

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

---

Front Matter

# 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 • PARIS

• SAN DIEGO • SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO



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

© 2011 Elsevier Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website [www.elsevier.com/permissions](http://www.elsevier.com/permissions).

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

## 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 on 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 have 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 of 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. III. Title.

TK1025.F58 2011

---

**British Library Cataloguing-in-Publication Data**

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

For information on all Syngress publications visit our website at [www.syngress.com](http://www.syngress.com)

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

Working together to grow  
libraries in developing countries

[www.elsevier.com](http://www.elsevier.com) | [www.bookaid.org](http://www.bookaid.org) | [www.sabre.org](http://www.sabre.org)

ELSEVIER

BOOK AID  
International

Sabre Foundation

---

# Table of Contents

[Acknowledgments \(Tony Flick\)](#)  
[Acknowledgments \(Justin Morehouse\)](#)  
[About the Authors](#)  
[About the Technical Editor](#)  
[Introduction](#)  
[Chapter 1: Smart Grid](#)  
[Chapter 2: Threats and Impacts](#)  
[Chapter 3: Threats and Impacts](#)  
[Chapter 4: Federal Effort to Secure Smart Grids](#)  
[Chapter 5: State and Local Security Initiatives](#)  
[Chapter 6: Public and Private Companies](#)  
[Chapter 7: Attacking the Utility Companies](#)  
[Chapter 8: Securing the Utility Companies](#)  
[Chapter 9: Third-Party Services](#)  
[Chapter 10: Mobile Applications and Devices](#)  
[Chapter 11: Social Networking and the Smart Grid](#)  
[Chapter 12: Attacking Smart Meters](#)  
[Chapter 13: Attacking Smart Devices](#)  
[Chapter 14: What's Next?](#)  
[Index](#)

---

## Acknowledgments (Tony Flick)

I want to thank my parents for pushing me into the computer science field, buying many computers along the way, and not getting too angry when I would secure their new computer by breaking it. After all, I was only following in my Dad's footsteps after he secured the dustbuster. My dad taught me many things in life and worked hard to give me a good life. From working midnight shifts to keep the streets safe and still finding the time to coach the teams I played on, I can only hope to be half the dad that you were to me someday. Although not the most conventional method, playing cards (euchre and poker were the best) with your collection of pennies, nickels, and dimes at the age of three made math classes enjoyable and easy throughout life. The other parents and teachers often asked me if my parents used flash cards or hired tutors to improve my math skills. I would just think back to the fun I had playing cards, while subconsciously learning the fundamentals of math. Mom, I know you were a little worried when you came home one day and heard me yell, "hit me!" during a poker game at the 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 only display green characters on the monitor. Playing video games and learning how to initially type with you on that old computer only grew my fascination with electronics, which drove me to the field of computer science and eventually security. I also want to thank you for working hard to give me a better life. I know it was not always easy, but I am eternally grateful for the opportunities you gave me in life.

My brother Matt, thank you for helping significantly with the application security portions of this book, letting me bounce ideas off of you, and providing a ton of great ideas that were used in the book. I am thankful that you always took the time out of your busy schedule to help me with homework and 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 teaching me how to write professionally. Even though I was playing video games with your future husband while you reviewed those reports, I did actually pay attention to your comments and learned from your gentle editing jokes. Hopefully, you can read this book to Brooke and Samantha; it is good to teach security at a young age.

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

Thank you Rachel Roumeliotis and Matthew Cater at Syngress for giving us the opportunity to write this book and guiding us along this journey. Christophe Veltsos, thank you for providing advice and suggestions that greatly enhanced the content of this book. Finally, thank you to my coauthor 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 understanding she showed me throughout the writing process. Without her, much of what I have accomplished and the person I have become today simply would not be. I am grateful to my parents, John and Susan, for always supporting me in whatever endeavors I pursue and teaching me that I am capable of almost anything if I put my mind to it.

