

Anurag K. Srivastava • Venkatesh Venkataramanan
Carl Hauser

Cyber Infrastructure for the Smart Electric Grid




IEEE PRESS

WILEY

Cyber Infrastructure for the Smart Electric Grid

Cyber Infrastructure for the Smart Electric Grid

Anurag K. Srivastava

West Virginia University, Morgantown, WV, USA

Venkatesh Venkataramanan

National Renewable Energy Laboratory, Golden, CO, USA

Carl Hauser

Washington State University, Pullman, WA, USA

WILEY


IEEE PRESS

This edition first published 2023

© 2023 John Wiley & Sons Ltd

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, except as permitted by law. Advice on how to obtain permission to reuse material from this title is available at <http://www.wiley.com/go/permissions>.

The right of Anurag K. Srivastava, Venkatesh Venkataramanan, and Carl Hauser to be identified as the authors of this work has been asserted in accordance with law.

Registered Office(s)

John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA

John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

Editorial Office

The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, UK

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

Limit of Liability/Disclaimer of Warranty

In view of ongoing research, equipment modifications, changes in governmental regulations, and the constant flow of information relating to the use of experimental reagents, equipment, and devices, the reader is urged to review and evaluate the information provided in the package insert or instructions for each chemical, piece of equipment, reagent, or device for, among other things, any changes in the instructions or indication of usage and for added warnings and precautions. While the publisher and authors have used their best efforts in preparing this work, they make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives, written sales materials or promotional statements for this work. The fact that an organization, website, or product is referred to in this work as a citation and/or potential source of further information does not mean that the publisher and authors endorse the information or services the organization, website, or product may provide or recommendations it may make. This work is sold with the understanding that the publisher is not engaged in rendering professional services. The advice and strategies contained herein may not be suitable for your situation. You should consult with a specialist where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor authors shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

Library of Congress Cataloging-in-Publication Data applied for

Hardback ISBN: 9781119460756

Cover Design: Wiley

Cover Image: © metamorworks/Shutterstock

Set in 9.5/12.5pt STIXTwoText by Straive, Chennai, India

Contents

About the Authors	<i>xi</i>
Acknowledgments	<i>xiii</i>
Acronyms	<i>xv</i>

1	Introduction to the Smart Grid	<i>1</i>
1.1	Overview of the Electric Power Grid	<i>1</i>
1.1.1	Power Grid Operation	<i>6</i>
1.2	What Can Go Wrong in Power Grid Operation	<i>8</i>
1.3	Learning from Past Events	<i>9</i>
1.4	Toward a Smarter Electric Grid	<i>12</i>
1.5	Summary	<i>13</i>
1.6	Problems	<i>13</i>
1.7	Questions	<i>14</i>
	Further Reading	<i>15</i>
2	Sense, Communicate, Compute, and Control in a Secure Way	<i>17</i>
2.1	Sensing in Smart Grid	<i>18</i>
2.1.1	Phase Measurement Unit (PMU)	<i>19</i>
2.1.1.1	Why Do We Need PMUs?	<i>19</i>
2.1.1.2	Estimation of Phasors	<i>21</i>
2.1.1.3	Phasor Calculation	<i>22</i>
2.1.1.4	Time Signal for Synchronization	<i>22</i>
2.1.1.5	PMU Data Packets	<i>23</i>
2.1.1.6	PMU Applications	<i>23</i>
2.1.2	Smart Meters	<i>24</i>
2.1.2.1	Communication Systems for Smart Meters	<i>25</i>
2.2	Communication Infrastructure in Smart Grid	<i>26</i>

2.3	Computational Infrastructure and Control Requirements in Smart Grid	26
2.3.1	Control Center Applications	28
2.4	Cybersecurity in Smart Grid	30
2.4.1	Methods to Provide Cybersecurity for Smart Grids	31
2.5	Summary	31
2.6	Problems	31
2.7	Questions	33
	Further Reading	33
3	Smart Grid Operational Structure and Standards	35
3.1	Organization to Ensure System Reliability	37
3.1.1	Regional Entities	38
3.2	Smart Grid Standards and Interoperability	39
3.3	Operational Structure in the Rest of the World	40
3.4	Summary	41
3.5	Problems	41
3.6	Questions	42
	Further Reading	42
4	Communication Performance and Factors that Affect It	45
4.1	Introduction	45
4.2	Propagation Delay	47
4.3	Transmission Delay	47
4.4	Queuing Delay and Jitter	49
4.5	Processing Delay	51
4.6	Delay in Multi-hop Networks	51
4.7	Data Loss and Corruption	52
4.8	Summary	53
4.9	Exercises	53
4.10	Questions	56
	Further Reading	56
5	Layered Communication Model	57
5.1	Introduction	57
5.1.1	OSI and TCP/IP Models	59
5.2	Physical Layer	60
5.3	Link Layer: Service Models	61
5.3.1	Ethernet	62
5.3.1.1	Link Virtualization	63

