure access controls at all levels within a typical brownfield substation installation. This aids system operators to cyber secure all critical OT assets. A practical case-study is undertaken to evaluate the security levels of a substation, based on a real-world reference substation architecture and the proposed method.

KEYWORDS

Architectural Levels - Assessment of Security Levels - Cyber Security - Cyber Attacks - OT Security - IEC 62443

1. Introduction

Increased power grid digitalisation and the transition to cyber-physical power systems raises questions, especially regarding vulnerabilities, cyber threats, and secure operation of the power system. It is well recognised that Information and Communication Technologies (ICTs) are vulnerable to cyber attacks. As a result, the beginning or middle of the life cycle of utility critical infrastructures pose serious cyber security threats. This is because for some of the equipment the concept of cyber security may be very limited or non-existential, e.g., segregation of critical assets. Furthermore, existing substation infrastructures comprise of a combination of heterogeneous, co-existing smart and legacy technologies. When these are upgraded with newer technologies such as Internet of Things (IoT) sensors, this gives rise to significant cyber security challenges that must be addressed. Accordingly, cyber security and resilience aspects are crucial for further digitalisation and modernisation of the power system. The IEC 62443 3-3, 4-2, and 2-4 are a set of standards that specifically address these issues. The standards serve as a cornerstone for a secure-by-design and defence in depth approach. This paper considers typical brownfield Operational Technologies (OTs) of substations. The security level of substation OT infrastructure needs to be upgraded, incorporate latest cyber security developments, and minimise the risk of cyber attacks and threats. The upgrades whilst being critical, are non-trivial to perform, as power grid OTs have extremely high uptime requirements with little to no time for patching or security related activities. Additionally, there is also the added risk of improper upgrades and limited possibilities for a roll-back. These risks further limit the willingness and possibilities for upgrades/patches. Consequently, this presents system operators with challenges for the implementation of up-to-date cyber security practices, e.g., authentication and access mechanisms, key management infrastructures, and verified certifying authorities and certificates for digital signatures. Hence, it is crucial to quantify the security levels of substation OT which this paper seeks to address.

1.1 Applicable Reference Model

A typical brownfield electrical substation consists of multiple components from various different vendors. Hence, to categorise the equipment into different levels of operation, the reference model based on the ISA IEC 62443-1-1/2007 standard is used. Similarly, the Purdue Enterprise Reference Architecture, also known as the Purdue model, was developed in the late 1990s to serve as a methodical approach to compartmentalise applications and features within an Industrial Control System (ICS). Over the years, it has been revised to take security and safety into account. Now, its intended purpose is to improve ICS efficiency and reduce costs through automation, based on digitalisation. Hence, the model is widely adopted across government sectors and industries to create a flexible defence-in-depth approach to secure critical ICS. Therefore, in this work, we address the cyber security of an existing substation by considering a modified Purdue model, based on the IEC 62443 standards. This is shown in Figure 1, consisting of six architectural stages in total, i.e., stages 0 to 5. It includes physical equipment such as current and voltage transformers, circuit breakers, and disconnects at stage 0, with relays and protection devices at stage 1. Site monitoring and local displays are covered under stage 2, while stage 3 includes Supervisory Control And Data Acquisition (SCADA), operations management, etc. Enterprise IT systems such as webmail servers fall under stage 4. Finally, stage 5 comprises of cloud-based solutions for monitoring and control applications. We envisage that the substations of the future will also comprise of stage 5. In the scope of this work, we consider stages 0-3.

1.2 State-of-the-Art and Gaps

Cyber security analysis of substations and industrial control systems based on modern-day standards such IEC 62443 and IEC 62351 is a relatively new development. This has gained invigorated attention in the wake of the increasing threat of cyber attacks on critical infrastructure systems. As noted in [1], concerns about protecting these systems against attacker actions has been growing since the impact of such attacks can have serious financial and societal consequences. The most crucial reference for this research is [2], which presents a clear understanding of this topic. In this work, the authors discuss the limitations of the Purdue model and present solutions to overcome the same. Likewise, leading industrial vendors and manufacturers have also published technical white papers on the implementation of IEC 62443 security levels for industrial control systems, such as in [3].

