

Anurag K. Srivastava • Venkatesh Venkataramanan
Carl Hauser

Cyber Infrastructure for the Smart Electric Grid




IEEE PRESS

WILEY

Table of Contents

[Cover](#)

[Title Page](#)

[Copyright](#)

[About the Authors](#)

[Acknowledgments](#)

[Acronyms](#)

[1 Introduction to the Smart Grid](#)

[1.1 Overview of the Electric Power Grid](#)

[1.2 What Can Go Wrong in Power Grid Operation](#)

[1.3 Learning from Past Events](#)

[1.4 Toward a Smarter Electric Grid](#)

[1.5 Summary](#)

[1.6 Problems](#)

[1.7 Questions](#)

[Further Reading](#)

[2 Sense, Communicate, Compute, and Control in a Secure Way](#)

[2.1 Sensing in Smart Grid](#)

[2.2 Communication Infrastructure in Smart Grid](#)

[2.3 Computational Infrastructure and Control Requirements in Smart Grid](#)

[2.4 Cybersecurity in Smart Grid](#)

[2.5 Summary](#)

[2.6 Problems](#)

[2.7 Questions](#)

[Further Reading](#)

3 Smart Grid Operational Structure and Standards

3.1 Organization to Ensure System Reliability

3.2 Smart Grid Standards and Interoperability

3.3 Operational Structure in the Rest of the World

3.4 Summary

3.5 Problems

3.6 Questions

Further Reading

4 Communication Performance and Factors that Affect It

4.1 Introduction

4.2 Propagation Delay

4.3 Transmission Delay

4.4 Queuing Delay and Jitter

4.5 Processing Delay

4.6 Delay in Multi-hop Networks

4.7 Data Loss and Corruption

4.8 Summary

4.9 Exercises

4.10 Questions

Further Reading

5 Layered Communication Model

5.1 Introduction

5.2 Physical Layer

5.3 Link Layer: Service Models

5.4 Network Layer: Addressing and Routing

5.5 Transport Layer: Datagram and Stream Protocols

5.6 Application Layer

[5.7 Glue Protocols: ARP and DNS](#)

[5.8 Comparison Between OST and TCP/IP Models](#)

[5.9 Summary](#)

[5.10 Problems](#)

[5.11 Questions](#)

[Further Reading](#)

[6 Power System Application Layer Protocols](#)

[6.1 Introduction](#)

[6.2 SCADA Protocols](#)

[6.3 ICCC](#)

[6.4 C37.118](#)

[6.5 Smart Metering and Distributed Energy Resources](#)

[6.6 Time Synchronization](#)

[6.7 Summary](#)

[6.8 Problems](#)

[6.9 Questions](#)

[Further Reading](#)

[7 Utility IT Infrastructures for Control Center and Fault-Tolerant Computing](#)

[7.1 Conventional Control Centers](#)

[7.2 Modern Control Centers](#)

[7.3 Future Control Centers](#)

[7.4 UML, XML, RDF, and CIM](#)

[7.5 Basics of Fault-Tolerant Computing](#)

[7.6 Cloud Computing](#)

[7.7 Summary](#)

[7.8 Problems](#)

[7.9 Questions](#)

Further Reading

8 Basic Security Concepts, Cryptographic Protocols, and Access Control

8.1 Introduction

8.2 Basic Cybersecurity Concepts and Threats to Power Systems

8.3 CIA Triad and Other Core Security Properties

8.4 Introduction to Encryption and Authentication

8.5 Cryptography in Power Systems

8.6 Access Control

8.7 Summary

8.8 Problems

8.9 Questions

Further Reading

9 Network Attacks and Protection

9.1 Attacks to Network Communications

9.2 Mitigation Mechanisms Against Network Attacks

9.3 Network Protection Through Firewalls

9.4 Intrusion Detection

9.5 Summary

9.6 Problems

9.7 Questions

Further Reading

10 Vulnerabilities and Risk Management

10.1 System Vulnerabilities

10.2 Security Mechanisms: Access Control and Malware Detection

10.3 Assurance and Evaluation

[10.4 Compliance: Industrial Practice to Implement NERC CIP](#)

