Chapter 83
Vulnerabilities and Threats in Smart Grid Communication Networks

Yona Lopes
Fluminense Federal University, Brazil

Vitor dos Santos Farias
Universidade Federal Fluminense, Brazil

Natalia Castro Fernandes
Fluminense Federal University, Brazil

Julia Drummond Noce
Universidade Federal Fluminense, Brazil

Tiago Bornia de Castro
Universidade Federal Fluminense, Brazil

João Pedro Marques
Universidade Federal Fluminense, Brazil

Débora Christina Muchaluat-Saade
Universidade Federal Fluminense, Brazil

ABSTRACT

Advances in smart grids and in communication networks allow the development of an interconnected system where information arising from different sources helps building a more reliable electrical network. Nevertheless, this interconnected system also brings new security threats. In the past, communication networks for electrical systems were restrained to closed and secure areas, which guaranteed network physical security. Due to the integration with smart meters, clouds, and other information sources, physical security to network access is no longer available, which may compromise the electrical system. Besides smart grids bring a huge growth in data volume, which must be managed. In order to achieve a successful smart grid deployment, robust network communication to provide automation among devices is necessary. Therefore, outages caused by passive or active attacks become a real threat. This chapter describes the main architecture flaws that make the system vulnerable to attacks for creating energy disruptions, stealing energy, and breaking privacy.

DOI: 10.4018/978-1-7998-5351-0.ch083

INTRODUCTION

According to the NIST (National Institute of Standards and Technology) conceptual model (NIST, 2014), smart grids are composed of seven logical domains, which have distinct characteristics, actors, and intelligent devices that must be interconnected. End devices have become smarter and may communicate seamlessly with data and control centers.

In the past, communication networks for electrical systems were restrained to closed and secure areas, which guaranteed network physical security. Due to the integration with smart meters, clouds, and other information sources, physical security to network access is no longer available, which may compromise the electrical system control and management.

Smart grid deployment begins with a massive insertion of smart meters. Also, the number of Intelligent Electronic Devices (IED) increases in order to support Distribution Automation (DA). In general, the quantity of automation sensors, such as smart meters and IEDS, and the amount of data collected from these sensors increase significantly. Smart grids bring a huge growth in data volume, which must be managed.

In order to achieve a successful smart grid deployment, robust network communication to provide automation among devices is necessary. Such scenario involves several nodes, links, systems, protocols, and technologies. A composition of different types of networks forms a broad and complex architecture. It brings several advantages such as visibility, availability, and remote control that make possible several new operations from the utility. In addition, new energy applications, such as capacity planning and peak power shaving, will improve the system. Moreover, new applications will facilitate the deployment of new energy services such as energy audits, demand response programs, and electric vehicle charging (Budka, Deshpande, & Thottan, 2014).

However, the same interconnected system that makes the grid smarter also brings security threats and makes the grid vulnerable to attacks. Thereat smart grids cannot advance without dealing with security problems. Attacks against the electrical power grid can directly impact the population and would affect people, trade, companies, and anyone who cannot stand without electric power. Any possibility of event that impacts confidentiality, integrity, and availability of smart grid domains is considered a threat.

Attacks attempting to gain advantage of the information exchange system vulnerabilities are known as data-centric threats. Such threats can be elusive and might result in critical damage to industrial infrastructure. A worm might reprogram an industrial control facility to degrade the equipment and generate false operation logs, compromising maintenance. An attacker can take control of the system or steal confidential information without physical access to the plant (Wei & Wang, 2016). Attacks against nuclear facilities such as the Falliere et al. (2011) worm incident and the Assante (2016) attack are a demonstration of the dangerous potential of cyber threats.

For instance, SCADA (Supervisory Control and Data Acquisition), which is a very important system that monitors the electrical system operation, must be interconnected with all that network structure. SCADA system vulnerabilities are usually correlated to the use of the Human Machine Interface (HMI) and data historians (Wilhoit, 2013). Data historians are log databases that store trends and historical information about processes of an industrial control system.

Compromising the HMI can lead the attacker to access secure areas where he can modify set points or controls. An improper opening or closing circuit breaker can cause unnecessary consumer shutdowns. Besides, if a circuit was undergoing maintenance, an improper closing circuit breaker would threaten human life.