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

Thank you to Rachel Roumeliotis, Matthew Cater, and Christophe Veltsos for the support and 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 emails. Finally, thank you to my coauthor, Tony Flick, for battling through these last couple of months 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 and is currently a principal with FYRM Associates. Tony's background is in network and application security, assessments, compliance, and emerging technologies. In the energy industry, Tony has performed network and application penetration testing, written and reviewed security policies and procedures, and provided guidance for utility companies and related technology vendors. He graduated from the University of Maryland, College Park, with a Bachelor of Science in Computer Science and a Bachelor of Science in Mathematics. Tony has spoken at Black Hat, DEF CON, ShmooCon, ISSA, and OWASP meetings on Smart Grid and application security concepts. Additionally, Tony has been recognized as a security subject matter expert and utilized by numerous media outlets including the Associated Press (AP), SC magazine, Dark Reading, and eWeek.

**Justin Morehouse** (CISSP, CISM, MCSE) has been working in the information security field for over eight years, primarily focusing on the areas of attack and penetration. He has performed over 200 security assessments for Fortune 1000 companies and Federal government agencies and is currently the assessment lead at one of the nation's largest retailers. Justin has developed numerous tools 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 George 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 Information Systems & Technology at Minnesota State University, Mankato, where he regularly teaches Information Security and Information Warfare classes. Christophe has presented at the local, regional, and national level, including at major security conferences like RSA.

Beyond the classroom, Christophe is also very active in the security community, engaging with community groups and business leaders as well as IT and security professionals. In 2007, he was elected president of the Mankato chapter of the Information Systems Security Association (ISSA). In 2008, he made numerous contributions to the SANS NewsBites newsletter as an advisory board member. In 2009, he joined and has contributed to the work of the privacy subgroup of the NIST Smart Grid Interoperability Panel Cyber Security Working Group (SGIP-CSWG), formerly known as 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 many information security and privacy related organizations including ISSA, ISACA, (ISC)<sup>2</sup>, and IAP. Both faculty and practitioner, Christophe maintains the [DrInfoSec.com](http://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 smart grid. By examining components of the smart grid in detail, you will obtain a strong understanding of how the confidentiality, integrity, and availability of these components can be both compromised and secured.

Discussing both the smart grid's strengths and weaknesses will help you understand threats and attacks, and hopefully prevent insecure deployments of smart grid technologies. In this book, you will also learn controls that will allow consumers, device manufacturers, and utility companies to minimize the risk associated with the smart grid. Each chapter aims to provide you with information 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 and application security of smart grid deployments. It will also provide value to those who are tasked with auditing smart grid deployments, as well as consumers utilizing smart grid devices. System engineers, application developers, and system integrators will find value in learning the strengths and 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 by implementing smart grid technologies, as both a provider of these technologies, as well as a consumer. This book will reinforce the value of funding and supporting security initiatives that help protect 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 nature of the subject matter, it is highly recommended that you read this book starting with [Chapter 1](#), “Smart Grid: What is it?” and finishing with [Chapter 14](#), “What's Next?” Later chapters reference material from previous chapters, building on the concepts, attacks, threats, and technologies already 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 to automatic meter reading (AMR). This chapter also discusses the infrastructure that will comprise the

smart grid, including automatic metering infrastructure (AMI). Finally, you will learn about 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 may affect consumers. One of the major goals of the smart grid is to provide more information to consumers, so that they can make informed decisions regarding their energy consumption. By providing information on the threats that consumers will face, readers will learn why they should seek 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 devastating 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 applies them specifically to utility companies and other organizations. This chapter discusses the threats and 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 that organizations manage risk and the potential impact of successful attacks. The threats and impacts discussed in this chapter are based in reality and are often overlooked when discussing the benefits of the smart grid. This chapter does not aim to spread fear, uncertainty, and doubt, but rather bring to light the potential impact of smart grid deployments so that protective measures can be implemented 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 a result, these governments are funding initiatives and enacting laws to ensure security is considered in smart grids. This chapter explains to readers the different roles that Federal agencies are performing and discusses the different smart grid security standards, guidelines, and best practices being developed by Federal agencies. This chapter also informs the readers of how the Federal government 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 to [Chapter 4](#), “Federal Effort to Secure Smart Grids,” this chapter discusses how government agencies are impacting the security of smart grids. Additionally, this chapter examines how the judicial system may use the massive amount of information that is collected in the smart grid. Finally, this chapter discusses the role that state and local agencies will need to perform to educate consumers on how to 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, this chapter discusses industry plans for self-policing, such as NERC's Critical Infrastructure Protection standards. Second, you will learn how compliance with such regulations does not equate to securing

