Anurag K. Srivastava • Venkatesh Venkataramanan
Carl Hauser

Cyber Infrastructure for the Smart Electric Grid

IEEE PRESS

WILEY

Table of Contents

List of Tables

List of Illustrations

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

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.

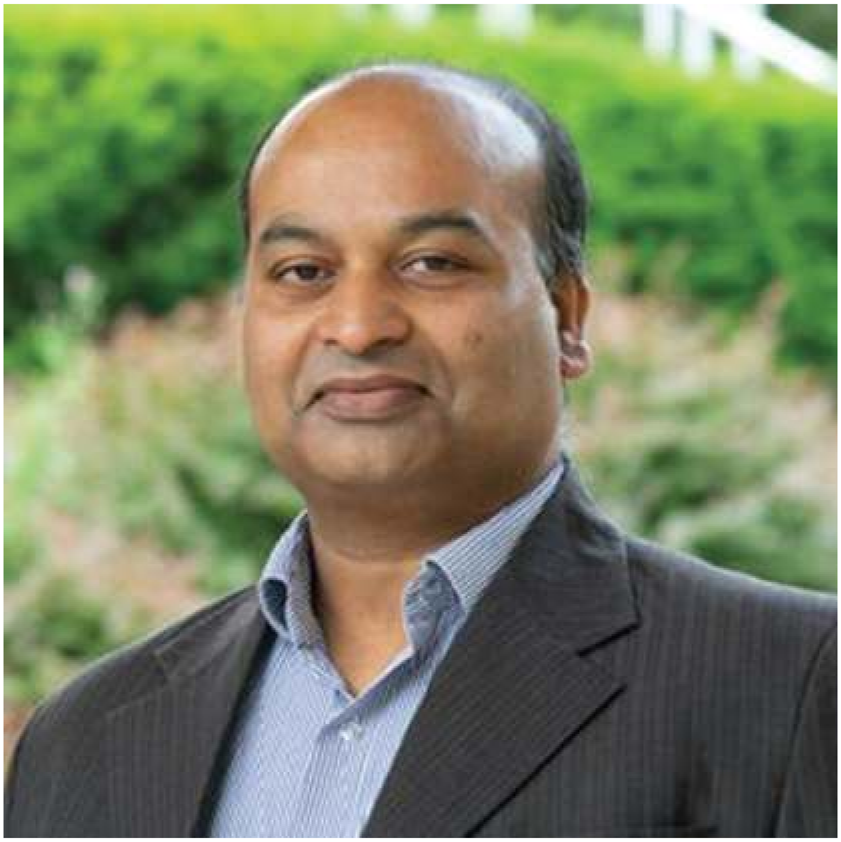
Wiley also publishes its books in a variety of electronic formats and by print-on-demand. Some content that appears in standard print versions of this book may not be available in other formats.

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.

