Brief Overview of Cybersecurity Issues on Smart Power Systems

Eduardo I. Ortiz-Rivera, IEEE Senior Member
University of Puerto Rico-Mayaguez
Department of Electrical and Computer Engineering
Mayaguez, PR, 00680
Email: eduardo.ortiz7@upr.edu

Luis Romero, IEEE Student Member
University of Puerto Rico-Mayaguez
Department of Electrical and Computer Engineering
Mayaguez, PR, 00680
Email: luis.romero14@upr.edu

***Abstract*—In this new technology era, the cybersecurity on the new generation renewable energy systems is constantly being tested to the limit on many ways. In order to ensure proper functionality and protection for these renewable energy systems and users is necessary to test these to ensure safe operation under hazardous conditions or other kind of threats. Given that some technologies currently implemented on renewable energy systems (like smart 3-Phase Inverters) are fairly new, a whole new world opens for threats like attacks generated by malicious actors. One example of these highly dependable systems are Smart Power Systems. Technology on these Smart Power Systems support several types of communications (mainly wireless) and present a challenge it self with its own vulnerabilities. The focus of this paper is to present the importance of Cybersecurity for improving these smart technologies by exploring its different vulnerabilities and possible testing vectors.**

I. Introduction

The deployment of renewable energy systems is becoming an essential need to advance our national interests and reduce our dependency on fossil fuels. Currently, the amount of energy produced by renewable sources is significantly smaller than the amount produced by the burning of fossil fuels.

Therefore, instead of a major overhaul of the electrical system, it has been proposed to attach renewable energy systems to the smart grid. This will create a large complex system in which the available infrastructure will interact with new generation facilities that will rely on various types of renewable energy sources. The benefits of this proposal are evident: (1) we can complement current infrastructure with newer and cleaner methods gradually, (2) the adoption can help research in the area without affecting our capability and (3) once the technology is mature enough that its generation levels can compare to those of the current infrastructure, the later can be phased-out gradually reducing the dependency on fossil fuels.

However, in order to provide energy to the country without interruptions, our infrastructure must be constantly monitored and protected from potential threats. In order to ensure protection, it is necessary to detect and eliminate vulnerabilities in critical systems before terrorists or enemies are able to exploit them successfully in an attack. The smart grid technology implemented on the electrical system can be exposed to such attacks due to potential security vulnerabilities that can be exploited such as: lack of encryption of sensitive data, firewalls not properly defined, and the use of foreign technology that may have hidden functionality that can potentially compromise the system, among others.

In this project we will use as the case of study the electrical system in Puerto Rico. Recently, Puerto Ricos electrical system has introduced solar and wind generation facilities to the current fossil-fuelbased generating system. This fact added to the relative small size of the system makes it a good evaluation scenario that is well suited to better understand or identify potential threats at a larger scale.

II. Cybersecurity on Power Systems

In this paper is primarily focus on examining different scenarios that could affect the resilience of the system if it is under attack or under any other unexpected failure. The main goal of this paper is to present the risks that the use of foreign technology in might pose to the deployment of renewable energy systems to the smart grid. In this paper will rely on a model of the Puerto Rico electrical system. In particular and with special interest to provide a cyber-secured power system.

A power systems with the proper cyber security should be able of addressing the following:

a. Robustness: 1. How to identify that the system is under attack? 2. Would it be possible to detect a hidden transmission signal?

b. Resiliency: 1. Evaluate the possibilities to isolate the source of the attack. 2. Would it be possible to disrupt or alter the malicious signal?

c. Reconfigurable: 1. How to maintain generation using the compromised renewable energy system? 2. How to recover from the attack?

It has been have identified the following potential attacks such that the system should be able to identify and react: 1. Changes in voltage phase in order of tampering the amount of energy distribution that may cause quick energy changes by the compromised resource. 2. Denial of service by blocking or diverting energy distribution. 3. Use of infected equipment to monitor, spy or affect behavior of the grid.

