Plotting a Path through High Voltage Power System Security using ICT

E. I. Igweonu, Robert Ben Joshua, Eguzo Chimezie V, and Oluwe Musbau Olajide.

Electrical Electronic Engineering Technology Department

Akanu Ibiam Federal Polytechnic Unwana.

ABSTRACT- The electric power sector is undergoing a period of unprecedented changes and the modern management of high voltage complex power systems demands the interoperability of economic, Computer science and electrical/electronic engineering. This synergy has led to the development of a more enhanced system, but has also exposed the system to other challenges. This paper highlights some of the security challenges experienced as a result of this convergence and how ICT can be utilized as a platform to proffer a sustainable solution for a more secure and reliable power infrastructure.

Keywords - cyber attack, security, reliability, protection, communication.

1. INTRODUCTION

Power systems are large-scale and complicated networks consisting of power generation (power plants), delivery (transmission and distribution grids) and consumption (customers) [1]. Service location, storage and IT solutions are also part of the infrastructure value chain found in power systems setup [2]. The interoperability of electrical, computer engineering and Information Technology (IT) resources has generated diverse concept of the power system infrastructure design and operation. The concept develops to include energy sustainability, consumer response, electrification of transportation and related areas [3]. This resulted to new and developing technologies like SCADA (Supervisory Control and Data Acquisition), AMI (Advanced Metering Infrastructure), EMS (Energy Management System) and other energy technologies. These technologies are primarily dependent on communication, control and computer capabilities that support new development in line with the current technological approach to power and energy resources. Monitoring of electric power systems in real time for reliability and presence of incipient faults requires distributed processing of vast amount of data from distributed networks.

The Use of modern communication, computing and control technologies provides tremendous opportunities in doing this and in the development of a secure, resilient and intelligent power system infrastructure. Unfortunately, the developed infrastructure will be vulnerable to many security threats from both internal and external sources if protection of the vulnerable system is not taken into consideration. The main focus of this paper is to explore security areas in the power system infrastructures and provide possible counter measures to forestall any unwanted incursions into these areas.

2. THE SECURITY CONCEPT

The concept of power system vulnerability is not only in the failure of the system to provide electric power but encompasses other aspects of system functionality like; System Reliability, Communication Reliability, Information Protection, Infrastructure Protection and Consumer Protection amongst others. Security in power system reliability applies to the ability of the system to deliver regular services to the consumer with measures to counter disturbances such as short circuits, loss of system elements due to natural causes or man-made, physical or cyber attacks.

Communication reliability in power system communication is of different facets including the probability of message loss, time delay (latency) in message delivering, variability of time delay (jitter) and quality of service (QoS). Security in terms of information protection involves measures employed to ensure anonymity of electronic information both in transit and when stored in digital systems, protection of information and commands used for power system control [4]. The interdependence of electric, telecommunication and computer infrastructures in the power and energy design scenario, has made the internet an inevitable tool for the functionality of this hybrid system. Hence an action in one part of the infrastructure network can rapidly create a chain reaction by cascading throughout the same network and even into other networks [5] Hence, there is the need to design, develop and

maintain a system that meets the need for performance, reliability, computation and communication attributes of the system while at the same time achieving appropriate levels of confidentiality, integrity and availability.

3. VULNERABILITY: CHALLENGES AND PROSPECTS

3.1 CYBERATTACKS

The number of cyber attacks and intrusion has risen very rapidly in recent years. Due to the increasing sophisticated nature and speed of malicious code, intrusions and Denial of Service (DoS), human responses may be inadequate. Figure 1 shows the evolution of these threats and the response type needed to combat it effectively [5]

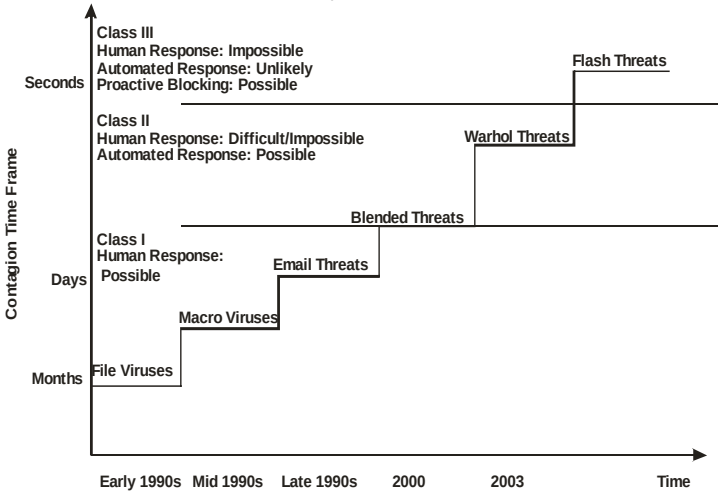

Fig 1: Cyber-threat evolution (IEE PES Jan/Feb 2012).

