An Augmented Smart Grid based SCADA Security Management System (SSMS) based on Zero-Trust Architecture

Abdul Wahid Mir[1], Irfan Rashid[2], K. R. Ram Kumar[3]

{wahids@live.com[1], samirfan@gmail.com[2], k.ramkumar@chitkara.edu.in[3]}

Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India[1,3], SSM College of Engineering, Srinagar, India[2]

Abstract. Critical infrastructures like electricity services are essential services that underprop a nation's society and aids to its economy, security, health and progress. Supervisory Control and Data Acquisition (SCADA) system i.e. industrial control system (ICS) for electricity utility sector forms the backbone of the operations and control processes. The security to this national level critical infrastructure must be a topmost priority for any nation. The aim of this research paper is to propose an augmented smart grid-based SCADA security management system (SSMS) for electricity utility companies that will empower them to protect their industrial control networks from security attacks and operational interruptions by providing complete and centralized visibility of operations network and security state of the deployed infrastructure. The paper will present the various components of SCADA security management systems and the proposed centralized SCADA security management system based on Zero-Trust architecture.

Keywords: SCADA, critical infrastructures, cyber security, security management system, smart grid, Zero-Trust.

1. Introduction

Critical infrastructure (CI) security is a perennial concern for the service providers with emerging new challenges starting to evolve with each passing day. Critical infrastructure facilities like nuclear plants, power plants, oil and gas refineries, etc. can benefit greatly by leveraging the connectivity, situational awareness and operations intelligence aided by the latest technological advances such as Smart Grid and Internet of Things (IoT), nevertheless it is impossible to anticipate all possible types of security attacks that is a major concern for all the stakeholders [1]. Traditional security measures are based on a notion of castle-and-moat i.e. outsiders access to the network is difficult while there is default trust within the network for the insiders. The issue with this approach is that if hackers succeed to pose as an insider, they will have access to everything within the network. The traditional security architecture is generally referred to as perimeter model in which the protection is ensured by implemented by having multiple layers of defenses. The outside attackers must go past each layer of defenses prior to gaining access whereas insider threats are not taken into consideration as there is implicit trust for the insiders [2].

In traditional security architecture, the network segregation in the form of various zones is implemented with one or more perimeter level firewalls. The level of trust is established at the

ICIDSSD 2020, February 27-28, New Delhi, India

DOI 10.4108/eai.27-2-2020.2303258

zone level that decides resources provision and reachability. The following are the typical levels of zones in the traditional security architecture [3]:

Table 1. Traditional Security Zones

#	Zone Level	Description
1	Internet zone	Services directly linked to public internet.
2	Demilitarized zone (DMZ)	The high-risk resources are kept in this zone that are connected to the public internet.
3	Trusted zone	This contains typical business application services like intranet-based applications.
4	Privileged zone	Highly critical services like Payment Card Industry (PCI) related servers or services are kept in this zone.

The traditional security architecture splits networks into segregated zones within one or more firewalls. Each zone is allotted a certain level of trust which decides which network resources are accessible or not accessible. In this model the high-risk resources such as web servers connected to the public internet are placed in “DMZ” or “demilitarized zone” that helps to monitor and control the traffic thoroughly.

The figure 1 below depicts the traditional security architecture and typical zoning mechanism:

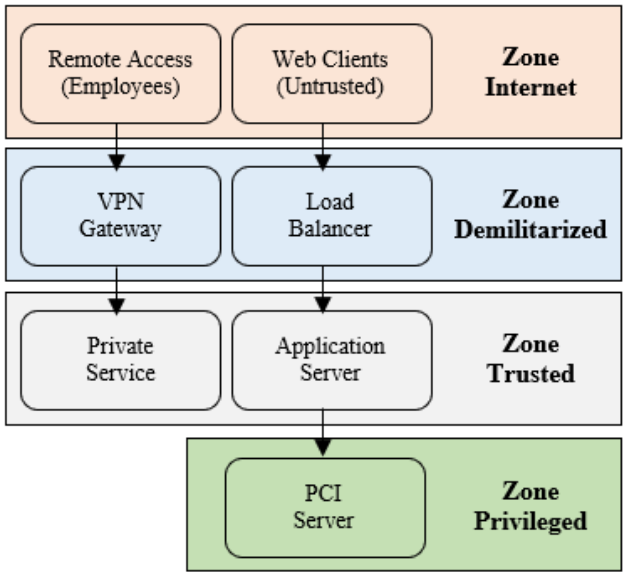

Fig. 1. Traditional Security Zones

The traditional security architecture has many disadvantages that include challenge to monitor and inspect the traffic within intra-zone, physical or logical host placements, multiple single points of failure, etc.

