International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Investigating Overall Structure of Cyber-Attacks on Smart-Grid Control Systems to Improve Cyber Resilience in Power System

Siddharth Suman[1], Muskaan Gupta[2]

[1,2]*Jagan Institute of Management Studies, Institutional Area, Sector-5, Rohini, New Delhi-110085, India*

Abstract— The utilization of knowledge and communication technologies and computer-based software to reinforce the standard, efficiency, and reliability of smart grids (SGs) have brought unwanted threats in these systems; one in all the foremost important of such threats is cyber-attack. Understanding the ways to detect and cater to cyber threats in SGs will increase the resilience of power systems. During this paper, conceptual models of SG vulnerabilities are presented to deal with the problem of the vulnerability of SG control systems against cyber-attacks. Different scenarios of cyber-attacks are then prohibited in SG control systems to reinforce their resilience.

1. INTRODUCTION

The main security problems with SG control systems against cyber- attacks are given in Figure 1. These issues are divided into four categories:

- Identifying different vulnerabilities and scenarios for attacking SG control systems and trying to forestall it
- Providing strategies to detect and identify the attack
- Recombining and using control tools to scale back the results of the attack and increase the system's self- healing properties
- Improving cyber security management in SG control systems

2. CONCEPTUAL MODEL OF CONTROL SYSTEMSVULNERABILITIES IN SMART GRID

Controlling of SG in energy systems has the task of directing and controlling physical processes. They typically comprise a group of multiple components including sensors, operators, processing units like programmable logic controllers (PLCs), communication networks, and central computers. There are several general models for elucidating the structure of smart control systems [1, 2]. A conceptual model of SG system vulnerabilities is presented in Figure 2. As will be seen from the Figure 2, the vulnerabilities of the SG system are divided into six categories:

1- Field equipment vulnerabilities
2- Field equipment communication network vulnerabilities
3- Local controller vulnerabilities like remote station units (RTUs) and PLCs
4- Vulnerabilities of control network communication protocols 5- Local area network (LAN) control vulnerabilities
6- Vulnerabilities of cooperative and financial-commercial networks

The layered structure of this conceptual model emphasizes that the kinds of vulnerabilities of every layer of SG system are different, and so each layer requires different security measures.

