PalArch's Journal of Archaeology of Egypt / Egyptology

Convergence of Cyber and Physical Security – A must for Smart Grid Systems

Saurabh Anand
Institute of Engineering and Technology, GLA University, Mathura, India
saurabh.anand@gla.ac.in

Saurabh Anand, Convergence of Cyber and Physical Security – A must for Smart Grid Systems-Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(9). ISSN 1567-214x, Keywords: Protection, Convergence, Cyber Physical Systems

Abstract-

In the field of information security the most obvious type of security is physical security. The key aim of physical protection is to have an atmosphere that is secure for all the properties and organizational interests. The need for physical security has been heightened by the rising number of laptops and telecommuters. Physical security includes security guards, locks and warning panels etc. that both the visitors and the internal workers will see. These visual security checks give a fair amount of recognition of the security position in place in an organization. An attacker can feel harder to work to outstrip an organization's security if a visual image of top-class security is provided in front of him. In this paper, we will discuss about the physical security of a power grid systems, which is of national importance. With this changing technology at a rapid pace, there is a need to integrate the security in grid systems with the IT infrastructure. Often the security aspects in a grid systems is considered revolving around networks, operation security etc. and majority times physical security gets ignored. In this paper, by means of an exhaustive study of all the existing research work related to security systems, we are emphasizing on the need for Cyber Physical Systems, and proposing the convergence of Cyber security with Physical security.

1 Introduction

Logical in nature controls are the subject of the security and countermeasures that are in place to secure information. Many that have physical access cannot even be hindered by the logical controls. They can only support by an unauthorized party in protecting resources from breach [1]. Physical security is thus still a very basic element in an organization's security strategy, as it is unable to protect the tools that form an accepted logical control. Servers can be used for accessing organization’s vital data if physical access is gained. All security activities set up to protect servers are software- based activities. If an unauthorized individual reboots the server and malicious scripts are running on the OS, then the attacker will set new access rules. This can create a very dangerous situation for the organization, as all their device passwords will be compromised in this way. There are also many economic explanations why physical security in any organization is of utmost importance particularly where an organiza- tion’s health directly impacts the society, government like a power grid system.

The latest government and private sector effort to safeguard vital infrastructures is another factor affecting physical security.

Physical security plays a significant part in securing an organization’s sensitive data. In order to protect that critical data in any premise, organizations generally em- ploy various mechanisms, of which the most popular remains the setting of a pass- word in a file. Although the files in the database have the users 'password in an encrypted format, there are several tools available which can decrypt these encrypted files and disclose the users' passwords. This can create a very dangerous situation for the organization, as all their system passwords would be leaked in this manner. An attacker may use information from one system to jeopardize the protection of another system.

2 Related Work

In this section we will study the previous work related to security aspect of power grid systems. Liu, et al. [2], in their work suggested certain privacy and cyber security issues. Using advanced sensing technologies and control methods, power grid systems are able to collect and analyze data on power consumption, transmission and generation in near real time. Moreover, the operating systems used in grid systems are proprietary and the networks are private unlike IT systems. Govindarasu, et al. [3], in their work Focuses on defining a detailed collection of cyber security issues and the need for protection at multiple levels of the cyber-physical power system, namely ICT network protection, information security, and app-level security. Cyber protection of the power grid-including prevention of threats, identification, mitigation and adaptation is one of the most critical R&D needs for the developing smart grid. Liu, et al. [4], in their work focused on the vulnerability in the cyber security applied on the control systems for the smart home. Further anomaly detection algorithm was considered using machine learning techniques [5] [6]. The proposed attacks investigate the power system's weakness as the attacks on the communication network are attempted by researching the interdependence between electricity pricing and energy load [4].