III. Historical Risks on the Use of Foreign Technologiesies on the Electric Grid

During the past decades, there have been several incidents that illustrate the potential risk of using or depending on foreign technology and components. Governments of developed nations, actively use technology as a lever with which to advance their policies and interests throughout the world. The issue of dependence of foreign technology for attaching renewable energy systems to the US smart grid infrastructure should be analyzed in the context of avoiding Americas vulnerability to foreign interests.

For example, during the 1960s, the US government ordered IBM to withhold computer technology from France with the purpose of limiting that nations capability of developing their nuclear program. During the Reagan administration, US firms were prohibited to supply technology that would aid in the development of a Soviet natural gas distribution pipeline for the European nations. Similarly, Japanese low-cost and high-efficient technology components have undermined American companies and put the country at risk of a potential denial of critical technologies from Japan that may carry national security liabilities.

In context of national security, it can be defined a foreign source as a source of supply or manufacture of technology that is located outside the United States and Canada. Similarly, a foreign dependency implies a foreign source for which there is no immediate available alternative within the United States or Canada. A foreign dependency whose lack of availability jeopardizes national security by limiting the development, or the operation of critical infrastructure for the country can be defined as a foreign dependency-based vulnerability.

Reliance on foreign suppliers for critical infrastructure and technologies for smart grid should raise concern at a national level. Particularly, given the distant position we currently are related to the rest of the world in terms of renewal energy systems. In this scenario, Germany is a leader in solar energy, which seems ironic if it is considered that solar resources in Germany are far less than those in the US. Spain is a leader in the utilization of wind technology and China is such a major manufacturer and potential market for renewable energy systems that it can be assumed that the design and production of renewal energy equipment will be greatly influenced by Chinese special interests in the matter. This condition may relegate US to the utilization of foreign technology for the deployment of our renewal energy systems posing a threat to US interests.

The case of Chinese intervention is not new. Several American companies such as Google have made complaints about cyber-attacks coming from Chinese locations. As recent as January 2013, it was disclosed that network equipment manufactured by a Chinese company with ties to the Chinese government was removed from Los Alamos National Laboratory (a nuclear research facility) under concerns that such equipment might contain hidden infrastructure or features that could allow the Chinese military to obtain crucial information from the system. The devices under particular concern consisted of the switches the lab uses to manage data traffic over their network. If such equipment were compromised, the attacker would potentially have access to all data that reached the equipment. A robust, resilient and reconfigurable system can help speed up the adoption of renewable energy systems in the US while maintaining our infrastructure safe from malicious attacks.

IV. Conclusion

This paper described a brief overview of cybersecurity issues on smart power systems. Clearly Smart Power Systems can be used for different civilian applications such as: better resilience of the electric grid, energy independence from the traditional utility, hybrid renewable energy systems for different energy sources, in addition to other applications. Part of the problems faced when employing these systems can be solved by locating and testing thoroughly its various components. Additionally, the development of cyber-protocols and double evaluations by the regulatory agencies could serve to mitigate potential cybersecurity issues on power systems. Finally, the selection of trustful foreign manufacturers can play a key role in the protection of the electric grid and minimization of a cyber-attack.

Acknowledgment

The authors would like to thank the members of the Minds2CREATE Research Team at UPRM for all their help and collaboration in the succes of this project.

References

[1] (2012) Smart grid initiatives address cyber security renewable energy intermittency:. [Online]. Available: http://www.renewableenergyworld.com/rea/news/article/2012/01/smart-grid-initiatives-address-cyber-security-renewableenergy-intermittency

[2] Cyber security for renewable energy systems:. [Online]. Available: http://www.ct-si.org/events/APCE/sld/pdf/50.pdf

[3] European renewable power grid rocked by cyber-attack:. [Online]. Available: http://www.euractiv.com/energy/european-renewable-power-grid-ro-news-516541

[4] J. C. O.-R. E. I. Navarro, Daniel*; Carlos Mendez. (2015) Leveraging cybersecurity for securing and testing current and future unmanned technologies. 2015 Conference for the Computing Alliance of Hispanic-Serving Institutions (CAHSI).

[5] ——. (2015, Aug.) Cybersecurity of unmanned aerial systems: Vulnerabilities and end-to-end exploitation of future deployable commercial systems. 2015 ASEE International Conference on Cyber Security.