[10.5 Summary](#)

[10.6 Problems](#)

[10.7 Questions](#)

[Further Reading](#)

[11 Smart Grid Case Studies](#)

[11.1 Smart Grid Demonstration Projects](#)

[11.2 Smart Grid Metrics](#)

[11.3 Smart Grid Challenges: Attack Case Studies](#)

[11.4 Mitigation Using NIST Cybersecurity Framework](#)

[11.5 Summary](#)

[11.6 Problems](#)

[11.7 Questions](#)

[Further Reading](#)

[Index](#)

[End User License Agreement](#)

List of Tables

Chapter 1

[Table 1.1 List of well-known blackouts around the world.](#)

Chapter 6

[Table 6.1 Application layer SCADA protocols.](#)

Chapter 7

[Table 7.1 Taxonomy of faults.](#)

[Table 7.2 Advantages of cloud computing over traditional on-site computatio...](#)

Chapter 9

[Table 9.1 Packet filtering rules - an example.](#)

Chapter 10

[Table 10.1 Goals and techniques of security testing.](#)

List of Illustrations

Chapter 1

[Figure 1.1 Major components of the power grid.](#)

[Figure 1.2 Interconnections in the North American Power Grid.](#)

[Figure 1.3 Structure of electricity flow from generating stations to the con...](#)

[Figure 1.4 Load curves for a typical day.](#)

[Figure 1.5 Voltage levels in the power grid.](#)

[Figure 1.6 Cyber-physical system layers.](#)

Chapter 2

[Figure 2.1 Sensing, communication, computation, and control for the cyber-ph...](#)

[Figure 2.2 Capturing data from different locations synchronously.](#)

[Figure 2.3 Phasor measurement unit architecture.](#)

[Figure 2.4 Sampling rate of waveforms for PMUs.](#)

[Figure 2.5 Original phasors and positive sequence components of phasors.](#)

[Figure 2.6 Phasor estimation using DFT.](#)

[Figure 2.7 PMU data packet.](#)

[Figure 2.8 PMU-based applications for the future smart grid.](#)

[Figure 2.9 Communication, computation, and control for smart grid.](#)

[Figure 2.10 Functions of control center.](#)

[Figure 2.11 Various control center applications and their timelines.](#)

Chapter 3

[Figure 3.1 Role of balancing authority.](#)

[Figure 3.2 Balancing authorities in the United States.](#)

[Figure 3.3 Interaction between utilities, enforcement agencies, and user gro...](#)

Chapter 4

[Figure 4.1 \$\rho/\(1 - \rho\)\$ for \$\rho\$ in \$\[0 \dots 0.95\]\$.](#)

Chapter 5

[Figure 5.1 OSI layered network model.](#)

[Figure 5.2 TCP/IP network model.](#)

[Figure 5.3 Ethernet frame format.](#)

[Figure 5.4 Institutional network using Ethernet.](#)

[Figure 5.5 MPLS format.](#)

[Figure 5.6 Overview of a router.](#)

[Figure 5.7 IP datagram format.](#)

[Figure 5.8 IP addressing - subnets.](#)

[Figure 5.9 IP addressing - host part and subnet part.](#)

[Figure 5.10 Routing algorithms set up.](#)

[Figure 5.11 Packet duplication strategies.](#)

[Figure 5.12 Sockets and processes.](#)

[Figure 5.13 TCP/UDP segment format.](#)

[Figure 5.14 TCP segment structure.](#)

[Figure 5.15 Link layer addressing.](#)

Chapter 6

[Figure 6.1 A typical SCADA system architecture.](#)

[Figure 6.2 DNP3 network stack.](#)

[Figure 6.3 IEC 61850 network stack.](#)

[Figure 6.4 ICCP protocol between control centers.](#)

