DEPARTMENT OF ELECTRICAL POWER ENGINEERING
FACULTY OF ELECTRICAL ENGINEERING
WROCLAW UNIVERSITY OF SCIENCE AND TECHNOLOGY

ABSTRACT
DOCTORAL DISSERTATION

CYBER SECURITY OF DISTRIBUTION SMART GRID

M.Sc. Robert Czechowski

SUPERVISOR
Prof. Eugeniusz Rosołowski, DSc, PhD

Co-supervisor
Piotr Pierz, PhD

Wroclaw University of Science and Technology

Wrocław
November 21, 2017

Abstract

The work discusses issues related to design and exploitation of secure distribution smart power grids. It presents the prospects for development of these grids, accounting for the issues of their digital security. It shows the components of a smart power system model responsible for digital communication, monitoring and control of the grids. The solution discussed in the work will allow for an increased level of security from the perspective of threats and potential attacks.

Chapter 1 (Security Policy of Smart Power Grids) presents an introduction to the concept of smart grids (including smart metering grids) and allows to understand the often underestimated role of a security policy, especially important for ensuring the security of critical systems. It goes into detail about the issues of system digital security, the rules of grid design and exploitation, and specifies the components of smart control and metering automatics. It also presents solutions on the organizational level, from the awareness and responsibility of workers employed by a given electric energy operator, to implementation of documents precisely and clearly specifying the rules of conduct in case of a security incident.

Chapter 2 (Smart Grid Logical Architecture) explains how smart grids are constructed from the perspective of their logical structure, with their division into roles and functions in the system taken into account. The chapter presents the models and individual logical areas of grid functionality and explains the dependencies and functions of all actors (participants). It thoroughly discusses transfer, distribution and low voltage grids, as well as micro generation, energy storage systems and smart household installations integrated with the operator's system. It also presents dependencies of interfaces and communication channels comprising: the time, priority and required response time of individual elements, necessary for efficient management of extensive power systems.

Chapter 3 (Research and simulations) presents five models of grids with varied degree of complexity and operating area within smart grid infrastructure. The chapter describes laboratory positions, test procedure, simulations and research findings of the following models: models of smart metering real grid (models 1-3), accounting for stability tests and logical event statistics, ICT infrastructure theoretical model (based on real data), have reflected support of control processes, as well as data exchange and agency (model 4), ICT infrastructure model designed in software CySeMoL[6], aimed at analysis of potential hazards that might result from cybernetic attacks against IT infrastructure and control and metering systems, and ATP-EMTP[7] distribution grid reference model (model 5). The selected models allow for metering instantaneous currents waveforms of voltage, power and energy selected by the user, as well as selected mechanical parameters. Based on analysis of individual models, it is possible to evaluate security and hazards, and their impact on specific types of researched interference and deliberate attacks. The models also allow for conducting analysis for a very large number of variants of system failure scenarios, and analysis of actions aimed at autonomous and automatic restoration of a grid unaffected by failure to its functionality. The analysed models allow the acquisition of research material for more precise and multi-criteria analysis of attacks according to accepted scenarios.

Chapter 4 (Risk analysis and threat assessment) is dedicated to issues of risk assessment, including the process of analysis and evaluation of probable threats. The chapter also touches

[6] CySeMoL ObjectModeler 2.3

[7] ATPDraw 6.2

upon the consequences of different attack scenarios, including an attack against a single component of a system, as well as attacks related to setting alteration in security automation systems (overriding threshold values), which may lead to a power system collapse, and subsequently to wide-area blackouts. The chapter goes into detail of potential possible forms of attack, from attacks against a backbone grid, an ICT operator center, to attacks against low voltage grids utilizing smart electricity meters, concentrators, ICT grid active devices and data transmission media.

Chapter 5 (Technical aspects of Smart Grid security) shows the present issues and problems encountered during smart grid design. It lists solutions and methods that might help increase their security. The chapter also presents the most commonly encountered problems occurring during modernization of existing and design of new power grids using digital automation systems and telecommunications solutions based on an IT technology. The chapter discusses the most important issues and problems encountered during exploitation of current (classic) power systems and grids, i.e.: electromagnetic radiation, variable shaping of information transfer route, time synchronization, redundant layouts and systems, or problems related to electricity theft. It describes algorithms for detection of anomalies, abuses and intrusions, as well as principles of grid traffic filtration based on pre-defined rules. It also discusses the principles of communication and authorization of users and devices in every area of a power system. It presents dedicated solutions available on the market, which are able to not only detect, but also effectively repel an attack, directly contributing to an increased security of the entire system.

Chapter 6 (Conclusions and final remarks) summarizes the conducted simulation research and analyses of acquired results. The goal of the work is to prove that the main role of an attack detection system implementation is to inform the system administrator about it for them to undertake actions aimed at mitigating the negative impact of a successful attack. Additionally, the work tackles open research problems, as well as specifies the possible directions for further research and design changes aimed at improvement of security in power systems.

Utilization of ICT protection measures in an extensive power system will significantly improve their efficiency and reliability, which is of key importance for the energy security of an entire country. Digital information exchange will be an inseparable part of smart power grids' evolution, and their security will be the priority for both transfer and distribution systems.

21.11.2017