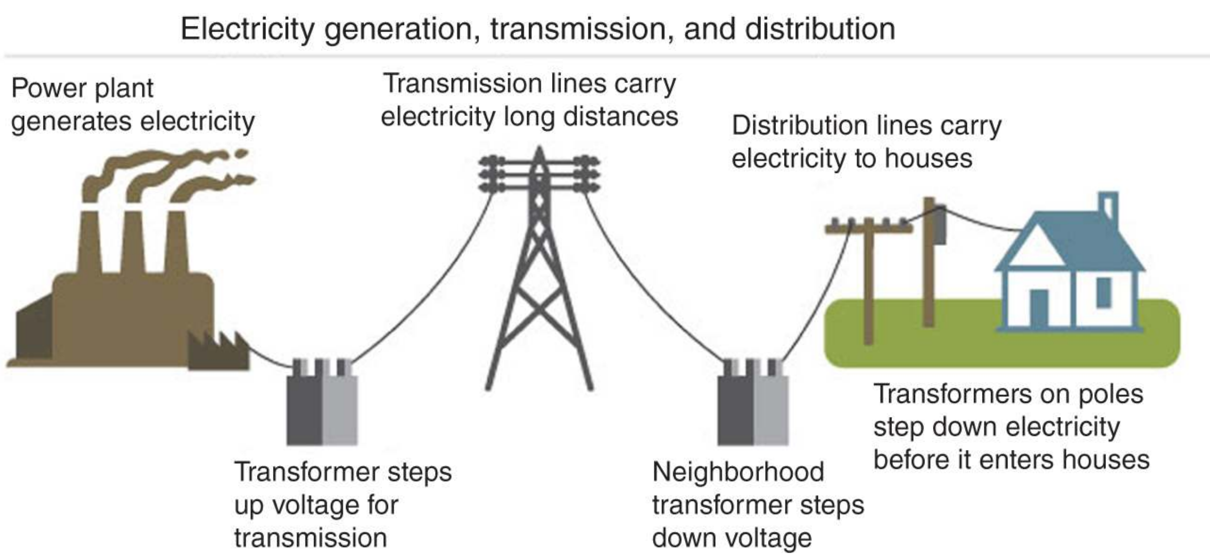


Figure 1.1 Major components of the power grid.

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

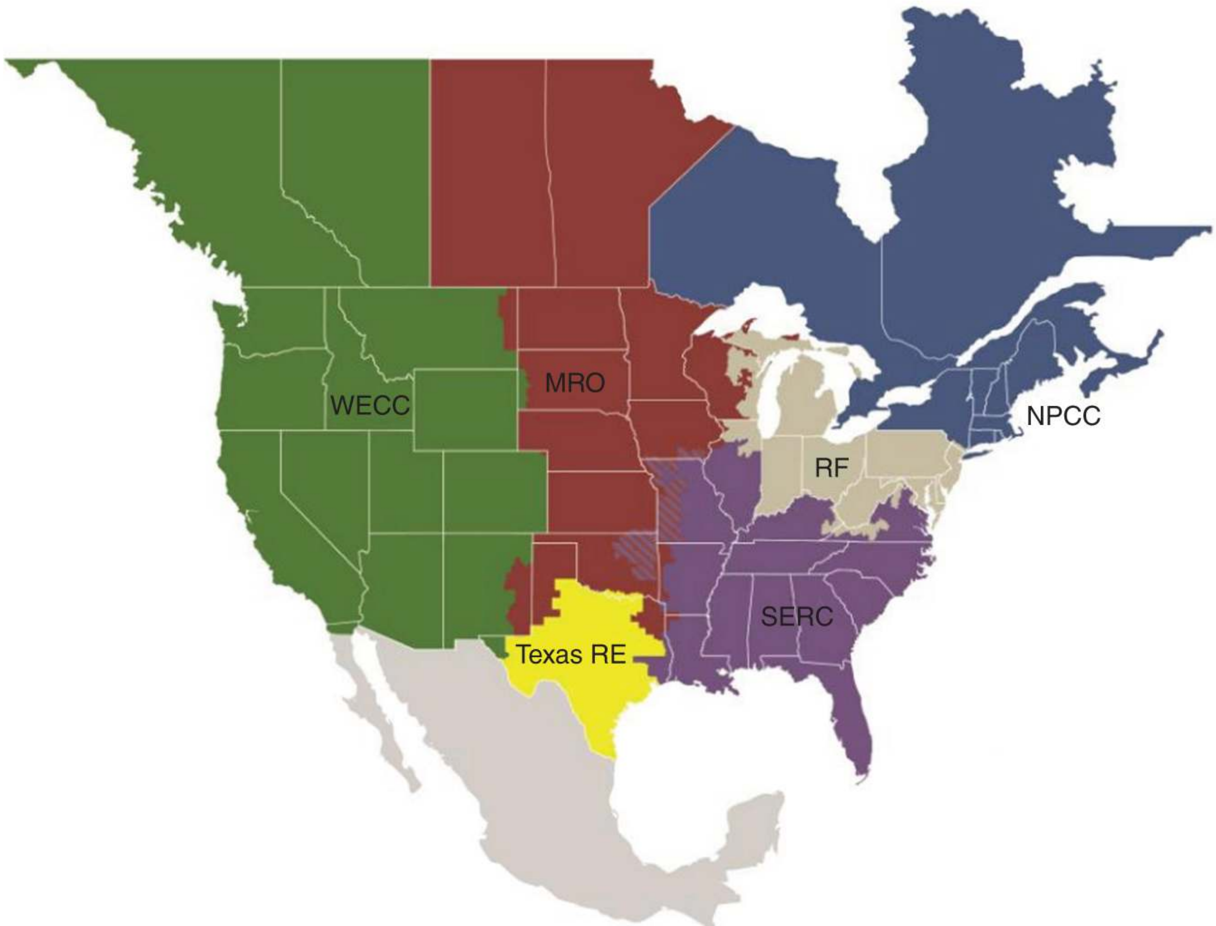


Figure 1.2 Interconnections in the North American Power Grid.