The increasing dependency of power systems on computer communication network and control has exposed the system to some of the threats illustrated in figure 1. Originally, the systems were designed for use with proprietary and standalone communication networks but because of the cost and productivity, these systems use the internet for higher functionality. To protect the infrastructure, some these security guides needs to be evoked to ensure protection and minimize disruption to operation.

- Layered Security: This involves integrating multiple security technologies at each computing layer to reduce unauthorized access. It also increases the cost and difficulty of compromising a system. The layers that must be included are: Personnel, Networks, Operating Systems, Application and Database. The security features needed in each of the layers include examination, detection, prevention and encryption. [5]
- Internet Protocol Transition: In application, the equipment in use is merely supported by Internet Protocol version 4 (IPV4) which with its current features will not stand the test of time in security as new technologies evolve. The IPV4 standards for data communication over public medium such as internet is optional using IPsec, this feature needs to be specifically configured for each network thus creating a security risk for transfer of sensitive data prior to configurations [7]. Modern layered communication protocols are required as an essential tool for modification, design and management of power systems. Internet Protocol Version 6 (IPV6) ensures this by providing a better protocol stack that addresses the issues of address availability, security, application and physical media management. These protocols share common addressing methods to simultaneously transport messages from multiple application layer protocols without compromising its security features [4].

3.2 INFRASTRUCTURE CHALLENGES (WIRELESS SENSOR APPLICATION)

The rate of hacking attacks experienced on critical infrastructures is continuously increasing, making the security of these infrastructures a big challenge. Some researchers have demonstrated the use of wireless sensor-based solution for cost effective electric system protection. Infrastructures like sub-stations, transformers, high-voltage circuit breakers, transmission lines, reactors etc. should be incorporated with wireless sensors and cameras that can be remotely monitored and controlled for information report on system disruptions to control centers. The sensors allow remote detection of medium- and low-voltage power transformer hotspots, through an infrared camera, to identify an emerging malfunction. All the monitored parameters will be visualized via the SCADA (supervisory control and data acquisition) system through a special-purpose interface and a graphical user interface [6]. In figure 2 (adopted from IEE PES as an illustration of wireless sensor based automated protection system), both consumers and power lines are monitored from a control center through the wireless sensors. The integration of these units will yield a sustainable energy management system that will give information on the condition of the equipment, substation, meters, energy usage patterns, voltage levels and other aspect of the power system.

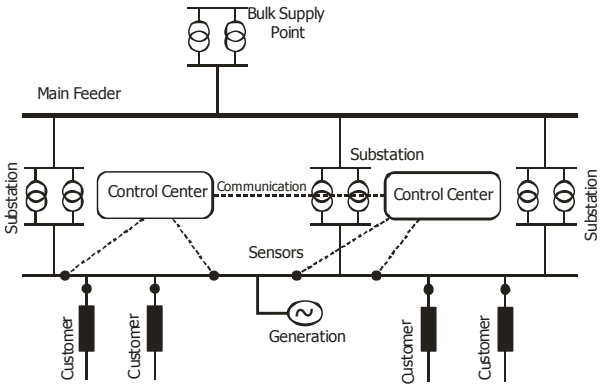

Figure 2: Wireless Sensor Automated Protection System.

CONCLUSION

The place of information communication technology (ICT) in high voltage power system security has been explored. To ensure the potency of sustainable power system management, the concept of security using information technology should be placed in the front burner. In terms of benefits; IT based security system will enable power system infrastructures stand up to internal and external disturbances, It will increase the cost of unauthorized disruption of system functionality and provide an a cost-effective real-time infrastructure monitoring process. The initial challenges of adopting these security techniques notwithstanding, the system will still come out as one of the best approaches to the security of high voltage power systems.

REFERNCES

1. Y. Serizawa, "Information and Communication Technologies for Stable Electric Power Supply" IPSJ Magazine, vol. 46, No. 3, pp. 294-299. Mar. 2005
2. THE CHINA GREENTECH REPORT www.china-greentech.com 2009
3. Manimaram G & Peter S; Smart Grid and Security, USA, IEEE Power and Energy (PES) magazine 10(1)16-17 Jan-Feb ed (2012).
4. Daniel N: Terms of Protection, IEEE Power and Energy (PES) magazine 10(1)18-23 Jan-Feb ed 2012
5. Massoud A & Anthony G "Smart Grid – Safe, Secure, Self-Healing: Challenges and Opportunities in Power System Security, Resiliency and Privacy" IEEE Power and Energy (PES) magazine 10(1)33-40 Jan-Feb ed (2012)
6. Wireless sensors for infrastructure protection: WSAN4CIP Project – retrieved from http://www.wsan4cip.eu/news/view/article/wireless-sensors-for-infrastructure.htm visited March 2012
7. E.C Arihilam, C.V Eguzo & E.E Osazuwa: Internet Protocol Transistion: Challenges and Prospect International Journal of Engineering Sceince, Vol 2 (6):PP 17-21. (2010)