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

---

## **Chapter 7: Attacking the Utility Companies**

---

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

## **Chapter 8: Securing the Utility Companies**

---

In this chapter, you will learn how to build or mature information security programs tailored for utility companies. By taking a detailed look at standards and best practices such as the ISO 27000 series and the ISF's Standard of Good Practice, you will understand the components necessary to implement a functional and effective Information Security program. This chapter also contains the authors' top 12 technical security practices that should be implemented to help secure smart grid 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 this chapter, you will learn why relaxing security controls for partners can introduce significant risk to your organization. This chapter explores the roles that third-party service providers can perform and how they can potentially be attacked. Additionally, this chapter discusses the risks that utility companies pose to third-party service providers. If the company you work for utilizes third-party partners with a utility company, then this chapter will help you secure your organization from getting 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 will learn how utility companies intend to utilize mobile devices and applications to help achieve the goals of the smart grid. This chapter details attacks against mobile devices and mobile applications designed to allow consumers and utility workers to interact with the smart grid. Finally, this chapter will 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 Facebook and Twitter. You will learn the reasons why smart device manufacturers, as well as consumers, are excited about the merger of these two technologies. This chapter then discusses the threats associated with providing energy-consumption data to the masses, as well as includes the authors' Smart Grid Social Networking Security Check List. This check list aims to provide those who plan to utilize social networking sites to capture and potentially distribute energy-consumption data, with a checklist 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 common security-testing frameworks. First, you will learn how to utilize ISECOM's *Open Source Security Testing Methodology Manual* (OSSTMM) to attack smart meters. This chapter includes discussion of the tools used to attack smart meters, as well as provides resources for you to obtain and utilize the same tools. Following the OSSTMM review, you will learn how to similarly apply NIST's Special Publication 800-42: Guideline on Network Security Testing to Attacking Smart Meters. This chapter will provide you with the information necessary to attack smart meters, as well as understand how they may be attacked.

## Chapter 13: Attacking Smart Devices

---

Where [Chapter 12](#), “Attacking Smart Meters,” reviewed the testing methodologies that can be used when attacking smart meters, this chapter shows you how to actually attack a smart device. First, the chapter discusses the process of selecting a target smart device. Then, you will learn how to utilize specific tools to perform network and application layer attacks against the selected smart device. The review is performed utilizing the common security-testing frameworks previously covered in [Chapter 12](#), “Attacking Smart Meters.” This chapter is technical and very hands on, so it is recommended that 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 this chapter, you will learn what to expect as a consumer, technology vendor, or utility company. The chapter then discusses what to expect if you are a security professional who works with the smart grid, as well as what some security professionals predict. Finally, this chapter describes how you can get involved in the smart grid community and stay current with the latest developments, as the smart grid becomes a reality.