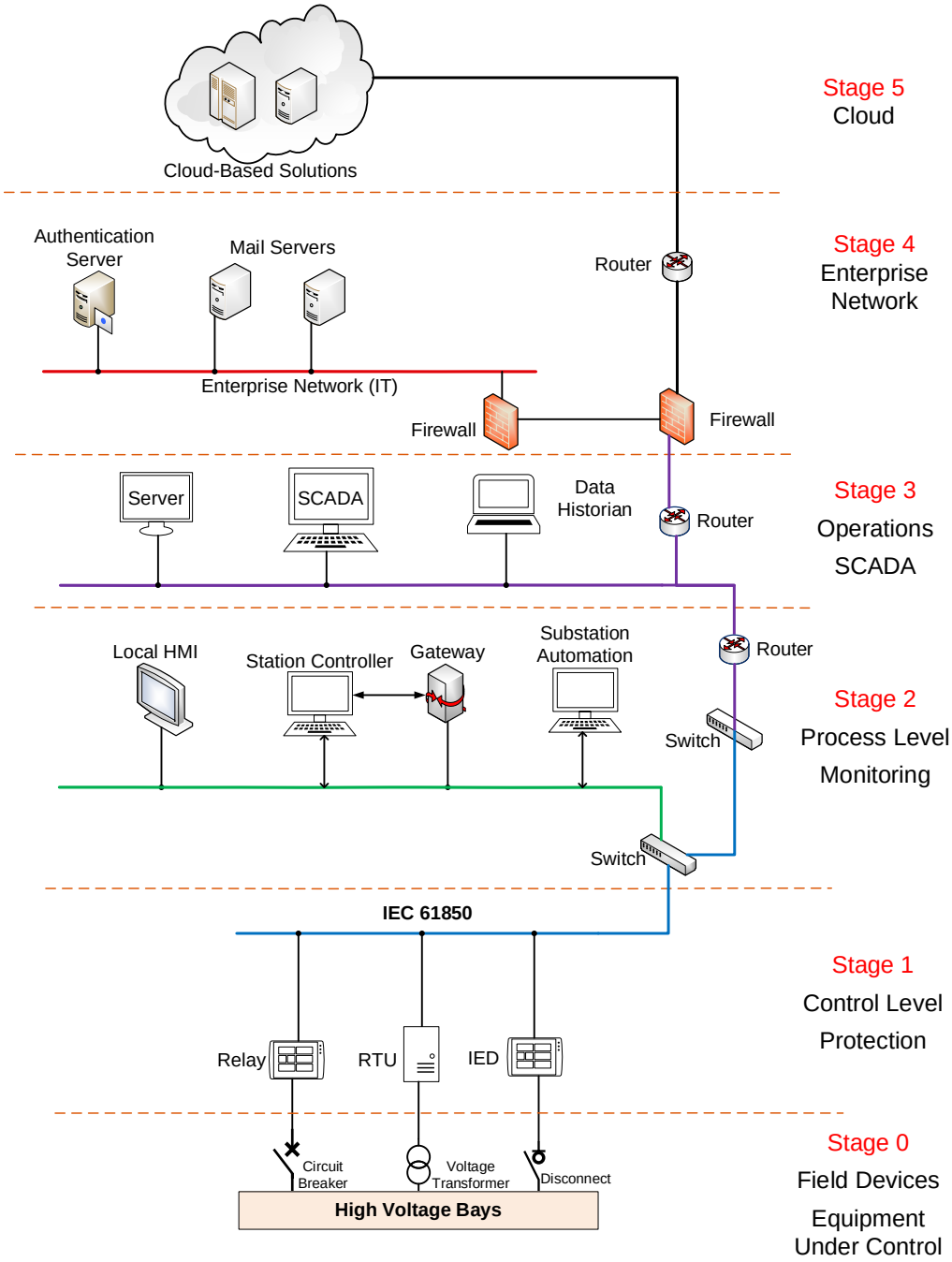

Figure 1: Purdue reference model for substations, modified based on IEC 62443-1-1/2007

