SYNGRESS

SECURING THE SMART GRID

Next Generation Power Grid Security

Tony Flick
Justin Morehouse

Securing the Smart Grid

Next Generation Power Grid Security

Tony Flick
Justin Morehouse

Syngress

Securing the Smart Grid

Next Generation Power Grid Security

Tony Flick
Justin Morehouse
Technical Editor
Christophe Veltsos

ELSEVIER AMSTERDAM • BOSTON • HEIDELBERG • LONDON • NEW YORK • OXFORD • PARI
• SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO SYNGRESS.
Syngress is an imprint of Elsevier

Copyright

Acquiring Editor: Rachel Roumeliotis
Development Editor: Matthew Cater
Project Manager: Julie Ochs
Designer: Alisa Andreola

Syngress is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely o their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they hav a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation o any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Flick, Tony.

Securing the smart grid : next generation power grid security / Tony Flick, Justin Morehouse technical editor, Christophe Veltsos.

p. cm.

Includes bibliographical references and index.

ISBN 978-1-59749-570-7 (pbk. : alk. paper)

1. Electric power systems--Security measures. I. Morehouse, Justin. II. Veltsos, Christophe. II Title.

TK1025.F58 2011

333.793'2–dc22 2010029873

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

Printed in the United States of America

10 11 12 13 14 10 9 8 7 6 5 4 3 2 1

Typeset by: diacriTech, Chennai, India

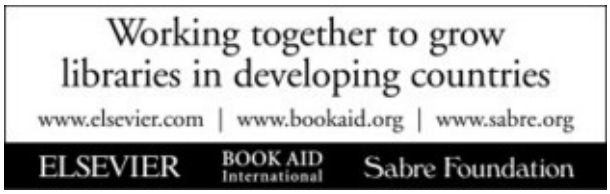

Table of Contents

Acknowledgments (Tony Flick)

I want to thank my parents for pushing me into the computer science field, buying many compute along the way, and not getting too angry when I would secure their new computer by breaking it. Aft all, I was only following in my Dad's footsteps after he secured the dustbuster. My dad taught m many things in life and worked hard to give me a good life. From working midnight shifts to keep th streets safe and still finding the time to coach the teams I played on, I can only hope to be half the da that you were to me someday. Although not the most conventional method, playing cards (euchre an poker were the best) with your collection of pennies, nickels, and dimes at the age of three made ma classes enjoyable and easy throughout life. The other parents and teachers often asked me if m parents used flash cards or hired tutors to improve my math skills. I would just think back to the fun had playing cards, while subconsciously learning the fundamentals of math. Mom, I know you were little worried when you came home one day and heard me yell, “hit me!” during a poker game at th age of three. But after all, I did eventually get a degree in math.

Mom, you introduced me to computers when you brought home the computer that could on display green characters on the monitor. Playing video games and learning how to initially type wi you on that old computer only grew my fascination with electronics, which drove me to the field computer science and eventually security. I also want to thank you for working hard to give me better life. I know it was not always easy, but I am eternally grateful for the opportunities you gave m in life.

My brother Matt, thank you for helping significantly with the application security portions of th book, letting me bounce ideas off of you, and providing a ton of great ideas that were used in the boo I am thankful that you always took the time out of your busy schedule to help me with homework an computer-based projects, and to play hours-upon-hours of video games.

I also want to thank my sister for having the patience to review my reports in college and teachin me how to write professionally. Even though I was playing video games with your future husban while you reviewed those reports, I did actually pay attention to your comments and learned from yo gentle editing jokes. Hopefully, you can read this book to Brooke and Samantha; it is good to teac security at a young age.

Over the past eight months, I locked myself in my office or hotel room on weeknights an weekends to write this book. I want to thank everyone who supported me during this time and allowe me to shut the world out in order to finish. I can only hope to repay the debt I owe to those wh brought me food when I was hungry and convinced me that taking a break to grab a drink, or two, wi friends and loved ones could only improve the book.

Thank you Rachel Roumeliotis and Matthew Cater at Syngress for giving us the opportunity write this book and guiding us along this journey. Christophe Veltsos, thank you for providing advic and suggestions that greatly enhanced the content of this book. Finally, thank you to my coautho Justin Morehouse, for working late nights and weekends to write this book.

Acknowledgments (Justin Morehouse)

I would like to thank my wife, Lisa, the love of my life, for the support, patience, and understandi she showed me throughout the writing process. Without her, much of what I have accomplished ar the person I have become today simply would not be. I am grateful to my parents, John and Susan, f always supporting me in whatever endeavors I pursue and teaching me that I am capable of almo anything if I put my mind to it.

Thank you to Rinaldi Rampen, Jeff LoSapio, and Mike Volk for recognizing in me the ability t become someone more than just another consultant and showing me that I could turn my passion in a career. Thank you to Steve Dunkle for reminding me that there is more in this world than just m career. Thank you to the Becks, Ryan, Melissa, and the Joels for your enduring support ar understanding.

