Chapter 11

Model-Based Evaluation of the Impact of Attacks to the Telecommunication Service of the Electrical Grid

M. Beccuti  
Università di Torino, Italy

S. Chiaradonna  
ISTI – CNR, Italy

F. Di Giandomenico  
ISTI – CNR, Italy

S. Donatelli  
Università di Torino, Italy

G. Dondossola  
RSE S.p.A., Italy

G. Franceschinis  
Università del Piemonte Orientale, Italy

ABSTRACT

This chapter is devoted to the study of the consequences of cyber-attacks to the telecommunication service of the electrical grid, which is an essential service for the grid control system. It is up to the control system to ensure that even very large power systems are kept in equilibrium even in presence of power contingencies. This chapter considers cyber-attacks of the Denial of Service (DoS) type, occurring while the electrical grid is already facing an electrical failure that requires a load shedding strategy. Using a model-based approach that uses the rich and flexible formalism provided by the tool Möbius, it is possible to investigate the interplay between an attack to the telecommunication service and the state of the grid in a number of different situations and for different characterizations of the DoS behaviour and severity. The formalism used allows to associate a (stochastic) duration and/or a probability to the events happening in the system, so as to take into account the variability in attacks’ behaviour, leading to a quantitative characterization of the impact of a DoS attack to the electrical grid.

DOI: 10.4018/978-1-4666-2964-6.ch011
INTRODUCTION

Energy Power Systems (EPS) can be considered as the composition of two major elements: the Energy Infrastructure (denominated in the following Energy Infrastructure EI) and the information and communication technology distributed control system (denominated in the following Information Infrastructure II) that supervises the EI. The supervision and control may be impaired by malfunctions in the underlying telecommunication system, or in some node of the control system itself. Even assuming that the II is working, we have to consider the possibility that cyber attacks may alter its correct behaviour: this may be due to a specific malware that alters the behaviour of the EI control algorithm, or the value of the control data transmitted, but it may be also due to an attack to the telecommunication network, provoking message losses and/or delays which may lead to a partial malfunctioning of the control system. Lost or delayed messages may not be so crucial when the EI is working in normal status, but they may have drastic consequences when the EI is facing an electrical failure. Since EPSs provide vital services to a variety of activities governing people life, it is of relevant importance to assess the possible cascading effects that failures in the II control subsystems may have, when they occur in critical scenarios of the EI.

Indeed an important step towards the design of a reliable service, consists in clarifying the (inter) dependencies between the electrical and information infrastructures. In particular it is important to investigate the possible consequences of a failure to one or more nodes of the II distributed control system, or to the telecommunication network supporting the information exchange among the distributed control system components at different levels in the EI control hierarchy. The large space of possible critical situations need to be explored selecting a set of representative scenarios (that should be enriched on the basis of the experience) and evaluating the possible behaviours as a function of the type of failure (e.g. those caused by an attack) and of the state of the EI when the failure comes into play. It is very important to have a reference framework to abstract out from the details of the specific scenario or experiment, recognize recurring patterns of cascading behaviour, and provide a quantitative evaluation of their impact.

Although the modelling of the types of failures that are characteristic of interdependent critical infrastructures has received increasing interest in the last years, after the large blackouts of electric power systems in 1996 and 2003, there is still no definite understanding on EPS interdependencies, and on the techniques to evaluate even the dependency between an II failure/malfunctioning and the services provided by the whole EPS. It is indeed of great importance for the utilities operating the infrastructures to have methods/tools for analysing threat impacts and technologies for avoiding, or limiting, most serious consequences.

Chapter “Cyber Risks in Energy Grid ICT Infrastructures” of this book has characterized and analysed the risk of different types of cyber attacks to the II, which is a fundamental step in setting up ICT countermeasures, but a complete evaluation of the attack impact requires an evaluation of the consequences of a successful attack on the overall behaviour of the electrical grid. In this chapter we propose a framework to understand and evaluate the cascading effects of attacks to the telecommunication service that supports the distributed control system of an energy grid in critical scenarios (like in presence of a failure of a grid component). A model-based approach is chosen, due to its high flexibility in exploring a wide range of alternatives at a limited cost and in representing at different abstraction levels the various layers of the EPS hierarchy (e.g. transmission versus distribution, local versus regional and multiregional as proposed for example in (Becchi, Chiaradonna, Di Giandomenico, Donatelli, Dondossola & Franceschinis, 2012), (Chiaradonna, Lollini & Di Giandomenico, 2007) and (Chiaradonna, Giandomenico & Nostro, 2011).