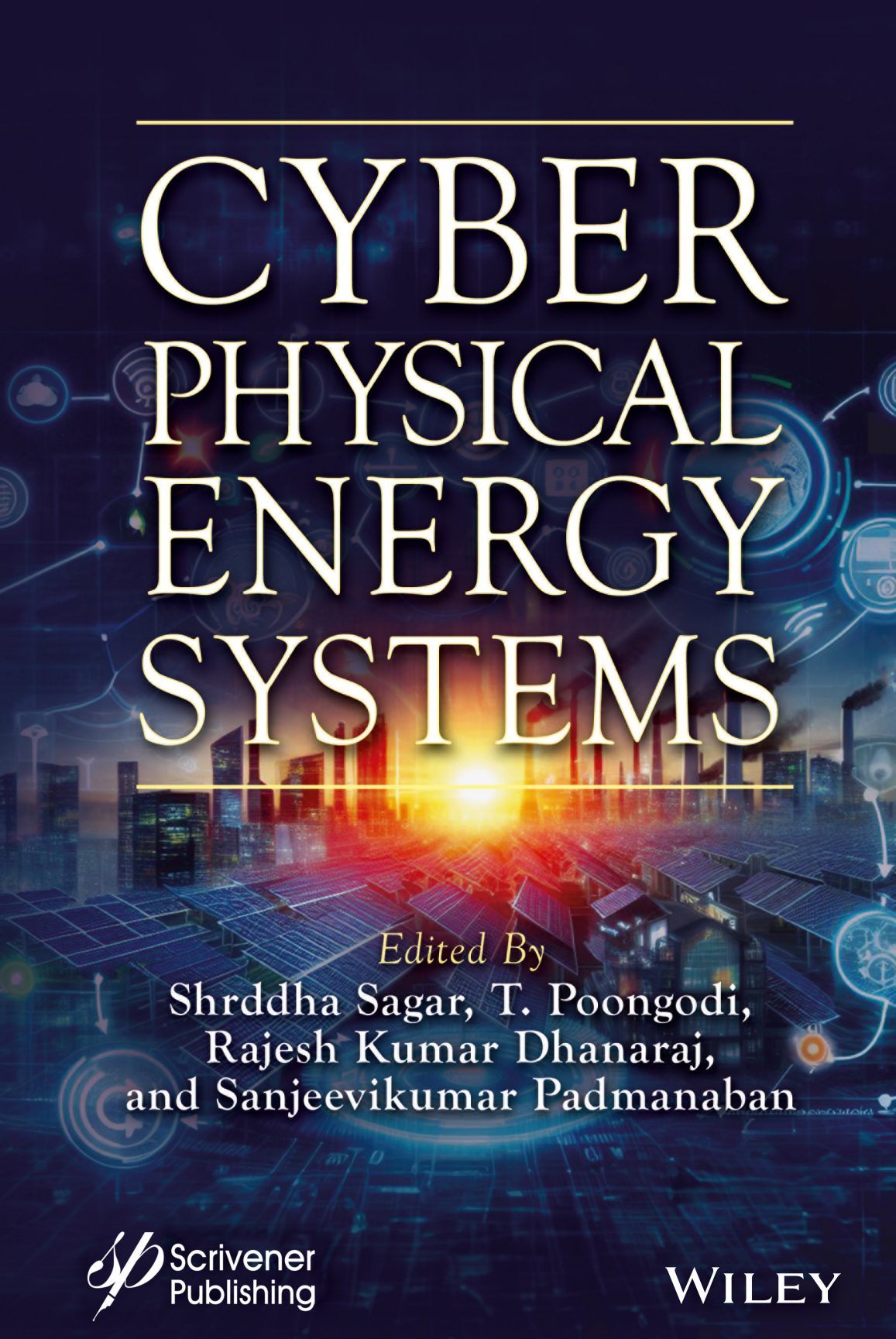
CYBER PHYSICAL ENERGY SYSTEMS



Edited By

Shrddha Sagar, T. Poongodi,
Rajesh Kumar Dhanaraj,
and Sanjeevikumar Padmanaban

Scrivener Publishing

WILEY

Cyber Physical Energy Systems

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Cyber Physical Energy Systems