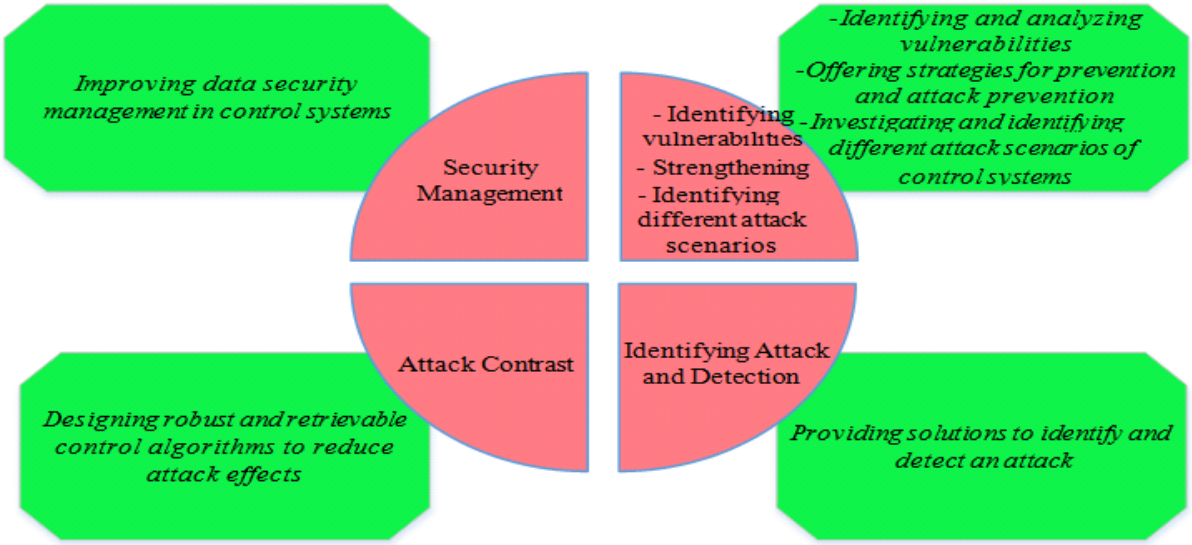

Figure 1. The main security issues of SG control systems against cyber-attacks

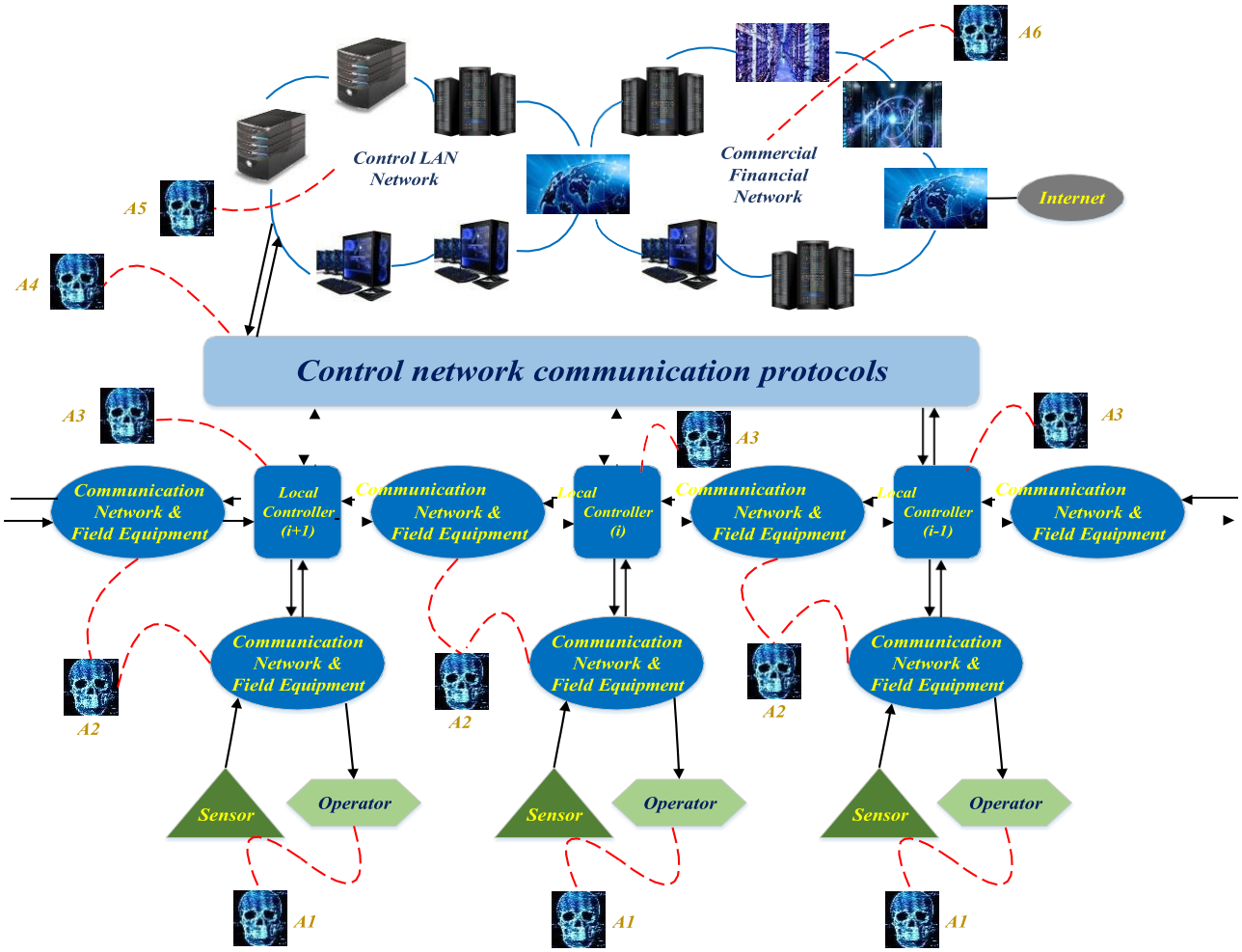

Figure 2. Conceptual model of SG control system vulnerabilities

3. IDENTIFY DIFFERENT VULNERABILITIES AND SCENARIOS OF CYBER-ATTACK IN SMART GRID CONTROL SYSTEMS

With the advancement of control and protection systems in SGs further as their use of the identical software, hardware and network platforms and having the identical standards, it's possible for unauthorized persons to access the interior layers of those systems. In general, an attacker who intends to attack a cyber-attack and damage an intelligent system faces two major challenges:

- Identifying, penetrating and accessing the system
- Taking full or partial control of the method and damage it

So the opening move in securing smart grid control systems is to spot vulnerabilities and access points. It will be divided into two major areas of facility and protocols. The devices utilized in smart grid control systems also make up two categories:
1- Equipment used solely for control systems, like sensors, actuators, RTUs, and PLCs
2- IT equipment utilized in other systems and networks like switches and computers

In this section, we first discuss variety of articles addressing the vulnerabilities of communication protocols of the SG system and their solutions. Then, considering the extent of kit vulnerabilities and articles during this field, top quality equipment vulnerabilities are discussed. Finally, four categories of scenarios for attack on control systems in SGs are investigated.

3-1- Communication vulnerabilities and attempts to forestall intrusive influence

Nowadays, many protocols are utilized in intelligent control systems. Most of those protocols are designed to extend efficiency, reliability in real-time operations, and support for economic and operational requirements. Unfortunately, most of those protocols have ignored any unnecessary security measures like authentication and cryptography to reinforce performance. Many are developed by others to use the Ethernet protocol and hook up with the net.

Therefore, the communication protocols of commercial control systems are very vulnerable and exposed many attacks [3]. Consistent with the American Gas Association reports, there are about 150 to 200 supervisory control and data acquisition (SCADA) protocols. The combination of those protocols in recent years has resulted in the attackers obtaining very accurate information on their function and structure.

In this way, attackers can identify and modify data packets by identifying vulnerabilities in these protocols [4]; just like the attack on Queensland's Australian Water and Wastewater system in 2000 when an attacker was able to infiltrate the field's communications network and produce 800,000 liters of sewage into the city's safe water cycle by having complete information about the attacking protocol. The vulnerabilities of those protocols are investigated in several sources. References [3, 5] discuss a spread of commercial protocols, their vulnerabilities and security solutions. One in every of the problems discussed during this source is that the Modbus protocol that lacks authentication, encryption, and encryption integrity. Therefore, the communication protocols of commercial control systems are very vulnerable and exposed many attacks [3]. In keeping with the American Gas Association reports, there are about 150 to 200 supervisory control and data acquisition (SCADA) protocols. The mixing of those protocols in recent years has resulted within the attackers obtaining very accurate information on their function and structure. during this way, attackers can identify and modify data packets by identifying vulnerabilities in these protocols [4]; just like the attack on Queensland's Australian Water and Wastewater system in 2000 when an attacker was able to infiltrate the field's communications network and produce 800,000 liters of sewage into the city's safe water cycle by having complete information about the attacking protocol. The vulnerabilities of those protocols are investigated in several sources. References [3, 5] discuss a spread of commercial protocols, their vulnerabilities and security solutions. One in every of the problems discussed during this source is that the Modbus protocol that lacks authentication, encryption, and encryption integrity.

One of the foremost useful and also dangerous features of Modbus is its ability to program controllers that several SG protocols share with Modbus. Thanks to this dangerous feature, attacker can use it to inject malware into PLCs and RTUs. One in every of the methods of intrusion detection in Modbus protocols is that the use of model-based intrusion detection systems. Reference [6] introduces three model-based methods for monitoring and detecting Modbus TCP protocol attack. These methods provide a protection mechanism with reference to the topology and communication structure of the SCADA network. So as to forestall unauthorized access to the protected system, firewalls are suggested as a security solution in many sources.

One in every of its tasks is to dam messages that aren't structured in accordance with the protected area communication protocol [7]. Another common thanks to increase the safety of communication protocols is to use cryptography. There are various traditional methods of encryption, but most aren't usable in smart grid control systems. The explanation is that the limited computing power and low data transmission speed of those components, which must also meet the real-time performance requirements. These limitations make it difficult to implement sophisticated encryption. Reference [8] has explored various encryption methods to confirm data confidentiality and integrity.

