International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 05 | May 2022 www.irjet.net p-ISSN: 2395-0072

A Review of Cybersecurity in Power Substations

S Vaishnav Ghautham[1], Varsha Madhukar[2], Sanjana Koppella[3], Ron CM[4], Sangeeta Modi[5]

[1 2 3 4]UG Student, Dept. of Electrical and Electronics Engineering, PES University, Bangalore, Karnataka, India
[5]Professor, Dept. of Electrical and Electronics Engineering, PES University, Bangalore, Karnataka, India

---

Abstract - *In recent times, automation has taken over major sectors of industry and society in attempts to overcome past constraints. Although it solved a set of issues it also gave rise to a new set of threats and problems. The electricity and power industry has also faced its fair share of such benefits and limitations with respect to its integration with automation. In this paper a deep dive into this integration with a special focus on power substations is discussed. The focus is fixed towards cybersecurity in digital electrical substations: what it is, what has been done, benefits and challenges faced, present solutions, our solutions and future scope of the same. The research is further concised to two major areas being the Grid components and the WAN as higher priority attack targets in case of a breach of security.*

Index Terms—*Substation, Cybersecurity, Protection measures*

1. INTRODUCTION

The word substation comes from the time before the distribution system became an electrical grid. As the central generating systems got larger and larger, the smaller generating systems were used as centers to further distribute power over a larger area. They became the intermediate steps between the consumer and generating stations in the process of power transfer. They are normally left unattended and rely on SCADA for remote control and access [3]. Cybersecurity refers to a set of devices/technology that provide defense and protection against cyber-attacks. It aims to protect against unauthorized exploitation of systems, networks and technologies [1]. With a lot of information being traversed and communication technology incorporated, power systems are exposed to cyber threats. By targeting the information exchange process, malicious attackers can inject false data to cause power outage, economic loss, and system instability. False injection of data can also be employed to mask existing power system faults.

This will affect the operator's visibility on the faults and prevent proper countermeasures from being taken. Malicious attackers can also penetrate a power system by attacking system state measurement and estimation and cause damage to the integrity of power system state information.

1.1 CHALLENGES IN SUBSTATION

With the advent of technology, the transfer of data and information has faced a new set of limitations. The sensitivity of data to manipulation is quite high thereby its protection is often in the form of data encryption. Such types of data corruption issues are also faced in power system grids where manipulations to the output data and error in parameter readings can cause an entire sector of a system to be shut down. This data corruption could be due to a hardware fault or due to unauthorized access to data points. A solution to such an issue would be to monitor the system parameters via a checkpoint format.

2. SIMULATION

A. Implementation of WAN Connectivity

A substation network where operators will be connected via an Ethernet switch to gain access to control the households in the network. Focus was to prevent an intruder in the network from controlling the substation.

A substation system network was developed, to which the operators would be connected via an Ethernet switch. The assumption was that anyone in the above network will have the access to controlling the households in the substation. The operators can control the power distribution to the households.

The Wi-Fi router was considered as an Ethernet switch. To the server machine households where connected, for this a Microcontroller (Arduino) was connected to a Windows laptop (server machine) via Serial Communication. The Arduino was connected to 3 households (3 LED's). A text file is shared in the network by the server machine with read and write access to everyone in the network. By modifying parameters in this file, the substation/ power supply to the households can be controlled. So a network where there are 3 operators out of which two are the trusted ones was considered. Every operator in the network would be recognized by their respective IP addresses.

The server machine which monitors the connections of the network will be hard fed with the trusted operators' IP addresses. The server machine checks for the IP addresses of the operators connected to the network. And if there is an address that does not exist in the trusted addresses list,

it will understand that there is an intruder in the network and will turn off the substation, making sure that no one in the network gets to control the households. So, in our simulation, the third IP address was the intruder, so the server machine understands that and turns off the substation.