The criticality of the industrial networks requires more attention to security and implementing strategies that will ensure the safety of assets and data in the critical infrastructures. A typical SCADA systems have evolved into complex infrastructures. These systems comprises of various local or internal networks, corporate networks, external networks

for VPN access, remote branch offices, substation networks, etc. This density has surpassed the traditional security architecture as there is no single rule of thumb which can ensure safety and security of critical infrastructures [4].

The latest security strategy that is gaining huge interest in industrial control systems is "Zero-Trust Architecture" that is based on principle of never trust, always verify.

2. Background - Zero-Trust Architecture

As per the National Institute of Standards and Technology (NIST), the operative definition of the Zero-Trust Architecture is *"Zero-Trust Architecture (ZTA) provides a collection of concepts, ideas, and component relationships (architectures) designed to eliminate the uncertainty in enforcing accurate access decisions in information systems and services"* [3]. It is impossible for the organizations to predict all possible types of attacks in the critical infrastructures beforehand. The zero-trust architecture offers an effective method to improve security posture by being better prepared to face and mitigate possible risks. Since "Trust" is a vulnerability and is its own exploit, it is very much pertinent to industrial control systems. ISA-99 and IEC 62443 industrial standards for industrial control systems put down the very detailed mechanism for the security implementation in terms of segmentation zones, secure channels between zones and endpoint security in order to ensure the security of the systems. Nevertheless, trust model is very much core of these industrial standards [5]. These security standards provide layered approach to security and major focus is on secure authentication of the users into the trust zone. Once the user is authenticated and inside the network, trust zone enables them to navigate through as most of the restrictions are lifted off. In most of the environments, there is no proper logging and auditing at the user's activity level which is being performed by them. In the traditional security model, the first line of defense is critical and failure to which can expose systems to serious vulnerabilities if they are exploited [6]. The zero-trust model is addressing this issue with better approach. With zero-trust approach, the security is focused towards securing the critical data and resources within an organization.

The figure 2. below represents the zero-trust security architecture. In this architecture, the supporting system is known as control plane and all the other components are known as data plane. The data plane is configured and coordinated by the control plane. The control plane allows access requests only from the authenticated and authorized users and devices. The control plane layer also allows the fine-grained policies implementation on the basis of parameters like role in the organization, type of device or time of day. Additionally, the access to higher level secure resources can be configured with stronger authentication policies and systems. Once the control plane has approved access to a request, the data plane will be configured as such that it only accepts traffic from the specific client only [7]. The key idea in this approach is that even if compromises with respect to the strength of these measures are made, a 3rd party is granted access and authenticated based on different types of inputs.