5.4	Network Layer: Addressing and Routing	64
5.4.1	IP Addressing	66
5.4.2	Routing	68
5.4.3	Broadcast and Multicast	68
5.5	Transport Layer: Datagram and Stream Protocols	70
5.5.1	UDP	72
5.5.2	TCP	73
5.6	Application Layer	75
5.7	Glue Protocols: ARP and DNS	76
5.7.1	DNS	77
5.8	Comparison Between OST and TCP/IP Models	78
5.9	Summary	78
5.10	Problems	79
5.11	Questions	80
	Further Reading	80
6	Power System Application Layer Protocols	81
6.1	Introduction	81
6.2	SCADA Protocols	82
6.2.1	DNP3 Protocol	83
6.2.2	IEC 61850	86
6.3	ICCP	87
6.4	C37.118	87
6.5	Smart Metering and Distributed Energy Resources	89
6.5.1	Smart Metering	89
6.5.2	Distributed Energy Resources (DERs)	91
6.6	Time Synchronization	92
6.7	Summary	92
6.8	Problems	93
6.9	Questions	94
	Further Reading	94
7	Utility IT Infrastructures for Control Center and Fault-Tolerant Computing	95
7.1	Conventional Control Centers	95
7.2	Modern Control Centers	97
7.3	Future Control Centers	98
7.4	UML, XML, RDF, and CIM	99
7.4.1	UML	100
7.4.2	XML and RDF	102

- 7.4.3 CIM (IEC 6170) 103
- 7.4.4 IEC 61850 103
- 7.5 Basics of Fault-Tolerant Computing 105
- 7.6 Cloud Computing 107
- 7.7 Summary 109
- 7.8 Problems 110
- 7.9 Questions 111
- Further Reading 111

8 Basic Security Concepts, Cryptographic Protocols, and Access Control 113

- 8.1 Introduction 113
- 8.2 Basic Cybersecurity Concepts and Threats to Power Systems 113
 - 8.2.1 Threats, Vulnerabilities, and Risks, What Is the Difference? 113
 - 8.2.2 Threats 114
 - 8.2.3 Vulnerabilities 114
 - 8.2.4 Risk 115
- 8.3 CIA Triad and Other Core Security Properties 116
 - 8.3.1 Privacy and Consumer Data 117
 - 8.3.2 Encryption and Authentication 117
 - 8.3.2.1 Kerckhoffs's versus Kirchoff's Law (Fundamental Cryptographic Principles and Threats) 118
 - 8.3.2.2 Symmetric Key Encryption 120
 - 8.3.2.3 Asymmetric Key 121
- 8.4 Introduction to Encryption and Authentication 123
 - 8.4.1 Message Authentication Codes (MACs) 123
 - 8.4.2 Digital Signatures 124
 - 8.4.3 Certificates 125
- 8.5 Cryptography in Power Systems 127
 - 8.5.1 IEC 62351 128
 - 8.5.2 DNP3 Secure Authentication (SA) 129
- 8.6 Access Control 131
 - 8.6.1 RBAC in IEC 62351 131
- 8.7 Summary 133
- 8.8 Problems 133
- 8.9 Questions 134
- Further Reading 134

9 Network Attacks and Protection 135

- 9.1 Attacks to Network Communications 135
 - 9.1.1 Denial-of-Service (DoS) Attack 135