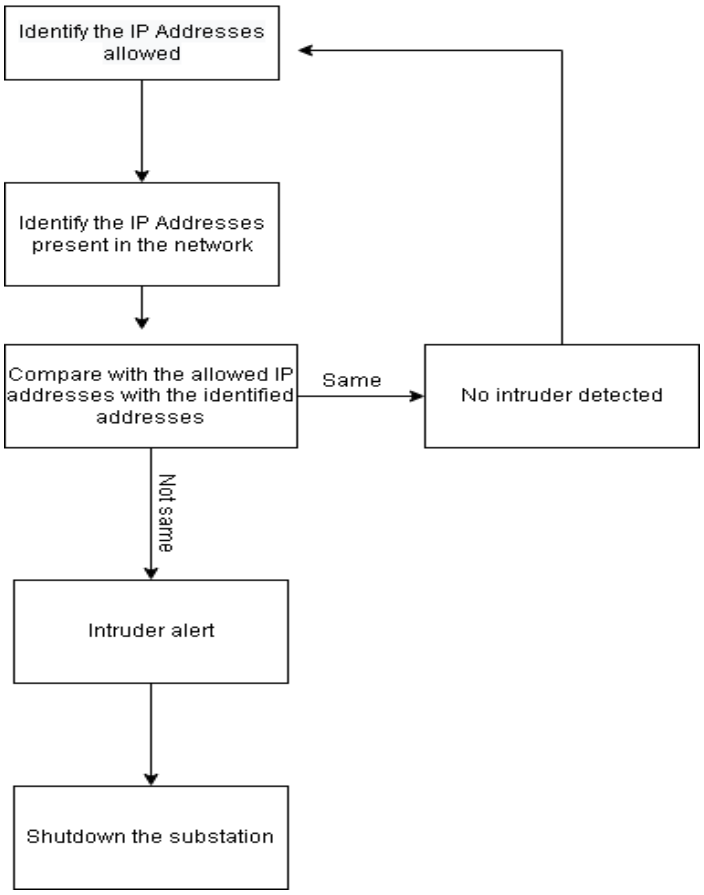

Fig-1: Workflow

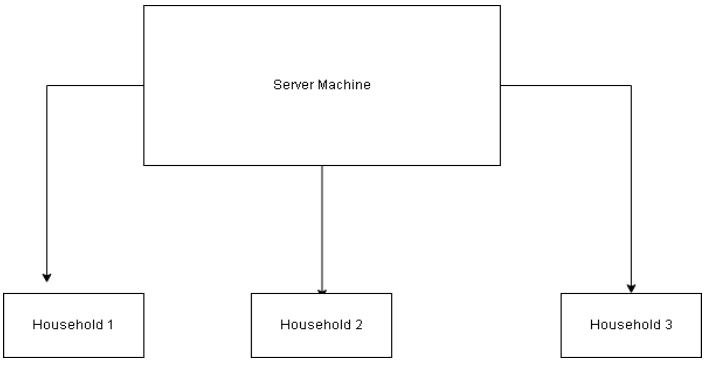

Fig-2: Communication Network of Substation

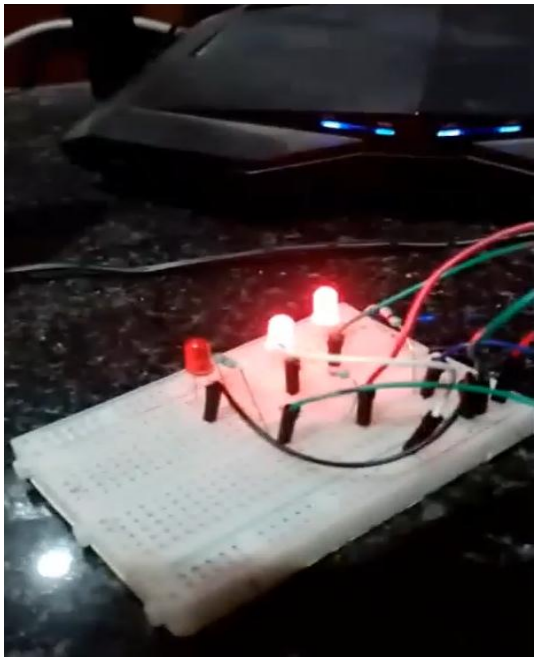

Fig-3: Substation Network

B. IED and Auxiliary power supply

A substation with 2, 100 kV inputs and one 2.2 kV input were modeled on Simulink. Of the 3 input lines, the 100 kV lines are permanently connected, and the 2.2 kV input line provides an intermittent supply, or is switched on only during power shortage. All input lines have a similar circuit of operation.