3-2- Control equipment vulnerabilities

Many cyberattacks on industrial control systems are exploited to take advantage of vulnerabilities on top of things equipment, one in every of which is that the Stuxnet attack.

Therefore, identification of those vulnerabilities is one in every of the problems of interest to researchers during this field [9].

In recent years, additionally to software vulnerabilities, various styles of hardware have also been heavily favored by security experts. These are widespread in processors and electronic components and are found even on telecommunication surfaces [10].

3-3- Investigation and identification of various scenarios of attacks on SG control systems

Overall, there are five styles of scenarios for attack on control systems of SGs:

3-3-1- Static false data injection attack

In static false data injection attack, the attacker changes the sensor output to such some way that the system doesn't cheat and fails to send the incorrect data to the controller. This scenario was first proposed in 2009 for an attack on the facility system and its faulty detection system, assuming the attacker had full knowledge of the system [11]. Within the references [12, 13], authors have proved that an attacker can even launch a successful attack even with partial awareness.

In a shot to counteract this attack, the source proposes two security measures for the facility grid state estimator, which is truly a measure of the minimum amount of attacker effort required to successfully execute an attack. These scales depend upon the topology of the facility grid and therefore the degree of availability of the sensor outputs. Reference [14] stated that complete encryption and out-of-the-box protection of all equipment isn't cost-effective and enforceable, which the success of the injection attack will be prevented by protecting a limited number of measurements and their output. The amount of those measurements is adequate to the amount of system state variables. In reference [15], two algorithms offer protection for a limited number of devices in such some way on provide maximum security against injection attacks. Reference [16] first described an optimal attack strategy that may cause maximum damage to the system, then by formulating the defense problem, it's been able to develop an optimal defense strategy and minimize the number of harm. The economic effects of the information injection attack on the electricity grid market performance were formulated in paper [17].

3-3-2- Attack on facility state estimator and wrong data injection

The purpose of the facility grid state estimator is to estimate the state variables of that system supported the measured data. In reference [18], the center of the state system matrix of the variables was described. Inappropriate estimates will be thanks to various reasons, like measurement failures or malicious attacks. In this scenario, it is assumed that the attacker knows the state matrix variables of the target power system and makes subversive measurements with knowledge of this matrix. It then injects these erroneous measurements into the control system to disrupt the state estimation process. Figure 3 provides a schematic overview of the data injection attack on power grid control system.

