IEEE STANDARDS ASSOCIATION

IEEE

IEEE
SMART GRID
RESEARCH

IEEE CYBER SECURITY FOR THE SMART GRID



IEEE 3 Park Avenue New York, NY 10016-5997 USA

Trademarks and Disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The Institute of Electrical and Electronics Engineers, Inc.

3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2013 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published September 2013. Printed in the United States of America.

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: 978-0-7381- 8517-0 STDVA98299

Print: 978-0-7381-8518-7 STDVAPD98299

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at:
http://standards.ieee.org/

IEEE SmartGrid Research has been obtained from sources believed to be reliable. Neither IEEE nor its authors guarantee the accuracy or completeness of any information published herein, and neither IEEE nor its authors shall be responsible for any errors, omissions, or damages arising out of the use of this information. References made to products, technology, solutions, trade names, vendors, or otherwise, do not constitute or imply its endorsement or recommendation by IEEE or its authors.

The information identified in this report are based on discussions with industry participants and Zinnov's ongoing research in smart grid and related markets. Conclusions drawn are anticipated only, and do not imply prediction of events in the future. Information provided in all segments is based on availability, and the willingness of participants in sharing these within the scope, budget, and allocated time-frame of the project, and reflects the views of industry participants.

Likewise, while the author and publisher believe that the information and guidance given in this work serve as an enhancement to users, all parties must rely upon their own skill and judgment when making use of it. Neither the author nor the publisher assumes any liability to anyone for any loss or damage caused by any error or omission in the work, whether such error or omission is the result of negligence or any other cause. Any and all such liability is disclaimed.

This work is published with the understanding that IEEE and its authors are supplying information through this publication, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in the publication.

Table of Contents

Executive summary **5**

Introduction 5

Cyber security assessment of the Smart Grid 5

Country analysis 6

Conclusion 7

Overview **8**

Introduction to Smart Grid 8

Smart grid representation 9

Issues with Smart Grids 10

Cyber security threats and agents 11

Smart Grid cyber security market size 13

Case studies 13

Case studies 14

Cyber security assessment of Smart Grid **15**

Cyber security framework 15

Communication 16

Advanced metering infrastructure 21

Control room 29

Substation 39

Electric vehicles 48

Country analysis **52**

United States 52

Germany 59

India 62

China 69

South Korea 73

Japan 80

Conclusion **90**

Cyber security framework 90

Country summary 94

Present investments in cyber security for Smart Grid 98

Future outlook for cyber security in Smart Grid 100

Action items for cyber security in Smart Grid 103

Acknowledgements **104**

Abbreviations **105**
References **109**
Authors **120**

Executive summary

Introduction

Countries across the globe are implementing smart grids in order to achieve reductions in emissions, increased grid efficiency, increased usage of renewable energy sources, increased consumer control over their energy consumption, and other economic benefits. Despite the promised benefits of the Smart Grid, there are various concerns that need to be addressed such as security threats, privacy concerns, high infrastructure costs, and increased tariffs for effective implementation.

A large number of possible threat scenarios and threat agents make it imperative for Smart Grid cyber security to be adequately addressed. This report details the cyber security vulnerabilities that exist in the Smart Grid value chain, the efforts undertaken by certain countries to mitigate these vulnerabilities, and the measures that need to be implemented going forward. Four such instances of cyber security breaches are highlighted in this report.

Cyber security assessment of the Smart Grid

This section of the report examines the cyber vulnerabilities that exist within the value chain, the existing standards and protocols for cyber fortification, and various technologies that can mitigate the threat. Five different components of the Smart Grid value chain are covered in detail, namely communication, Advanced Metering Infrastructure (AMI), control room, substation automation, and electric vehicles.

The communication layer is the backbone of the Smart Grid and is vulnerable to cyber attacks. In the past, utilities carried out communication operations over their networks. However, to meet the communication needs of a larger number of end points (namely the customer base), third-party communication service providers are now playing a more active role in rollout plans. This report details the different types of communication media (wired and wireless) that are used in each segment of the Smart Grid value chain. The cyber security threats for some of these technologies are also detailed.

This report discusses the architectural layout and information flow within the AMI, and the standards and protocols that ensure the cyber security of the AMI network. Various types of cyber attack intrusion methods, and the motives behind them, are discussed. The different types of security breaches in AMI are categorized according to the threat level of each of them, and are also categorized by the type of impact that they can have (based on three security parameters: confidentiality, integrity and availability). This report also highlights detection technologies that can help fortify the AMI network.

The Demand Response Automation Server (DRAS), used for automating dynamic pricing and messages, is also vulnerable to several breaches. This report showcases the varying levels of impact of these cyber vulnerabilities associated with the Demand Response Management System and the DRAS, based on the security parameters of confidentiality, integrity, availability, or a combination of these.

The wide deployment of networking technologies in Supervisory Control and Data Acquisition (SCADA), and its high connectivity with other networks such as corporate networks exposes it to a plethora of cyber attacks. This report details the general layout of the SCADA system and its various interactions with other entities. It discusses multiple cyber threats faced by SCADA systems, and determines their impact on confidentiality, integrity, and availability.