Thank you to Rachel Roumeliotis, Matthew Cater, and Christophe Veltsos for the support ar vision you provided me with while authoring this book. Thank you to Matt Flick, Jeff Yestrumska Rich Robertson, and Shawn Moyer for picking up my random calls or responding to my countless mails. Finally, thank you to my coauthor, Tony Flick, for battling through these last couple of month to see this book to press.

About the Authors

Tony Flick (CISSP) has been working in the information security field for more than seven years an is currently a principal with FYRM Associates. Tony's background is in network and applicatio security, assessments, compliance, and emerging technologies. In the energy industry, Tony ha performed network and application penetration testing, written and reviewed security policies an procedures, and provided guidance for utility companies and related technology vendors. He graduate from the University of Maryland, College Park, with a Bachelor of Science in Computer Science and Bachelor of Science in Mathematics. Tony has spoken at Black Hat, DEF CON, ShmooCon, ISSA, an OWASP meetings on Smart Grid and application security concepts. Additionally, Tony has bee recognized as a security subject matter expert and utilized by numerous media outlets including th Associated Press (AP), *SC* magazine, Dark Reading, and eWeek.

Justin Morehouse (CISSP, CISM, MCSE) has been working in the information security field for ov eight years, primarily focusing on the areas of attack and penetration. He has performed over 20 security assessments for Fortune 1000 companies and Federal government agencies and is current the assessment lead at one of the nation's largest retailers. Justin has developed numerous too including PassiveRecon and GuestStealer, and has spoken at DEF CON, EntNet, ISSA, ISACA OWASP and ShmooCon conferences. He graduated with a bachelor's degree from The Georg Washington University and a master's degree in Information Assurance from Norwich University Justin is currently an adjunct professor at DeVry University and leads the OWASP Tampa Chapter.

About the Technical Editor

Dr. Christophe Veltsos (CISSP, CISA, CIPP) is a faculty member in the Department of Informatic Systems & Technology at Minnesota State University, Mankato, where he regularly teache Information Security and Information Warfare classes. Christophe has presented at the local, regiona and national level, including at major security conferences like RSA.

Beyond the classroom, Christophe is also very active in the security community, engaging wi community groups and business leaders as well as IT and security professionals. In 2007, he w elected president of the Mankato chapter of the Information Systems Security Association (ISSA). 2008, he made numerous contributions to the SANS NewsBites newsletter as an advisory boa member. In 2009, he joined and has contributed to the work of the privacy subgroup of the NIS Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG), formerly known a the NIST Cyber-Security Coordination Task Group (NIST-CSCTG).

Christophe holds a PhD from the University of Louisiana at Lafayette and is a member of mar information security and privacy related organizations including ISSA, ISACA, (ISC)², and IAP Both faculty and practitioner, Christophe maintains the DrInfoSec.com blog.

Introduction

Information in This Chapter

- Book Overview and Key Learning Points
- Book Audience
- How This Book Is Organized
- Conclusion

Book Overview and Key Learning Points

This book provides you 14 chapters of content exploring the strengths and weaknesses of the sma grid. By examining components of the smart grid in detail, you will obtain a strong understanding how the confidentiality, integrity, and availability of these components can be both compromised ar secured.

Discussing both the smart grid's strengths and weaknesses will help you understand threats ar attacks, and hopefully prevent insecure deployments of smart grid technologies. In this book, you wi also learn controls that will allow consumers, device manufacturers, and utility companies minimize the risk associated with the smart grid. Each chapter aims to provide you with informatio that can be used to not only secure current implementations, but future ones as well.

Book Audience

This book will prove to be a valuable resource for anyone who is responsible for the network application security of smart grid deployments. It will also provide value to those who are tasked wi auditing smart grid deployments, as well as consumers utilizing smart grid devices. System enginee application developers, and system integrators will find value in learning the strengths ar weaknesses of the smart grid, and utilize this knowledge to secure current and future deployments.

Executive-level management will gain an appreciation for the complex issues presented b implementing smart grid technologies, as both a provider of these technologies, as well as a consume This book will reinforce the value of funding and supporting security initiatives that help protect th smart grid deployments that will soon touch nearly every home, business, and organizations.

How This Book Is Organized

This book is divided into 14 chapters, each diving deep into specific subject matter. Due to the natu of the subject matter, it is highly recommended that you read this book starting with Chapter “Smart Grid: What is it?” and finishing with Chapter 14, “What's Next?” Later chapters referen material from previous chapters, building on the concepts, attacks, threats, and technologies alread discussed.

Chapter 1: Smart Grid: What Is It?

In this chapter you will learn about the history of electrical grids, ranging from Tesla and Edison automatic meter reading (AMR). This chapter also discusses the infrastructure that will comprise th

smart grid, including automatic metering infrastructure (AMI). Finally, you will learn abo international initiatives and review why the smart grid needs to be secured.