Hong, et al. [7], proposed a method of simultaneous intrusion detection, which is capable of detecting the same kind of attacks at multiple substations and their locations. The result is a modern, integrated method to detect and prevent cyber intrusions at a single substation or multiple power grid substations. Through advanced automation technology, an electrical grid can recognize and isolate failed areas and restore unaffected areas through technologies that can perform auto-healing [8]. Sun, et al. [9], in their work has given us a survey of state-of-art techniques which are used in Cyber physical Systems (CPSs). Many of the problems related to the power grid are also addressed in their survey, such as cyber vulnerability assessment, CPS structure in a smart grid, CPS test beds and cyber protection systems. Dan, et al. [10], in their work focused on a strong amalgamation of IT with power system. The electricity grid must increasingly rely on reliable and stable communication and IT infrastructure operations. The primary reasons for The integration are improved market productivity and performance, and decreased operational costs, for example by enabling corporate decision-makers to quickly access vital data regarding their operational assets. The flow of knowledge across network frontiers in the smart grid is expected to increase.

3 Background

Physical Security Design – Cybersecurity is an emerging challenge for power systems, as it strongly affects their reliability and the whole energy system cost[12].There has to be a design that will make an organization safe and still make it comfortable for the other employees. Reviewing the current organization is a crucial necessity, because it can provide an indication of the features, procedures and conditions that that impact an organization's overall safety requirements. The design team will adopt an all-inclusive strategy so that health and protection can be maximized. This site design will be the result of function-security integration such that a balance can be achieved between the various design elements and the related objectives. There are two methods by which physical security design can be attained: Human Interaction and Automation. The detection of weaknesses must be accompanied by reverse engineering techniques, where the forms in which the intruders can be overcome are to be found. There are certain issues that need to be solved in a Physical Security Design such as fragmentation load, a careful layout of the structure is necessary; the debris which can be hazardous in nature must be minimized.

Physical Threats – Physical security deals with theft, intruders, vandalism, physical destruction and environmental issues etc. There are various threats that an organization faces. They are mentioned below:

•Threats due to natural environment: Earthquakes, volcano eruptions, tornadoes, floods, storms, extreme temperature conditions, fire etc.

•Threats due to supply systems: Outages in the distribution of power, interruptions in communication and stoppage in the supply of natural resources such as steam, air, gas etc.

•Threats which are man-made: Explosions, unauthorized access (both external and internal), damage by angry employees, case of vandalism, accidents due to employee's error, fraud, theft etc.

•Threats occurring because of political motivation: Riots, strikes, civil disobedience, bombing, terrorist attacks etc.

4 Proposed-Convergence of Cyber and Physical Security

In the last decade, significant focus has been put on enhancing cyber security. A good investment return (ROI) can be earned if cyber security is strategically improved as the threat of malicious code attacks and hacking incidents has grown considerably over the years. For example: When an intruder who is clearly unauthorized to access an organization's facility violates the physical security measures being enforced and enters the facility. Then, the attacker may access the systems which are held in the protected perimeter of the organization and are linked to the network. In this situation, he can gain control of the organization's network and would infringe data. Therefore, the above mentioned example clearly validates that there is a sure shot relation between cyber and physical security. Therefore it can be seen that even though the best practices in cyber security are in place, physical protection still plays a very important role in protecting resources. If an attacker passes the physical security checks then the network is compromised, because the attacker has now got the control of the system. Despite the fact that physical protection and cyber security are inseparable entities and rely on one another, some companies are still considering these two entities as they have no interaction with each other. In addition to all this, already developed thing includes a linear programming relaxation that improves the scalability, and as such practicality, of the diagnosis filter design [11].

5 Discussion

In this work we have discussed the need for cyber and physical security in grid systems, which are of national importance. The smart grid evolution is modeled by the integration of power systems and a communication network overlay to facilitate a bi-directional flow of information and energy in the grid[13]. Further, we have seen some background things related to physical security such as physical security design, physical security threats, and physical security tools and techniques. In the section related work, we have reviewed the work of authors who have done their research related to grid systems and other control systems. Authors have emphasized on different threats, vulnerability issues. In this paper, we have explained the importance of convergence of cyber and physical security systems. These days, even the proprietary systems and private networks needs to get integrated with the IT infrastructures. Above all, various factors driving cyber and physical security are discussed.

