Cyber-Physical Security of Smart Power and Integrated Energy Systems Using A Novel Feasibility Area Approach

Ahmed Abdelaziz Sayed Abdelaziz

A dissertation submitted to the faculty of graduate studies in partial fulfillment of the requirements for the degree of doctor of philosophy

Graduate Program in
Electrical Engineering and Computer Science
Lassonde School of Engineering, York University
Toronto, Ontario, Canada

July 2026

© Ahmed Abdelaziz, 2026

Abstract

The global drive toward decarbonization has accelerated the transformation of conventional power systems into Smart Power Systems (SPSs), enabled by two tightly coupled developments: the large-scale integration of Renewable Energy Sources (RESs), Energy Storage Systems (ESSs), and flexible demand at the physical layer, alongside the deployment of advanced Information and Communication Technologies (ICT) for real-time monitoring, communication, and control at the cyber layer. The interaction of these layers gives rise to a Cyper-Physical Power System (CPPS), where physical and cyber processes are deeply interdependent. In parallel, increasing electrification has driven the development of Integrated Energy Systems (IESs), which couple power systems with gas, transportation, and heating networks. While this coupling improves operational efficiency and enables multi-energy optimization, it also significantly increases system complexity and enlarges the overall Cyber-Physical Systems (CPSs) risk surface. A key consequence of this evolution is that disturbances are no longer confined to a single domain but can propagate across interconnected infrastructures. Moreover, heterogeneous cybersecurity practices across sectors introduce uneven protection levels, creating exploitable vulnerabilities that further motivate the development of advanced security frameworks. The severity of this evolving threat landscape is reflected in recent sophisticated cyber-physical incidents, including the 2022 Sandworm campaign in Ukraine, which combined cyber intrusions with physical disruption. Such attacks exploit increasing system uncertainties arising from high penetration of RESs, emerging IES components such as Electric Vehicles (EVs), and the expanded reliance on ICT-enabled infrastructure. Collectively, these factors expose critical infrastructure to coordinated and multi-layered cyber threats, highlighting the urgent need for resilient and adaptive cybersecurity solutions.

To address these challenges, this thesis adopts a structured research methodology centered on: i) accurate modeling of CPPS and IES vulnerabilities; ii) analysis of the operational impacts of cyberattacks; iii) investigation of new vulnerabilities introduced by IES integration; iv) development of advanced Stealthy Infiltrated Cyber Attacks (SICAs) capable of bypassing existing defense mechanisms; v) assessment of current cybersecurity strategies; and vi) design of adaptive and resilient security solutions validated under both standalone SPS and interconnected IES environments. The primary objective is to strengthen the cyber-physical security of SPSs and IESs by developing a novel Feasibility Areas (FAs) framework that characterizes the normal operating region of Power System State Variables (PSSVs) and detects abnormal deviations under realistic operating conditions.

The research is organized into three main domains. The first focuses on standalone SPS security within a broader CPPS context. In this domain, a comprehensive testbed is developed that incorporates high penetration of RES and ESS, alongside layered cybersecurity mechanisms, in-

cluding Bad Data Detection (BDD), primary and secondary information protection layers, and integration with State Estimation (SE) and centralized Energy Management System (EMS) functions, forming a complete digital twin representation of the SPS. Within this environment, a new class of cyberattacks, referred to as SICAs, is introduced. These attacks are designed to bypass multi-layered defense systems. To counteract them, a novel FA-based detection framework is developed and embedded within the cybersecurity architecture to identify SICA at an early stage, preventing their propagation within the SPS.

Second, the scope is extended to IES, where a multi-energy testbed is developed by integrating power and gas transmission systems, power and transportation networks within distribution grids and Hydrogen Refueling Stations (HRSs), incorporating Power-to-X and X-to-P technologies such as Power-to-Hydrogen (PtH), Gas–fired Generation (GfG), and Hydrogen-to-Power (HtP). This domain examines a range of cyberattack models, including SICA targeting secondary information in power-gas IES, with a focus on coupling units and the propagation of disturbances from the gas network; stealthy False Data Injection Attacks (FDIAs) affecting power-transportation IES, particularly through manipulation of HRS related information; as well as Denial-of-Service (DoS) and coordinated bi-level Distributed Denial-of-Service (DDoS) attacks on EMS layers. Within this framework, the effectiveness of the proposed FA-based detector is evaluated, along with the required adaptations for operation in IES environments. The study further reinforces the detection framework by integrating a cyber-resilient EMS capable of operating under severe information loss, supported by Time Frequency Spectrum (TFS)-based forecasting using a Deep Neural Network (DNN), and convex HRS scheduling under high uncertainty conditions.