The IEC 62443/1-1 standard defines three substation security levels, as follows:

1) Security Level Target (SL-T): as the name suggests, the SL-T is a security level assigned to a stage, based on a comprehensive risk assessment. The main goal of SL-T is to determine the required effectiveness of countermeasures, devices, and systems in place to prevent a security compromised of the system under consideration. For any system, computing the SL-T is based on multiple layers of security and overall impact.
2) Security Level Actual (SL-A): the SL-A on the other hand is the true security level of a stage. It is a function of time and decreases with it, due to degradation of countermeasures, new vulnerabilities and threats, etc. Hence, the objective of any system operator is to ensure that at any given instant of time, for a particular stage, $\boldsymbol{SL-A \geq SL-T}$.
3) Security Level Capability (SL-C): the SL-C is defined as the set of countermeasures and inherent security properties of devices and systems within a stage that contribute to it. It can

be calculated as a measure of the effectiveness of a countermeasure, device, or system for the addressed security property. For example, these can include factors such as preserving confidentiality of messages / information / communication, detection of tampering, security status, etc.

1.3 Bridging the Gaps between Security Levels

Typically, there is a knowledge gap of the target (SL-T) and achieved/actual security levels (SL-A) within a substation. Therefore, in this paper we propose:

1) An iterative method to calculate the actual and target cyber security levels of substations in the OT domain. The iterative method involves a step-by-step approach to calculate the substation security levels based on IEC 62443. The proposed method can be adopted for different substation architectures to determine the target security level of a substation.
2) A blueprint to enhance the cyber security of electrical substations by providing a set of countermeasures to harden OT systems. The latest countermeasures are aimed at dealing with emergent threat actions, in comparison to well-known countermeasures such as disabling open ports and unused services.
3) A practical case-study is undertaken to evaluate the security levels of a substation, based on a real-world reference substation architecture and the proposed method.

2. Attack Paths in a Substation

An attack path in a substation refers to the means by which a malicious actor may take to deliberately tamper with the services of at least one protection, automation or control device. As previously mentioned, a substation can be segregated into different architectural stages, as defined by the Purdue model. This allows for network segmentation in the substation to bolster cyber security. Consequently, attack paths for each stage can then be individually analysed.

2.1 Cyber Security Management System for Substations

The IEC 62443 2-1 presents the elements that constitute a Cyber Security Management System (CSMS) for ICS. These elements represent what shall and should be included in the CSMS in order to protect ICS against cyber attacks. The elements are presented in the following three main categories: 1) risk analysis, 2) addressing risks with CSMS, and 3) monitoring and improving CSMS. In this work, we consider that CSMS is an essential prerequisite for making the systems safe and secure.

2.2 OT Security Architecture

Operational technologies of substations are undergoing a major technological face shift. This is primarily driven by the adoption of Ethernet-based network protocols as defined by IEC 61850, digitalisation, and emerging new technologies such as cloud-based solutions. The increased use of digital technologies brings numerous benefits but also cyber security challenges, as evidenced through various reported cyber attacks on critical infrastructures. The holistic study of the combined substation OT and cyber security necessitates the use of a reference architecture. This architecture is applied to understand the OT network topology for substation automation, along with the cyber security requirements for each stage. The reference architecture of a real-world substation automation project is illustrated in Figure 2.

2.3 Common Vulnerabilities and Exposures in Substations

The risk of cyber attacks on substations can be manifold when the OT networks do not meet the required cyber security norms. Consequently, malicious actors may exploit publicly known vulnerabilities to cause damages to Safety (S), Environment (E), Finance (F), and Reputation (R) of an organisation. Based on the exploits made available as Common Vulnerabilities and Exposures (CVEs) by the National Vulnerability Database (NVD) of the United States government, the list of reported CVEs for a substation by January 2022 is summarised in Table I. The Common Vulnerabilities Scoring System (CVSS) score indicates the severity of the attack if a vulnerability is successfully exploited. From the total number of substation CVEs, i.e., 612, it is evident that the assumption of substation OT networks being air gapped and therefore secure is far from reality.