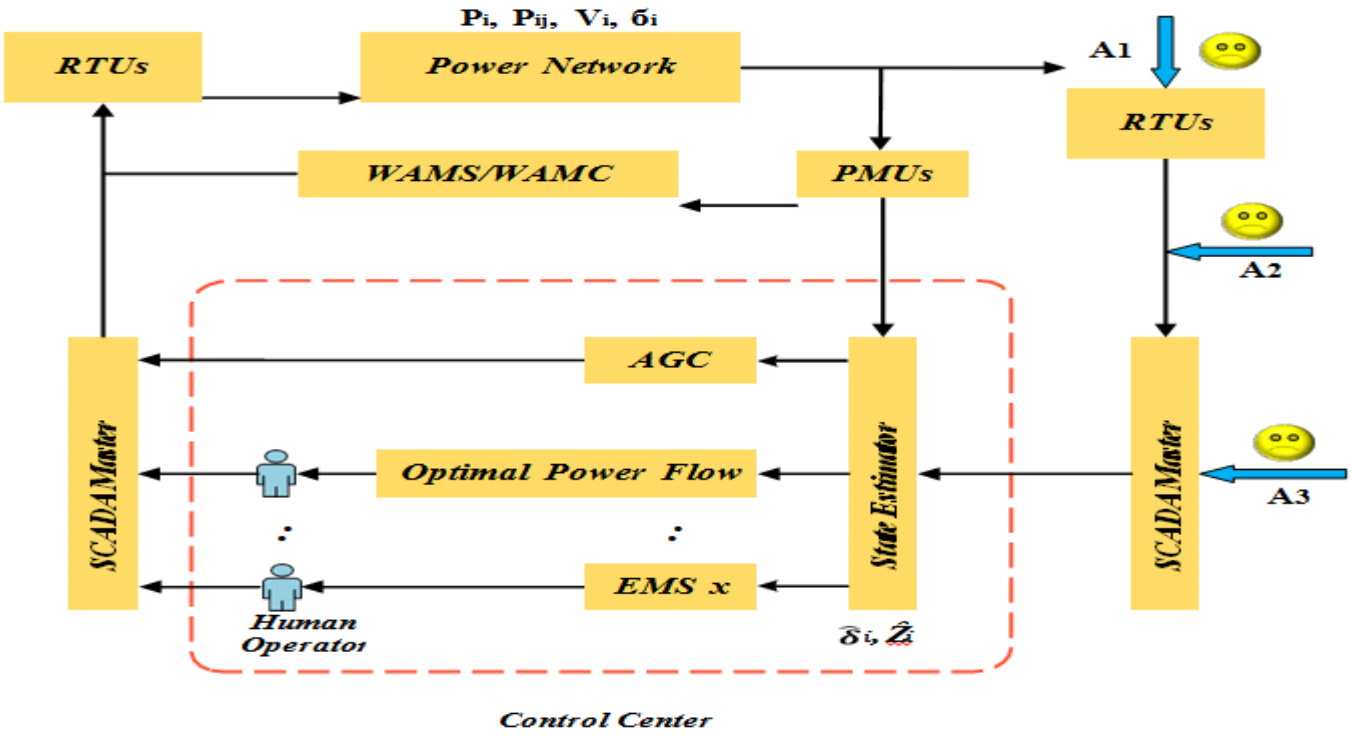

Figure 3. Schematic overview of the data injection attack on power grid control system

3-3-3- Invalid dynamic data injection attack

The attack attempts to inject the incorrect data dynamically and make an unstable and invisible fashion within the system. Reference [19] assumed that the attacker's purpose is to inject the incorrect data, destabilize the system, and remain secret. The author used the Kalman filter and therefore the linear–quadratic– Gaussian (LQG) controller to observe and control the discontinuous linear system over time, moreover on detect the attack of a false dynamic data injection. Finally, this text described the necessities for a successful attack and proposes a technique to counter attack supported the employment of plug- in sensors.

3-3-4- Information recovery attack

One of the foremost dangerous attacks is that the information recovery attack. As observed within the "data injection" attacks, if the attacker can access the sensor or operator output data, he can enter the incorrect data in an intelligent and purposeful manner, or accidentally, and control Error making the receiver [20]. In an information recovery attack, the attacker records the sensor or operator information under normal system conditions and sends it to the control network at the time of the attack and sabotage [21]. As such, the system is cleverly deceived and, additionally to the loop control, the system goes into danger. a technique to counter this attack is to feature a Gaussian random input with a mean of zero to the system input [22]. Random input is an authentication signal and it's attempted to be optimally designed to attenuate impact on system performance.

3-3-5- Stealth attack

The attack is really a closed-loop information reconstruction attack. In other words, the attack output is reconstructed as a control system to eliminate the effect on the sensor output and keep the attack hidden. In these types of attacks, attacker should have a radical understanding of the physical model of the system in restraint so as to simulate a model like it. As shown in Figure 4, the attacker puts the simulated model and its controller between the system and therefore the master controller; and by sending arbitrary signals to the most controller input, it hides the attack and replaces the arbitrary work point.