Third, the proposed FA-based framework is extended beyond attack detection to enable extraction of critical stealthy FDIAs characteristics, including attack localization and magnitude estimation. This is achieved by incorporating both spatial distribution and temporal correlation properties into the FA formulation, allowing a more informative representation of PSSV behavior under normal and compromised conditions. To further enhance real-time applicability, a recursive FA estimation algorithm is introduced. In this formulation, FA parameters are updated iteratively using previously estimated values, thereby reducing computational burden while preserving estimation accuracy. This recursive mechanism enables efficient adaptation to evolving system conditions and supports scalable deployment in large-scale SPS and IES environments.

Dedication

To my father and my mother,
to my wife; Aliaa and my daughter: Masah,
to my brothers: Mahmoud, Mohamed, and Ayman,
and to my friends and people helped me during my journey.

Acknowledgments

The journey toward earning a doctoral degree and completing this dissertation has been a truly enriching experience, marked by many joyful moments as well as a few challenging ones. This achievement would not have been possible without the contributions, assistance, and unwavering support of numerous individuals.

First and foremost, I would like to express my deepest and most sincere gratitude to my research supervisor, ***Prof. Hany E.Z. Farag***, for granting me the opportunity to conduct research under his supervision in the Smart Grid Lab. His invaluable patience, continuous guidance, and insightful advice have supported me throughout every stage of this dissertation.

I am also sincerely grateful to my doctoral committee members, ***Prof. Houshang Karimi*** and ***Prof. Afshin Rezaei***, for their constructive feedback and support throughout the Ph.D. milestones. I would also like to extend my appreciation to the ***defense committee members*** for generously sharing their knowledge and expertise. My thanks also go to the members of the EECS graduate office for their assistance with administrative and academic formalities.

I am thankful to my office mates in the Smart Grid Lab, ***Abdullah Hassan*** and ***Yahia Ahmed***, as well as my former colleagues ***Dr.Abdullah AlObaidi***, ***Dr.Nader El-Twaweel***, and ***Gouri Barai***, for their encouragement and moral support. I am particularly grateful to my post-doctoral fellow, ***Dr. Hadi Khani***, for the valuable discussions and for generously sharing his research experience, as well as to ***Abdullrhman Ayad*** for his support. My special and heartfelt thanks go to my sincere friends, ***Dr. Mohsen Khalaf*** and ***Dr. Muhammed Abo-Elhamd***, for their guidance and support during difficult times.

Last but certainly not least, I wish to express my deepest appreciation for the love and support of my parents, my wife, ***Aliaa Elkosy***, my daughter ***Masah***, and my beloved family, including ***My Father*** and ***My Mother*** and my brothers ***Mahmoud***, ***Mohammed***, and ***Ayman***. Their encouragement, patience, and unwavering belief in me sustained me throughout this journey, and this work would not have been possible without them.

Table of Contents

Abstract . . . . . **i**

Dedication . . . . . **iv**

Acknowledgments . . . . . **v**

Table of Contents . . . . . **vi**

List of Tables . . . . . **xii**

List of Figures . . . . . **xiii**

Acronyms . . . . . **xvii**

Nomenclature . . . . . **xix**

Chapter 1: Introduction **1**
1.1 Motivation 2
1.2 Research Gaps 5
1.2.1 Thesis Contribution 10
1.3 Thesis Organization and Layout 12

Chapter 2: Literature Survey **15**
2.1 Electric Power Systems 16
2.1.1 Generation Technologies: 17
2.1.2 Energy Storage Systems Technologies in Power System 18
2.1.3 Market Regulations and Demand Side Participation 20
2.2 Structure of Cyber-Physical Power System 21
2.2.1 Monitoring System and Advanced Metering Infrastructures 22
2.2.2 Central Control System Applications 24
2.2.2.1 Steady-State Operation 25
2.2.2.2 Dynamic Operation 27
2.2.3 Power System Control Elements and Actuators: 28
2.3 Structure of Integrated Energy Systems 29
2.3.1 Electric Smart Power System Model 31
2.3.2 Integrated Power and Transportation System 32
2.3.2.1 Energy Conversion Between Power and Transportation Using Node-Based Methods 34