A substation is one of the most critical components of the grid as it is exposed to both cyber and physical vulnerabilities. A compromised substation can result in power outage, grid instability, loss of SCADA control, and loss of SCADA related information. This report discusses the primary and secondary components and architectural layout of an automated substation, and examines substation cyber threats and preventative security measures, including protocols and standards that have been framed and established by the IEEE, IEC, and NERC in order to secure substations.

Electric vehicles will form an important component of Smart Grids, especially due to the proliferation of vehicle-to-grid (V2G) technologies, which enable electric vehicles to be used as distributed energy sources. The current investments in cyber security for electric vehicles, the growth rate of these investments over the next few years, and the focus areas for cyber security investments for electric vehicles are detailed in this report.

Country analysis

This report showcases the various endeavors undertaken by six countries—United States, Germany, India, China, South Korea, and Japan—with respect to cyber security for the Smart Grid.

In the U.S., the implementation of a Smart Grid was given priority in 2007 with the passing of the Energy Independence and Security Act. In 2009, the American Recovery and Reinvestment Act further reinforced the efforts to build a modern, secure Smart Grid system. This report details some of the prominent challenges being faced by the U.S. with respect to cyber security of its Smart Grid in particular, and critical infrastructure in general. It also speaks of the need to have a federal body leading the effort of cyber fortification, the NERC's transmission planning standards for evaluating the system under myriad conditions, and the executive order on cyber security signed by President Barack Obama in February 2013.

Germany's Smart Grid road map can be broadly divided into three distinct phases by the German BDEW (German Association of Energy and Water Industries): preparation phase (2012 to 2014), implementation phase (2014 to 2018) and marketing phase (2018 to 2022). This report lists the standards framed by the IEC to secure, regulate, and standardize the adoption of the Smart Grid in Germany. It also showcases the security portfolio for Smart Grids that the BSI is working on in order to ensure cyber security and data protection.

India intends to implement a Smart Grid nationally by 2027, in three five-year stages. Under the National Smart Grid Mission (NSGM), India envisages investment of more than INR 314 billion from 2012 to 2017, with 14 pilot projects dealing with multiple Smart Grid technologies. Smart Grid implementation in India is overseen by the India Smart Grid Forum (ISGF) and the India Smart Grid Task Force (ISGTF). This report highlights the objectives and roadmap of the ISGF's Working Group on Cyber Security, which aims to conduct a security audit of Indian electricity organizations.

China envisages the Smart Grid to be implemented in a three-stage process, culminating in 2020: planning and trial phase, all-round construction, and monitoring phase. A total of 228 pilot projects have been commissioned across China to analyze different aspects of Smart Grid deployment, challenges, and solutions. This report sheds light on certain security-specific standards for Smart Grids that China has released. With China's heavy focus on cyber security for Smart Grids, its cyber security market is estimated to reach USD 50 billion by 2020, largely driven by measures to fortify Smart Grid systems.

South Korea pursues their Smart Grid initiative as a national policy in order to achieve their vision of "low carbon, green growth." The Korea Smart Grid Institute (KSGI) was launched in August 2009 as the Secretariat of Smart Grid Initiatives and Projects in South Korea. Its Smart Grid implementation is broadly segmented into three phases:

- Phase 1: Construction and operation of the Jeju (an autonomous island) test bed
- Phase 2: Expansion into metropolitan areas
- Phase 3: Completion of a nationwide intelligent power grid

The national South Korean Smart Grid roadmap is composed of five implementation areas: smart power grid, smart place, smart transportation, smart renewables, and smart electricity service. This report discusses some of the protocols that ensure cyber security for AMI for Jeju and highlights the security requirements of the AMI system and the guidelines for AMI security protocol.

Japan's Smart Grid deployment is guided by its long-term "Smart Community" roadmap. Four large-scale pilot projects—Kyoto Keihanna district, Yokohama city, Toyota city, and Kitakyushu city—have been commissioned in Japan to study different aspects of the Smart Grid. Japan's New Energy and Industrial Technology Development Organization (NEDO) has collaborated with various institutions across the world to run pilot programs that were selected on the basis of their geographic, environmental, and economic resemblance to regions in Japan. Japan released "Information Security Strategy for Protecting the Nation" in 2010, which is supplemented by an annual Information Security Review. This report highlights the policies, background, and key actions of the strategy. It also highlights certain specific measures that need to be undertaken to secure critical infrastructure in Japan per its 2012 Information Security Review.

Conclusion

Through this study, it has been concluded that the different players within the Smart Grid ecosystem need to interact closely and establish a framework in order to facilitate a standardized security model. In order to realize a secure, stable, and efficient Smart Grid system, it needs to be equipped with self-healing features, which are discussed herein. This report also details the technologies and architectural guidelines for a five-step security framework: prevention, detection, response, recovery, and communication. Highlighted are the existing standards of cyber security for Smart Grids in the U.S., Germany, India, China, South Korea, and Japan, and the requirements for the future.

This report takes a look at the amount invested in Smart Grid cyber security by venture capitalists compared to other Smart Grid technologies, as well as a comparison of a number of venture capital deals by different Smart Grid technologies. Thus, the future outlook for the Smart Grid cyber security is determined. Stakeholders across the Smart Grid value chain believe that the industry is adapting to the prospect of increased debilitating cyber attacks and taking appropriate measures. This report highlights the action items that need to be addressed collectively by all stakeholders in the Smart Grid ecosystem for security to be effectively realized.