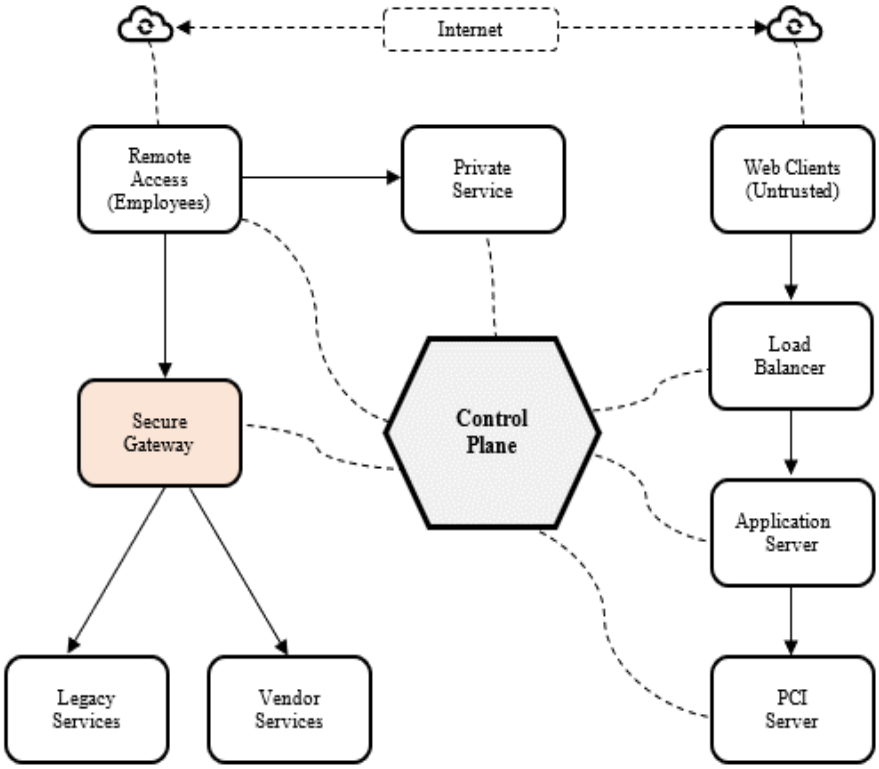

Fig. 2. Zero Trust Security Architecture

2.1. Tenets of Zero-Trust Architecture

The following are the six tenets of the zero-trust architecture:

i. The resources within an organizations are categorized in terms of availability of data sources and computing services.
ii. The communication within an organization is to be secured irrespective of its source or location.
iii. Each organizational resources are available via access control criteria of individual connection to each resource.
iv. The access policy determines the access control criteria for the resources that mandates the user identity state, user behavioral attributes, user requesting source or system, etc.
v. The organization ensures the security state of all its systems and sub-systems is at adequate level with proper monitoring mechanisms for the same.
vi. The user authentication process is not static but dynamic with stringent enforcement of the polices prior to any access provisions.

3. Zero-Trust Architecture - Logical Components

The zero-trust architecture comprises of many logical components which are part of an organizational resources and deployed within it. The components can be either on-premise or on cloud and the selection of model totally depends upon the deployment model and organizational requirements. The figure 3. below illustrates the relationship of the components and their data or command exchanges.

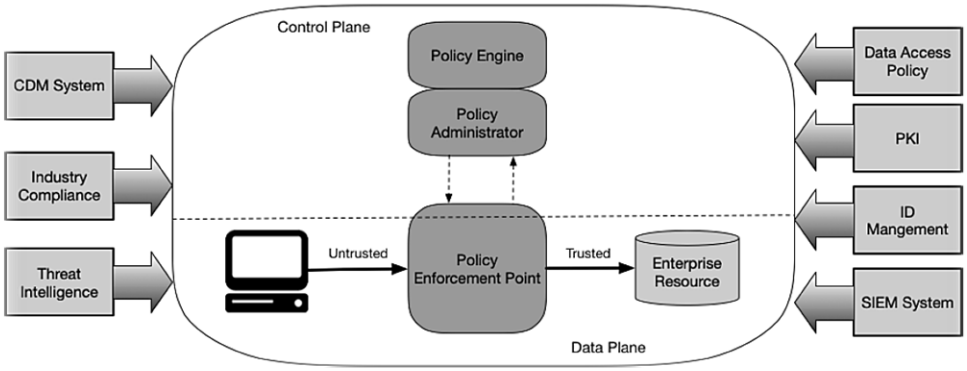

Fig. 3. Zero-Trust Logical Components
Source: NIST SP 800-207 [3]

The following *table 2.* below list the components of the Zero-Trust Architecture:

Table 2. Zero-Trust Architecture - Logical components

Component	Description of the Component
Policy Engine (PE)	▪ It is responsible for the final decision to grant access to a resource for a specific client or subject. ▪ It uses enterprise policy in conjunction with input from external sources (e.g., IP blacklists, threat intelligence services) as input to a "trust algorithm" to decide to grant or deny access to the resource. ▪ It is paired with the Policy Administrator component. ▪ It makes and logs the decision made while the Policy Administrator executes the decision i.e. approval or denial.
Policy Administrator (PA)	▪ It is responsible for establishing the connection between a client and a resource. ▪ Authentication token or credential used by a client to access a resource is generated. ▪ It works with the Policy Engine and depends on its decision to finally allow or deny the connection. ▪ In deployments the Policy Engine and Policy Administrator are implemented as a single service, but they are logically divided into its two logical components. ▪ It communicates with the Policy Enforcement Point (PEP) while creating the connection that is done via the control plane.