2.3.2.2 Energy Conversion Between Power and Transportation Using Network Flow Models . . . 35
2.3.2.3 Cyber-Physical Layers of Integrated Power and Transportation System . . . 36
2.3.3 Integrated Power and Natural Gas System . . . 37
2.3.3.1 Energy Conversion Between Power and Gas Systems . . . 38
2.3.3.2 Cyber-Physical Layers of Integrated Power and Gas System . . . 39
2.3.4 Integrated Power and Heat System . . . 39
2.3.4.1 Energy Conversion Between Power and Heat Systems . . . 41
2.3.4.2 Cyber-Physical Layers of Integrated Power and Heat System . . . 41
2.4 Cyber-Physical Security Background and Taxonomy . . . 42
2.4.1 Cyber-Physical Incidents . . . 42
2.4.2 Cyber-Physical Attacks Taxonomies . . . 44
2.4.2.1 Threat Actors Taxonomy . . . 45
2.4.2.2 Cyber-Physical Attacks Domain Taxonomy . . . 46
2.4.2.3 Cyber-Physical Attacks Target Taxonomy . . . 47
2.4.2.4 Cyber-Physical Attacks Formulation and Model Taxonomy . . . 48
2.4.2.5 Cyber-Physical Attacks Impact Taxonomy . . . 50
2.5 Smart Power Systems Situational Awareness and State Estimation . . . 51
2.5.1 Role of State Estimation . . . 51
2.5.1.1 Hybrid Measurements State Estimation . . . 53
2.5.2 State Estimation of Integrated Energy Systems . . . 56
2.5.3 State Estimation and Bad Data Detection . . . 56
2.6 Beyond State Estimation, Attack Formulation and Challenges . . . 57
2.6.1 Basic Cyber-Physical Attacks . . . 58
2.6.2 Stealthy False Data Injection Attacks and Minimal Residual Strategies . . . 59
2.6.3 Multi-level Cyber-Physical Attacks . . . 60
2.6.4 Data-Driven Based Cyber-Physical Attacks . . . 61
2.7 Defense Strategies of Cyber-Physical System . . . 62
2.7.1 Active Schemes . . . 63
2.7.1.1 Active Watermarking . . . 63
2.7.1.2 Time-Varying Models . . . 64
2.7.2 Passive Schemes . . . 65
2.7.2.1 Passive Threshold-Based Methods . . . 65
2.7.2.2 Interval State Estimation Models . . . 65
2.7.3 Data-Driven Based Cyber-Physical Security . . . 66

Chapter 3: Stealthy Infiltrated Cyber Attacks and Feasibility Area of Smart Power Systems . . . 68
3.1 Introduction . . . 68
3.2 Problem Formulation and Preliminaries . . . 70
3.2.1 Testbed of Smart Power Systems . . . 70
3.2.1.1 Primary Information Module . . . 71
3.2.1.2 State Estimation Situational Awareness Module . . . 72
3.2.1.3 Primary Information Cybersecurity Module . . . 74

3.2.1.4 Energy Management System and Computational Algorithm Module . . . 75
3.2.1.5 Secondary Information Module . . . 78
3.2.1.6 Secondary Information Cybersecurity Module . . . 79
3.2.2 Primary and Secondary information Basic and Stealthy False Data Injection Attack Modeling . . . 79
3.2.2.1 Basic False Data Injection Attacks on Primary and Secondary Information . . . 80
3.2.2.2 Stealthy False Data Injection Attacks on Primary Information . . . 80
3.2.2.3 Stealthy False Data Injection Attacks on Secondary Information 81
3.3 Proposed Stealthy Infiltrated Cyber Attacks model . . . 81
3.3.1 Proposed Model of Stealthy Infiltrated Cyber Attacks on Primary Information . . . 81
3.3.2 Proposed Model of Stealthy Infiltrated Cyber Attacks on Secondary Information . . . 82
3.3.3 Implementation Algorithm of Stealthy Infiltrated Cyber Attacks . . . 82
3.4 Proposed Feasibility Area Approach for Stealthy Infiltrated Cyber Attacks Detection . . . 84
3.4.1 Proposed Feasibility Area Framework Structure and Preliminaries . . . 84
3.4.1.1 Exact Feasibility Area Estimation Using Bi-Level Robust Optimal Power Flow . . . 84
3.4.1.2 Approximate Feasibility Area Estimation Using Historical Operating Data . . . 86
3.4.2 Feasibility Area Classifiers Parameters Estimation . . . 89
3.4.2.1 Rectangular Feasibility Area Classifier . . . 89
3.4.2.2 Circular Feasibility Area Classifier . . . 90
3.4.2.3 Elliptic Feasibility Area Classifier . . . 90
3.4.2.4 Convex-Hull Feasibility Area Classifier . . . 90
3.4.2.5 Single-Class Support Vector Machine Feasibility Area Classifier . 91
3.4.3 Performance Metrics for the Feasibility Area-Based SICA Detection . . . 92
3.5 Numerical Results . . . 92
3.5.1 Test System and Simulation Environment . . . 92
3.5.2 State Estimation and Primary and Secondary Information Cyberattacks . 94
3.5.2.1 Performance of State Estimation and Cybersecurity Layer Design 94
3.5.2.2 Design and Performance of Bad Data Detection and Advanced False Data Injection Attack Detection Layers . . . 95
3.5.2.3 Basic and Stealthy False Data Injection Attack Implementation . 96
3.5.3 Stealthy Infiltrated Cyberattack Implementation . . . 99
3.5.4 Performance of Feasibility Area-Based for Stealthy Infiltrated Cyberattack Detection . . . 100
3.5.4.1 Individual Performance of Feasibility Area Classifiers . . . 101
3.5.4.2 Performance of Feasibility Area Across All Power System State Variables . . . 102
3.5.4.3 Performance of Feasibility Area-Based Deep Neural Network Model in Detecting Stealthy Infiltrated Cyberattacks . . . 102

