1

Introduction

1.1 Cyber-Physical Perspectives of Smart Grids

Electrical power grids are interconnected critical infrastructures that serve a single critical objective: continuously providing energy supplies to meet the demands. Achieving this objective requires each power grid to include three main components: power generation, power consumption, and power delivery. *Power generation* produces electricity at power plants using various energy sources, including fossil fuels, nuclear power, and renewable energy sources (RESs) such as wind, solar, and hydro. *Power consumption*, also known as load demands, refers to various physical processes that require a certain amount of electrical energy to achieve their predefined functionality, e.g., lighting, motor movement, etc. *Power delivery* refers to the transmission or distribution systems that provide reliable and sufficient physical connectivity between power generation and consumption units, often located in different geographical locations.

Modern power grids are gradually evolving into a smart grid. These changes are often observed in three main aspects. First, off-the-shelf computing technologies transform traditional legacy metering devices into an embedded computer system. For example, many intelligent relays are equipped with general-purpose CPUs and run customized operating systems, allowing for the automation of complex decision-making at remote field sites without requiring a centralized control center. Second, off-the-shelf communications network technologies connect physical devices in wide geographical locations to collect increasing amounts of data at a high frequency. This wide-area monitoring capability enables the detection of power grid anomalies with greater accuracy and timeliness. Third, distributed energy resources' (DERs) involvement blurs the boundary between power generation and consumption. For example, a residential site, regarded as a power

Cyber-Physical Security and Resilience for Smart Grids and Renewable Energy,
First Edition. Hui Lin.

consumption site in a traditional power grid, can now generate its electricity using a rooftop solar panel. Consequently, the traditional one-way flow of electricity becomes a two-way or an interconnected electricity network, introducing opportunities to satisfy various load demand situations and challenges to efficiently and effectively allocate heterogeneous energy sources.

These understandings lead to the following definitions of smart grids from certain established sources:

- "A Smart Grid is a modern electricity system. It uses sensors, monitoring, communications, automation, and computers to improve the flexibility, security, reliability, efficiency, and safety of the electricity system." [1]
- "Smart Grid generally refers to a class of technology people are using to bring utility electricity delivery systems into the 21st century, using computer-based remote control and automation. These systems are made possible by two-way communication technology and computer processing that has been used for decades in other industries. They are beginning to be used on electricity networks, from the power plants and wind farms all the way to the consumer of electricity in homes and businesses. They offer many benefits to utilities and consumers – mostly seen in big improvements in energy efficiency on the electricity grid and in the energy users' homes and offices."

All these technological advancements inspire us to provide a cyber-physical perspective of smart power grids, based on which we can further understand the security properties. But exactly, what are cyber-physical systems (CPSs)? We can begin with the traditional *control systems* to gain a better understanding of their concepts. As shown in Figure 1.1, even though control systems can have various appearances, e.g., automobiles, medical devices, power grids, and agriculture, they operate on top of a typical feedback loop, involving two interactions performed interchangeably. On the one hand, sensors collect measurements from physical processes, and a control center uses them as input to control algorithms, continuously obtaining the updated models of the physical processes. When the physical processes require adjustment to ensure its long-term stability, the control center leverages actuators to deliver commands generated by the control algorithms according to physical states.

Traditional control systems relied on legacy sensors and actuators to perform sensing and actuation tasks. To enhance operational efficiency and reduce administrative costs, engineers have increasingly adopted off-the-shelf computing components and network infrastructure as replacements. This shift has driven the evolution of control systems into CPSs.

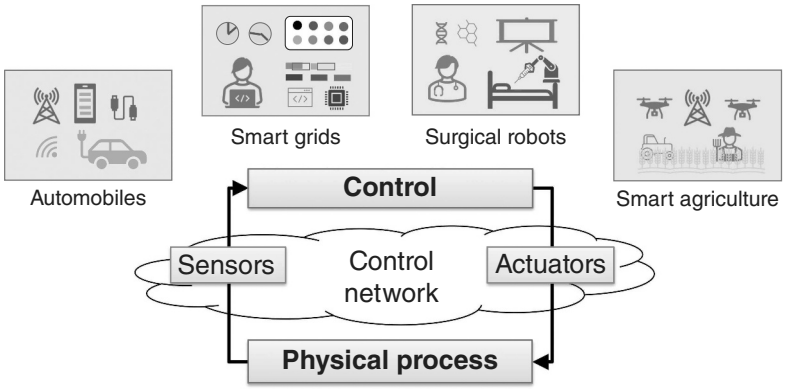

Figure 1.1 Various control systems following a typical feedback loop. A control algorithm leverages various *sensors* to collect measurements from a physical process, to monitor the system's run-time states accurately. If a control command is needed, the control algorithm uses *actuators* to deliver them and maintain continuous and stable operations in the physical process.