9.1.1.1	Flooding	136
9.1.1.2	Malformed Packet	137
9.1.1.3	Reflection	137
9.1.1.4	DDoS	138
9.1.2	Spoofing	138
9.1.2.1	ARP Spoofing	139
9.1.2.2	Other Spoofing	139
9.2	Mitigation Mechanisms Against Network Attacks	140
9.2.1	Network Protection Through Security Protocols	140
9.2.1.1	TLS	141
9.2.1.2	IPsec	143
9.3	Network Protection Through Firewalls	144
9.4	Intrusion Detection	145
9.4.1	Anomaly-Based Detection	147
9.4.2	Signature-Based Detection	147
9.5	Summary	148
9.6	Problems	149
9.7	Questions	150
	Further Reading	150
10	Vulnerabilities and Risk Management	151
10.1	System Vulnerabilities	151
10.1.1	Software Vulnerabilities	152
10.1.2	Hardware and Side-Channel Vulnerabilities	155
10.1.3	Social Engineering	155
10.1.4	Malware	156
10.1.5	Supply Chain	158
10.2	Security Mechanisms: Access Control and Malware Detection	159
10.2.1	Access Control	159
10.2.2	Malware Detection	160
10.3	Assurance and Evaluation	161
10.3.1	Port Scanning	161
10.3.2	Network Monitoring	162
10.3.3	Network Policy Analysis	163
10.3.4	Vulnerability Scanning	163
10.3.5	Continuous Monitoring	163
10.3.6	Security Assessment Concerns	165
10.3.7	Software Testing	165
10.3.8	Evaluation	166
10.4	Compliance: Industrial Practice to Implement NERC CIP	167
10.5	Summary	167

10.6	Problems	167
10.7	Questions	168
	Further Reading	169
11	Smart Grid Case Studies	171
11.1	Smart Grid Demonstration Projects	171
11.2	Smart Grid Metrics	173
11.3	Smart Grid Challenges: Attack Case Studies	174
11.3.1	Stuxnet	175
11.3.2	Ukraine Attack	176
11.4	Mitigation Using NIST Cybersecurity Framework	178
11.5	Summary	180
11.6	Problems	180
11.7	Questions	181
	Further Reading	181
	Index	183

About the Authors



Anurag K. Srivastava, PhD, is the Raymond J. Lane Professor and Chairperson of the Lane Department of Computer Science and Electrical Engineering in the Benjamin M. Statler College of Engineering and Mineral Resources at West Virginia University. He is the director of the Smart Grid Resiliency and Analytics Lab (SGREAL) and an IEEE Fellow.



Venkatesh Venkataramanan, PhD, is a Researcher at the National Renewable Energy Laboratory, working on cyber-physical systems. He was previously with Washington State University and Massachusetts Institute of Technology.



Carl Hauser, PhD, is emeritus faculty in Computer Science at Washington State University. He received his PhD from Cornell University. Following 20 years in industry at IBM Research and Xerox Research, he joined WSU where he conducted research on communications and cybersecurity for electric grid operations.

Acknowledgments

Authors are thankful to students who were brave enough to take the team-taught course offered at the Washington State University. Students shaped up the course material development process over multiple offerings. Authors are also thankful to the US Department of Energy and the Power System Engineering Research Center (PSERC) for supporting the course development. We acknowledge the support from our colleagues including Dr. Adam Hahn, Prof. David Bakken, Dr. Min Sik Kim, and Prof. Anjan Bose.

Acronyms

ASTA	Arrivals See Time Averages
BHCA	Busy Hour Call Attempts
BR	Bandwidth Reservation
b.u.	bandwidth unit(s)
CAC	Call/Connection Admission Control
CBP	Call Blocking Probability(-ies)
CCS	Centum Call Seconds
CDTM	Connection-Dependent Threshold Model
CS	Complete Sharing
DiffServ	Differentiated Services
EMLM	Erlang Multirate Loss Model
erl	The Erlang unit of traffic-load
FIFO	First in–First out
GB	global balance
GoS	Grade of Service
ICT	Information and Communication Technology
IntServ	Integrated Services
ITU-T	International Telecommunication Unit – Standardization sector
IP	Internet Protocol
LIFO	Last in–First out
LHS	left hand side
LB	local balance
MMPP	Markov Modulated Poisson Process
MPLS	Multiple Protocol Labeling Switching
MRM	multi-retry model
MTM	multi-threshold model
PASTA	Poisson Arrivals See Time Averages
pdf	probability density function
PDF	probability distribution function

PFS	product form solution
QoS	quality of service
RED	random early detection
r.v.	random variable(s)
RLA	reduced load approximation
RHS	right-hand side
SIRO	service in random order
SRM	single-retry model
STM	single-threshold model
TH	Threshold(s)
TCP	Transport Control Protocol
UDP	User Datagram Protocol

1

Introduction to the Smart Grid

The power grid has been evolving from a physical system to a “cyber-physical” system to sense, communicate, compute, and control with enhanced digitalization. The cyber-physical smart grid includes components from the physical power system, digital devices, and the associated communication infrastructure. To realize the vision of the smart grid, massive amounts of data need to be transferred from the field devices to the control devices or to the control centers. As more optimal algorithms are deployed for best possible control at a faster time scale, the communication infrastructure becomes critical to provide the required inputs. At the same time, increased number of “smart” devices in the grid also increase the attack surface for potential cyber attacks. It is necessary to study the power system’s exposure to risks and vulnerabilities in the associated cyber system.