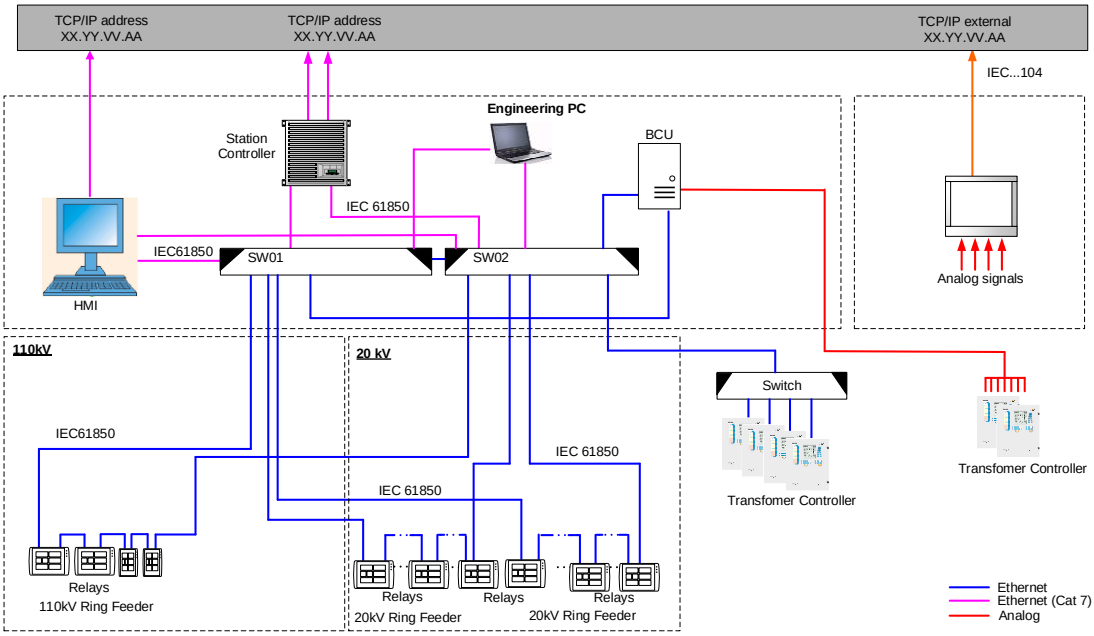

Figure 2: Substation reference architecture

Table I: Summary of CVEs and possible exploits of substation equipment

Level	Device	CVEs	Major CVE	CVSS	Exploit
0	Merging Units	8	2021-27452	9.8	Malicious control
0	Circuit Breakers	3	2021-21294	7.5	Resource consumption
1	Protection Relays	27	2021-33719	9.8	Buffer copy
2	Network Switches	201	2021-40113	9.8	Remote code execution
3	Network Routers	163	2021-41435	9.8	Brute-force protection bypass
3	Substation Controllers	210	2021-40358	9.8	Unauthorised access
	Total	612			

3. Security Levels Calculation and Countermeasures Blueprint

In this section, a method is proposed to calculate the target security level, i.e., SL-T, as defined by IEC 62443/3-3 for the substation reference architecture.

3.1 Evaluation of SL-T

The target security level for critical infrastructures, particularly in the energy domain must be as high as possible to ensure an uninterrupted service. Accordingly, for the aforementioned substation reference architecture, a Security Level 4 (SL 4) is considered. According to IEC 62443, SL 4 is defined as “security protection against intentional violation using sophisticated means with extended resources.” Based on [4] and IEC 62443, the proposed method for iterative calculation of SL-T is presented as a flowchart in Figure 3.

A sample calculation of SL-T for the reference architecture for a threat action in architectural stage 3 is as follows:

1. Identify the threat action, e.g., phishing using social engineering.
2. For the identified threat action (phishing), conduct the impact analysis on safety, finance, environment, and reputation. The results of the analysis are depicted in Figure 4 in stage 3.
3. The impact on safety is calculated to be ‘5’ as phishing leads to unauthorised access. Adversaries can maliciously tamper with equipment, thereby jeopardising the safety and health of personnel.