Chapter 2: Threats and Impacts: Consumers

This chapter explores potential threats and impacts to the smart grid, and in particular, how they ma affect consumers. One of the major goals of the smart grid is to provide more information consumers, so that they can make informed decisions regarding their energy consumption. E providing information on the threats that consumers will face, readers will learn why they should se to minimize the risks associated with the smart grid. This chapter furthers the awareness of the threats so that utility companies, technology vendors, and consumers can try to avoid devastati impacts of a successful attack.

Chapter 3: Threats and Impacts: Utility Companies and Beyond

This chapter reviews similar information to Chapter 2, "Threats and Impacts: Consumers," but appli them specifically to utility companies and other organizations. This chapter discusses the threats a impact to such organizations, categorized by the impact to the CIA Triad: Confidentiality, Integrity and Availability. In this chapter, you will learn how the smart grid will forever change the way tha organizations manage risk and the potential impact of successful attacks. The threats and impac discussed in this chapter are based in reality and are often overlooked when discussing the benefits the smart grid. This chapter does not aim to spread fear, uncertainty, and doubt, but rather bring light the potential impact of smart grid deployments so that protective measures can be implemente to prevent such attacks before it is too late.

Chapter 4: Federal Effort to Secure Smart Grids

Many countries consider the security of their electric grids to be a matter of national security and as result, these governments are funding initiatives and enacting laws to ensure security is considered smart grids. This chapter explains to readers the different roles that Federal agencies are performi and discusses the different smart grid security standards, guidelines, and best practices bei developed by Federal agencies. This chapter also informs the readers of how the Federal governme is planning to help utility companies and technology vendors secure the smart grid.

Chapter 5: State and Local Security Initiatives

This chapter focuses on the efforts of state and local governments and organizations. Similar Chapter 4, "Federal Effort to Secure Smart Grids," this chapter discusses how government agenci are impacting the security of smart grids. Additionally, this chapter examines how the judicial syste may use the massive amount of information that is collected in the smart grid. Finally, this chapt discusses the role that state and local agencies will need to perform to educate consumers on how securely interact with the smart grid.

Chapter 6: Public and Private Companies

This chapter discusses how public and private companies can help secure the smart grid. First, th chapter discusses industry plans for self-policing, such as NERC's Critical Infrastructure Protecti standards. Second, you will learn how compliance with such regulations does not equate to securi

the smart grid. Finally, this chapter reviews how technology vendors can fill the gaps betwee compliance and security.

Chapter 7: Attacking the Utility Companies

This chapter addresses the numerous different attack vectors that utility companies should be prepare for. Penetration testing and vulnerability assessments are an integral part of any organization security program. However, limiting testing to only certain attack vectors can give an organization false sense of security. Whether you work for a utility company or a third party that performs securi assessments, this chapter will help you perform a comprehensive security assessment of utili companies.

Chapter 8: Securing the Utility Companies

In this chapter, you will learn how to build or mature information security programs tailored f utility companies. By taking a detailed look at standards and best practices such as the ISO 270 series and the ISF's Standard of Good Practice, you will understand the components necessary implement a functional and effective Information Security program. This chapter also contains t authors' top 12 technical security practices that should be implemented to help secure smart gr deployments. If you work for a utility company, then this chapter is for you!

Chapter 9: Third-Party Services

This chapter examines the trust relationship between utility companies and third parties. In th chapter, you will learn why relaxing security controls for partners can introduce significant risk your organization. This chapter explores the roles that third-party service providers can perform a how they can potentially be attacked. Additionally, this chapter discusses the risks that utili companies pose to third-party service providers. If the company you work for utilizes third parties partners with a utility company, then this chapter will help you secure your organization from gettin attacked through a trusted partner.

Chapter 10: Mobile Applications and Devices

In this chapter, the use of mobile applications and devices within the smart grid is analyzed. You wi learn how utility companies intend to utilize mobile devices and applications to help achieve the goa of the smart grid. This chapter details attacks against mobile devices and mobile applications designe to allow consumers and utility workers to interact with the smart grid. Finally, this chapter wi describe how to secure mobile devices, as well as mobile applications.

Chapter 11: Social Networking and the Smart Grid

This chapter discusses the integration of smart devices and social networking sites such as Faceboo and Twitter. You will learn the reasons why smart device manufacturers, as well as consumers, a excited about the merger of these two technologies. This chapter then discusses the threats associate with providing energy-consumption data to the masses, as well as includes the authors' Smart Gr Social Networking Security Check List. This check list aims to provide those who plan to utili social networking sites to capture and potentially distribute energy-consumption data, with a che list of controls to help secure their implementations.

Chapter 12: Attacking Smart Meters

In this chapter, you will learn how to systematically attack smart meters using one of two commo security-testing frameworks. First, you will learn how to utilize ISECOM's *Open Source Securi Testing Methodology Manual* (OSSTMM) to attack smart meters. This chapter includes discussion the tools used to attack smart meters, as well as provides resources for you to obtain and utilize t same tools. Following the OSSTMM review, you will learn how to similarly apply NIST's Speci Publication 800-42: Guideline on Network Security Testing to Attacking Smart Meters. This chapt will provide you with the information necessary to attack smart meters, as well as understand ho they may be attacked.