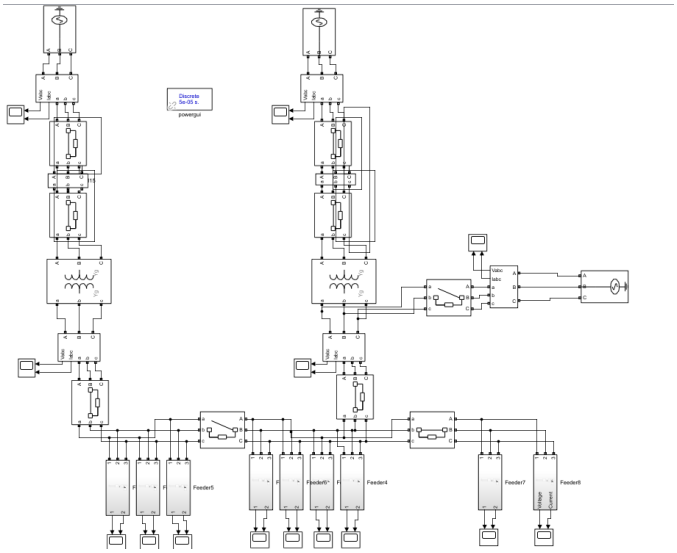

Fig-4: Model of a Substation using Simulink

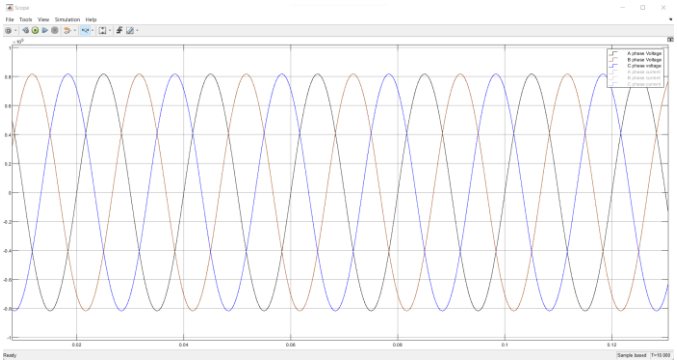

Fig-5: 3 phase Input Voltage to the Substation

Fig-6: 3 phase Input Current to the Substation

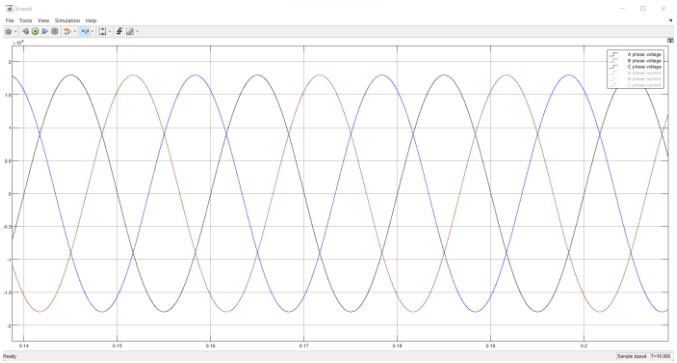

Fig-7: Auxiliary Supply 3 phase Input Voltage to the Substation

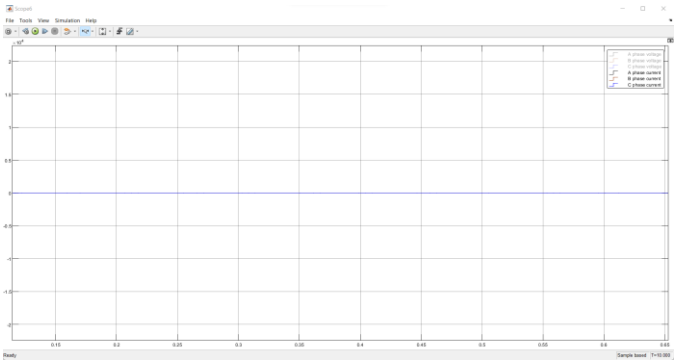

Fig-8: Auxiliary Supply 3 phase Input Current to the Substation

The input voltage and current are measured using a measurement block, and the input is fed to a circuit breaker, which trips the circuit when current goes beyond limits. A 3-phase step-down transformer steps the voltage down to 2.2 kV from 100 kV. Another layer of IED protection is provided here with a circuit breaker. This voltage is distributed to various wards using a feeder circuit for each ward. The feeder circuits are essentially composed of another layer of IED (circuit) protection, and 3 phase voltage and current are the outputs to this block.

