
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

© 2025 Scrivener Publishing LLC

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

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>.

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.

Limit of Liability/Disclaimer of Warranty

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. 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. 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.

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	xxi
1 Cyber-Physical Systems: A Control and Energy Approach	1
<i>Shaik Mahaboob Basha, Gajanan Shankarrao Patange, V. Arulkumar, J. V. N. Ramesh and A. V. Prabu</i>	
1.1 Introduction	2
1.1.1 Background and Motivation	2
1.1.2 Testbeds, Revisions, and a Safety Study for Cyber-Physical Energy Systems	4
1.1.3 CPES Test Chamber	4
1.1.4 Significance and Contributions of Testbed	6
1.1.5 Testbed Setup	8
1.1.6 Illustration of Hybrid CPES Testbed Structure	9
1.2 Studies on CPES Safety	10
1.2.1 Attacks in the CPES System	11
1.2.2 Evaluation of Attack Impacts on CPES	12
1.2.3 CPES's Assault Detection Algorithms	13
1.2.4 CPES's Assault Mitigation and Defense Systems	14
1.2.5 Dangerous Imagery	15
1.2.6 Attack Database	17
1.3 Threat Evaluation	18
1.4 Theory of Cyber-Physical Systems Risk	20
1.4.1 Challenger Type	20
1.4.2 Attack Type	20
1.5 Threat Evaluation Methodology	22
1.5.1 Cyber-System Layer	25
1.5.2 Physical-System Layer	27
1.6 Experimental Setup for Cross-Layer Firmware Threats	28
1.6.1 Risk Model	29
1.6.2 Threat Evaluation	33
1.7 Conclusion	33
References	35

2	Optimization Techniques for Energy Management in Microgrid	37
	<i>Shenbaga Bharatha Priya A., Indra Singh Bisht, N. Balambigai, Sumit Kataria and R. Ramalakshmi</i>	
2.1	Introduction	38
2.1.1	Microgrid Systems	40
2.1.2	Energy Management System	41
2.1.3	Energy Management of Distribution System	42
2.1.4	Techniques to Take Into Account While Implementing the EMS	43
2.1.5	Strategies for Reducing Risk	43
2.1.6	Monitoring Power Systems	49
2.1.7	Demand Response, Price Strategy, and Demand Side Management	50
2.2	Explanation Methods for EMS	55
2.3	EQN EMS on an Arithmetic Optimization Basis	57
2.4	Heuristic-Oriented Methods to EMS Problem-Solving	60
2.5	EMS Solution Techniques Using Meta-Heuristics	60
2.6	Alternative EMS Implementation Strategies	62
2.6.1	SCADA System	63
2.7	Conclusion and Viewpoints	67
	References	68
3	Cyber-Physical Energy Systems for Smart Grid: Reliable Distribution	71
	<i>Jyoti Parashar, A. Devipriya, R. Lokeshkumar, J.V.N. Ramesh and Arindam Pal</i>	
3.1	Introduction	72
3.1.1	Need for Sustainable and Efficient Power Generation Through Smart Grid Technology and Cyber-Physical Technologies	72
3.1.2	CPES: The Integration of Physical and Digital Worlds	73
3.2	Cyber-Physical Energy Systems (CPES)	74
3.3	Forming Energy Systems	76
3.4	Energy Efficiency	77
3.4.1	CPES Usage on Smart Grids	78
3.5	Smart Grids	79
3.6	Cyber-Physical Systems	81
3.7	SG: A CPS Viewpoint	84
3.7.1	Challenges and Solutions for Coordinating Smart Grids and Cyber-Physical Systems	85
3.7.2	Techniques of Correspondence	87