[Figure 6.5 IEEE C37.118 data format.](#)

[Figure 6.6 General smart metering architecture.](#)

Chapter 7

[Figure 7.1 Architecture of a conventional control center.](#)

[Figure 7.2 Architecture of a modern control center.](#)

[Figure 7.3 Architecture of future control centers.](#)

[Figure 7.4 UML class.](#)

[Figure 7.5 UML inheritance](#)

[Figure 7.6 UML association.](#)

[Figure 7.7 UML composition.](#)

[Figure 7.8 UML aggregation.](#)

[Figure 7.9 CIM for a breaker.](#)

[Figure 7.10 Cascading faults.](#)

Chapter 8

[Figure 8.1 Likelihoods and consequences of threats.](#)

[Figure 8.2 Energy consumption data impacts on consumer privacy.](#)

[Figure 8.3 Symmetric and asymmetric encryption.](#)

[Figure 8.4 Hash functions.](#)

[Figure 8.5 MAC algorithm.](#)

[Figure 8.6 Certificate generation.](#)

[Figure 8.7 DNP3 authentication techniques. \(a\) Challenge-Response. \(b\) Aggre...](#)

[Figure 8.8 Access control overview.](#)

[Figure 8.9 Examples of RBAC roles.](#)

Chapter 9

[Figure 9.1 Reflection attack.](#)

[Figure 9.2 ARP spoofing attack.](#)

[Figure 9.3 Security enhancements in the TCP/IP stack.](#)

[Figure 9.4 TLS protocol stack.](#)

[Figure 9.5 Typical TLS handshake.](#)

[Figure 9.6 IPsec ESP modes of operation.](#)

[Figure 9.7 Firewall showing separation between the critical enterprise netwo...](#)

[Figure 9.8 Intrusion detection systems.](#)

[Figure 9.9 Attack detection cases.](#)

[Figure 9.10 Snort IDS.](#)

Chapter 10

[Figure 10.1 Bugs and vulnerabilities in software.](#)

[Figure 10.2 Run-time memory of a process.](#)

[Figure 10.3 Buffer overflow - manipulation of ret value.](#)

[Figure 10.4 Hardware access control layers.](#)

[Figure 10.5 Port scanning mechanism.](#)

[Figure 10.6 Network monitoring mechanism.](#)

[Figure 10.7 Network policy review.](#)

[Figure 10.8 Vulnerability scanning mechanism.](#)

[Figure 10.9 Continuous monitoring using the SCAP protocol.](#)

Chapter 11

[Figure 11.1 Conceptual model of the future smart grid.](#)

[Figure 11.2 LNK vulnerability - from infected removable drive to gaining ele...](#)

[Figure 11.3 Infected host communicating with command and control server to r...](#)

[Figure 11.4 Steps in the Ukraine cyber attack of 2018.](#)

[Figure 11.5 Defense-in-depth approach to mitigate cybersecurity concerns....](#)

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

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 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.

