Chapter 15
Cyber Risks in Energy Grid ICT Infrastructures

Giovanna Dondossola
RSE S.p.A., Italy

Fabrizio Garrone
RSE S.p.A., Italy

Judit Szanto
RSE S.p.A., Italy

ABSTRACT

The objective of the chapter is to present the role of cyber security experiments within a methodological approach for the evaluation of cyber risks in grid control systems. As a starting point, a cyber-power risk index has been defined to support the identification of relevant risk factors across network attack models. Instances of attack models have been then experimented on an ICT architecture implementing grid operation scenarios with the double aim of evaluating the attacks' effects by means of communication performance measures and of tuning the configuration of security mechanisms. The chapter discusses the results of a variety of attack experiments and their role in the calculation of the risk index.

INTRODUCTION

Distributed intelligence and interconnected communication networks are recognized key factors for the operation of energy grid infrastructures in today's competitive power markets. However energy delivery systems are vulnerable to cyber attacks. Many cyber security studies have demonstrated the vulnerability of SCADA (Supervisory Control And Data Acquisition) systems to unauthorized access and several real-world cases of intrusion occurred in different critical sectors, including power systems. Unfortunately very few of the incidents have been publicly reported, and initiatives aimed at sharing cybersecurity information by creating an open repository of industrial incidents have been strongly opposed due to their confidental nature. The success of the Stuxnet worm (Falliere, 2010), affecting Siemens's nuclear power plant controllers in 2010, was an example of how nowadays sophisticated and well resourced attackers can develop complex cyber attacks causing severe damage to power infrastructures.

DOI: 10.4018/978-1-4666-5942-1.ch015

The probability of success of a cyber attack to smart grid control infrastructures will increase with the massive deployment of advanced automation and communication technologies relying on standardized protocols. Therefore the cyber security of information and communication networks that constitute the core of the next generation delivery system represents an emerging research topic as well as a European priority (COM, 2009). One major issue in the development of the cyber risk assessment methodologies is the lack of historical data series to be used for the assignment of values to the probabilities of vulnerability existence, threat occurrence and attack successfulness. This is due on one hand to the sensitiveness of vulnerability issues, on the other hand to the rareness of threats and attacks.

A way of bypassing the scarcity of data inherent to ICT (Information and Communication Technologies) incidents in upcoming smart grid infrastructures is to set up a test platform on which to run repeatable experiments and collect data statistics on the successfulness of attack processes in realistic grid operation scenarios. Inside the experimental environment it is possible to reduce the complexity of the grid control infrastructure by using a scaled down ICT architecture having its focus on those information flows that are most critical to the secure and economical operation of smart grids.

The objective of the chapter is to present the role of cyber security experiments within a methodological approach to evaluate the exposition of grid control systems to cyber risks. The distinctive feature of the methodology is the centrality of the attack concept: attacks are the cyber contingencies of the risk index whose success probability is conditioned by ICT vulnerabilities and intentional threats. As attacks are in fact cyber technical processes, the evaluation of their probability of success may benefit from experimental results gained on test architectures.

The chapter will start with the identification of the key items of the cyber-power risks, followed by the presentation of the scope and the sample results from an experimental activity, ending with a discussion about the inputs provided to the cyber-power risk evaluation. The contribution of the chapter to the cyber risk evaluation of grid control systems is at methodological level, with an emphasis on the role of security experiments. The calculation of a risk quantitative value of a specific grid control infrastructure is out of scope of the present chapter.

BACKGROUND

The experimental evaluation of cyber attacks targeting grid control systems is of fundamental value for research related to the protection of critical information infrastructures, specifically in the ICT-energy cross sectors. The key issues about dependencies in critical infrastructures were addressed the first time in the United States by (Rinaldi, 2004), where a *dependency* is defined as a connection between two infrastructures, through which the state of one infrastructure influences or is correlated to the state of the other.

Since 2004 the Swiss Federal Institute of Technology started to publish an inventory of national and international infrastructure protection policies updated on a bi-annual basis (Wenger, 2008). At governmental level the Department of Energy stipulated a huge research program specific to a National SCADA Test Bed for the energy sector (DoE, 2008).

Within the community of experts in power system security the problems arising from system interdepencency stressed the need to extend the power system transient analysis with new approaches able to deal with cascading contingency chains (Amin, 2001; CIGRE, 2007; PSERC, 2005). The intensive networking at the core of advanced grid control favours the occurrence of cascading phenomenons in the power system.

The CRUTIAL European Project developed two testbeds (Deconinck, 2009) demostrating the