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.

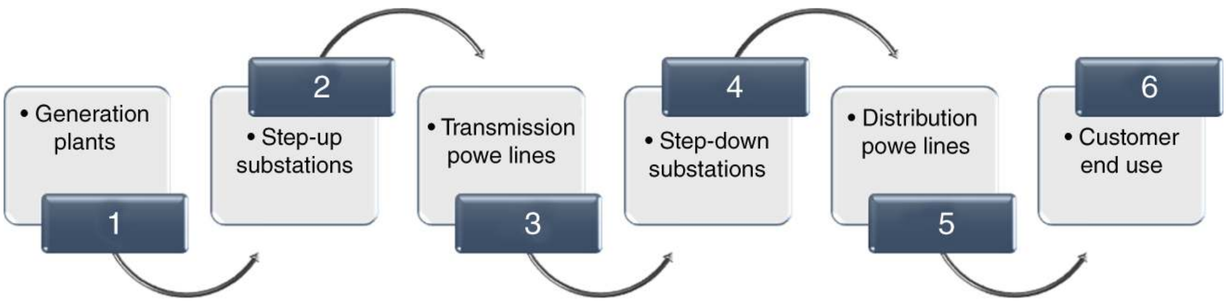


Figure 1.3 Structure of electricity flow from generating stations to the consumer.

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.

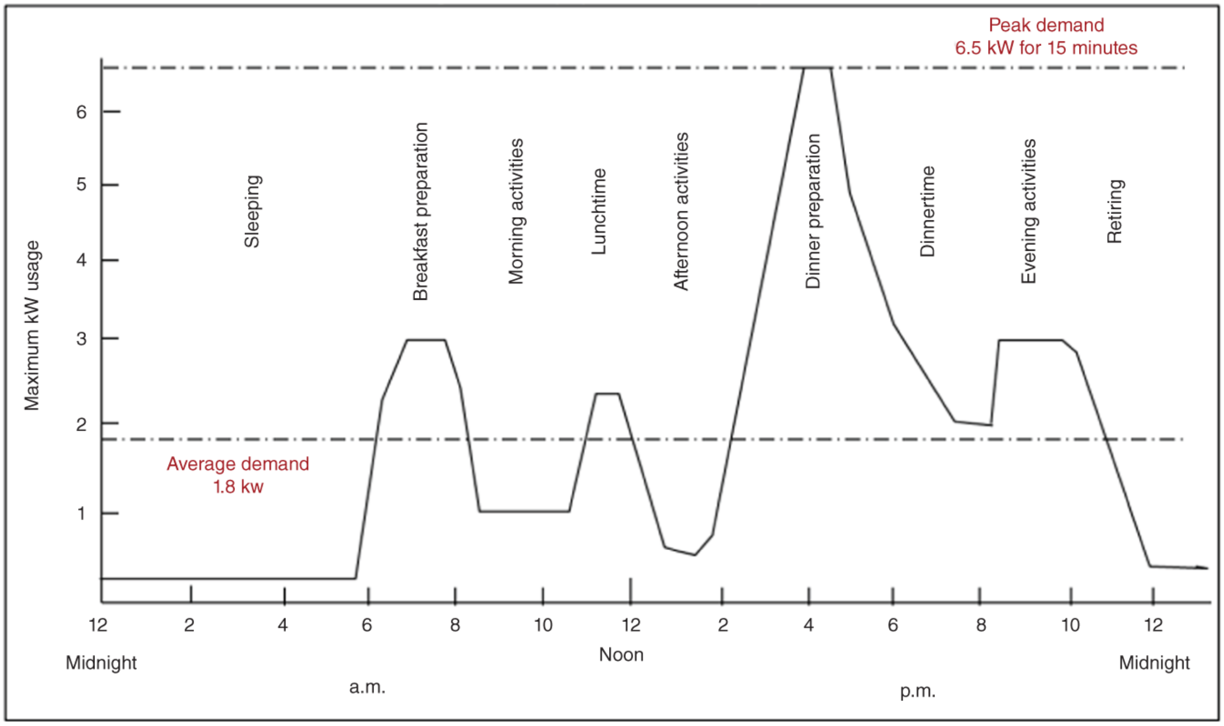


Figure 1.4 Load curves for a typical day.