Edited by

Shrddha Sagar

T. Poongodi

Rajesh Kumar Dhanaraj

and

Sanjeevikumar Padmanaban

WILEY

This edition first published 2025 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

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

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-394-17252-8

Front cover images supplied by Pixabay.com
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The rapid evolution of technology has steered in an era where the integration of cyber-physical systems (CPS) with energy management is redefining how we approach energy consumption and distribution. As cities grow smarter and industries become increasingly interconnected, the need for efficient, reliable, and secure energy systems has never been more critical. This book explores the multifaceted landscape of energy management in cyber-physical environments, focusing on the interplay between control systems, smart grids, and the Internet of Things (IoT). The rise of explainable AI technology further enhances these systems by providing transparency in decision-making processes, making it easier for stakeholders to understand and trust AI-driven recommendations. Through a comprehensive analysis of these topics, we aim to provide readers with a deeper understanding of how cyber-physical systems can transform energy management practices. From the implementation of adaptive power system resource management to the exploration of user interfaces in smart cities, our goal is to highlight the innovative approaches shaping the future of energy consumption. In summary, this book serves as a guide for researchers, practitioners, and policymakers eager to navigate the complexities of energy management in cyber-physical systems. By embracing the synergy between technology and energy, we can forge a sustainable future that prioritizes efficiency, reliability, and security.

1

Cyber-Physical Systems: A Control and Energy Approach

Shaik Mahaboob Basha[1], Gajanan Shankarrao Patange[2], V. Arulkumar[3]*, J. V. N. Ramesh[4] and A. V. Prabu[5]

[1]Electronics and Communication Engineering, N.B.K.R. Institute of Science and Technology, Vidyanagar, Tirupati, Andhra Pradesh, India
[2]Mechanical Engineering, CSPIT–Chrusat, Charotar University of Science and Technology, Charusat Campus Changa, Anand, Gujarat, India
[3]School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
[4]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
[5]Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India

Abstract

Cyber-physical systems (CPS) combine analogue and digital components to interact with the real world and are crucial to business and industry, including infrastructure like energy systems. Due to their critical nature, CPS is vulnerable to cyber-attacks, particularly phishing software that can impair their functionality. Attacks on CPS, especially on mission-critical components like energy distribution networks, can have severe consequences. To improve CPS protection, a technology demonstrator can replicate CPS behavior and identify vulnerabilities and protection mechanisms. A scenario modeling technique can accurately depict CPS components, relationships, attackers, access points, and network attacks. Risk modeling can outline the necessary resources to replicate CPS and generate large representations to assess network efficiency. The methodology includes evaluating the network using specific indicators, prioritizing cyber-attack prevention based on their impact on system function, and analyzing and preventing attacks using four example patterns that targeted CPES. This article aims to provide a staged

**Corresponding author*: arulkumar.v@vit.ac.in

Shrddha Sagar, T. Poongodi, Rajesh Kumar Dhanaraj and Sanjeevikumar Padmanaban (eds.) Cyber Physical Energy Systems (1–36) © 2025 Scrivener Publishing LLC

process for conducting in-depth security evaluations that result in a safer and more durable CPS.

***Keywords*:** Cyber-physical systems, energy systems, technology, CPES, network's efficiency and risk analysis

1.1 Introduction

1.1.1 Background and Motivation

Energy systems have transitioned over the last few years from a single-directional production and dissemination system to an amplified distributed structure that supports both conventional sources of energy and distributed generation in the form of centralized generation, like wind and solar power, and distributed storage, like energy storage devices and energy storage systems by thermal means. The advancement of communications and information technologies, electronic control networks, environment monitoring, and integrated industrialized IoT technologies has largely made it possible for EPS to be transformed into CPES. The National Institute of Standards and Technology recognizes "designs that include electronic, analog, and hardware elements." The characteristics of the network and the rules that govern its functioning define these parameters. By smoothly merging material objects with social, electronic, and connectivity elements meant to function via integrative physics and analytical reasoning, CPES are powerful complex systems revolutionizing the way conventional EPS functions. As a result, CPES contributes significantly to the transformation of EPS by enabling effective organization, more adaptable oversight, cyber-secure operational processes, framework efficiency, reconfigurable power generation (TES), and advancements in voltage stability, reliability enhancements, toughness, interconnectivity, and relatively clean energy production. Controlling and retaining protected access to critical framework resources and functions (for CPES: gen console deposits, recurrence consistency restrictions, power cable safeguards, and so on) as well as maintaining the confidentiality, ease of access, and truthfulness of the information being presented (for example, regulating the sequence of oversight monitoring and data procurement) pose significant challenges to CPES stability. As a huge development network of systems, CPS uses a variety of computer elements, including smart electronic devices, programmable controllers, and remote terminal modules, many of which were not created with safety in mind. Such gadgets' architecture, firmware, and networking technology are often created using commercially available parts. As a result,