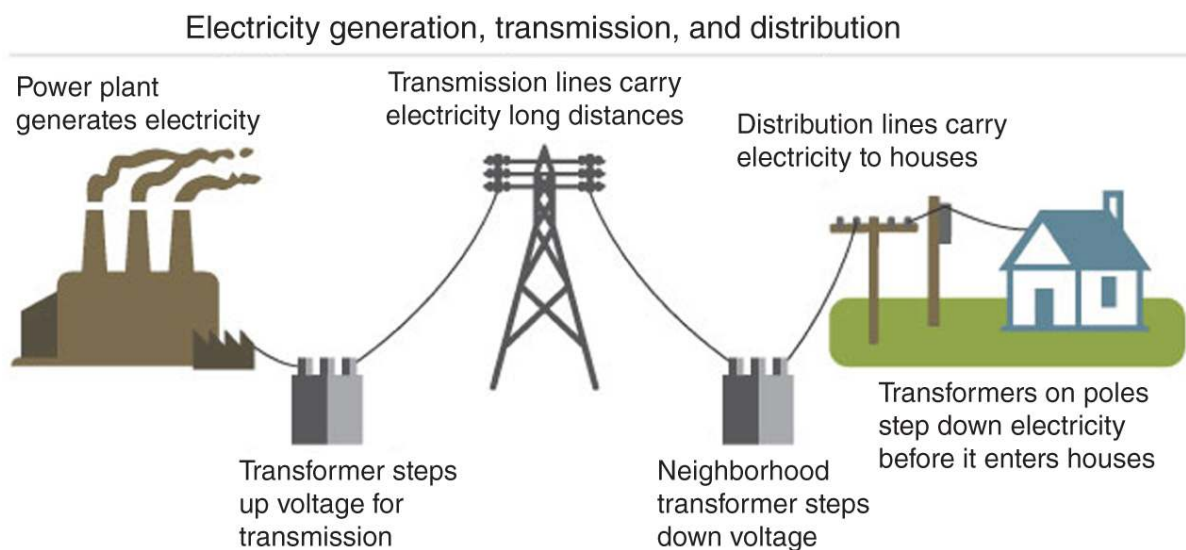


Figure 1.1 Major components of the power grid.

Source: Energy Information Administration (EIA), public domain.