## Conclusion

---

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

## Smart Grid

### What Is It?

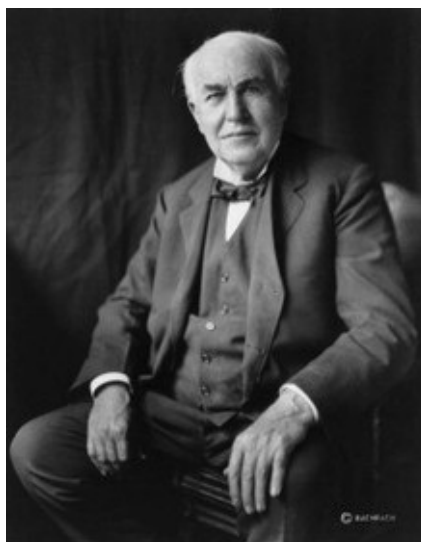
#### Information in This Chapter

- 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 technology to power generation, transmission, and consumption, smart grids are touted to revolutionize our economy, environment, and national security. Corporations large and small foresaw the emerging markets for smart grid technologies and rushed to be the first to deliver. More often than not, security has taken a backseat to the rush to implement. This book will take a look at the potential consequences of designing and implementing smart grid technologies without integrating security. We will also offer recommendations on how to 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. Thomas Edison's, as shown in [Figure 1.1](#), direct current (DC) and Nikola Tesla's, as shown in [Figure 1.2](#), 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. Power generation is the first step in delivering electricity and is performed at power station (coal, nuclear, geothermal, hydro, and so on). Power transmission is the second step in delivering electricity and involves the transfer of electricity from the power stations to power companies' distribution systems. Finally, power distribution completes the electric grids' functions by delivering power to consumers. The major difference between power transmission and power distribution is that power transmission utilizes infrastructure that can handle high voltage (110+ kV), whereas power distribution utilizes 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 complete infrastructure that encompasses power generation, transmission, and distribution, or it can refer to a subset of a larger infrastructure.

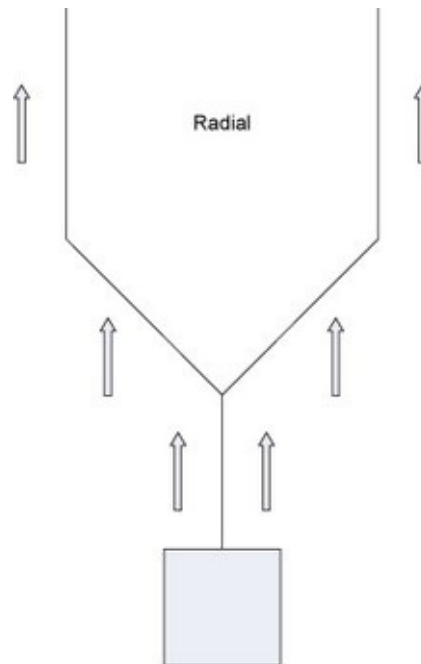
Distribution networks are less complicated than that of transmission networks, as transmission networks are often interconnected with other regional transmission networks to provide greater redundancy. At first glance, this interconnection appears to provide greater reliability in feeding distribution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

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

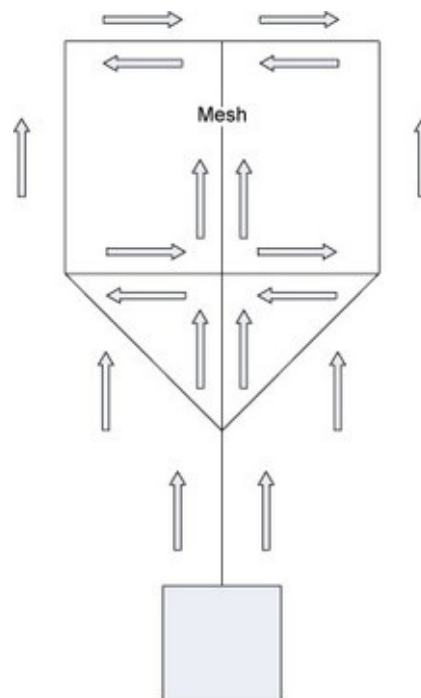
There are two primary topologies in use in the United States for power distribution. The most common topology is the radial grid, as shown in [Figure 1.3](#). In a radial grid, electricity is distributed from a substation in a pattern that resembles a tree with many branches and leaves. As the electricity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



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



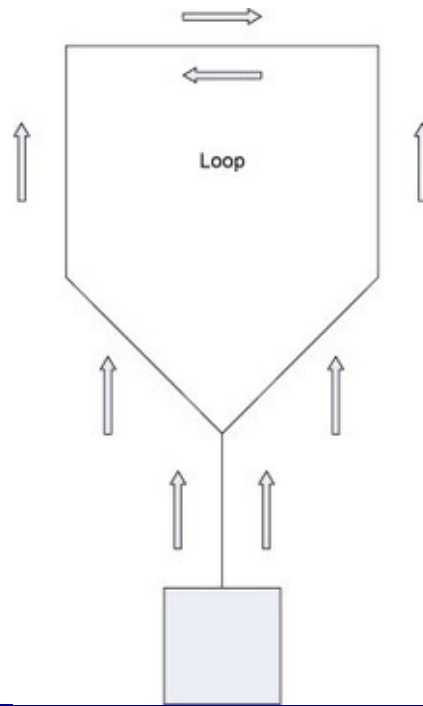
**Figure 1.3** Radial grid.