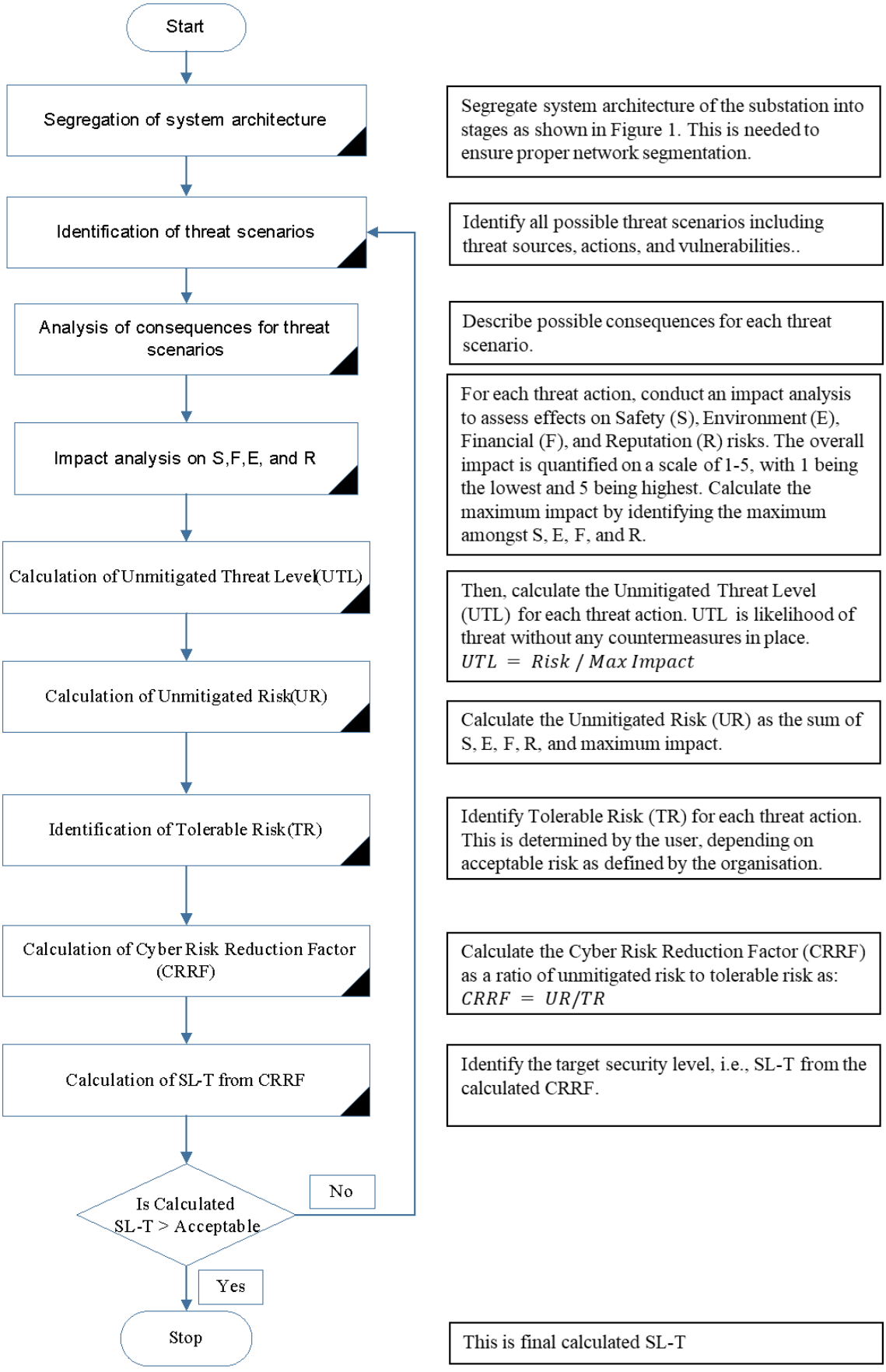

Figure 3: Flowchart of iterative method to calculate target substation security level

4. The impact on environment is calculated to be ‘4’ as adversaries can create service discontinuity such as a blackout.
5. The financial impact is calculated to be ‘4’ as adversaries may cause a blackout, amounting to significant financial losses for a large organisation.
6. The impact on reputation is calculated to be ‘4’ as harm to the company's reputation extends internationally through public media outlets and leads to negative publicity.
7. Calculate unmitigated risk as sum of steps 3-6 and maximum impact, max (S, F, E, R) = 5. In this case, the unmitigated risk is 22.
8. Owing to the nature of critical infrastructures the tolerable risk is calculated as 4. Thereby, the CRRF is calculated to be 5, as shown in Figure 5.
9. Based on the lookup table, CRRF from step 8 corresponds to a target security level of 3.