3.5.4.4 Generalization and Adaptation of the Feasibility Area-Based Deep Neural Network Under New Attacks and Normal Operating Disturbances . . . 105
3.6 Summary and Conclusion . . . 107

Chapter 4: Feasibility Area Applications in Smart Power and Integrated Energy Systems . . . 109
4.1 Introduction . . . 109
4.2 Power and Gas Integrated Energy Systems Problem Formulation and Preliminaries 111
4.2.1 Testbed of Power and Gas Integrated Energy Systems . . . 111
4.2.1.1 Energy Management System of Power and Gas Integrated Energy Systems Module . . . 112
4.2.1.2 Primary and Secondary Information Cybersecurity Module . . . 115
4.2.2 Development of Stealthy Infiltrated Cyberatacks On Power and Gas Integrated Energy Systems . . . 116
4.2.3 Application of Feasibility Area On Power and Gas Integrated Energy Systems . . . 117
4.3 Power and Transportation Integrated Energy Systems Problem Formulation and Preliminaries . . . 118
4.3.1 Testbed of Power and Transportation Integrated Energy Systems . . . 118
4.3.1.1 Energy Management System of Power and Transportation Integrated Energy Systems Module . . . 119
4.3.1.2 Primary and Secondary Information Cybersecurity Module . . . 122
4.3.2 Development of Cyberattacks On Power and Transportation Integrated Energy System . . . 122
4.3.2.1 Proposed False Data Injection Attack on Power and Transportation Integrated Energy Systems . . . 123
4.3.2.2 Proposed Distributed Denial-of-Services Attacks False Data Injection Attack on Power and Transportation Integrated Energy Systems . . . 125
4.3.3 Proposed Cyber Resilience Energy Management System of Power and Transportation Integrated Energy System . . . 127
4.3.3.1 Time-Frequency Spectrum-Based Deep Neural Network . . . 128
4.3.3.2 Robust Hydrogen Refueling Stations Power Limits Estimation . 129
4.3.3.3 Convex Resilience Optimal HRSs Scheduling . . . 130
4.4 Numerical Results of Power and Gas Integrated Energy System . . . 131
4.4.1 Test System and Simulation Environment . . . 131
4.4.2 Power and Gas Integrated Energy System Optimal Energy Flow . . . 132
4.4.3 Power and Gas Integrated Energy System Secondary Information Cybersecurity Layer . . . 133
4.4.4 Power and Gas Stealthy Integrated Energy System Stealthy Infiltrated Cyberattacks . . . 135
4.4.5 Performance of Feasibility Area-Based Deep Neural Network Model in Detecting Stealthy Infiltrated Cyberattacks on Power and Gas Integrated Energy System . . . 135
4.5 Numerical Results of Power and Transportation Integrated Energy System . . . 138

4.5.1 Test System and Simulation Environment . . . 138
4.5.2 Power and Transportation Integrated Energy System Energy Management System . . . 140
4.5.3 Power and Transportation Integrated Energy System Cyberattacks . . . 141
4.5.3.1 Power and Transportation Integrated Energy System Stealthy False Data Injection Attacks . . . 141
4.5.3.2 Power and Transportation Integrated Energy System Single DoS and Coordinated Bi-Level DDoS Attacks . . . 142
4.5.4 Performance of Feasibility Area-Based Deep Neural Network Model in Detecting Stealthy False Data Injection Attacks on Power and Transportation Integrated Energy System . . . 145
4.5.5 Performance of The Proposed Cyber-resilient Hydrogen Refueling Station Energy Management System . . . 147
4.6 Summary and Discussion . . . 150

Chapter 5: Advanced Feasibility Area Considering Spatial Distribution and Temporal Correlation Properties . . . 152
5.1 Introduction . . . 153
5.2 Advanced Feasibility Area Formulation and Preliminaries . . . 154
5.2.1 Feasibility Area Spatial Distribution Property . . . 154
5.2.1.1 Spatial Distribution of Rectangular Feasibility Area . . . 155
5.2.1.2 Spatial Distribution of Circular Feasibility Area . . . 155
5.2.1.3 Spatial Distribution of Elliptic Feasibility Area . . . 155
5.2.1.4 Spatial Distribution of Convex-Hull Feasibility Area . . . 156
5.2.1.5 Spatial Distribution of Single Class SVM Feasibility Area . . . 156
5.2.2 Optimal Tuning of Combined Sigmoid-Expansion Deep Neural Network . 157
5.2.3 Feasibility Area Temporal Correlation Property . . . 158
5.2.4 Recursive Feasibility Area Estimation Algorithm . . . 159
5.2.4.1 Outliers-Based Recursive Feasibility Area Estimation Algorithm 160
5.2.4.2 Samples Distribution-Based Recursive Feasibility Area Estimation Algorithm . . . 162
5.3 Numerical Results . . . 162
5.3.1 Test System and Simulation Environment . . . 162
5.3.2 Performance of Advanced Feasibility Area with Spatial Distribution Property . . . 164
5.3.3 Performance of Advanced Feasibility Area with Temporal correlation Property . . . 166
5.3.4 Performance of Recursive Feasibility Area Estimation Algorithm . . . 168
5.3.5 Performance of Stealthy False Data Injection Attack Features Extraction Using Proposed Advanced Feasibility Area . . . 169
5.4 Summary and Discussion . . . 173

