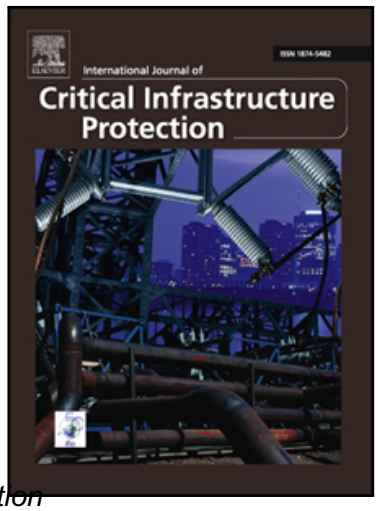

Standards on Cyber Security Assessment of Smart Grid

Rafał Leszczyna

PII: S1874-5482(16)30142-1
DOI: 10.1016/j.ijcip.2018.05.006
Reference: IJCIP 252

To appear in: *International Journal of Critical Infrastructure Protection*

Received date: 21 October 2016
Revised date: 21 May 2017
Accepted date: 27 May 2018

Please cite this article as: Rafał Leszczyna, Standards on Cyber Security Assessment of Smart Grid, *International Journal of Critical Infrastructure Protection* (2018), doi: 10.1016/j.ijcip.2018.05.006

Standards on Cyber Security Assessment of Smart Grid

Rafał Leszczyna*

Gdańsk University of Technology, Narutowicza 11/12, 80-952 Gdańsk, Poland
e-mail: rle@zie.pg.gda.pl

Abstract

Security evaluation of communication systems in smart grid poses a great challenge to the developers and operators. In recent years many new smart grid standards were proposed, which paradoxically results in the difficulty in finding a relevant publication in this plethora of literature. This paper presents the results of a systematic analysis which aimed at addressing this issue by identifying standards that present sound security assessment guidance. This should help practitioners in choosing the standards that are applicable to their area. Additionally the contents extracted from the standards can serve as a useful guidance on security assessments of smart grid components.

Keywords: cyber security, security assessment, critical infrastructures, smart grid

1. Introduction

The transformation from traditional power infrastructure to a new form of electricity network called *smart grid* should result in many significant social and technological benefits connected to the decentralised nature of the grid and the utilisation of Information and Communication Technologies (ICT) to enable two-way power and information flows.

From the users' point of view, the smart grid gives the opportunity of actively controlling their energy usage, taking advantage of flexible energy plans and even becoming small-scale electricity suppliers. As for energy providers, it enables time-based pricing, better capacity and energy utilisation planning, and more flexible adjustment to the market demands. The grid enhances energy transmission management and increases resilience to control-system failures [96, 145].

At the same time the intense use of Information and Communication Technologies brings in many new concerns. Smart grid is a collection of different legacy systems surrounded with new technologies and architectural approaches, compliant to different standards and regulations that all need to be combined into one communication network. The interlinked smart grid communication systems have many vulnerabilities that differ across networks [145].

The smart grid interconnection with the Internet exposes the grid to new types of risks, including Advanced Persistent Threats (APT), Distributed-Denial-of-Service (DDoS), botnets and zero-days [26, 141, 145, 10]. Stuxnet, Duqu, Red October, or Black Energy are just few examples of modern threats that appeared since 2010 [118, 41, 126, 125, 139, 57]. The new variant of Black Energy threat, called Disakil is being linked to the Ukrainian power outages in December, 2015 [135]. Sophistication of these attacks raises very quickly.

Securing the smart grid requires a multidisciplinary approach that combines various technologies and incorporates managerial, policy, legal aspects and more. The crucial part of this process is formed by security assessment [26, 47, 94] i.e. evaluating the level of security and identifying potential vulnerabilities that can be exploited by attackers.

There is a strong need for the assurance that information technologies embedded in the smart grid will not induce failures or facilitate the intrusion by malicious agents (e.g. hackers, virus). It is also important to understand what is the impact of cyber attacks on power facilities in the smart grid [46].

Operators and security officers seek for systematic security assessment methodologies that can provide the assurance of reliable and secure operation of the grid [92]. Security experts agree that standardised solutions and practices should be used in the first place [137, 140].

In recent years numerous smart grid standards were published. This results in the situation that operators find it difficult to orientate themselves in this plethora of literature, for instance, when choosing a standard applicable to a particular domain or functional area of the grid. Each time they want to choose a standard-recommended solution, they are forced to conduct a time consuming study in order to select the relevant standards.

The study presented in this paper aims at addressing this problem by identifying the standards that can be applied to security assessments of smart grid components. Based on a systematic literature review that comprised three main stages, 35 cyber security publications of relevance were identified. To the best of the author's knowl-

*Corresponding author