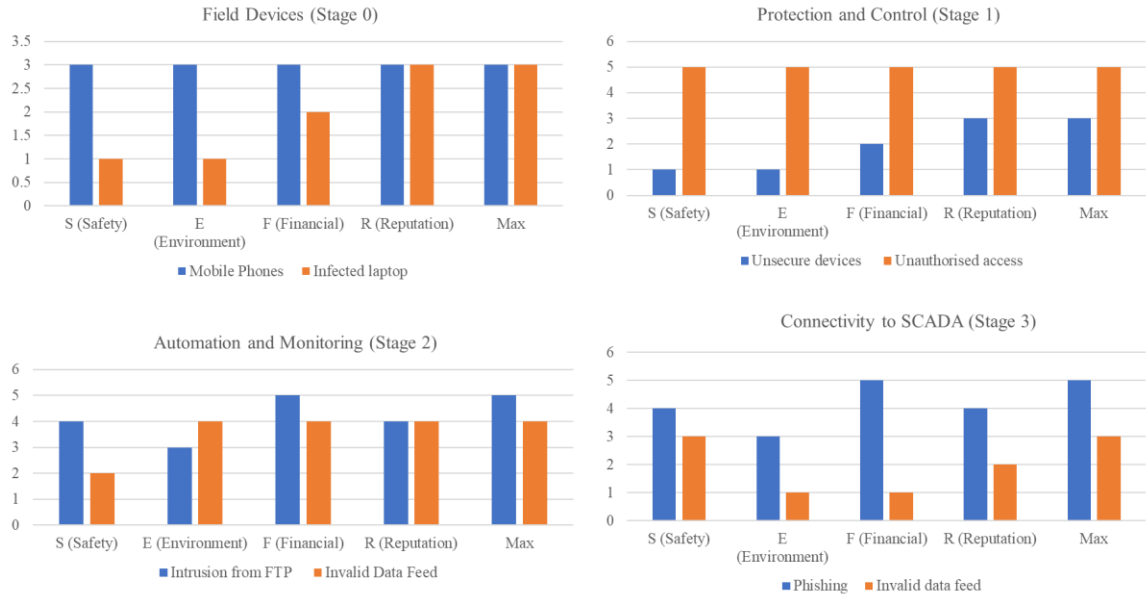

Figure 4: Sample calculation of risks for identified threat actions against each stage

Tolerable Risk = 4		
RISK	CRRF	SL-T
1	0.25	0
2	0.5	0
3	0.75	0
4	1	0
5	1.25	0
6	1.5	1
7	1.75	1
8	2	1
9	2.25	1
10	2.5	1
11	2.75	2
12	3	2
13	3.25	2
14	3.5	2
15	3.75	2
16	4	3
17	4.25	3
18	4.5	3
19	4.75	3
20	5	3
21	5.25	4
22	5.5	4
23	5.75	4
24	6	4
25	6.25	4

			Likelihood				
			Improbable	Rare	Unlikely	Possible	Likely
			1	2	3	4	5
Impact	Trivial	1	1	2	3	4	5
	Minor	2	2	4	6	8	10
	Moderate	3	3	6	9	12	15
	Major	4	4	8	12	16	20
	Critical	5	5	10	15	20	25

Figure 5: CRRF lookup table (left) and impact-likelihood risk matrix (right)

3.2 Definition of SL-A for the reference architecture

From the reference architecture, based on the security properties of devices and systems, it is inferred that the achieved security level is SL 3. According to IEC 62443, SL 3 is defined as "protection against intentional violation using sophisticated means with moderate resources, specific skills and moderate motivation." The SL-A of a zone depends on inherent security properties of devices and systems within it. No additional countermeasures other than existing ones are considered in the calculation.