3.7.3	Data Protection	88
3.7.4	Data Skill and Engineering	89
3.7.5	Distributed Computation	90
3.7.6	Distributed Intellect	91
3.7.7	Distributed Optimization	92
3.7.8	Distributed Controller	92
3.8	Upcoming Prospects and Contests	93
3.8.1	Big Data	95
3.8.2	Cloud Computing	96
3.8.3	IoT	97
3.8.4	Network Science	98
3.8.5	Regulation and Guidelines	99
3.9	Conclusion	100
	References	101
4	Evolution of AI in CPS: Enhancing Technical Capabilities and Human Interactions	103
	<i>Namya Musthafa, P. Suresh and Yazid Musthafa</i>	
4.1	Introduction to Cyber-Physical System	104
4.2	The Cyber-Physical Systems Architecture	105
4.2.1	5C Architecture or CPS	106
4.2.1.1	Connection	107
4.2.1.2	Conversion	107
4.2.1.3	Cyber	107
4.2.1.4	Knowledge	108
4.2.1.5	Configuration	108
4.3	Cyber-Physical Systems as Real-Time Applications	109
4.3.1	Robotics Distributed	109
4.3.2	Manufacturing	110
4.3.3	Distribution of Water	110
4.3.4	Smart Greenhouses	111
4.3.5	Healthcare	111
4.3.6	Transportation	112
4.4	Impact of AI on Cyber-Physical Systems	114
4.5	Policies	116
4.6	Expected Benefits and Core Promises	117
4.7	Unintended Consequences and Implications for Policy	118
4.7.1	Negative Social Impacts	119
4.7.2	Cybersecurity Risks	119
4.7.3	Impact on the Environment	120
4.7.4	Ethical Issues	121

4.7.5	Policy Implications	122
4.8	Employment and Delegation of Tasks	123
4.9	Safety, Responsibility, and Liability	123
4.10	Privacy Concerns	124
4.10.1	Data Collection and Use	124
4.10.2	Data Security	125
4.10.3	Data Sharing	125
4.10.4	Bias and Discrimination	126
4.10.5	User Empowerment	126
4.11	Social Relations	127
4.11.1	Cyber-Physical Systems and Transport	127
4.11.2	Trade of Dual-Use Technology	128
4.11.3	Civil Liberties (Data Protection, Privacy, etc.)	128
4.11.4	Safety (Such as Risk Analysis, Product Safety, etc.)	129
4.11.5	Healthcare (Medical Devices, Clinical Trials, and E-Health Devices)	131
4.11.6	Energy and Environment	132
4.11.7	Horizontal Legal Issues (Cross-Committee Considerations)	133
4.12	Economic Study on CPS	133
4.12.1	Better Resource Allocation	134
4.12.2	Enhanced Marketability	135
4.12.3	Robustness and Resilience	135
4.12.4	Regulatory Compliance	136
4.12.5	Making Decisions in Real-Time	136
4.13	Case Studies	137
4.13.1	The Daily Lives of Older Persons and Disabled Individuals with CPS	138
4.13.2	CPS in Healthcare	140
4.13.3	CPS for Security and Safety	142
4.14	Conclusion	143
	References	143
5	IoT Technology Enables Sophisticated Energy Management in Smart Factory	147
	<i>Deependra Rastogi, Prashant Johri, Swati Verma, Vanita Garg and Hradesh Kumar</i>	
5.1	Introduction	148
5.2	IOT Overview	151
5.2.1	The Evolution of the Internet	152
5.2.2	IoT Sensing	153