flaws in such elements may be transferred to the CPS environment, potentially opening the door for nefarious adversaries seeking to disrupt CPS operations. In April 2019, a notification of a suspicious occurrence involving hostile conduct directed toward CPS operations was made.

The assailants used a recognized CPES weakness, specifically a web application firewall gap, to access one of the developed countries' grid structures and launch a cognitive dissonance assault. The assault led to a communication issue here between the system for energy management and the facility's generating units, which briefly disrupted operations. There is an increase in unauthorized access via hacking, with attackers exploiting current and reported flaws to breach CPS. In 2020, "98% of the holes accessed are known to safety specialists, while not a day's worth of faults constitute just 0.5% of the responsibility exposed throughout the last decades," according to international security. This statistic provides proof of this. The assailants may be persuaded to violate these networks in order to gain monetary or political gain because of the significance of CPS and CPES, specifically for productivity expansion and population health at the global, regional, and micro levels.

Therefore, it is crucial to assess the CPES' stability and resistance to assaults in actual settings. In addition, since EPS—also known as the "biggest networked mechanism on the ground" [1]—integrates the impact of cyber across all sectors and sizes, the assessment of cyber threats becomes increasingly complicated and difficult. Sincerely, EPS activities might be understood by simulating certain unusual activities (such as failures, unbalanced voltage situations, frequency variations, etc.). To capture the nonlinear response of these standardization processes, increasingly precise descriptions and depictions are needed given the recent advancements toward smart and linked CPES. The improvement of CPES integrity and dependability necessitates the ongoing exploration of possible vulnerabilities [2]. The concept of security must take into account the CPES structure's characteristics in extensive testing settings that permit the interface of hardware components that are intended to function in the "actual" network. Equipment (HIL) hardware platforms are useful in this situation because they provide testing procedures for determining how well physical and digital components are working together in limited circumstances.

In order to conduct cyber resilience and assess the consequences, recognize security weaknesses across numerous levels (e.g., memory modules, system software, applications, procedures, and methods), incorporate detection mechanisms and preventative measures algorithms, and evaluate the effectiveness of countermeasures without posing an undue financial burden or safety risks, protection HIL configurations are essential [3].

This article's main goal is to provide a methodology that integrates conceptual and framework protection research studies, assessing CPS system behavior using testing ground settings and ultimately resulting in much more secure CPES designs. Assessment and experimentation research projects must be characterized and modeled, taking into account both the virtual and physical domains, in order to enable functional prototypes to accurately represent the features of the malware context. The research papers must provide thorough explanations of the tools and indicators that will be used to assess the effectiveness, dependability, and durability of the CPES. The evaluation configuration should also record the opponent's vulnerability assessment attributes and the assault strategy. Threat modeling attributes for a possible enemy include antagonistic information, finances, the system's access, and precision. Risk evaluation features for the attacking approach comprise offensive incidence, repeatability, and search capabilities, points in different targeted resources, attacker tactics, and foundation. Experts and interested parties may completely evaluate and identify potential threats present in the CPES under assessment by performing this task in a comprehensive and methodical manner.

1.1.2 Testbeds, Revisions, and a Safety Study for Cyber-Physical Energy Systems

This section describes the many CPES test chambers created by various research organizations and lists the tools used to carry out their research purposes.

We outline various types of CPES development studies seen in the field and discuss well-known examples from each. Additionally, we examine how vulnerability definition, prevention, and mitigation approaches may assist vulnerability analyses by identifying, avoiding, and reducing threats.