**Figure 1.4** Mesh grid.

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

topology, the looped topology is costlier than the radial topology, as each end of the loop must meet 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's future. According to Carol Browner, director of the White House Office of Energy and Climate Change, "We [the United States] have a very antiquated (electric grid) system in our country...The current system is outdated, it's dilapidated."<sup>1</sup> Across all three functions of an electrical grid—power generation, transmission, and distribution—significant improvements can be made to increase the reliability and efficiency of power generation, transmission, and distribution.

Deregulation is often touted as a means to modernizing today's electrical grids. Deregulation encompasses moving from today's regulated landscape where often larger power companies are granted monopoly status and control power generation, transmission, and distribution for a geographic area to a deregulated landscape where the free markets would dictate all three functions of the electrical grids. In a deregulated landscape, power generation, transmission, and distribution could be handled by separate companies, all working to provide more efficient, reliable, and cost-effective solutions.

Many other ideas exist to modernize today's electrical grids. The most prominent of which is the smart grid. Recent initiatives championed by the Obama Administration, including \$3.4 billion awarded for projects such as smart meter implementations, grid infrastructure advancement, and manufacturing smart appliances<sup>2</sup> will soon be a reality.

## What Is Automatic Meter Reading (AMR)?

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

companies could more easily obtain meter readings in near real time, and provide customers with consumption-based bills. Previously, the electric companies relied on estimates when billing customers. With better, timelier information, electric companies were able to improve energy 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 data collection, utility employees leverage handhelds and notebook computers. For data transport, wired and wireless networks are deployed to remotely read meter data.

### Handhelds

Supporting utility employees' efforts to quickly and efficiently obtain meter readings, handheld devices, much like your common Personal Digital Assistant (PDA), as shown in [Figure 1.6](#), are utilized. These devices read meter data in one of two ways. First, the electric worker can utilize "touch" technology to read a meter by simply touching the meter with a probe. This probe stores the meter data to the handheld for later retrieval and processing. Second, the handheld device may instead be fitted with a wireless receiver that reads the data transmitted by the meter, again with the data 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 physically visiting each meter, as with the handheld devices, a mobile computer can be installed inside of an electric worker's vehicle to wirelessly read meters. Usually these deployments involve a combination of technologies, including a wireless technology, software, and the necessary hardware (GPS antennas, and so on).

### Wireless Networks

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

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

When Wi-Fi is chosen as the technology for remote data transport, traditionally the meters are not themselves Wi-Fi enabled, rather a management station that they report to (through RF) utilizes Wi-Fi to communicate its aggregated data to the electric company. This is the deployment model utilized by the city of Corpus Christi in Texas. In this deployment, the power meters mostly rely on the use of batteries and thus utilizing Wi-Fi was impractical because of its relatively high power consumption when compared with RF. The power consumption requirements of Wi-Fi technology remain a barrier to its inclusion in AMR deployments.

## Power Line Communication (PLC)

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

## Hybrid Models

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

## AMR Network Topologies

---

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

- **Star network** – A star network topology is implemented when meters transmit data to a central location. This central location can be a repeater, which then forwards the data to the electric companies, or it can simply act as data storage. A star network topology can utilize wireless technologies, PLC, or both.
- **Mesh network** – A mesh network topology is implemented when the meters themselves both transmit and receive data from other meters. Meters act much like the repeaters in a star network 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 to be included from the design phase. With such a wide range of technologies possessing the ability to impact the confidentiality, availability, and integrity of data being transmitted across the AMR infrastructure, it is imperative to evaluate the security posture of each individual technology, as well

as its interactions with other technologies.

## Future Infrastructure

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

## Justifications for Smart Grids

The proposed smart grids seek to remediate these issues, as well as numerous others. The major justifications for smart grids tend to fall into three categories: economic, environmental, and reliability. The United States Department of Energy (DOE) defines the goals of a smart grid as 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 accustomed to the on-demand availability of electricity. Currently, this combination requires utility companies to generate enough supply to meet the electrical demand at any given moment. Because the exact demand is unknown, utility companies generate more electricity than is needed to compensate for the unexpected rise in consumption and achieve this level of service. This system of supply and demand results in 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 factors. Specifically, a drop in voltage from a power supply can cause brownouts, whereas environmental factors ranging from falling trees to thunderstorms and hurricanes can cause blackouts. Although these reliability problems tend to occur on a local scale, they can lead to more widespread problems that affect larger areas. [Table 1.1](#) describes the different categories of power outages.