Chapter 13: Attacking Smart Devices

Where Chapter 12, “Attacking Smart Meters,” reviewed the testing methodologies that can be us when attacking smart meters, this chapter shows you how to actually attack a smart device. First, th chapter discusses the process of selecting a target smart device. Then, you will learn how to utili specific tools to perform network and application layer attacks against the selected smart device. Th review is performed utilizing the common security-testing frameworks previously covered in Chapt 12, “Attacking Smart Meters.” This chapter is technical and very hands on, so it is recommended th you read Chapter 12, “Attacking Smart Meters,” before reading this chapter.

Chapter 14: What's Next?

This chapter wraps up the book by preparing you for what is coming next with the smart grid. In th chapter, you will learn what to expect as a consumer, technology vendor, or utility company. Th chapter then discusses what to expect if you are a security professional who works with the smart gri as well as what some security professionals predict. Finally, this chapter describes how you can g involved in the smart grid community and stay current with the latest developments, as the smart gr becomes a reality.

Conclusion

Writing this book has been a rewarding experience for both of us, and we hope that you will enjoy This book reviews current and theoretical threats and attacks against today's smart grid and sma devices. As the smart grid evolves, so with these threats and weaknesses. However, the fundament controls that we discuss in this book should transcend and provide you with a solid foundation f securing today's and tomorrow's smart grid deployments.

Chapter 1

Smart Grid

What Is It?

Information in This Chapter

- A Brief History of Electrical Grids
- What Is Automatic Meter Reading (AMR)?
- Future Infrastructure
- What Is a Smart Grid?
- What Is AMI?
- International Initiatives
- Why Do We Need to Secure the Smart Grid?

Over the past several years, the promise of smart grids and their benefits has been widely publicized. Bringing updated technologi to power generation, transmission, and consumption, smart grids are touted to revolutionize our economy, environment, and nation security. Corporations large and small foresaw the emerging markets for smart grid technologies and rushed to be the first to deliv More often than not, security has taken a backseat to the rush to implement. This book will take a look at the potential consequenc of designing and implementing smart grid technologies without integrating security. We will also offer recommendations on how address these consequences so that the promise of smart grids can be fulfilled … securely.

A Brief History of Electrical Grids

Technologies related to electric grids have roots dating back to the late nineteenth century. Thoma Edison's, as shown in Figure 1.1, direct current (DC) and Nikola Tesla's, as shown in Figure 1. alternating current (AC) continue to be utilized to this day. Today, electricity is transmitted using AC while DC has special applications, usually within residential and commercial buildings.

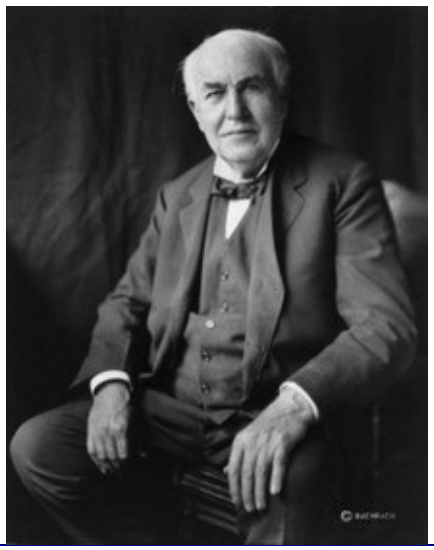

Figure 1.1 Thomas Edison.

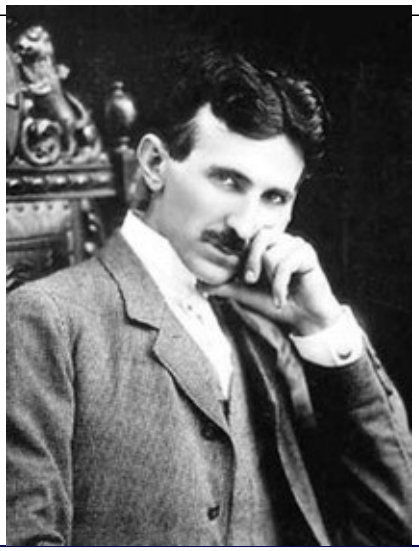

Figure 1.2 Nikola Tesla.

What Is an Electric Grid?

Electric grids perform three major functions: power generation, transmission, and distribution. Pow generation is the first step in delivering electricity and is performed at power station (coal, nuclea geothermal, hydro, and so on). Power transmission is the second step in delivering electricity ar involves the transfer of electricity from the power stations to power companies' distribution system Finally, power distribution completes the electric grids' functions by delivering power to consumer The major difference between power transmission and power distribution is that power transmissio utilizes infrastructure that can handle high voltage (110+ kV), whereas power distribution utiliz infrastructure that can handle medium (<50 kV) and low (<1 kV) voltage.

Grid Topologies

In its simplest form, an electric grid is a network. The use of the term "grid" can refer to a comple infrastructure that encompasses power generation, transmission, and distribution, or it can refer to subset of a larger infrastructure.