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

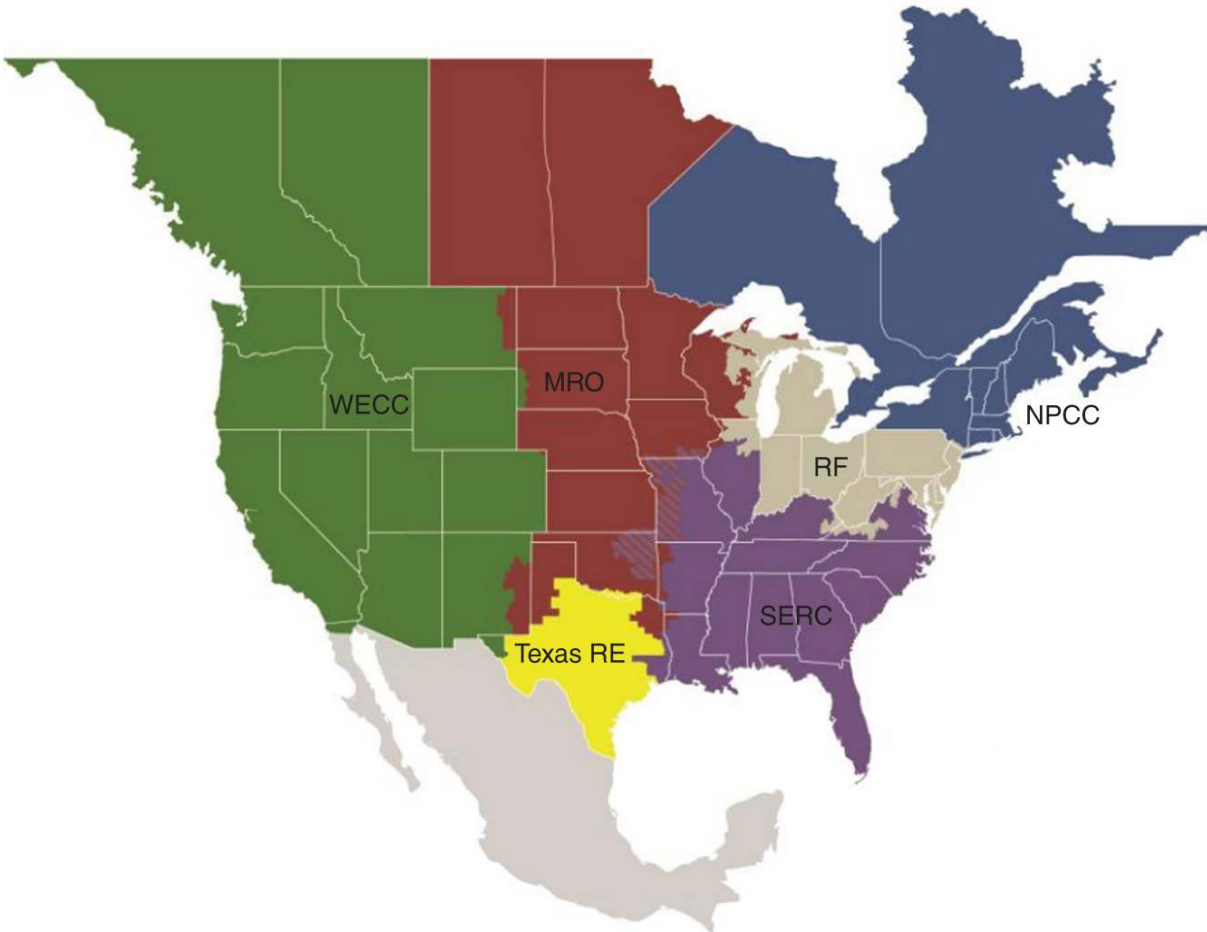
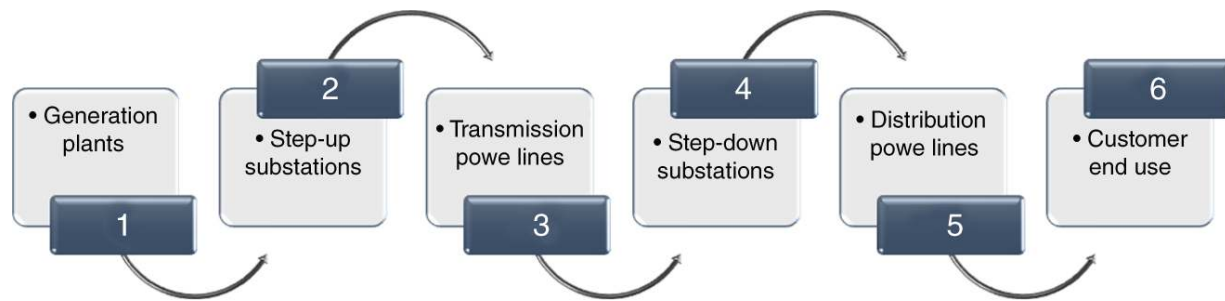