1.1.3 CPES Test Chamber

EPS have been built and modeled over the years using transversal topologies in which electricity is generated at massive mass energy plants and then transferred to users via various transmitting and circular delivery networks. The integration of renewable energies (RES) with distributed generation resources (DERs) required little effort [4]. Nevertheless, as RES and DER adoption rise and the grid is modernized using ICT, the intricacy of EPS also increases. In contrast, RES and DERs can be applied to supply dependable, reasonably priced, and environmentally friendly power to

meet client demands. On the other hand, hackers may covertly implant their assaults on weak systems and equipment by making use of the fact that these capabilities are not generally regulated and are instead ultimately controlled by providers [5, 6]. Due to the complexity of the current EPS and the reliance of all these systems on ICT for inter-system interaction, there are several potential points of assault. Even if there is a clear need for safe and robust EPS, the problem is made worse by our lack of expertise working with and organizing such complex infrastructures. We lack the tools necessary to identify and lessen the effects of unforeseen unfavorable occurrences on the functioning of the power grid. The organization's reliance on CPES interconnectedness, the layout of its electricity monitoring system, regulation, and prediction techniques, which are highly secure, heavily depends on the presence of reflective structures where future security features and methods can be evolved and analyzed. In-depth system assessments may be carried out in a perfect setting on CPES functional prototypes without affecting the true power system. When transferring particular processes to the real system, test chambers are used to minimize the risk and eliminate any possible negative effects. The verification and influence assessment of new EPS hardware (such as the assimilation of PV centres, infrastructure for EV recharging, etc.), updated tactics (such as the prioritization of electricity conveyance among RES, DER, or other sources of energy generation), as well as remediation techniques for unforeseen events (such as flaws, mechanical failures, cyber threats, etc.) are a few examples of these processes. Figure 1.1 shows the primary design components of such computer network testbeds. The following is a list of potential protection activities that might be carried out on CPES testbeds:

- Teach partners and clients in a replicated or modeled CPES scenario.
- Assess the functionality of process standardization comprehensively, that is, from the smallest operating levels (such as sensors, controllers, processes, etc.) to the top levels, such as remote monitoring and control.
- Create and evaluate cyber-physical measurements and assess the security of the system.
- Test new security technologies, including data encryption, access control, and systems that detect and prevent intrusions (IDS/IPS).
- Assess the effect of assaults on the EPS's physical and virtual realms.

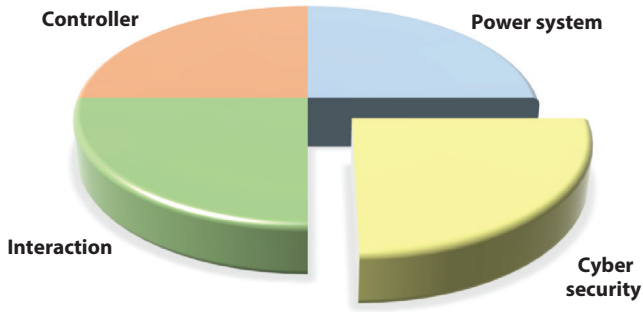


Figure 1.1 Cyber-physical test chamber constituents for the EPS study.

- Analyze the success of preventive tactics for negative cyber-physical occurrences.

1.1.4 Significance and Contributions of Testbed

Numerous institutions and established labs have created internal testbeds for study as well as for education and instruction due to the significance of vulnerability investigations for CPS and vital CPES facilities [7]. Various testbeds have been created and put into use based upon the request area with study purpose. The true modeling CPS testbeds that are now accessible are listed in Table 1.1 besides their unique capabilities. Our classification of technological testbeds takes into account factors such as structure, cost, and dependability. We also provide a thorough breakdown of the variations among intrusion detection and prevention and software-aided test environments. Equipment-oriented trial runs are intended to formally examine CPS and often include a number of real-world physical elements—for instance, CPES equipment-oriented testbeds include actual hardware like generators, switches, switchgear, ESS, photovoltaic systems, wind generators, etc. These testbeds enable contributors to (i) make decisions based on pragmatic experiments rather than theoretical assessments, (ii) analyze CPS behavior under abnormal conditions to demonstrate the potential without interfering with the proper machine's procedure, and (iii) predict cyberattacks or malfunction remediation and statistically control. However, device-oriented testbeds have three major drawbacks, namely: (i) they are not inexpensive because the testbed elements must match the actual hardware used on the ground, (ii) after the device and testbed setups are set up, any change or augmentation of the network infrastructure can either take a significant amount of time or be virtually and financially impractical,