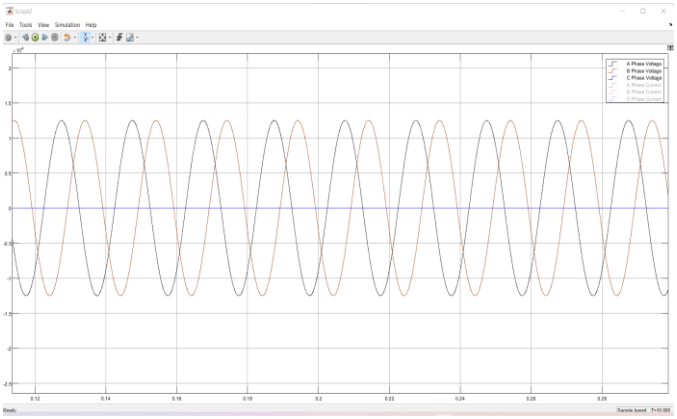

Fig-9: 3 phase Input Voltage to the Feeders

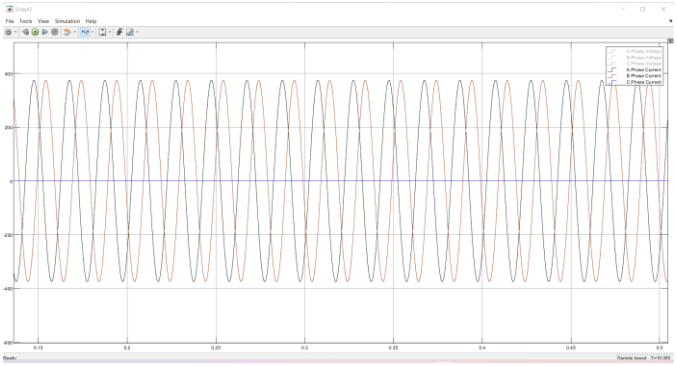

Fig-10: 3 phase Input Current to the Feeders

The sets of feeders are separated from each other using a bus coupler. These feeder circuits are followed by another step-down transformer on the distribution side. Load Flow analysis was conducted on this system, and the voltage and current flows were analyzed at different parts of the substation. Load Flow Analysis is done using the equation given below:

$$\frac{P_i - jQ_i}{V_i^*} = V_i \sum_{j=0}^{n} y_{ij} - \sum_{j=1}^{n} y_{ij} V_j \qquad j \neq i$$

Fig-11: Load Flow Equation

3. RESULTS AND CONCLUSION

With the advent of technology and its integration to every domain, past constraints were solved and efficiency was improved. However, this was also followed by a new set of problems such as Hacking, Fraud etc., which were overcome by the integration of cybersecurity into various systems. With the rise of Smart Grids and related technologies, a similar system can be implemented in these Smart Grids which work with WAN network connectivity. A server machine will monitor all the connections in the network and if an intruder is detected, suitable actions will be taken.

Fig-12: The server machine detects that there's an intruder in the network and shuts the substation down

Upon the detection of an intruder on the network, the substation network is shut down making it inaccessible by an user. To make up for this shutdown, an auxiliary power supply is added to the substation network so that the households don't experience power cuts[1]. The use of a two-way communication between the clients and the server machine, further improves the transparency in the system, and ensures timely maintenance and reduced power outages on the customer end.

