Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 28 (2014) 575 – 582

Procedia Computer Science

Conference on Systems Engineering Research (CSER 2014)

Eds.: Azad M. Madni, University of Southern California; Barry Boehm, University of Southern California; Michael Sievers, Jet Propulsion Laboratory; Marilee Wheaton, The Aerospace Corporation
Redondo Beach, CA, March 21-22, 2014

Mitigating The Risk Of Cyber Attack On Smart Grid Systems

Eric B. Rice[a]*, Anas AlMajali[b]

[a]*Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California, USA*
[b]*Information Sciences Institue, University of Southern California, Los Angeles, California, USA*

Abstract

Smart Grid technologies are being developed to upgrade the power grid with networked metrology and controls that can improve efficiency and provide new methods to manage the system. While these technologies offer great benefits, they also introduce new classes of risk, most notably creating new attack vectors that can be exploited by cyber attack. To assess and address risks in cyber-physical systems like these, the system designer's toolset needs to include concepts drawn from cyber security, reliability, and fault tolerance design, integrated into a common methodology. In this paper, we discuss the fragmented landscape of studies into the risk of cyber attack on smart metering systems, and then draw on concepts from systems engineering and fault tolerance design to organize and unify the pieces.

Keywords: Smart Grid, Systems Engineering, Cyber Security, Cyber-physical Systems

* Corresponding author. Tel.: +1-818-393-6643.
E-mail address: Eric.B.Rice@jpl.nasa.gov

doi:10.1016/j.procs.2014.03.070

1. Introduction

Smart Grid technologies are being developed to upgrade the national power infrastructure with networked metrology and control infrastructure. These efforts aim to improve operational efficiency in the near term, and create new opportunities for advanced technologies in the future. Smart Grid solutions may greatly improve the reliability of the grid and reduce costs of power delivery, but they also introduce new reliability and cyber security risks. Demand Response (DR) technologies provide the utility a path to manage system load in addition to the available supply, creating control loops that may couple loosely with existing controls. Advanced Metering Infrastructure (AMI) deployments are intended to improve the efficiency of meter reads, but also provide other monitor and control capabilities, such as the ability to connect or disconnect service to a customer by remote command. In both examples, new control paths are added that may affect the individual and aggregate behavior of loads on the power grid in ways that have not previously been experienced by grid operators.

The risks introduced by AMI deployments are of particular interest because of the immediacy of AMI deployments. Commercial AMI networks are being deployed worldwide, with penetration rates in the U.S. reaching as high as 30.2% in 2012[2]. These commercial deployments commonly follow current best practices for security, which include protections for the core data security concerns of integrity, availability, and confidentiality[3]. Although these security designs can provide assurance that cyber attacks will be less likely to succeed, the consequence of a successful attack may still be high. A compromise of metering networks may allow adversarial access to control functions that, if corrupted, have consequences above and beyond the integrity or availability of data in the system, including risks to human safety and system integrity. As market penetration increases, so do the potential risks associated with the security of these controls.

Over the last several years, there have been numerous publications that attempt to characterize risk of cyber attack directed at smart grid technologies. Some of these efforts have focused on breadth-first analysis of risk, with only a cursory discussion of mitigations. Others have focused on one element of the system, or on a limited scenario, demonstrating robustness of that part of the system to a given attack. Studies that address mitigation of attacks tend to focus on a single feature or component, with little discussion of the properties of the end-to-end system that make the mitigation viable.

In this study, we intend to tie together some of the independent threads in the literature, by applying systems engineering and fault management concepts to an example cyber-physical scenario. In our previous work[1], we built a simple model that allowed us to study the inter-system interactions of a metering network with the power system during a load-drop attack, in which an adversary gains access to control functions of the AMI to send a sequence of service disconnect commands to customer meters. In this discussion, we apply broader systems and fault management concepts to expand that analysis to characterize the range of potential behaviors and outcomes, and to derive constraints for detection and response techniques that may help reduce the consequence of such an attack.

2. Related Works

In approaching this analysis, we draw on three threads from related disciplines. We aim to contribute to the existing body of work in smart grid attack analyses by applying concepts from fault management systems design within a broader framework of systems engineering for security.

2.1. Smart Grid Cyber Attack Analyses

A number of publications in recent years have attempted to address the risk of cyber attacks against metering infrastructure. Broader papers have performed analyses of the threats to power infrastructure in general and AMI systems in particular, while more focused works have attempted to characterize one part of the system during an attack. Sridhar et al[5] performed an end-to-end assessment of the risks the power system faces from malicious attack. While the analysis includes concepts of control loop integrity and load drop attacks directed at AMI systems, it stops short of describing the mechanisms by which an attack would impact the grid, or estimating the potential outcome of a particular scenario. Clements et al.[6] provide more detailed analysis of the Western Electricity Coordinating Council (WECC) service area response to specific load-drop and oscillatory load control attacks. Results showed