3.3 Analysis of SL-C and Countermeasures

From the studied reference architecture, based on the security properties of devices and systems, it is observed that there is a gap of one security level between the SL-T and SL-A, i.e., SL 4 – SL 3. To address this gap, identified security countermeasures must be implemented to reduce the actual risk of threat actions. All countermeasures cannot be implemented at once due to financial and time-based constraints. Therefore, there will be iterations of countermeasures subject to the constraints. Based on the level of implementation, the mitigated risk level reduces in proportion to applied countermeasures. The most general countermeasures applicable to substations are summarised in Table II.

Table II: List of countermeasures using state-of-the-art cyber security practices

Countermeasure	Description	Application
Policies and procedures	Definition and reinforcement of appropriate/inappropriate behaviour.	Zero trust architecture, policy documents, procedures,
Hardening	Strengthen the system by adopting necessary security measures.	Adoption of IEC 62351-6, disabling open ports, services.
Flow controls	Control the flow of data in and out of the system	Use of next generation firewalls, proper configuration of routers, switches, and firewalls.
Integrity controls	Prevention of unauthorised data disclosure	Default deny mechanism, Encrypted communications, use of VPNs, firewall whitelisting.
Early warning indication	Provide alerts and alarms of suspicious activities	Intrusion detection and prevention systems, and security incidents and event management.
Access controls	Manage user authentication for both logical and physical access	Jamming of mobile devices, limiting wireless communications within substation perimeter.

4. Conclusions and Recommendations

In this paper, we developed a method and blueprint to enhance the cyber security of electrical substations by evaluating the actual and target security levels, as defined by IEC 62443. The OT community is mainly comprised of experts handling electrical equipment. However, with the increasing importance of cyber security in critical electrical infrastructures, there is an urgent need for the combination of expertise in both the OT and cyber security domains. Therefore, the most important aspect for achieving cyber security of the substation is knowledge about the actual security and target security levels. Using the proposed method, a systematic approach is undertaken to evaluate the security levels of a reference substation architecture. The method can be adopted for different substation architectures to determine the target security level. Once calculated, along with the achieved security level, the necessary countermeasures are implemented. Depending on the complexity of the project, financial capabilities, time constraints, and cyber security expertise, the approach may need iterations for achieving the security level as close as possible to the target security level. Owing to the importance of this critical infrastructure and rapidly evolving cyber threat landscape, the iterations must be completed in a timely manner. Periodic audits may also be conducted to ascertain that the substations are hardened and secure.

There is a knowledge gap in the OT community on the security standards to be implemented. Therefore, we recommend the usage of IEC 62443 standards for industrial control and automation

systems, which were developed by OT and cyber security experts. Furthermore, we recommend the MITRE ATT&CK framework for industrial control systems to study cyber attacks and adversarial behaviour. The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described for the ICS knowledge base. Based on real-world incidents of cyber attacks on ICS, we recommend the use of the proposed countermeasures to reduce the impact of the attack. We also foresee the need for the collaboration between industry and academia to test and verify cyber security countermeasures in laboratory settings before actual real-world deployment.

BIBLIOGRAPHY

[1] AL. Franceschett et.al, "A Holistic Approach - How to Achieve the State-of-art in Cybersecurity for a Secondary Distribution Automation Energy System Applying the IEC 62443 Standard" (in Proc IEEE PES Innov Smart Grid Tech Conf, September 2019, pages 1–5)

[2] D. Dolezilek, D. Gammel, and W. Fernandes, "Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems" (in Proc Int Conf Dev in Power Syst Prot, July 2020, pages 1–6)

[3] D. DesRuisseaux, "Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications," 2018. [Online]. Available: https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Name=998-20186845_GMA-US.pdf&p_Doc_Ref=998-20186845

[4] J. Braband, "Why 2 times 2 ain't necessarily 4 - at least not in IT security risk assessment" (arXiv.org, doi: arXiv:1603.03710)