Distribution networks are less complicated than that of transmission networks, as transmissio networks are often interconnected with other regional transmission networks to provide great redundancy. At first glance, this interconnection appears to provide greater reliability in feedin distribution networks, but many factors come into play in ensuring continuous power to en consumers.

Transmission networks must effectively manage both power generation and consumption as power failure, or spike in consumption in one area may result in adverse affects in another area of th network. The United States established the North American Electric Reliability Corporation (NERC www.nerc.com) to ensure the reliability of the bulk power system in North America. This nonprof organization's area of responsibility includes the contiguous United States, Canada, and part of th Baja peninsula in Mexico.

There are two primary topologies in use in the United States for power distribution. The mo common topology is the radial grid, as shown in Figure 1.3. In a radial grid, electricity is distribute from a substation in a pattern that resembles a tree with many branches and leaves. As the electrici is carried across the power lines, its strength is reduced until it reaches its final destination. The oth

primary topology utilized for power distribution is mesh grid, as shown in Figure 1.4. Mesh gri provide greater reliability than radial grids because in a radial grid, each branch and leaf receiv power from a single source (the tree), whereas in a mesh grid, power can be provided through oth sources (other branches and leaves). Radial grids do provide limited redundancy, in that a secon substation in close proximity can feed into the grid, but this assumes that the secondary substation not suffering from the same condition as the primary.

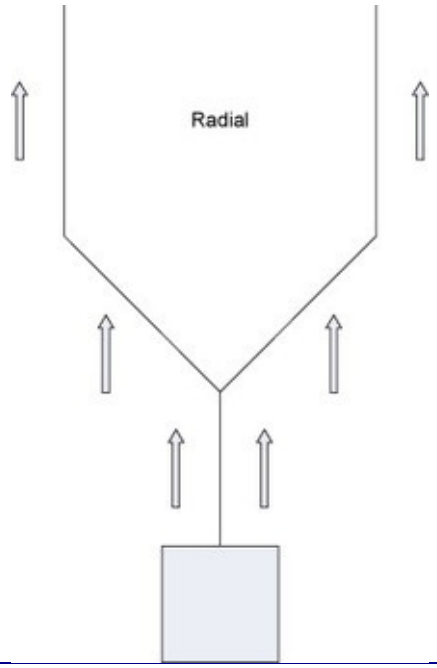

Figure 1.3 Radial grid.

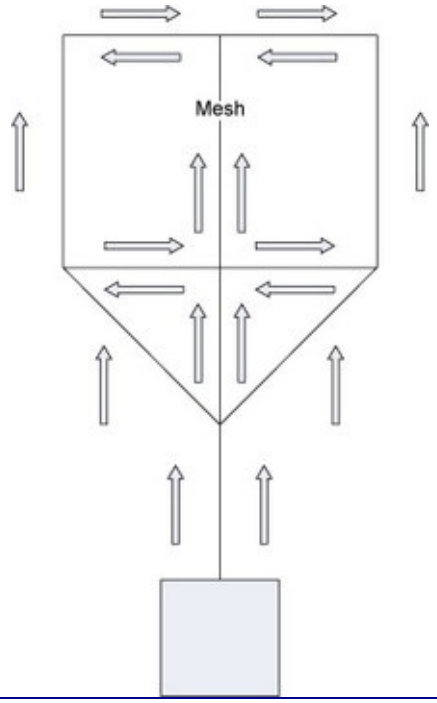

Figure 1.4 Mesh grid.

The looped topology, utilized primarily in Europe, is a mix between the radial and mesh topologie A looped topology, as shown in Figure 1.5, is much like a radial topology, except that each branch ar leaf has two separate paths from the substation. Where the radial topology is vulnerable to sing points of failure, the looped topology provides greater reliability. The goal of the looped topology is be able to withstand a disruption in the grid, regardless of where it may occur. Much like the mes

topology, the looped topology is costlier than the radial topology, as each end of the loop must me
the requirements for power and voltage drops.

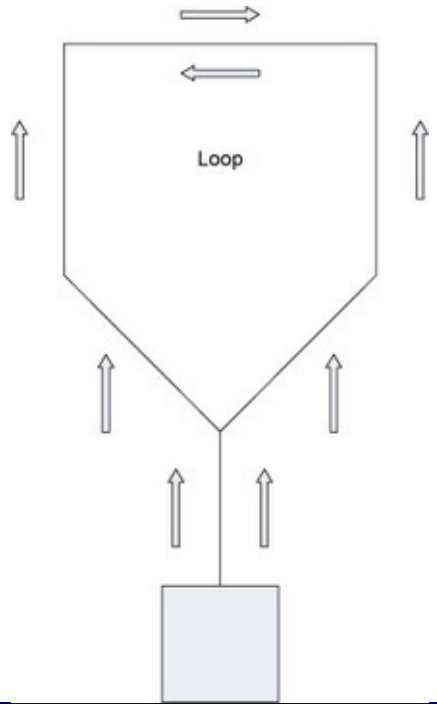

Figure 1.5 Loop topology.