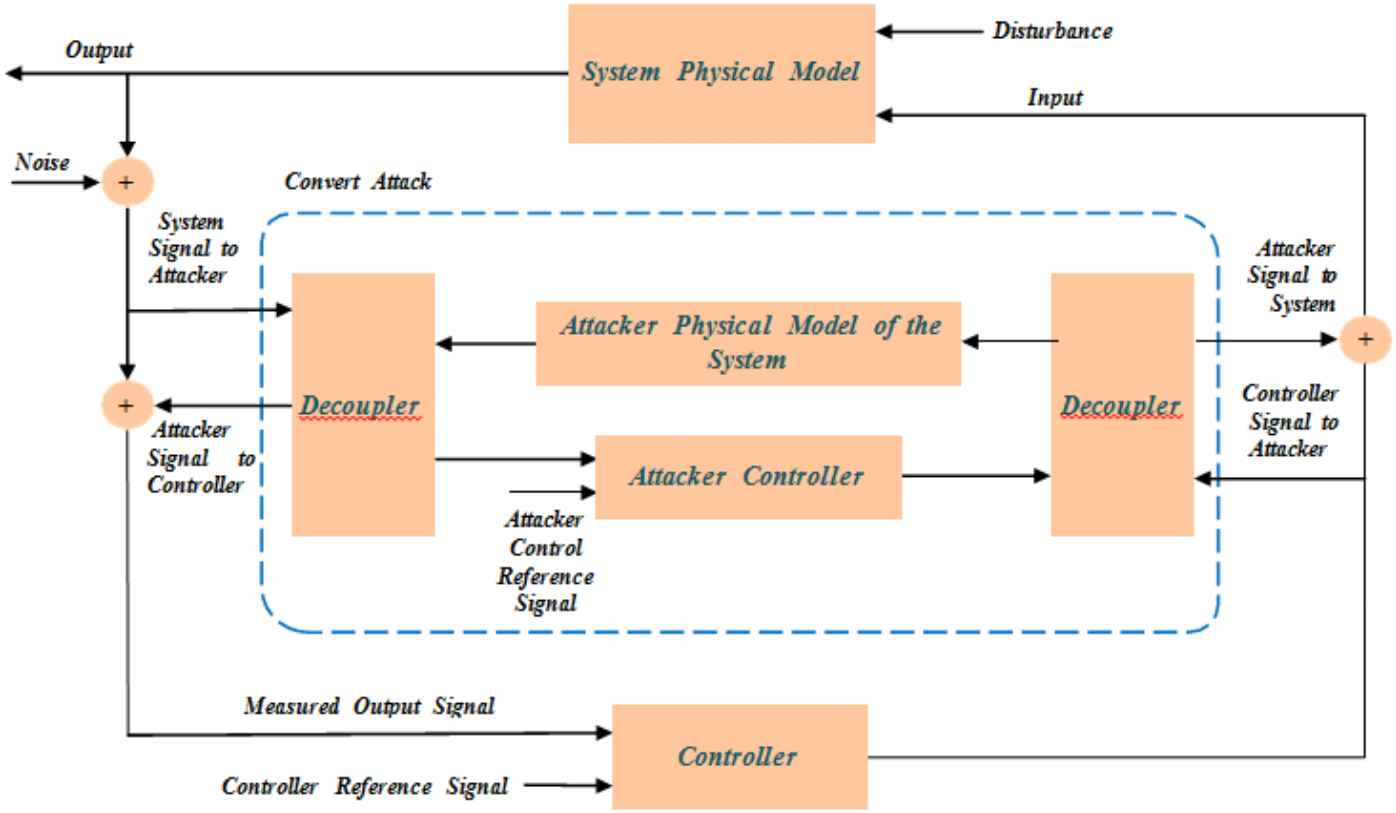

Figure 4. Block diagram of stealth attack on power grid control system

4. IMPROVING CYBER SECURITY MANAGEMENT IN SG CONTROL SYSTEMS TO ENHANCE RESILIENCE OF POWER CONTROL SYSTEMS

In order to realize optimal security, additionally to using appropriate security strategies there must be good security management. Appropriate security management tools include security policies, strategies, and programs that are supported accurate threat and risk analysis. In other words, given the wide selection of cyber threats that industrial control systems are exposed to, it's essential to spot and analyze these threats to supply an optimal and cost-effective safeguard strategy. In general, the sector of study of the articles during this section is categorized as follows:

1- Providing methods for identifying cyber threats and assessing their risks in industrial control systems

2- Considering such analysis and evaluations to extract and choose the optimal and cost-effective defense strategy and formulate a security plan

Much effort has been made to supply methods for identifying threats and risks in addition as analyzing them in industrial control systems. In reference [23], it's attempted to estimate the safety threats of cyber-physical systems using the sport theory method.