Chapter 6: Conclusion and Future Work . . . 175
6.1 Summary and Conclusions . . . 175
6.2 Future Work . . . 180

List of Publications . . . 181

List of Publications **182**

References **185**

List of Tables

2.1 Summary of Energy Storage Technologies in Power Systems 20

4.1 Impact of DoS and DDoS Cyberattack 144

5.1 Computational effort of the FA parameter estimation using traditional and recursive estimation algorithm 169

List of Figures

1.1 Overlay of the cyber-physical methods developed in this thesis for smart power and IESs. . . . 4
1.2 Smart power and IES cybersecurity research trends and gaps. Note: "Articles" refers to journal publications released by recognized publishers, whereas "All documents" includes journal articles as well as standards, white papers, and preprints. 8

2.1 Structure of the SPSs and Emerging Technologies. . . . 16
2.2 Structure of the Cyper-Physical Power Systems. . . . 22
2.3 List of Steady-State and Dynamic Applications Performed by Central Control Systems. . . . 25
2.4 Structure of the deep IESs including electric power, transportation, gas, and thermal energy systems. . . . 29
2.5 Integration of power and transportation systems. . . . 32
2.6 Integration of power and gas systems. . . . 38
2.7 Integration of power and heat systems. . . . 40
2.8 Taxonomy of Cyber-Physical Attacks. . . . 45
2.9 Supervisory Control and Data Acquisition (SCADA), Phasor Measurement Unit (PMU) and hybrid measurements reportingtime frame. . . . 53
2.10 Hybrid SE architectures, 1) Direct measurement fusion, 2) parallel state fusion, and 3) sequential measurement-state fusion. . . . 54
2.11 Defense strategies against false data in CPS . . . 63

3.1 Testbed and simulation environment of the smart power system . . . 70
3.2 Testbed applications . . . 86
3.3 High level representation of an FA-based SICA detection framework. . . . 88
3.4 The IEEE 30-bus transmission system employed for numerical studies showing PMUs and SCADA measurements, and FDIA of primary and secondary information. . . . 93
3.5 Healthy and SICA scenario generation flowchart. . . . 93
3.6 Performance of SE in removing measurements error. . . . 94
3.7 SE estimated state x^* and the actual state x^{act}. . . . 95
3.8 SE objective $J(x)$ and residual $r = |z - h(x^*)|$ Probability Distribution Function (PDF). . . . 95
3.9 Advanced stealthy FDIA forecasting-based detection layer training performance and optimal state x^* forecasting error. . . . 96
3.10 SE estimated state x^* and the actual state x^{act} under basic FDIA. . . . 97
3.11 SE objective $J(x)$ and residual $r = |z - h(x^*)|$ PDF under basic FDIA. . . . 97

3.12 Performance of stealthy FDIA a) bypass the BDD layer, and b) optimal designed attack vector a_t. 98
3.13 SE estimated state x^* and the actual state x^{act} under stealthy FDIA. 98
3.14 Weighted Least Square (WLS) objective $J(x)$ under stealthy FDIA and forecasted threshold using advanced stealthy FDIA detection layer. 98
3.15 Performance of SICA; a) WLS objective $J(x)$ under SICA and forecasted threshold, b) optimal designed attack vector a_t. 99
3.16 Estimated deterministic and non-deterministic FA: a) rectangular, circular, and elliptic classifiers, b) Convex-Hull classifier, c) single-class Support Vector Machine (SVM). 100
3.17 Complex plane representation of the PSSV under healthy and SICA; a) Bus 2 real and imaginary voltage values, b) Branch 29-30 active and reactive power values. . 101
3.18 True Positive (TP) and False Negative (FN) values for window sizes of 24, 48, and 168 hours: a) $TP_{\phi_{Rec}}$ b) $TP_{\phi_{Cir}}$ c) $TP_{\phi_{Ell}}$ d) $TP_{\phi_{CH}}$ e) $TP_{\phi_{SVM}}$ f) $FN_{\phi_{Rev}}$ g) $FN_{\phi_{Cir}}$ h) $FN_{\phi_{Ell}}$ i) $FN_{\phi_{CH}}$ j) $FN_{\phi_{SVM}}$. 102
3.19 Feasibility Area Uncertainty Ratio (FAUR) under healthy operation and attacked scenarios 103
3.20 Structure of the FA-based DNN SICA detection. 103
3.21 Training performance of different DNN structures. B: Basic DNN, F: Feedforward FA-based DNN, R: Residual FA-based DNN, T: Training, and V: Validation. 104
3.22 Comparison of various performance metrics a) Accuracy with respect to PSSVs variation compared with basic-Pattern Recognition Neural Network (PRNN), b) proposed Proposed FA-PRNN Vs DNN b) Proposed FA-PRNN Vs common Machine Learning (ML) methods [1]. 105
3.23 12Performance of the proposed FA-PRNN under a) unseen type of SICA over the primary information, b) system reconfiguration with no previous knowledge, c) system reconfiguration with 1% retrain on new system configuration. 107