The core concept rooted in CPS is closely related to "cybernetics," which was initially proposed by Norbert Wiener in 1948 [2]. Around 2006, Dr. Helen Gill of the US National Science Foundation (NSF) formally introduced the term CPSs to describe the evolutionary shift observed in industrial control systems and traditional embedded systems. Currently, there is no standard definition of CPS. However, the National Institute of Standards and Technology (NIST) provides the following reference definition [3]. "Cyber-Physical Systems (CPSs) comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. CPSs will bring advances in personalized health care, emergency response, and traffic flow management."

1.2 Grid Integrated with Renewable Energy

The International Energy Agency (IEA) published a prediction for renewable energy growth until the middle of this century, shown in Figure 1.2. According to its model, we anticipate that power generation based on solar photovoltaic (PV) systems (including both utility and distributed sources) will increase by more than 80 times during the 2023–2028 period compared to the generation between 2005 and 2010. Similarly, the global grid-connected wind power generation is expected to increase sixfold.

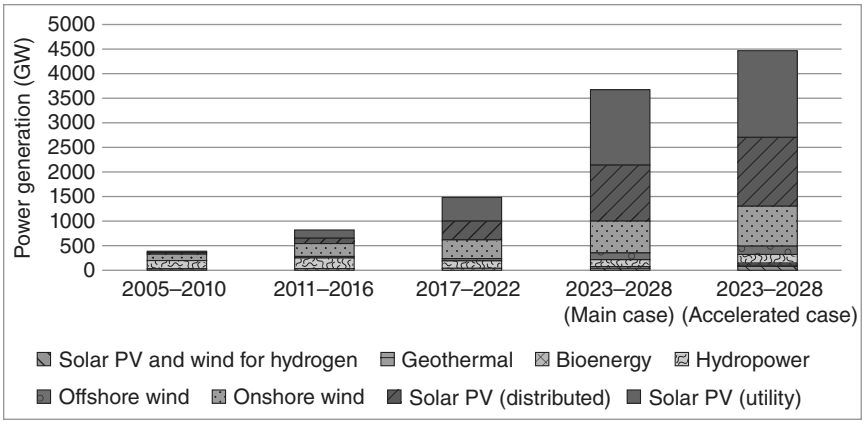

Figure 1.2 The forecast of renewable energy growth by technology, main, and accelerated cases for 2005–2028 from the IEA [4] ([5]/CC BY 4.0).

While solar PV still dominates the share of renewable energy generation, wind electricity has become a surging source. However, unlike solar PV, wind power farms utilize various technologies, necessitating further in-depth research and development. Among them, onshore wind is expected to dominate the market for the foreseeable future, primarily because it is not restricted by the coastline near a sea or an ocean; it can be deployed in various geographic areas and under different climatic conditions. However, for the area near the shore, offshore wind, whether floating or fixed, is a great attraction, as it experiences fewer intermittent features compared to onshore wind due to the flat sea, fewer obstacles, and more predictable air flows. Onshore wind power remains one of the most mature RESs. Offshore wind technology is derived mainly from its onshore counterpart, which has undergone rapid technological advancements in recent years. Because of these reasons, an offshore wind turbine can produce up to twice as much electricity as an onshore wind turbine. Furthermore, it poses fewer problems in terms of social acceptability, as they are often not visible and are located in rural residential areas.

1.3 Emergence of Cyber-Physical Attacks

The newly emerging cyber-physical attacks pose a significant threat to today's power grid infrastructure and present substantial challenges to existing security measures. Employing a sophisticated interplay between cyber and physical devices, adversaries can coordinate the compromise of computing devices and the disruption of physical processes to maximize impact and conceal the consequences of the disruption [6]. For example, Russian hackers coordinated

cyberattacks with missile strikes targeting Ukraine's energy infrastructure in October 2023, causing an outage affecting hundreds of thousands of Ukrainian civilians [7]. This attack, which can combine various attack strategies, presents the following unique features:

- **Physical disruption:** the ultimate objective of physical disruption is to introduce irreversible consequences, e.g., economic losses and human casualties. Making things worse, existing security solutions focus on detecting, preventing, and mitigating cyber components, with little domain knowledge of physical infrastructure.
- **Stealthiness:** the adversaries can rely on operations encoded in legitimate formats but with a different parameter to launch attacks. A benign operation for one physical state may become malicious for a different physical state, making it difficult to build a whitelist or blacklist to detect the attacks preemptively.
- **Complication:** adversaries can leverage the complicated and proprietary interactions between cyber and physical components to launch the attack, whose life cycle experiences a long period and exploits resources in different geographical locations and under the administration of various actors. While adversaries can obtain high-level coordination, security solutions are separated among different administrations.