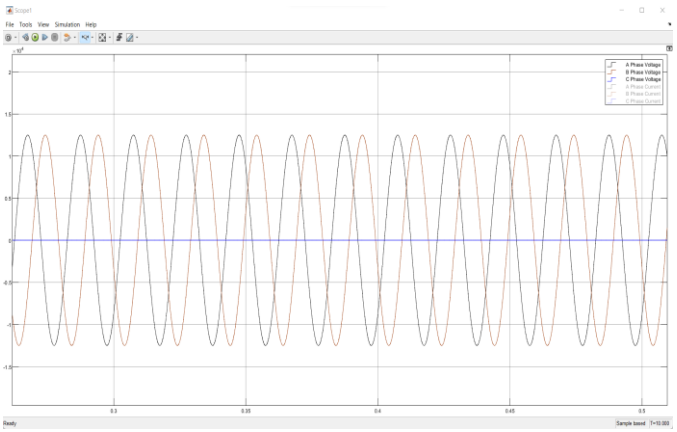

Fig-13: 3 phase Output Voltage from the Feeders

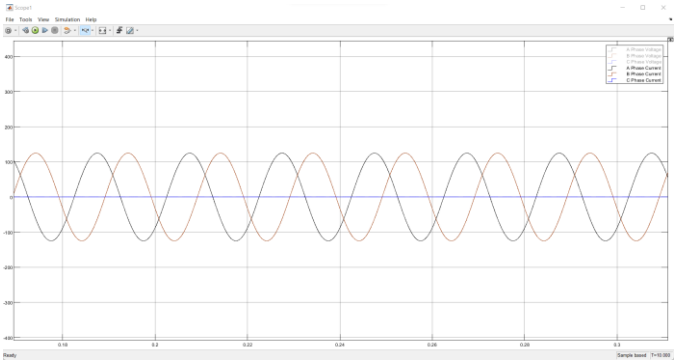

Fig-14: 3 phase Output Current from the Feeders

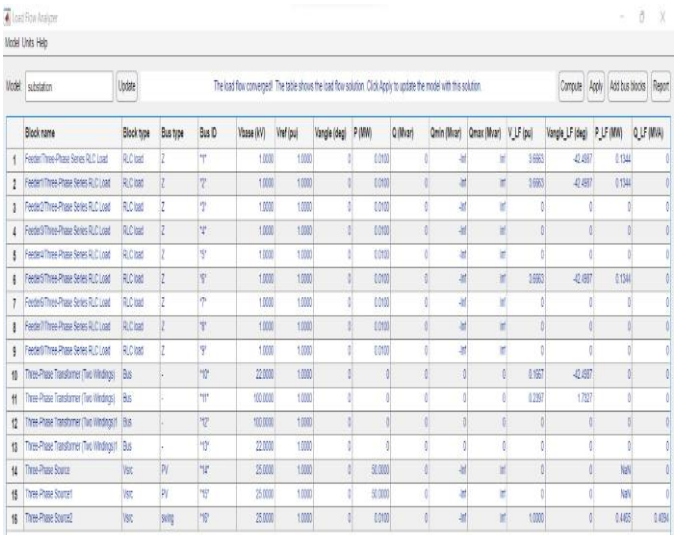

Fig-15: Load Flow Analysis of the substation

4. FUTURE SCOPE

The server machine used was a Windows 10 Laptop and the whole process took place using Python language. Primitive languages like C, C++ can give faster results. Instead of using a Windows 10 machine, a Windows Server machine can be used where the whole process of server maintenance is easier. Other machines that run on Linux distributions can be used for easier understanding and faster results. Instead of turning off the whole substation, banning that respective IP address from the network would be a better solution in scenarios that are not as severe.

REFERENCES

[1] Irina Kolosok, Elena Korkina," Problems of Cyber Security of Digital Substations", VI International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security', 2019

[2] M. N. Dazahra, F. Elmariami, A. Belfqih, J. Boukherouaa, "A Defense-in-depth Cybersecurity for Smart Substations", International Journal of Electrical and Computer Engineering (IJECE),Morocco, December 2018,

[3] "Cyber security for power grid protection devices", DNV, Edition August 2021

[4] N. Srinivas and S. Modi, "A Comprehensive Review of Microgrid Challenges and Protection Schemes", SPAST Abs, vol. 1, no. 01, Oct. 2021.,

[5] N. P. Srinivas and S. Modi, "Pole-to-Pole Fault Detection Algorithm Using Energy Slope for Microgrids," 2022 International Conference on Electronics and Renewable Systems (ICEARS), 2022, pp. 288-294, doi: 10.1109/ ICEARS53579.
2022. 9752299.,

[6] N. Srinivas, S. Singh, M. Gowda, C. Prasanna and S. Modi, "Comparative Analysis of Traditional and Soft Computing Techniques of MPPT in PV Applications," 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), 2021, pp. 1-6, doi: 10.1109/GUCON50781.2021.9573876.,

[7] Durgaprasad S., Nagaraja S., Modi S. (2022) HVDC Fault Analysis and Protection Scheme. In: P. S., Prabhu N., K. S. (eds) Advances in Renewable Energy and Electric Vehicles. Lecture Notes in Electrical Engineering, vol 767. Springer, Singapore. https://doi.org/10.1007/978-981-16-1642-618.,NirupamaPSrinivasandSangeetaModi2022 ECSTrans.10713345

[8] https://www.ripublication.com/irph/ijee16/ijeev9n105.pdf