4.1 Testbed and simulation environment of the power and gas IESs. 111
4.2 Testbed and simulation environment of the power and transportation IESs. . . . 118
4.3 Structure of the cyber-resilience EMS against DDoS attacks. 127
4.4 The IEEE 30-bus transmission system integrated with a 20–node gas transmission grid employed for numerical analysis. 131
4.5 Healthy and SICA scenario generation flowchart on power and gas IES. 132
4.6 Power and gas IES operation state under operation. 133
4.7 PtH and GfG units scheduling with respect to the electricity price. 133
4.8 Structure of Cal+Regression-DNN secondary information cybersecurity layer. . . 134
4.9 Performance of Cal+Regression-DNN in forecasting the setpoints of PtH unit 1. . 134
4.10 SPS operation state under SICA. 136
4.11 The number of effective PSSV for different lengths of historical data window a) M^{FA}=24-hour, b) M^{FA}=48-hour, c) M^{FA}=168-hour. 137
4.12 Detection performance of the proposed FA-PRNN in the power and gas IES. . . . 137
4.13 IEEE 33-bus distribution system integrated with HRSs and transportation system at Bus 7, Bus 14, and Bus 29 distributed HRSs used for numerical studies. . . . 139
4.14 Healthy, stealthy FDIA, and DDoS attacks scenario generation flowchart on HRSs power and transportation IES. 139

4.15 Performance of the HRSs under healthy operation; a) Revenue, b) PtH and HtP power setpoints and Operating Reserve (OR) signal, c) PtH and HtP hydrogen flow and HRSs hydrogen demand, d) HRSs hydrogen storage State of Charge (SoC) as well as upper bound and lower bound reserve margin, and e) HRSs bus voltage. 141
4.16 Performance of the HRSs under compromise of OR power signal; a) OR signal, b) PtH and HtP power setpoints and the OR signal, c) Revenue. 142
4.17 Performance of the HRSs EMS under healthy state and DoS for the hydrogen demand ; a) Hydrogen demand , b) PtH and HtP power setpoints and the OR signal, c) Revenue. 143
4.18 Performance of the HRSs EMS under healthy and the investigated Bi-level coordinated DDoS attack; a) DDoS attack vector, b) PtH and HtP power setpoints and the OR signal, c) Revenue. 144
4.19 The FA's ability to detect attack patterns and DNN training performance; a) PSSV representation in the complex domain showing features overlap, b) FAUR, c) Performance of the DNN. 146
4.20 Training and testing performance of the DNN models in reconstruct the HRSs attacked information. 147
4.21 Power limits of the HRSs; a) PtH power limits, b) HtP power limits. 148
4.22 Performance of the convex resilience HRSs optimal scheduling; a) DDoS attack vector, b) reconstructed hydrogen demand and its uncertainty, c) reconstructed hydrogen tank SoC and its uncertainty, d) the PtH and HtP power setpoints and power limits beside the OR signal and it uncertainty, c) Revenue. 149

5.1 Spatial distribution of PSSV using expansion factor and sigmoid-expansion flag. . 156
5.2 Illustration of recursive FA estimation for convex-hull 160
5.3 The IEEE 30-bus transmission system employed for numerical studies showing Optimal Power Flow (OPF) control units. 163
5.4 Healthy and stealthy FDIAs scenario generation flowchart. 163
5.5 Variation the expansion factor values under different attack magnitudes. a) Expansion factor versus time of operation b) PDF of the PSSVs expansion factor. . 165
5.6 Expansion factor values at different FA classifiers ϕ under a) Single bus attack, and b) Double bus attacks. 165
5.7 The impact of size of the past M-hours window on the expansion factor. 166
5.8 Cosine similarity and temporal correlation evaluated over a historical one-week window (168 hours), highlighting the operating states with the highest similarity to the current PSSV. 167
5.9 Complex plane representation of the PSSV under healthy considering temporal correlation and cosine similarity. 168
5.10 Extraction of stealthy FDIA characteristics using a) Multi-classification DNN, b) Regression DNN. 170
5.11 DNN training performance for detection of stealthy FDIA using basic PSSVs features (W/O), traditional FA (TFA), and proposed advanced FA (AFA) under different attacks magnitude value. T: training, V: validation. 171