5.2.3	IOT Data Protocol and Architecture	154
5.3	IOT Enabling Technology	156
5.3.1	Application Domain	157
5.3.2	Middleware Domain	158
5.3.3	Network Domain	159
5.3.4	Object Domain	160
5.4	IOT in Energy Sector	160
5.4.1	Internet of Things and Energy Generation	161
5.5	Challenges of Applying IOT	164
5.6	Reference Architecture for IoT-Based Smart Factory	164
5.7	Characteristics of Smart Factory	168
5.8	Challenges for IoT-Based Smart Industry	169
5.9	How IoT Will Support Energy Management in Smart Factory	170
5.10	IoT Energy Management Architecture for Industrial Applications	171
5.10.1	IoT-Based Energy Management Technology	172
5.10.2	Energy Harvesting	174
5.11	Case Study: Smart Factory	174
5.11.1	Supply Side	175
5.11.2	Photovoltaic Power Generation	175
5.11.3	Smart Micro-Grid	176
5.11.4	Demand Side	177
5.11.5	Virtualization	177
5.12	Conclusion	177
	References	178
6	IOT-Based Advanced Energy Management in Smart Factories	183
	<i>M. Nalini, Dhanashree Varadharajan, Nithyashree Natarajan and Yogabhuvaneswari Umasankar</i>	
6.1	Introduction	184
6.2	Smart Factory Benefits of IOT-Based Advanced Energy Management	185
6.3	Role of IOT Technology in Energy Management	186
6.4	Developing an IOT Information Model for Energy Efficiency	186
6.5	Integrating Intelligent Energy Systems (IES) and Demand Response (DR)	187
6.6	How to Accurately Measure and Manage Your Energy Usage	187
6.7	Introduction to Energy Efficiency Measures	188
6.8	Identifying Opportunities to Reduce Energy Use	188
6.9	Monitoring and Measuring Energy Usage	189

6.10	Establishing Accounting and Incentives	190
6.11	Sustaining the Long-Term Benefits of Optimized Energy Usage	190
6.12	Role of Cyber Security When Implementing IoT-Based Advanced Energy Solutions	191
6.13	Materials Required in Smart Factories	192
6.14	Methods in IoT-Based Smart Factory Implementation	197
6.15	Steps for Developing an IoT-Based Energy Management System	204
6.15.1	Assess Current Energy Usage	204
6.15.2	Develop an Energy Conservation Plan	204
6.15.3	Implement IoT Technology	204
6.15.4	Monitor Results	204
6.16	Challenges For Adopting IoT-Based Energy Management Systems	205
6.16.1	Big Data and Analytics	205
6.16.2	Connectivity Constraints	205
6.16.3	Data Security and Privacy Issues	205
6.16.4	Device Troubleshooting	205
6.17	Recommendations for Overcoming the Challenges With Implementing IoT-Based Advanced Energy Solution	206
6.17.1	IoT-Enabled Automation	207
6.17.2	Smart Sensors	207
6.17.3	Predictive Analytics	207
6.18	Case Studies	207
6.18.1	Automated Demand Response (ADR)	207
6.18.2	Automated Maintenance	208
6.18.3	Predictive Analytics	208
6.19	Case Studies for Successful Implementation	208
6.20	Applications	208
6.21	Different Techniques for Monitoring and Control of IoT Devices	212
6.22	Literature Survey	212
6.23	Conclusion	215
	References	215
7	Challenges in Ensuring Security for Smart Energy Management Systems Based on CPS	217
	<i>V. M. Meera and K. P. Arjun</i>	
7.1	Introduction	218
7.1.1	Brief Overview of Smart Energy Management Systems and Cyber-Physical Systems	218

7.1.2	Importance of Security in CPS-Based Smart Energy Management	219
7.2	Cyber-Physical Systems and Smart Energy Management	220
7.2.1	CPS Architecture and Components	220
7.2.2	Types of CPS-Based Smart Energy Management Systems	223
7.2.3	Common Communication Protocols Used in CPS-Based Smart Energy Management	228
7.2.4	Cyber Security Threats in CPS-Based Systems	232
7.3	Security Challenges in CPS-Based Smart Energy Management	235
7.3.1	Cyber Security Threats to CPS-Based Smart Energy Management Systems	237
7.3.2	Vulnerabilities of Communication Protocols Used in Smart Energy Management	241
7.3.3	Attack Vectors for Compromising CPS-Based Smart Energy Management Systems	243
7.4	Cyber Security Standards and Guidelines for Smart Energy Management	247
7.4.1	Cyber Security Incidents in Smart Energy Management	251
7.5	Conclusion	252
	References	253
8	Security Challenges in CPS-Based Smart Energy Management	255
	<i>Lucia Agnes Beena T., Vinolyn Vijaykumar and Mercy P.</i>	
8.1	Introduction	256
8.2	CPS Architecture	257
8.3	The Driving Forces for CPS	262
8.3.1	Big Data	262
8.3.2	Cloud	262
8.3.3	Machine-to-Machine Communication and Wireless Sensor Networks	263
8.3.4	Mechatronics	263
8.3.5	Cybernetics	264
8.3.6	Systems of Systems	264
8.4	Advances in Cyber-Physical Systems	265
8.4.1	Application Domains of CPS	265
8.4.1.1	Industrial Transformation	265
8.4.1.2	Smart Grid	266
8.4.1.3	Healthcare	267