The core of the emerging cyber-physical attacks is leveraging domain-specific knowledge of target systems into the attack strategies. Consequently, they can have very different attack strategies for different physical processes. While many studies and research literature discussed cyber-physical attacks in the context of general-purpose industrial control systems, the Internet of Things, and conventional bulky power grids, the vulnerabilities in newly developed inverter-based renewable energy technologies and how security measures evolve are unclear. This book will serve as a starting point to equip future engineering students and researchers with the necessary knowledge to explore this unknown field.

1.4 Topics Covered

Chapter 2 (Computer Network Primer) presents the fundamental knowledge related to computer networks. We focus on the application layer and transport layer services, presenting how their services evolve from general-purpose computer network design to meet specific functionality and quality-of-service requirements in critical infrastructures, such as power grids.

Chapter 3 (Fundamentals of Cybersecurity) introduces the fundamental concepts related to system and network security, and how confidentiality, integrity,

and availability features are related to the cyber-physical infrastructure of power grids. We present introductions to encryption/decryption methodologies, which are essential to understanding various security concepts. Reviewing this knowledge can put all readers on the same page and equip them with the same terminology.

Chapter 4 (Fundamentals of Power Grid Control and Operation) introduces the fundamental knowledge of power grid control operations. The introductory nodal analysis will be presented to derive the power flow equations, which serve as the basis for diverse control operations in modern power systems, including optimal power flow analysis, unbalanced three-phase analysis, and volt-var controls. Domain-specific knowledge is heavily used to describe power-grid-specific security measures.

Chapter 5 (Communications Network Infrastructure for Smart Grids) presents the communication infrastructures that are specifically designed and implemented for today's smart grids. The network protocols and infrastructure configurations are presented to understand the attack strategies adopted by adversaries, such as cyber-physical attacks.

Chapter 6 (Cyber-Physical Attacks and Disruption Against Smart Grids) combines security knowledge and actual incidents to present the attacks and disruptions targeting modern smart grids. We specifically focus on how adversaries leverage domain-specific knowledge to introduce severe disruptions and how the attack strategies shape today's security solutions.

Chapter 7 (Cyber Defense to Increase Smart Grids Resilience) includes state-of-the-art security solutions designed and implemented to detect, prevent, and mitigate attacks and disruptions targeting smart grids. We specifically focus on how cyber defense combines domain-specific knowledge in power grids with today's security solutions to boost their performance in this critical infrastructure.

Chapter 8 (AI for Smart Grid Resilience: Opportunities and Challenges) presents the smart grids enhanced with artificial intelligence (AI) to achieve human-on-the-loop automation. The chapter explores the opportunities and challenges of leveraging the same AI technology to enhance smart grid resilience and mitigate cyber threats.

Chapter 9 (Resilience of Smart Grids Enhanced with Renewable Energy) describes the renewable energy technologies adopted in today's smart grids. We present how the unique mechanical and electrical components used by solar PV and wind turbines can reshape communications network infrastructures and the corresponding security and resilience measures.

1.5 Target Audience

This book is aimed at students, researchers, and on-site engineers. It provides a systematic overview of knowledge from various disciplines to inform the initiation of related courses and research projects. For advanced researchers who need to focus on specific topics, the book provides a comprehensive survey of incidents, attacks, security solutions, and offshore wind technologies.

References

1 Singer J. Enabling Tomorrow's Electricity System: Report of the Ontario Smart Grid Forum. Independent Electricity System Operator; 2009.
2 Wiener N. Cybernetics; Or Control and Communication in the Animal and the Machine. John Wiley & Sons; 1948.
3 Cyber-Physical Systems Public Working Group Smart Grid and Cyber-Physical Systems Program Office. Framework for Cyber-Physical Systems: Volume 1, Overview. National Institute of Standards and Technology; 2017.
4 Kamwa I. Offshore wind energy transmission: challenges and innovations in collecting and transmitting electricity from sea to cities [Editor's voice]. IEEE Power and Energy Magazine. 2024; 22(5): 4–19.
5 International Energy Agency (IEA). Renewable Capacity Growth by Technology, Main and Accelerated Cases, 2005-2028; 2024. [Online] Available at: https://www.iea.org/data-and-statistics/charts/renewable-capacity-growth-by-technology-main-and-accelerated-cases-2005-2028.
6 Urbina DI, Giraldo JA, Cardenas AA, Tippenhauer NO, Valente J, Faisal M, et al. Limiting the Impact of Stealthy Attacks on Industrial Control Systems. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016. p. 1092–1105. https://doi.org/10.1145/2976749.2978388.
7 Greenberg A. Sandworm Hackers Caused Another Blackout in Ukraine – During a Missile Strike. Wired; 2021. [Online] Available at: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/.