5.12 Performance of multi-class detection of DNN to extract features of the stealthy FDIA without FA and with TFA, and the proposed AFA schemes. Classes number (0:healthy), (1,2,3: single bus attack 5,10,15%), (4,5,6: double bus attack 5,10,15%), (7,8,9: triple bus attack 5,10,15%). 172
5.13 Regression DNN performance (a) Training performance (b)-(d) Attack magnitude estimation over Buses 3,7, and 25, respectively. 172

Acronyms

ACE	Automatic Generation Control Error.
AFA	Arc Flash Analysis.
AGC	Automatic Generation Control.
AI	Artificial Intelligence.
AMI	Advanced Metering Infrastructure.
ANN	Artificial Neural Network.
BDD	Bad Data Detection.
CA	Contingency Assessment.
CHP	Combined Heat and Power.
CNN	Convolutional Neural Networks.
CPPS	Cyper-Physical Power System.
CPS	Cyber-Physical System.
CWT	Continuous Wavelet Transform.
DAM	Day-Ahead Market.
DDoS	Distributed Denial-of-Service.
DER	Distributed Energy Resource.
DG	Distributed Generation.
DL	Deep Learning.
DNN	Deep Neural Network.
DoS	Denial-of-Service.
DP	Differential Protection.
DR	Demand Response.
DSM	Demand Side Management.
DSSE	Distribution System State Estimation.
DVS	Dynamic Voltage Stability.
ED	Economic Dispatch.
EMS	Energy Management System.
ESS	Energy Storage System.
ET	Electric Transit.
ETD	Energy Thief Detection.
EV	Electric Vehicle.

FA	Feasibility Area.
FACTS	Flexible AC Transmission System.
FAUR	Feasibility Area Uncertainty Ratio.
FDIA	False Data Injection Attack.
FN	False Negative.
FTU	Feeder Terminal Unit.
GA	Genetic Algorithm.
GfG	Gas–fired Generation.
GHG	Green House Gas.
GNN	Graph Neural Networks.
GPS	Global Positioning System.
GRBF	Gaussian Radial Basis Function.
GtP	Gas-to-Power.
GtV	Grid-to-Vehicle.
HRS	Hydrogen Refueling Station.
HtP	Hydrogen-to-Power.
IBR	Inverter-Base Resource.
ICE	Internal Combustion Engine.
ICT	Information and Communication Technologies.
IED	Intelligent Electronic Device.
IES	Integrated Energy System.
ISE	Interval State Estimation.
LFC	Load Frequency Control.
LSTM	Long short-term memory.
MESS	Mobile Energy Storage System.
ML	Machine Learning.
MU	Merging Unit.
OCP	Over Current Protection.
OOS	Out-of-Step.
OPEX	Operating Expenditure.
OPF	Optimal Power Flow.
OR	Operating Reserve.
PC	Protection Coordination.
PDF	Probability Distribution Function.
PMU	Phasor Measurement Unit.
PRNN	Pattern Recognition Neural Network.

PSSV	Power System State Variable.
PtG	Power-to-Gas.
PtH	Power-to-Hydrogen.
PtTh	Power-to-Thermal.
PtX	Power-to-X.
PV	Photovoltaic.
RES	Renewable Energy Source.
RL	Reinforcement Learning.
ROFC	ROFC.
RTM	Real-Time Market.
RTU	Remote Terminal Unit.
SCADA	Supervisory Control and Data Acquisition.
SE	State Estimation.
SICA	Stealthy Infiltrated Cyber Attack.
SM	Smart Meter.
SoC	State of Charge.
SPS	Smart Power System.
STFT	Short-Term Fourier Transform.
SVM	Support Vector Machine.
SVR	Secondary Voltage Regulation.
TFS	Time Frequency Spectrum.
THD	Total Harmonic Distortion.
TP	True Positive.
TSA	Transient Stability Analysis.
UC	Unit commitment.
UE	User Equilibrium.
UFLS	Under Frequency Load Shedding.
VtG	Vehicle-to-Grid.
VVC	Voltage Var Control.
WAMS	Wide Area Monitoring System.
WLS	Weighted Least Square.
XtP	X-to-Power.
ZIB	Zero Injection Bus.