Figure 1.2 Interconnections in the North American Power Grid.

Source: North American Energy Reliability Corporation (NERC), public domain.

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) 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.



[Figure 1.3](#) Structure of electricity flow from generating stations to the consumer.

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 throughout the day. The peak demand occurs in the early evening when people return from work and are engaged in family activities or dinner preparation. The power demand rises and falls throughout the day depending on other activities, such as a peak when people are getting ready for work or troughs when they are sleeping. These load curves are constantly monitored and predicted by the utilities and operators to plan for the operation of the grid, and they are

updated at regular intervals to account for changes in behavior, such as the COVID-19 pandemic.

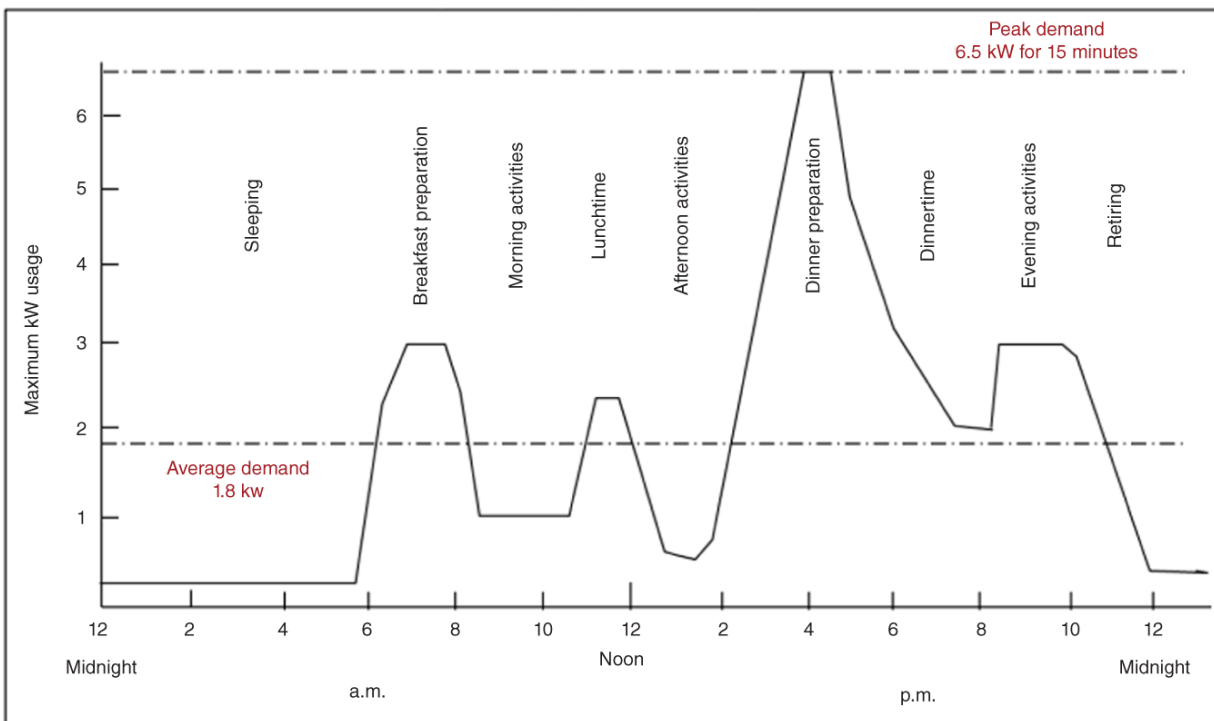


Figure 1.4 Load curves for a typical day.

Source: US Department of Energy, Office of Electricity Delivery and Energy Reliability.

The power distribution system is the last leg of the power delivery from the substations to the consumer. The three components of the power grid are usually defined by the voltage levels at which they operate at. Generation happens at generating stations at low voltages, following which the power is immediately transformed to much higher voltages on site. Generation plants send the power where they are stepped up till 20,000 V, following which they are fed to the transmission grid where they can be stepped up as high as 765,000 V, commonly written and referred to as 765 kV. The power is stepped up to these very high values to reduce losses in transmission, which are directly proportional to the current and inversely proportional to the voltage. The distribution system

substation is considered to be at the 13.2 kV level (or could be higher), following which the voltage is stepped down to be sent to the consumers. This structure is illustrated in [Figure 1.5](#).