1.1 Overview of the Electric Power Grid

The electric power grid can be defined as the entire apparatus of wires and machines that connects the sources of electricity with the customers. A power grid is generally divided into four major components as shown in Figure 1.1:

1. Generation
2. Transmission
3. Distribution
4. Loads

Electricity was first generated, sold, and distributed locally in 1870s via direct current (DC) circuits over very small distances. As the demand for electricity became more widespread, the cost of construction and distribution of local generation and DC circuits to carry the power over long distances became prohibitively expensive. Hence, alternating current (AC) generation, transmission, and distribution became the standard that is used to this day. However, the

Cyber Infrastructure for the Smart Electric Grid, First Edition.

Anurag K. Srivastava, Venkatesh Venkataramanan, and Carl Hauser.

© 2023 John Wiley & Sons Ltd. Published 2023 by John Wiley & Sons Ltd.

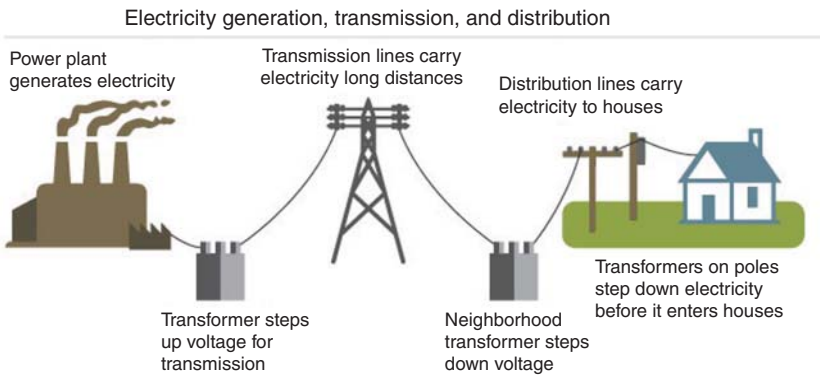


Figure 1.1 Major components of the power grid. Source: Energy Information Administration (EIA), public domain.

infrastructure of the power grid is getting older – the average age of a transformer is greater than 50 years old and has already exceeded its expected lifetime. The electric grid faces several problems, including a problem with the oncoming retirement of at least 5% of the workforce and one of the lowest R&D expenditure as compared to other critical infrastructures.

The situation is getting better, however, with increasing interest in national security and acknowledgment of the critical role that the power grid plays in the overall quality of life. In a full circle, localized generation using distributed energy resources (DERs) is making a comeback, with a combination of both AC and DC systems. Today's generation systems are a combination of different types of sources – including fossil fuels, natural gas, renewable resources, and nuclear energy. These generation systems are often located in remote areas for ease of doing business and for environmental reasons.

The power that is generated at the generating stations is brought to the consumers by a complex network of transmission lines. The North American power grid comprises of four major interconnections as shown in Figure 1.2:

1. Western interconnection
2. Eastern interconnection
3. Quebec interconnection
4. Electricity Reliability Council of Texas (ERCOT) interconnection

These interconnections are zones in which the electric utilities are electrically tied together, indicating that the areas are synchronized to the same frequency and power can flow freely in that area. The interconnections operate nearly independently of each other except for some high-voltage direct current (HVDC)



Figure 1.2 Interconnections in the North American Power Grid. Source: North American Energy Reliability Corporation (NERC), public domain.

interconnections between them. DC converter substations enable the synchronized transfer of power across interconnections regardless of the operating frequency as DC power is non-phase dependent.

The flow of electricity is instantaneous, indicating that the power that is being consumed is also being simultaneously generated. Commercially viable mechanisms for storing electricity for longer duration do not exist currently; hence, the power plants and the grid are constantly operating. The structure of the flow of electricity is illustrated in Figure 1.3, which shows the critical nature of the transmission system in bringing electricity from the generating plants to the customer's use.

Power demand constantly fluctuates throughout the day depending on consumer behavior. There are various factors that create this changing behavior, including population density, work schedules, weather, and other activities. In addition, special activities that involve a large number of people also have to be considered, such as big sporting events or an impending weather event over a large area. Figure 1.4 shows a typical daily "load" curve as it is referred to, which shows how the electric load varies across a day depending on the activities