**Table 1.1** Power outage categories<sup>4</sup>

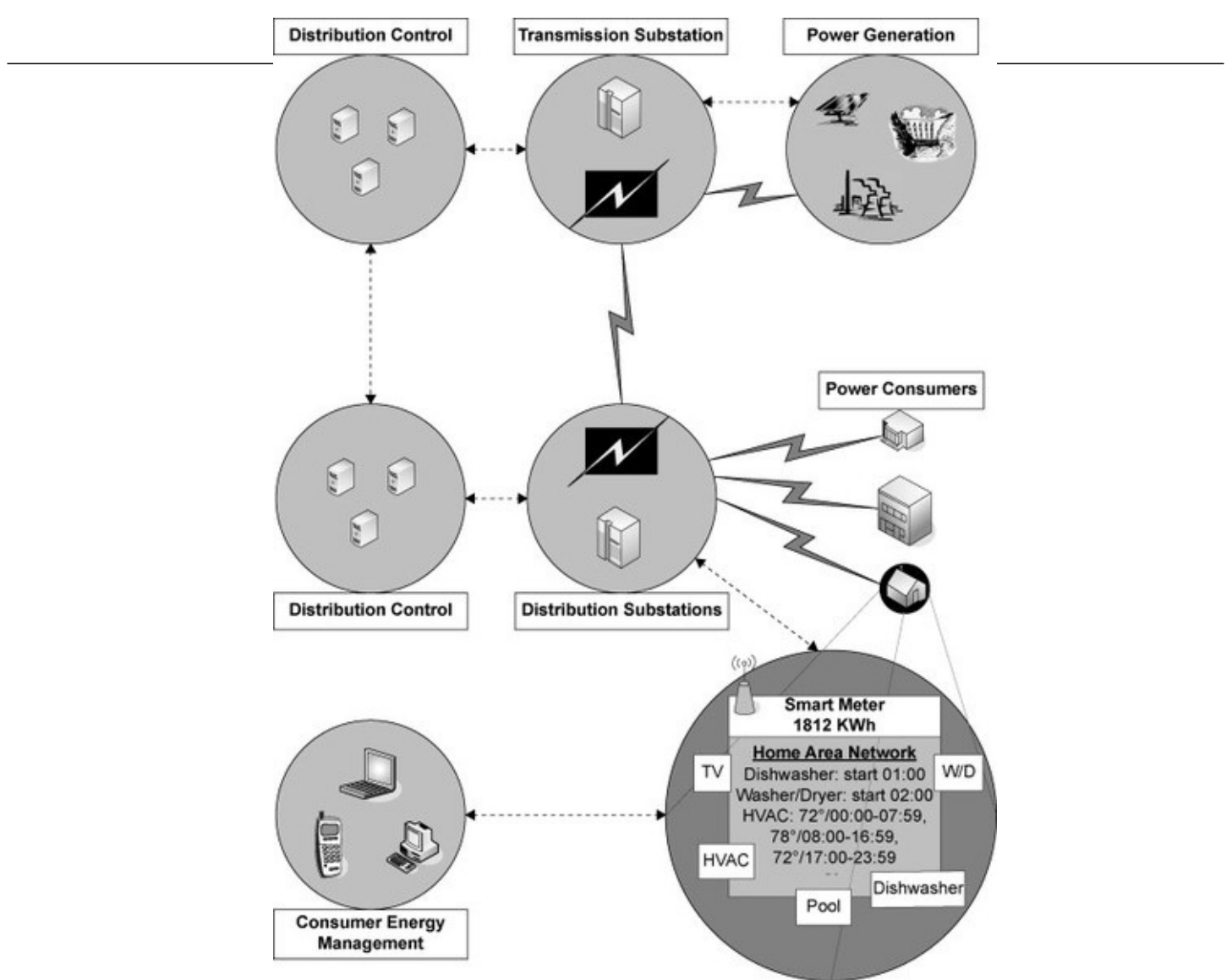
Category	Description
Dropout	A loss of power that has a short duration, on a timescale of seconds, and is usually fixed quickly.
Brownout	The electrical power supply encounters a partial drop in voltage, or temporary reduction in electric power. In the case of a three-phase electric power supply, when 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 referred to as a load shedding.