Policy Enforcement Point (PEP)	▪ It is responsible for enabling, monitoring, and finally terminating connections between a subject and organizational resource. ▪ It is a single logical component in zero trust architecture and can be broken into two different components i.e. client (e.g., agent on end-user's laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for connections.
Continuous Diagnostics and Mitigation (CDM) System(s)	▪ These systems gather information about the organizational system's current state and applies updates to configuration and software components. ▪ Continuous Diagnostics and Mitigation (CDM) System(s) system provides the PE with the information with respect to the system making an access request i.e. whether it is running the required patched operating system and applications or whether the system has any already identified vulnerabilities.
Industry Compliance System	▪ This system ensures that the organization remains compliant with any regulatory requirements it may need compliance towards such as HIPAA, PCI-528 DSS, FISMA, etc. ▪ It also includes all the policy rules an organization develops to ensure compliance.
Threat Intelligence Feed(s)	▪ It provides information from external sources that help the PE in access decisions. ▪ These feeds could be from multiple service providers that take data from several external sources and deliver information about recently discovered vulnerabilities or attacks. ▪ It also comprises of DNS blacklists, discovered malware, or command and control systems that the PE will want to deny access to from organizational systems.
Data Access Policies	▪ These are set of attributes, rules, and policies about data access developed by the organization around organizational resources. ▪ These set of rules can be encoded by the PE or generated dynamically by the PE. ▪ These policies are the baseline for granting access to a resource since they provide the basic access privileges for actors and applications in the organization.
Enterprise Public Key Infrastructure (PKI)	▪ PKI is responsible for generating and logging certificates issued by the organization to the resources, applications and actors. ▪ It also includes the global certificate authority (CA) ecosystem and the Federal PKI3, that may or may not be integrated with the organizational PKI.
ID Management System	▪ It is responsible for creating, storing, and managing organizational user accounts and identity records. ▪ It contains the mandatory user information like name, email address, certificates, etc. and additional organizational details such as role, location, access attributes, or related systems/applications. ▪ It regularly uses other systems like PKI for the artifacts related with user accounts.

Security Incident and Event Management (SIEM) System	▪ This system aggregates system logs, network traffic, resource entitlements, and additional events that provide feedback on the security posture of organizational information systems. ▪ The collected data is used to enhance policies and advise of possible active attacks against organizational systems.

4. Deployed Variations of the Zero-Trust Architecture

The following are the four types of deployment variations for the Zero-Trust Architecture:

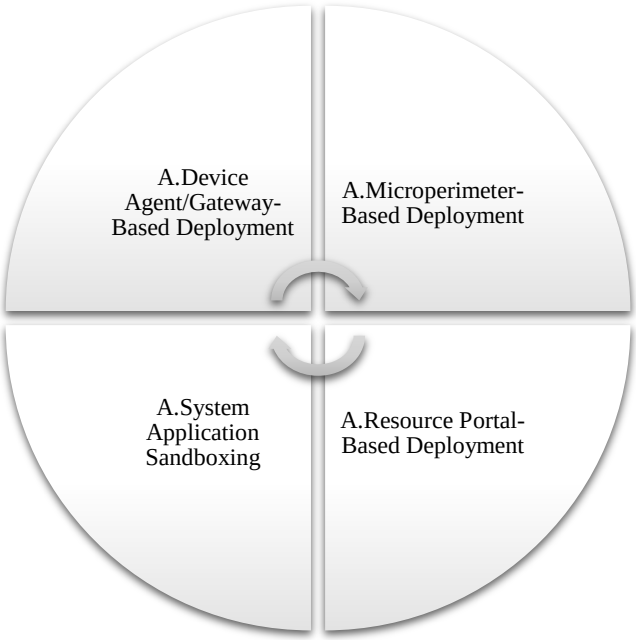

Fig. 4. Deployment Variations

5. Trust Algorithm - Zero-Trust Architecture

Organizations with a zero-trust architecture deployment, the policy engine can be assumed as the master controller and the PE's trust algorithm its main thought process. Policy engine decides to deny or grant access to the requestors demanding the access to the resources by a process defined by the trust algorithm.