8.4.1.4	Smart Parking System	268
8.4.1.5	Household CPS	269
8.4.1.6	Aerospace	269
8.4.1.7	Agriculture	270
8.4.1.8	Construction	270
8.5	Energy Management through CPS	271
8.5.1	Energy Management of CPS for Smart Grid	272
8.5.2	Energy Management of CPS for Smart Building Structure	273
8.5.3	Energy Management of CPS for Autonomous Electric Vehicles in Smart Transportation	274
8.5.4	Energy Management of CPS for Smart Industry	275
8.5.5	Energy Management of CPS for Home Automation	276
8.6	Security Issues in CPS	277
8.6.1	Threats	278
8.6.1.1	Cyber Threats	278
8.6.1.2	Physical Threats	279
8.6.2	CPS Vulnerabilities	280
8.6.3	CPS Attacks	280
8.6.4	CPS Failures	280
8.6.5	Risk Identification and Management	281
8.6.6	Protecting CPS	281
8.6.7	Security Solutions for CPS	282
8.7	Open Challenges and Future Directions	283
8.7.1	Open Challenges	284
8.7.1.1	Infrastructure Challenges	284
8.7.1.2	Network Communication Challenges	284
8.7.1.3	Control Operational and Computational Challenges	285
8.7.1.4	CPS Deployment Challenges	285
8.7.2	Future Directions	285
8.8	Conclusion	286
	References	287
9	Blockchain-Based Energy Transmission System: Design, Optimization, and Data-Driven Modeling	291
	<i>Prabha Selvaraj, Rohit Kumar Das, Vijay Kumar Burugari, Ganesh Reddy Karri, Kanmani P. and Anupama Namburu</i>	
9.1	Introduction	292
9.2	Literature Review	294
9.2.1	Essential Parts of a Blockchain Include	296

9.2.2	Blockchain and Smart Agreements	300
9.2.2.1	Blockchain 3.0 Scalability and Interoperability	301
9.2.2.2	Interoperability	302
9.2.2.3	Blockchain 4.0 Scalability	302
9.2.2.4	Energy Efficiency	303
9.2.2.5	Possible Solutions	303
9.3	Case Study and Application	304
9.3.1	Energy Transmission Monitoring with Advanced Metering Infrastructure	311
9.3.2	Energy Optimization with Home Automation	312
9.3.3	Renewable Microgrids	312
9.3.4	Blockchain for Electric Vehicles	314
9.4	Conclusion	317
	References	317
10	Explainable AI Technology in E-CPS: Policy Design, Economic Research, and Case Studies	325
	<i>Thangaraja Arumugam, Saritha Bantu, Yeligeni Raju, Renuka Deshmukh and B. Raja Mannar</i>	
10.1	Introduction	326
10.1.1	Terminology	326
	Nomenclature	326
10.2	E-CPS Arrangement	327
10.2.1	E-CPS Framework	328
10.3	Case Study: Method Depiction	329
10.3.1	Fixing Constraints	330
10.3.2	Information Preparation	330
10.3.3	Prediction Framework	331
10.3.4	Controlling Approach	332
10.3.5	Result Analysis	334
10.3.6	Overview	334
10.4	Transformation of the Power Infrastructure	335
10.4.1	Cyber-Physical System	336
10.4.2	Power Effectiveness—Cumulative Power Efficacy	339
10.5	Power Managing Structures	341
10.5.1	Following that are Some Notable Instances of How CPS Affects Power Sources	343
10.5.2	Data Analysis	346
10.5.3	Utilising Agent-Based Modelling and Linear Optimization for Improved Urban Planning	346