5. CONCLUSIONS

In addition to exploiting unknown vulnerabilities, cyber attackers are developing more sophisticated methods to attack smart grid control systems. Thus, after probing IT-

Based security strategies, they're virtually confronted with an

Impression system without security protections. On the opposite hand, the ultimate goal of attackers is to wreck and disrupt the optimal functioning of the physical system in restraint, which is ignored in IT-based security strategies. It can only be stated that IT-based security strategies alone cannot provide a depth defense strategy (the in-depth defense

strategy allows the attacker to taste each layer again to a security layer that eliminates Designed to cut back the attack (or reduce its impact) to regulate systems. Therefore, this text identified various vulnerabilities and scenarios of cyber-attack in smart grid control systems so on increase system resilience of grid and to cut back the consequences of such attacks.

REFERENCES

1. S. Amin, "On cyber security for networked control systems," UC Berkeley, 2011.
2. M. Ghiasi, "Detailed study, multi-objective optimization, and design of an AC-DC smart microgrid with hybrid renewable energy resources," Energy, vol. 169, pp. 496-507, 2019.
3. D. J. Teumim, Industrial network security: Isa, 2010.
4. V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," computers & security, vol. 25, pp. 498-506, 2006.
5. B. Wang, M. Dabbaghjamanesh, A. K. Fard, and S. Mehraeen, "Cybersecurity Enhancement of Power Trading Within the Networked Microgrids Based on Blockchain and Directed Acylic Graph Approach," IEEE Transactions on Industry Applications, 2019.
6. S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for SCADA networks," in Proceedings of the SCADA security scientific symposium, 2007, pp. 1-12.
7. Y. Chen, J. Hong, and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," IEEE Transactions on Smart Grid, vol. 9, pp. 2541-2552, 2016.
8. D. Puthal, X. Wu, S. Nepal, R. Ranjan, and J. Chen, "SEEN: A selective encryption method to ensure confidentiality for big sensing data streams," IEEE Transactions on Big Data, 2017.
9. Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1-6.
10. R. Arghandeh, A. von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," Renewable and Sustainable Energy Reviews, vol. 58, pp. 1060-1069, 2016/05/01/ 2016.
11. R. Deng, P. Zhuang, and H. Liang, "False data injection attacks against state estimation in power distribution systems," IEEE Transactions on Smart Grid, vol. 10, pp. 2871-2881, 2018.
12. A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in 49th IEEE conference on decision and control (CDC), 2010, pp. 5991-5998.
13. X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," IEEE Transactions on Smart Grid, vol. 5, pp. 1665-1676, 2014.
14. R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, and T.
15. J. Overbye, "Detecting false data injection attacks on dc state estimation," in Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010.
16. G. Dan and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 214-219.
17. Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," IEEE Transactions on Parallel and Distributed Systems, vol. 25, pp. 717-729, 2013.
18. L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," IEEE Transactions on Smart Grid, vol. 2, pp. 659-666, 2011.
19. A. Monticelli, State estimation in electric power systems: a generalized approach: Springer Science & Business Media, 2012.
20. K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," IEEE transactions on control of network systems, vol. 1, pp. 370- 379, 2014.
21. Y. Mo and B. Sinopoli, "Secure control against replay attacks," in 2009 47th annual Allerton conference on communication, control, and computing (Allerton), 2009, pp. 911-918.
22. M. H. Amini, H. Arasteh, and P. Siano, "Sustainable Smart Cities Through the Lens of Complex Interdependent Infrastructures: Panorama and State-of-the-art," in Sustainable Interdependent Networks II: From Smart Power Grids to Intelligent Transportation Networks, M. H. Amini, K. G. Boroojeni, S. S. Iyengar, P. M. Pardalos, F. Blaabjerg, and M. Madni, Eds., ed Cham: Springer International Publishing, 2019, pp. 45-68.
23. S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber- physical resilience of electrical power systems against

malicious attacks: A review," Current Sustainable/Renewable Energy Reports, vol. 5, pp. 14-22, 2018.

24. S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber-physical systems," IEEE Network, vol. 27, pp. 19-24, 2013.