The Policy engine receives input from multiple sources i.e. user roles and attributes, database of policies containing information stored about the users, , behavior patterns of users recorded in past, various threat intelligence sources, and additional metadata sources. The process is represented in the *figure 5* below:

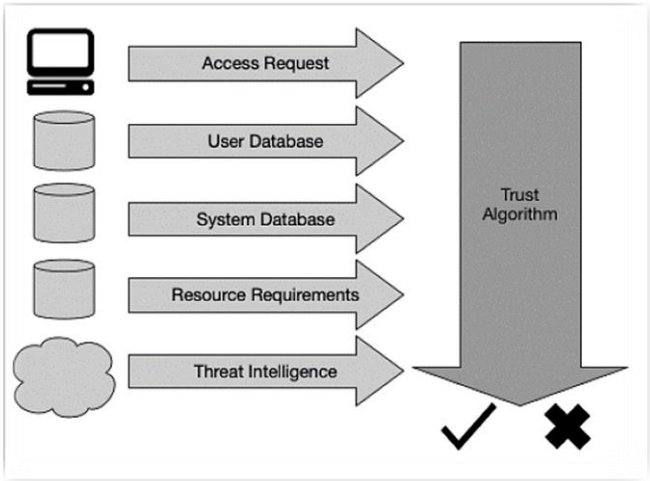

Fig. 5. Trust Algorithm - Zero-Trust Architecture

As shown in the figure 5 above, the inputs can be categorized based on what they provide to the trust algorithm. The five types of inputs as shown in the figure 5 are as under:

i. **Access request:** *They are the actual requests from the end users using applications.*

ii. **User Database:** *This determines the requesters identification that is requesting access to a resource and consists of identification, attributes, and privileges.*

iii. **System Database:** *This database contains the observable status of each organization owned system.*

iv. **Resource Requirements:** *These are set of policies in addition to the user ID and attributes database.*

v. **Threat intelligence:** *This consists of the feeds from the internet about general threats and active malware operating on the Internet.*

5.1. Trust Algorithm Variations

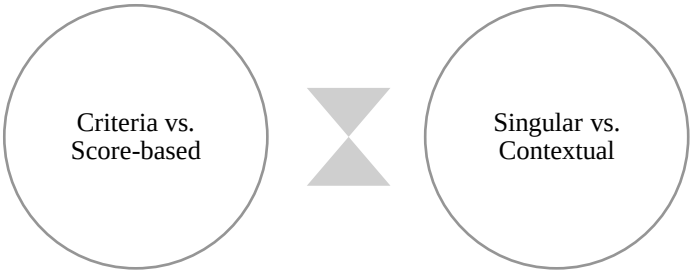

Fig. 6. Trust Algorithm Variations

6. Zero-Trust Architecture Implementation in SCADA Systems

SCADA system environments have become more connected rather than isolated systems that they used to be in the past, "Security by Obscurity" is no longer appropriate security strategy [8]. The kind of sophisticated adversaries exploit the vulnerabilities found in today's operational environments. With sophisticated kind of the adversary, the legacy strategies of trusted and untrusted are not appropriate and demands the concept of Zero-Trust within Industrial control systems networks. Implementing a zero-trust environment means to adopt a strategy that will ensure that no traffic within an organization's network is any more trustworthy than traffic coming from external network. The insider risks, policy gaps, vulnerable endpoints and numerous potential threats require a novel approach like zero-trust security model.

The zero-trust security model is based upon three main notions i.e. *a) All resources with the organization must be accessed in a secure manner irrespective of their location, b) Access control is strictly enforced and on a "need-to-know" basis, and c) All the traffic with the network must be inspected and logged.*

The following are the ten principles as per UK National Cyber Security Center (NCSS) [6] which can be used as a starting point for building the baseline for Zero-Trust architecture:

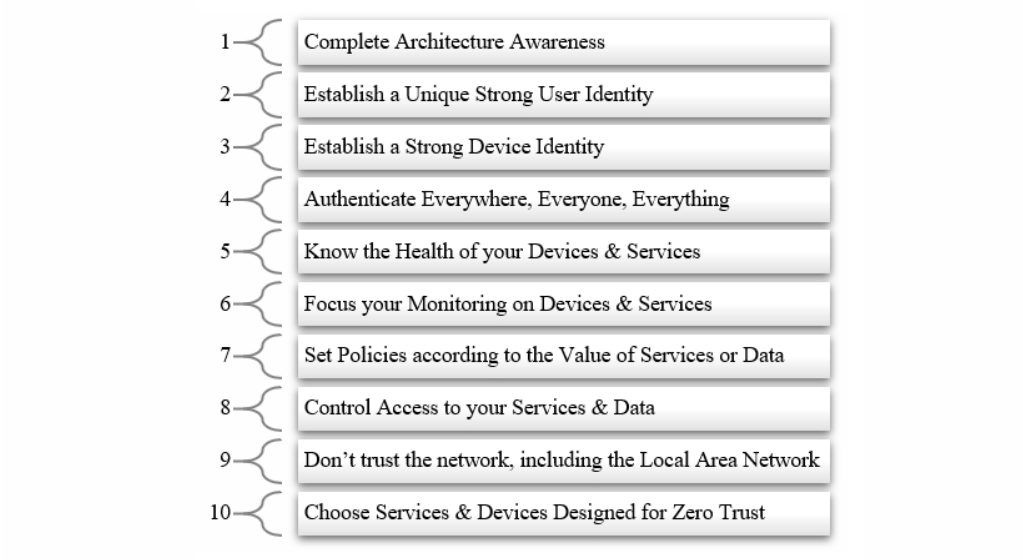

Fig. 7. Baseline for Zero-Trust Architecture

Zero-Trust security architecture offers organizations various benefits that include:

a) It helps to reduce complexity of the security stack
b) It helps to resolve security skills shortage
c) It helps to Protect business and customer data
d) It helps to deliver excellent security and end-user experience
e) It helps to lower breach detection time and attain visibility into enterprise traffic

Conclusion

With constantly evolving threat landscape, the traditional approach of *"trust but verify"* doesn't cater to the needs of security for the critical infrastructures as in case of SCADA systems in electricity business, the Zero-Trust model offers a novel approach to the security. There is the need to have a flexible security strategy that leverages modern technology. Accomplishing Zero-Trust is frequently perceived as expensive and complicated way of achieving the security goals. Conversely, Zero-Trust can be built upon the existing architecture and don't require to replace or change all existing technologies already implemented by the organization. Security strategy based on the Zero-Trust model will help to reduce the probabilities of breaches and toughen the defenses of the organizations especially operating in the critical infrastructural based SCADA systems.

References

[1] Mir, A. and Ketti Ramachandran, R. (2019), Security gaps assessment of smart grid-based SCADA systems, Information and Computer Security, Vol. 27 No. 3, pp. 434-452. https://doi.org/10.1108/ICS-12-2018-0146

[2] A. W. Mir, K. R. Ram Kumar, (2019). A Survey on Security Challenges and Research Opportunities in Smart Grid based SCADA Systems. International Journal of Computer Sciences and Engineering, Vol. 7 No. 3, pp. 734-755. https://doi.org/10.26438/ijcse/v7i3.689706

[3] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2019). Zero-Trust Architecture (No. NIST Special Publication (SP) 800-207 (Draft)). National Institute of Standards and Technology.

[4] Gordon, S. (2019). A matter of trust. Network Security, Vol. 2019(5), pp. 9-11.

[5] Keeriyattil S. (2019) Zero-Trust Networks with VMware NSX: Getting Started. In: Zero-Trust Networks with VMware NSX. Apress, Berkeley, CA

[6] Zero-Trust architecture design principles. (2019). National Cyber Security Center, United Kingdom. Available at: https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles [Accessed 10 Jan. 2020].

[7] Berhe, A. B., Kim, K. H., & Tizazu, G. A. (2017, July). Industrial control system security framework for ethiopia. In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN) (pp. 814-817). IEEE.

[8] Huda, S., Yearwood, J., Hassan, M. M., & Almogren, A. (2018). Securing the operations in SCADA-IoT platform based industrial control system using ensemble of deep belief networks. Applied Soft Computing, 71, 66-77.

Additional References

[1] Hopkins, S., & Kalaimannan, E. (2019). Towards establishing a security engineered SCADA framework. Journal of Cyber Security Technology, 3(1), 47-59.

[2] Babay, A., Schultz, J., Tantillo, T., Beckley, S., Jordan, E., Ruddell, K., ... & Amir, Y. (2019, June). Deploying Intrusion-Tolerant SCADA for the Power Grid. In 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) (pp. 328-335). IEEE.

[3] Zaheer, Z., Chang, H., Mukherjee, S., & Van der Merwe, J. (2019, April). eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices. In Proceedings of the 2019 ACM Symposium on SDN Research (pp. 49-61).

[4] Sideris, A., Tsiktsiris, D., Ziouzios, D., & Dasygenis, M. (2019). Smart Grid Hardware Security. In IoT for Smart Grids (pp. 85-113). Springer, Cham.