## Renewable Energy Sources

Traditional power generation relies on an inexhaustible supply of energy resources that has negative effects on the world. In such a scenario, centralized power generation that relies on an endless supply of the traditional energy resources would excel. However, limited resources and concerns over environmental impact are driving the movement for clean and renewable energy sources, such as wind and solar. Unfortunately, these types of clean, renewable resources have problems of their own including localization and continuity. For example, a solar power plant could generate large amounts of electricity if located in Florida; however, the output would be negligible if located in Antarctica. Additionally, current solar power plants all but cease to generate power during the night or during severe weather such as thunderstorms and hurricanes, which would drive the need for alternate sources of energy to meet demand. As a result, the current electric grid simply does not 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 single authoritative definition for the question: What is a smart grid? However, the definitions from the various authoritative organizations, such as DOE, NERC, and SmartGrids Technology Platform ([www.smartgrids.eu/](http://www.smartgrids.eu/)), follow a common theme: Smart grids utilize communication technology and 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 will continue to evolve as the existing technologies evolve and new technologies are developed. The types of configuration, and implementation of these technologies and the access to and transmission and use of 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 a combination of different technologies. According to DOE, the following technologies are considered Key Technology Areas<sup>3</sup> :

- 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 grid in real time. This type of communication improves the operator's ability to manage grid operations. For example, in the current grid, operators are unaware of blackouts until customers notify them, 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 problem resolution and decreased operational costs. In order to achieve this capability, the components of smart grids require two-way communication abilities. Different smart grid implementations will employ different technologies, but they will all require an underlying network for data transport. Current smart grids utilize the networking technologies that are also used in AMR deployments, as previously discussed in the “AMR Network Topologies” section of this chapter.

## Advanced Components

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

## Advanced Control Methods

Utilizing the two-way communication component described in the “Integrated Two-Way Communication” section of this chapter, the advanced control methods allow operators (human or machine) to manage the various smart grid components. Specifically, the advanced control methods enable advanced data collection, as well as diagnostics and appropriate maintenance. For example, an operator could identify a problem with a component and apply a patch remotely, thus saving time and 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 security functionality. The most common of these technologies is the smart meter. [Figure 1.8](#) displays an example of a current smart meter. A smart meter monitors usage statistics and reports the usage details to the utility company, consumers, and third-party service providers. Depending on the smart meter and supporting infrastructure, the smart meter can be used for other administrative functions, such as power outage notification and remotely disabling service.



**Figure 1.8** Example smart meter.

## Improved Interfaces and Decision Support



- [Hiroshima Notes here](#)
- [download online The Masked Monkey \(The Hardy Boys, Book 51\)](#)
- [download online Birth of an Industry: Blackface Minstrelsy and the Rise of American Animation pdf](#)
- [The 3-Day Solution Plan: Jump-start Lasting Weight Loss by Turning Off the Drive to Overeat: Lose Up to 6 Pounds in 3 Days! online](#)
- [download online Hotlanta \(Hotlanta, Book 1\) pdf, azw \(kindle\), epub](#)
- [Hitler's Charisma: Leading Millions into the Abyss \(The Dark Charisma of Adolf Hitler\) online](#)
  
- <http://wind-in-herleshausen.de/?freebooks/Hiroshima-Notes.pdf>
- <http://transtrade.cz/?ebooks/Herr-Arnes-penningar-Liljecronas-hem-K--rkarlen.pdf>
- <http://dadhoc.com/lib/Birth-of-an-Industry--Blackface-Minstrelsy-and-the-Rise-of-American-Animation.pdf>
- <http://nexson.arzamaszev.com/library/Snip--Burn--Solder--Shred--Seriously-Geeky-Stuff-to-Make-with-Your-Kids.pdf>
- <http://growingsomeroots.com/ebooks/Hotlanta--Hotlanta--Book-1-.pdf>
- <http://cambridgebrass.com/?freebooks/Lonely-Planet-Italy--11th-Edition---Travel-Guide-.pdf>