6 Conclusion

In this paper, we have explained the need for convergence of cyber and physical security in grid systems. Since the risk involved in an attack due to unavailability of physical security systems can be fatal, there is a need to put in place all the techniques covered under the concept of physical security. Risk can be modelled as the combined probability of power system impact due to attacks and of successful interruption into the system[14]. The impact of a real-time cyber attack on the multimachine power system is studied in terms of voltage stability and generation loss[15]. We have discussed in depth about CPS systems, in future work, we may observe this approach for different parameters simultaneously in grid systems to check their efficiency and re- liability.

References

1. Azmi IM, Zulhuda S, Jarot SP.: Data breach on the critical information infrastructures: Lessons from the wikileaks. In Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec) (pp. 306- 311). IEEE. (2012)
2. Liu J, Xiao Y, Li S, Liang W, Chen CP.: Cyber security and privacy issues in smart grids. IEEE Communications Surveys & Tutorials. 14(4):981-97 (2012)
3. Govindarasu M, Hann A.: Sauer P. Cyber-physical systems security for smart grid. Power Systems Engineering Research Center.(2012)
4. Liu Y, Hu S, Ho TY.: Vulnerability assessment and defense technology for smart home cyber security considering pricing cyberattacks. In2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD) (pp. 183-190). IEEE. (2014)
5. Agrawal S, Agrawal J.: Survey on anomaly detection using data mining techniques. Procedia Computer Science;60:708-13 (2015)
6. Musumeci F, Rottondi C, Nag A, Macaluso I, Zibar D, Ruffini M, Tornatore M. An overview on application of machine learning techniques in optical networks. IEEE Communications Surveys & Tutorials;21(2):1383-408.(2018)
7. Hong J, Liu CC, Govindarasu M. Integrated anomaly detection for cyber security of the substations. IEEE Transactions on Smart Grid 5(4):1643-53 (2014)
8. Kezunovic M. Smart fault location for smart grids. IEEE transactions on smart grid;2(1):11-22 (2011)

9. Sun CC, Liu CC, Xie J. Cyber-physical system security of a power grid: State-of-the-art. Electronics.5(3):40. (2016)
10. Dán G, Sandberg H, Ekstedt M, Björkman G. Challenges in power system information security. IEEE Security & Privacy (4):62-70. (2012)
11. Pan, K., Palensky, P., & Esfahani, P. M. (2019). From static to dynamic anomaly detection with application to power system cyber security. IEEE Transactions on Power Systems, 35(2), 1584-1596.
12. Dagoumas, A. (2019). Assessing the impact of cybersecurity attacks on power systems. Energies, 12(4), 725.
13. Hammad, E., Ezeme, M., & Farraj, A. (2019). Implementation and develop- ment of an offline co-simulation testbed for studies of power systems cyber security and control verification. International Journal of Electrical Power & Energy Systems, 104, 817-826.
14. Sheela, A., Revathi, S., & Iqbal, A. (2019, August). Cyber risks assessment for intelligent and non-intelligent attacks in power system. In 2019 2nd International Conference on Power and Embedded Drive Control (ICPEDC) (pp. 40-45). IEEE.
15. Poudel, S., Ni, Z., & Malla, N. (2017). Real-time cyber physical system test bed for power system security and control. International Journal of Electrical Power & Energy Systems, 90, 124-133.

16. Alok kumar and Narendra Kumar“VANILLA Framework for Model Driven Re-Engineering of Declarative User Interface” PALArch, vol. 17(9), pp 7120 – 7130, 2020 (https://archives.palarch.nl/index.php/jae/article/view/5392)

17. Alok kumar and Narendra Kumar “A novel approach for Pre-validation, Auto resiliency & Alert Notification for SVN to Git Migration using IoT devices” PALArch, vol. 17(9), pp 7031 – 7145, 2020(https://archives.palarch.nl/index.php/jae/article/view/5394)