Modernizing the Electric Grids

Currently, the electrical infrastructure in the United States is not up to the task of powering America future. According to Carol Browner, director of the White House Office of Energy and Clima Change, “We [the United States] have a very antiquated (electric grid) system in our country…Th current system is outdated, it's dilapidated.”[1] Across all three functions of an electrical gri significant improvements can be made to increase the reliability and efficiency of power generatio transmission, and distribution.

Deregulation is often touted as a means to modernizing today's electrical grids. Deregulatio encompasses moving from today's regulated landscape where often larger power companies a granted monopoly status and control power generation, transmission, and distribution for a geograph area to a deregulated landscape where the free markets would dictate all three functions of t electrical grids. In a deregulated landscape, power generation, transmission, and distribution could b handled by separate companies, all working to provide more efficient, reliable, and cost-effecti solutions.

Many other ideas exist to modernize today's electrical grids. The most prominent of which is t smart grid. Recent initiatives championed by the Obama Administration, including $3.4 billio awarded for projects such as smart meter implementations, grid infrastructure advancement, a manufacturing smart appliances[2] will soon be a reality.

What Is Automatic Meter Reading (AMR)?

Evolving from Tesla's design, the automatic meter reading (AMR) infrastructure introduce automation to the electric grid in 1977 (read more at www.metretekfl.com). Through a combination technologies, including wired and wireless networks, AMR's most significant advancement resulted electric companies being able to remotely read meters. Once AMR was implemented, the electr

companies could more easily obtain meter readings in near real time, and provide customers wi consumption-based bills. Previously, the electric companies relied on estimates when billi customers. With better, timelier information, electric companies were able to improve energ production through tighter control during peak and low demand periods.

AMR Technologies

To support the advancements of the AMR infrastructure, several technologies are utilized. For da collection, utility employees leverage handhelds and notebook computers. For data transport, wir and wireless networks are deployed to remotely read meter data.

Handhelds

Supporting utility employees' efforts to quickly and efficiently obtain meter readings, handhe devices, much like your common Personal Digital Assistant (PDA), as shown in Figure 1.6, a utilized. These devices read meter data in one of two ways. First, the electric worker can utili "touch" technology to read a meter by simply touching the meter with a probe. This probe stores t meter data to the handheld for later retrieval and processing. Second, the handheld device may inste be fitted with a wireless receiver that reads the data transmitted by the meter, again with the da stored for later retrieval and processing.

Figure 1.6 A wireless handheld device.

Notebook Computers

Utility employees also utilize traditional mobile computers in meter reading. Rather than physical visiting each meter, as with the handheld devices, a mobile computer can be installed inside of a electric worker's vehicle to wirelessly read meters. Usually these deployments involve a combinatio of technologies, including a wireless technology, software, and the necessary hardware (GP antennas, and so on).

Wireless Networks

For data transport, a broad range of wireless technologies are utilized by the electric companies read meter data. Radio Frequency (RF), Wi-Fi, Bluetooth, and even cellular technologies are current in use. A majority of AMR devices utilize RF wireless technologies, with narrow band, direc

sequence spread spectrum (DSSS), and frequency-hopping spread spectrum (FHSS) being the mo
common. Less common technologies such as Zigbee and Wavenis have found their way into AM
deployments. When wireless communications are utilized, device makers either license frequenci
from government agencies such as the Federal Communications Commission (FCC) or use unlicens
frequencies.

When Wi-Fi is chosen as the technology for remote data transport, traditionally the meters are n
themselves Wi-Fi enabled, rather a management station that they report to (through RF) utilizes Wi-
to communicate its aggregated data to the electric company. This is the deployment model utilized b
the city of Corpus Christi in Texas. In this deployment, the power meters mostly rely on the use
batteries and thus utilizing Wi-Fi was impractical because of its relatively high power consumptio
when compared with RF. The power consumption requirements of Wi-Fi technology remain a barri
to its inclusion in AMR deployments.

Power Line Communication (PLC)

Power line communication (PLC) provides a completely remote solution for reading meter data. Da
from meters is transmitted across the existing power line infrastructure to the local substation. Fro
the local substation, data is then transported to the electric companies for processing and analysi
This type of dedicated infrastructure from the meter to the electric company is commonly referred
as a “fixed” network.

Hybrid Models

Although some AMR deployments may rely on a single technology for each part of its deploymen
others utilize a hybrid model where multiple technologies are used. For example, data transport ma
primarily rely on PLC, but RF may be utilized if the PLC is unavailable. Other hybrid models ma
rely on RF to send data to aggregation points and then utilize PLC or Wi-Fi to transport data to th
electric company.

AMR Network Topologies

Utilizing one or a combination of the aforementioned technologies, electric companies create
network from which meter information is obtained. These networks take on one of several topologie
including the following:

- Star network – A star network topology is implemented when meters transmit data to a centr
location. This central location can be a repeater, which then forwards the data to the electr
companies, or it can simply act as data storage. A star network topology can utilize wirele
technologies, PLC, or both.
- Mesh network – A mesh network topology is implemented when the meters themselves bo
transmit and receive data from other meters. Meters act much like the repeaters in a star networ
and eventually data reaches the electric companies or a data storage device.