10.5.4	Enhancing Compatibility and Utilization of e-CPS Components for Improved Administration of Commercial Structures	347
10.5.5	e-CPS Effects on the Power Change	348
10.5.6	Policies Involved and Economics Research	349
10.6	Protection Policies	350
10.7	Urgent Need for Effective Governance of AI and e-CPS	351
10.8	Conclusions	352
	References	354
11	Infrastructural Data Visualization and Improved User Interfaces of Energy Consumption in Smart Cities	357
	<i>Prabha Selvaraj, Kanmani P., T.Y.J. Naga Malleswari, Vijay Kumar Burugari and S. Sudheer Mangalampalli</i>	
11.1	Introduction	358
11.1.1	Internet of Things (IoT)	360
11.1.2	Big Data	360
11.1.3	Cloud Computing	361
11.1.3.1	Infrastructure in Smart City	361
11.1.3.2	Types of Smart Infrastructure	362
11.1.4	Issues with Smart City Infrastructure	363
11.1.4.1	Organizational Issues	363
11.1.4.2	Data Quality and Collection Issues	363
11.1.4.3	Governance and Privacy Issues	364
11.1.4.4	Maintenance and Durability	364
11.2	Literature Review	364
11.3	Visualization Tools and Interfaces Used in Smart Cities Using IoT	367
11.4	Energy Representation Frameworks	368
11.5	Materials and Methods	369
11.5.1	Smart Cities and Energy Consumption	369
11.5.1.1	Active Approach	371
11.5.1.2	Passive Approach	371
11.5.2	Importance of Energy-Efficient in Sustainable Buildings	371
11.5.3	Energy Consumption and Management in Smart Cities	375
11.5.4	Materials and Strategies	379
11.5.4.1	Requirements and Work Processes	379
11.5.4.2	Data Collection	380

11.5.5	Visual Encoding and Communication Plan	381
11.5.5.1	Map and Local Area Wayfarer	381
11.5.5.2	Scatterplot and Examination Diagram	382
11.6	Case Study and Applications	384
11.6.1	Functionalities of the Energy Hub Platform	384
11.6.1.1	Mechanisms of the Energy Conservation for Smart Cities	385
11.6.1.2	Smart Electricity Grids for Smart Cities	385
11.6.1.3	Data Visualization and Its Importance in Smart Cities	387
11.6.1.4	Security Challenges in Smart City	387
11.6.1.5	Smart Transportation and Smart Traffic Management	388
11.6.1.6	Domestic Renewable Energy System Integration in Cities	389
11.7	Factors for the Improvement of Energy Efficacy in Smart Cities	389
11.7.1	Prediction of Electrical Consumption in Smart Cities	389
11.8	Conclusion and Future Scope	391
	References	391
12	Power Management in Intelligent Buildings Based on Daily Demand Prediction	399
	<i>V. Geethapriya, D. Sivamani, D. Shyam, A. Sangari, M. Manish, Prasheetha and Divina Julia</i>	
12.1	Introduction	399
12.1.1	Summary from Introduction	401
12.2	The Power Management System Block Diagram	401
12.3	Working Task of Power Management System	405
12.4	Simulation Model of Power Management System	406
12.5	Hardware Implementation of Power Management System	408
12.6	Safety Precautions in Smart Building Implementation	411
12.7	Conclusion	412
	References	413
13	Schemes and Security Attacks on the Integrity of Cyber-Physical Systems in Energy Systems	415
	<i>Rajesh Kumar, Charanjeet Singh, Yeligeti Raju, Pratap Patil and K. Saravanan</i>	
13.1	Introduction	416