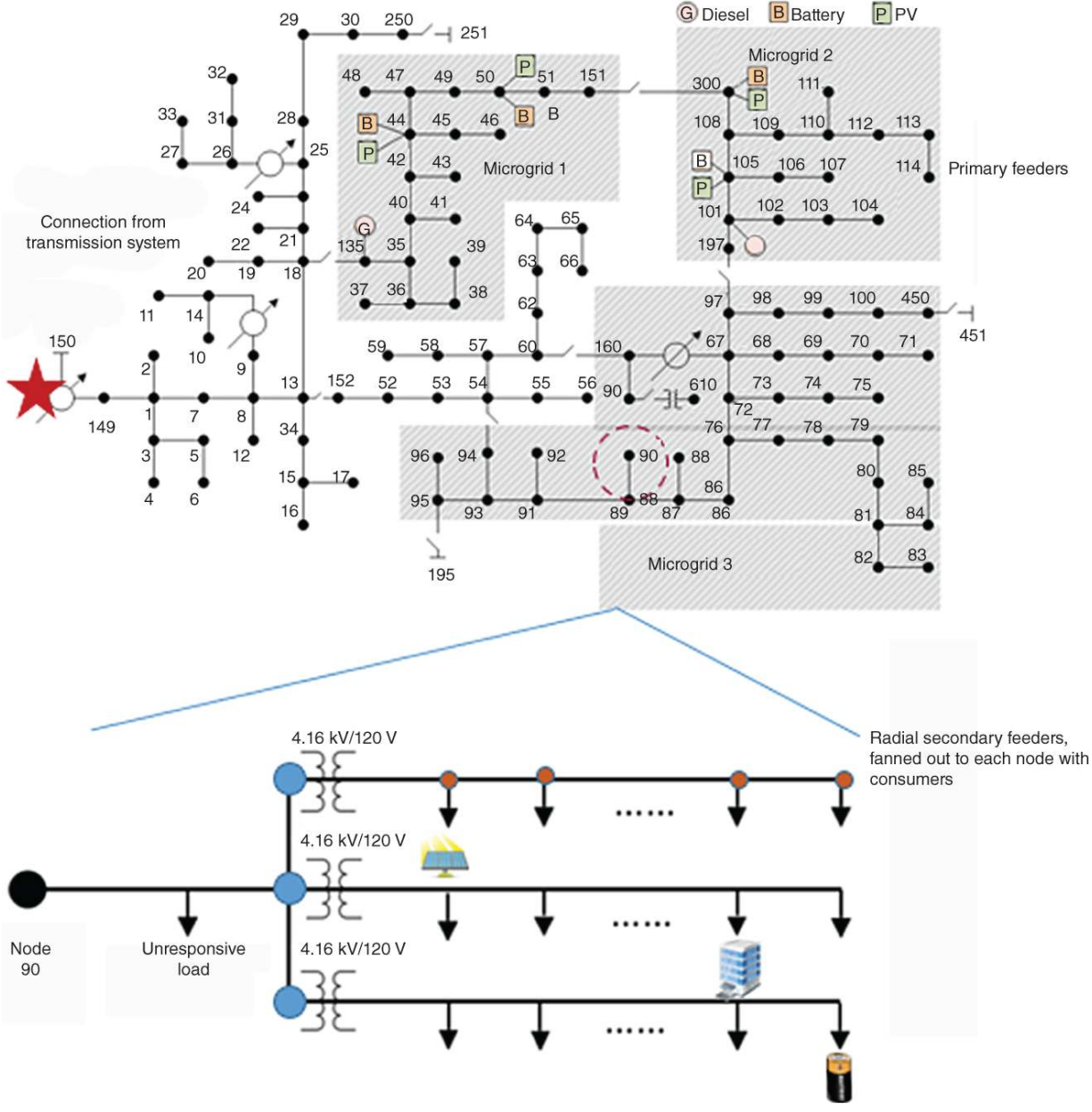


Figure 1.5 Voltage levels in the power grid.

Energy control centers have traditionally been the decision centers for the electric generation and transmission centers. There are enabled by the wide area measurements

fed to the control centers by the SCADA (Supervisory Control And Data Acquisition) and other measurement systems. The control center operator(s) is a key part of the overall operation of the grid with various responsibilities including but not limited to the following:

1. Monitor and react to key system performance indices such as voltage, frequency, power quality, and other metrics (such as reliability metrics).
2. Respond to emergencies and alerts - the control system operator has to handle the alerts from various algorithms and applications running at the control center. In addition, they also deal with emergencies such as trees hitting transmission lines or fires because of malfunctioning equipment.
3. Ensure system reliability by scheduling maintenance on equipment in anticipation of failures.
4. Respond to larger customer requests such as industries or other infrastructures. This could be a larger consumer who is testing their on-site back-up generation or infrastructural loads such as the transit system.
5. Coordinate with other stakeholders such as generation companies, transmission operators, utilities, and maintenance crews among others to ensure seamless operation.
6. Ensure that system operation is compliant with system regulations put in place by authorities such as FERC and NERC at all times.

In short, the control system is responsible for ensuring that electricity is being generated, transmitted, and distributed to the consumers in a safe and reliable manner. It coordinates all system operations with the other