What Does It All Mean?

Looking at all of the parts that make up an AMR infrastructure, it is easy to see that security needs
be included from the design phase. With such a wide range of technologies possessing the ability
impact the confidentiality, availability, and integrity of data being transmitted across the AM
infrastructure, it is imperative to evaluate the security posture of each individual technology, as we

as its interactions with other technologies.

Future Infrastructure

As described in “A Brief History of Electrical Grids” section of this chapter, the current electric pow infrastructure was designed to utilize existing technology and handle the requirements defined duri the nineteenth and twentieth centuries. The increasing demands on an aging infrastructure can only l met by the fine-grain control and insight into consumer demand that the smart grid promises deliver.

Justifications for Smart Grids

The proposed smart grids seek to remediate these issues, as well as numerous others. The maj justifications for smart grids tend to fall into three categories: economic, environmental, a reliability. The United States Department of Energy (DOE) defines the goals of a smart grid a follows:

- Ensuring its reliability to degrees never before possible
- Maintaining its affordability
- Reinforcing our global competitiveness
- Fully accommodating renewable and traditional energy sources
- Potentially reducing our carbon footprint
- Introducing advancements and efficiencies yet to be envisioned.

Waste

Electricity must be consumed as soon as it is produced and consumers have grown accustom to the o demand availability of electricity. Currently, this combination requires utility companies to genera enough supply to meet the electrical demand at any given moment. Because the exact demand unknown, utility companies generate more electricity than is needed to compensate for the unexpect rise in consumption and achieve this level of service. This system of supply and demand results waste when demand is overestimated and rolling blackouts when demand is underestimated.

Reliability

In addition to waste, the reliability of the electric grid can be disrupted by numerous factor Specifically, a drop in voltage from a power supply can cause brownouts, whereas environment factors ranging from falling trees to thunderstorms and hurricanes can cause blackouts. Althoug these reliability problems tend to occur on a local scale, they can lead to more widespread proble that affect larger areas. Table 1.1 describes the different categories of power outages.

Table 1.1 Power outage categories[4]

Category	Description
Dropout	A loss of power that has a short duration, on a timescale of seconds, and is usually fixed quickly.
Brownout	The electrical power supply encounters a partial drop in voltage, or temporary reduction in electric power. In the case of three-phase electric power supply, when a phase is absent, at reduced voltage, or incorrectly phased.
Blackout	An affected area experiences a complete loss of electrical power, ranging from several hours to several weeks.
Load	An electric company either reduces or completely shuts off the available power to sections of the grid. Sometimes referr

shedding to as rolling brownouts and rolling blackouts.

Renewable Energy Sources

Traditional power generation relies on an inexhaustible supply of energy resources that has n negative effects on the world. In such a scenario, centralized power generation that relies on a endless supply of the traditional energy resources would excel. However, limited resources an concerns over environmental impact are driving the movement for clean and renewable energ sources, such as wind and solar. Unfortunately, these types of clean, renewable resources hav problems of their own including localization and continuity. For example, a solar power plant cou generate large amounts of electricity if located in Florida; however, the output would be negligible located in Antarctica. Additionally, current solar power plants all but cease to generate power durin the night or during severe weather such as thunderstorms and hurricanes, which would drive the nee for alternate sources of energy to meet demand. As a result, the current electric grid simply does n properly accommodate renewable energy sources.

What Is a Smart Grid?

A smart grid is not a single device, application, system, network, or even idea. There is no singl authoritative definition for the question: What is a smart grid? However, the definitions from th various authoritative organizations, such as DOE, NERC, and SmartGrids Technology Platfor (www.smartgrids.eu/), follow a common theme: Smart grids utilize communication technology an information to optimally transmit and distribute electricity from suppliers to consumers. Figure 1 illustrates the basic concepts of a smart grid. Additionally, smart grid is not a static concept. It wi continue to evolve as the existing technologies evolve and new technologies are developed. The typ configuration, and implementation of these technologies and the access to and transmission and use relevant information are of primary concern in securing smart grids and for this book.