13.1.1	CPS Protection Purposes	416
13.1.2	Confidentiality	417
13.1.3	Authenticity	418
13.1.4	Accessibility	418
13.1.5	Resilience	419
13.1.6	Trustworthiness	419
13.2	CPS Safety Methodologies	420
13.2.1	Threat Categorisation	420
13.2.2	Spying	420
13.2.3	Sneaky Deceit Assault	421
13.2.4	Attack Using a Vulnerable Key	421
13.2.5	Assault on the Centre Spy	421
13.2.6	Jamming Assault	421
13.2.7	Replay Attack	421
13.2.8	Refusal of Package Assault	421
13.2.9	Assault Demonstrating	422
13.2.10	Assault Sensing	422
13.2.11	Safety Resolutions	423
13.2.12	Construction and Designing for Protection	423
13.2.13	Safety in Definite CPS	424
13.2.14	Energy System Safety	424
13.2.15	Medicinal CPS Safety	424
13.2.16	Portable CPS Safety	425
13.2.17	Motorised CPS Safety	426
13.3	Shielding in Contradiction of Information Safety Assaults	426
13.3.1	Enhancing Data Security in the Electricity System Through a Markov Decision Process (MDP)	427
13.3.2	Evaluating the Effectiveness of a Determination Method for Data Security Assaults in Power Systems	428
13.4	Scheme Variants	428
13.4.1	Assault Variant	430
13.5	Supervised Learning in Depth	431
13.5.1	DQND Scheme	432
13.5.2	Assault Situations	432
13.5.3	Markov Resolution Concepts	434
13.5.4	Assessment Spatial and Sliding Windows Measurements	436
13.5.5	DQND Scheme	436
13.5.6	System Education	437
13.5.7	Efficiency Assessment	438

13.5.8	Algorithm 1: Education Phase of DQND	439
13.5.9	Algorithm 2: Evaluation Phase of DQND	440
13.5.10	Assessment Metrics	440
13.5.11	Standards	441
13.6	Discussion	441
13.7	Conclusion	442
	References	443
14	Adaptive Power System Resource Management in Cyber-Physical Energy Systems	445
	<i>Virendra Singh Kushwah, Indra Singh Bisht, Charanjeet Singh, K. Gurnadha Gupta and K. Suresh</i>	
14.1	Introduction	446
14.1.1	Modelling and Simulation of CPES for Integrating Data Networks with Electricity Networks	447
14.1.2	Actual-Period Energy Network Modelling and Simulation using RTLAB and OPNET Modeller with SITL Integration	447
14.1.3	Cyber Attack on Ukraine's Power Grid in 2015: Incident Overview and Implications for Critical Infrastructure Security	448
14.1.4	CPES Sensitivity Evaluation Process Utilising Virtualized CP Linkages	449
14.2	CPES Structures	450
14.2.1	Diversified	451
14.2.2	Self Determination	451
14.2.3	Actual Period	451
14.2.4	Reconstitute	452
14.2.5	Consistency	452
14.2.6	Intensely Encapsulated	452
14.3	Development of CPES Structures	452
14.3.1	Assistances of Cyber-Physical Energy System	454
14.3.2	CPES Difficulties	454
14.3.3	CPES Forming	455
14.3.4	Computer Estimation of the Variability of the Network	455
14.4	Resource Management in Socio-CPS	456
14.5	Associated Study	456
14.5.1	Assessment of CP Multilateral Implications	457
14.6	The Integrated Modelling Platform for the CPES	458
14.6.1	Nodal Junction	459