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.

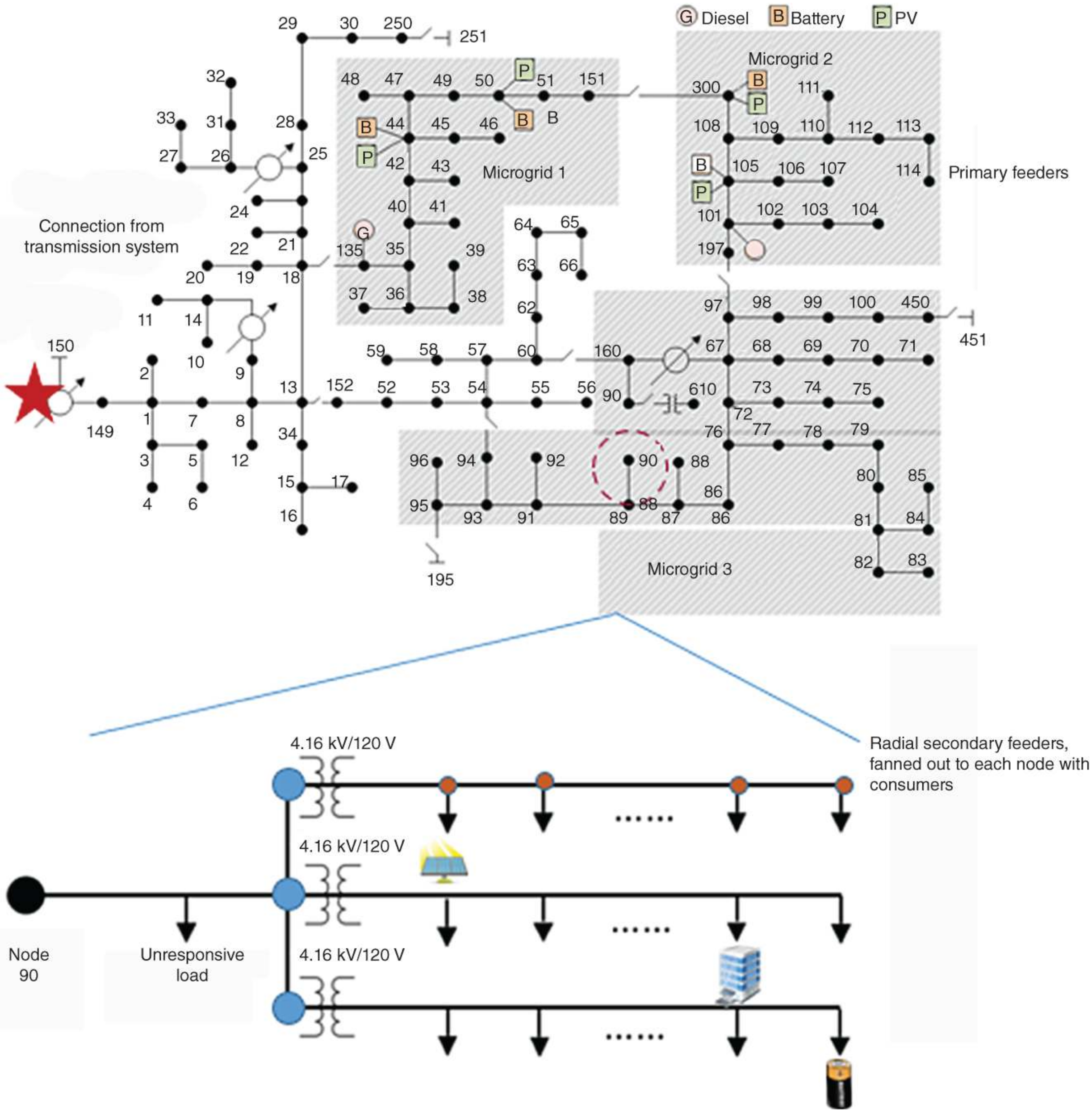


Figure 1.5 Voltage levels in the power grid.

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