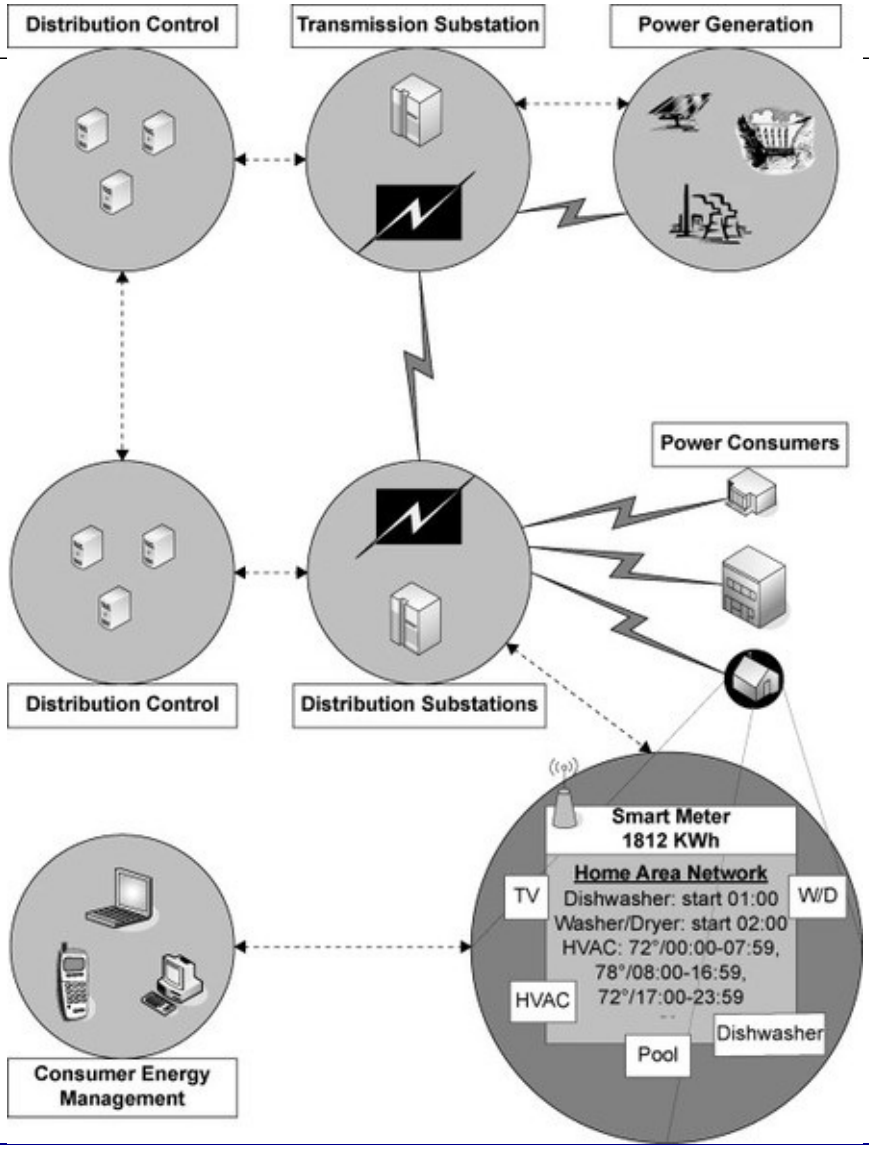

Figure 1.7 Basic smart grid diagram.

Components

To achieve the desired goals of reliable, efficient, and clean energy distribution, smart grids employ combination of different technologies. According to DOE, the following technologies are considere Key Technology Areas[3] :

- Integrated two-way communication
- Advanced components
- Advanced control methods
- Sensing and measurement technologies
- Improved interfaces and decision support
- Applications of smart grid technology.

Integrated Two-Way Communication

Two-way communication enables operators to monitor and interact with components of the smart gr in real time. This type of communication improves the operator's ability to manage grid operation For example, in the current grid, operators are unaware of blackouts until customers notify ther typically by way of telephone calls to a customer support center. In a smart grid, operators are able

detect and manage the problem without any notification from customers, resulting in faster proble resolution and decreased operational costs. In order to achieve this capability, the components smart grids require two-way communication abilities. Different smart grid implementations wi employ different technologies, but they will all require an underlying network for data transpo Current smart grids utilize the networking technologies that are also used in AMR deployments, previously discussed in the "AMR Network Topologies" section of this chapter.

Advanced Components

Advanced components include the areas of superconductivity, fault tolerance, excess electrici storage, smart devices, and diagnostics equipment. This technology actively determines the electric behavior of the grid.[3] For example, the excess electricity that is created during the day by solar pow plants could be stored in electrical storage devices and used during the night when the solar pow plant is unable to generate electricity. So-called smart devices can provide useful consumptio feedback to both the consumer and the energy providers to enable better energy managemer Although the above-mentioned list may appear to be a dispersed variety of technological devices, th Key Technology Area involves smart grid components that will provide unique advantages ov technology of the current grid.

Advanced Control Methods

Utilizing the two-way communication component described in the "Integrated Two-Wa Communication" section of this chapter, the advanced control methods allow operators (human machine) to manage the various smart grid components. Specifically, the advanced control metho enable advanced data collection, as well as diagnostics and appropriate maintenance. For example, operator could identify a problem with a component and apply a patch remotely, thus saving time a costs associated with sending crews to the location of the problem.

Sensing and Measurement Technologies

New sensing and measurement technologies support smart grid stability, health, and securi functionality. The most common of these technologies is the smart meter. Figure 1.8 displays current smart meter. A smart meter monitors usage statistics and reports the usage details to the utili company, consumers, and third-party service providers. Depending on the smart meter and supportin infrastructure, the smart meter can be used for other administrative functions, such as power outa notification and remotely disabling service.

Figure 1.8 Example smart meter.

Improved Interfaces and Decision Support