14.6.2	PP Linkages	459
14.6.3	Nodal Junctions	459
14.6.4	CP Linkage	460
14.7	Assault from Without and Compounding Collapse	461
14.7.1	Procedure for Appropriate Load Diminishment	462
14.8	The Combination of Assault and Defence	463
14.8.1	Issues with Bi-Level Computing	463
14.8.2	Defence of Resource Allocation	464
14.8.3	Methodology for Security Testing	467
14.9	Case Studies	467
14.10	Conclusions and Future Work	473
	References	474
15	Cyber-Physical Energy Systems for Electric Vehicles	477
	<i>ShaikMahaboob Basha, Akilandeswari P., Suguna M., Prakash D., Biruntha S. and Vivekanandan P.</i>	
15.1	Introduction	478
15.1.1	Smart-Use CPESs of Emerging Technologies for Sustainable Energy Solutions	478
15.1.2	Technology for Power Storage and Fuel Cells for CPES in EVS	479
15.1.3	Vehicle Cyber-Physical Energy Systems: Problems and Implications	480
15.1.4	Electric Drive-Train	481
15.1.5	Managing Storage Units (Batteries)	481
15.1.6	Dispersed Managing Batteries	482
15.2	Suggested Type	482
15.2.1	Activity Tracking Technique Deployment in CPES Using Electro-Mechanical Connections	483
15.2.2	MPSSU uses Ultra-Capacitors for Higher Energy Distribution and Rapid Power Outages	488
15.3	Outcomes from Experiments and Simulations	489
15.3.1	Modeling the DC Bus Network for SCPEDS Using the Port-Hamiltonian Approach	489
15.3.2	Electric Vehicle Energy Conversion and Inversion Simulation using the PSIM Program	491
15.3.3	Additional Energy Management Techniques Explored in Studies	493
15.4	Discussion	495
15.4.1	Power-Controlling and Autonomous Vehicle Diagnosis Using Genetic Algorithms (GAs)	495

15.5	Conclusion	497
	References	498
16	Design and Implementation of IoT-Based Advanced Energy Management System for Smart Factory	501
	<i>S. Jayanthi, N. Suresh Kumar, Zafar Ali Khan N., S. Sreenatha Reddy, R. Santhosh and Pachipala Yellamma</i>	
16.1	Introduction	502
16.1.1	Driving Factors	503
16.1.2	Industry 5.0	504
16.1.3	Smart Metres	505
16.2	Challenges Faced by Factories Today	506
16.2.1	How Do Businesses Try to Get Over the Obstacles That Exist in Their Manufacturing Plants?	506
16.2.2	Prospects of Industrial IoT	507
16.2.3	Impact of IoT on Smart Factories	507
16.3	Home Energy Management Systems (HEMSs)	509
16.4	Micro Grid for Integration of Several Sources and Storage	510
16.4.1	Deming Cycle	512
16.4.2	Setbacks of Effective Smart Energy Systems	514
16.4.3	Essential Sensing Technologies in Smart Factories	514
16.4.4	Four Cognitive Facets Define a Smart Factory	516
16.4.5	Reasons Why Industries Need to Fully Utilise IoT's Benefits	518
16.5	Proposed Robust Energy Management System for Smart Factories	521
16.6	Conclusion	523
16.7	Future Trends	524
	References	525
	Index	529

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.

Cyber-Physical Systems: A Control and Energy Approach

Shaik Mahaboob Basha¹, Gajanan Shankarrao Patange², V. Arulkumar^{3*},
J. V. N. Ramesh⁴ and A. V. Prabu⁵

¹*Electronics and Communication Engineering, N.B.K.R. Institute of Science and Technology, Vidyanaagar, 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

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.

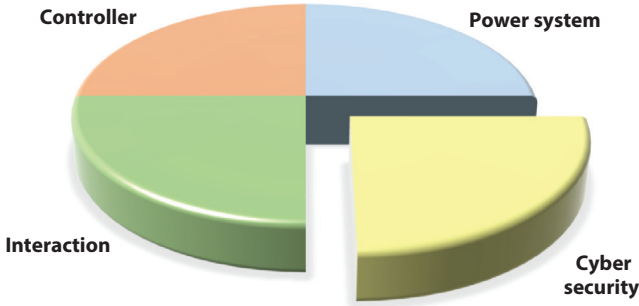


Figure 1.1 Cyber-physical test chamber constituents for the EPS study.

- 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,