Nomenclature

Sets and Indices

Symbol	Description
$\boldsymbol{\mathcal{B}}$, and b, b'	Set of buses and indices.
$\boldsymbol{\beta}$	Set of transmission lines.
$\boldsymbol{\mathcal{G}}$, and g	Set of generators and index.
$\boldsymbol{\mathcal{D}}$	Set of electrical loads.
$\boldsymbol{\mathcal{D}}^{ad}$, and d	Set of adjustable demand units and index.
$\boldsymbol{\mathcal{S}}$, and s	Set of ESS and index.
$\boldsymbol{\mathcal{RES}}$, and f	Set of RES units and index.
$\mathcal{T}$, and t	Set of time periods and index.
M^{Ft}	Forecasting horizon for the EMS.
M^{His}	Historical horizon for forecasting.
$\mathbb{X}$	Set of state and decision variables.
n	State-variable index in $\mathbb{X}$.
I^P, I^S	Sets of primary and secondary information.
$\boldsymbol{\mathcal{M}}$, and m	Set of SE measurements and index.
k	WLS iteration index.
Φ, and ϕ	Set of FA classifiers and classifier index.
$\mathcal{S}^{FA}$, and τ	Set of FA historical samples and sample index.
τ^{HL}, τ^{A}	Healthy and attacked datasets.
N	Total number of PSSVs.
G^T	Transportation network graph.
$\boldsymbol{\mathcal{N}}^T, \boldsymbol{\mathcal{R}}^T$	Transportation network nodes and links.
$\mathcal{O}, \mathcal{D}^T$	Sets of origin and destination nodes.
o, d	Origin and destination node indices.
$\boldsymbol{\mathcal{P}}_{o,d}$	Set of paths between origin and destination nodes (o, d).
p^{th}	Transportation network path index.
G^G	Natural gas network graph.
$\boldsymbol{\mathcal{N}}^G$, and i, i'	Set of gas network nodes and indices.
$\boldsymbol{\mathcal{L}}^G$	Set of gas pipelines.
$\mathcal{L}_p, \mathcal{L}_a$	Sets of passive and active gas pipelines.
$\boldsymbol{\mathcal{EL}}$, and e	Set of PtH units and index.
$\boldsymbol{\mathcal{GFG}}$, and q	Set of GfG units and index.
$\boldsymbol{\mathcal{G}}^G$, and g	Set of gas supply units and index.
l	Gas compressor or active-pipeline index.
G^H	District heating network graph.
$\boldsymbol{\mathcal{N}}^H$, and i, i'	Set of heat network nodes and indices.

Symbol	Description
$\boldsymbol{\mathcal{L}}^H$	Set of district heating pipelines.
$\boldsymbol{\mathcal{H}}$, and h	Set of HRSs and index.
$\mathbb{M}$, and m	Set of HRS operation scenarios and index.

Parameters

Symbol	Description
$\mathtt{G}_{bb'}$	Network conductance between buses b and b'.
$\mathtt{B}_{bb'}$	Network susceptance between buses b and b'.
$g_{bb'}, b_{bb'}, b_{bb'}^{sh}$	Line series conductance, susceptance, and shunt susceptance between buses b and b'.
$\Theta_{P,X}$	Set of states describing the coupling between power and external energy systems.
$\underline{P_{bb'}^F}, \overline{P_{bb'}^F}$	Minimum and maximum active power flow limits of line (b, b').
$\underline{Q_{bb'}^F}, \overline{Q_{bb'}^F}$	Minimum and maximum reactive power flow limits of line (b, b').
$\underline{V}_b, \overline{V}_b$	Minimum and maximum allowable voltage magnitude at bus b.
$\mathcal{Q}$	Origin-destination demand matrix.
$q_{o,d}$	Transportation demand from origin o to destination d.
$\mathcal{C}_{ii'}^2$	Pipeline hydraulic resistance coefficient between nodes i and i'.
z, e	Measurement and error vectors.
$h(x)$	Measurement function.
σ_m	Standard deviation of measurement m.
R	Measurement error covariance matrix.
W	Measurement weighting matrix.
ϵ	SE convergence tolerance.
τ_{χ^2}	BDD Chi-test threshold.
τ_{t,χ^2}	Adaptive Chi-test threshold for stealthy FDIA.
Δx	Basic attack state change limits.
$\lvert\Delta e_t\rvert, \Delta\delta_t$	Sampled magnitude and phase angle measurement errors at time t.
e_t^R, e_t^I	Real and imaginary PMU measurement errors at time t.
$e_t^{P/Q}$	Active/reactive SCADA measurement error sample at time t.
$Tp_{t,bb'}$	Transformer tap position of line (b, b') at time t.
$SW_{t,b}$	Switching status at bus b and time t.
Gs_t	Solar irradiance at time t.
$Temp_t$	Ambient temperature at time t.
v_t^{wind}	Wind speed at time t.
c_t^{Ele}	Electricity price at time t.
$SoC_{t,b}$	Storage system SoC at bus b and time t.
Δt	Time-step duration.
$OPEX(\cdot)$	Operating cost function.
c_1^g, c_2^g, c_3^g	Generation cost coefficients.
$c^s, c^{\hat{f}}, c^d$	OPEX cost coefficients of ESS, RES, and adjustable demand.
η^s	Charging/discharging efficiency of storage unit s.
E_b^{Dad}	Total energy requirement of adjustable demand at bus b.
$\underline{P}_b^{Con}, \overline{P}_b^{Con}$	Minimum and maximum storage converter power limits at bus b.
$\Delta I_t^P, \tau_t^{Fr}$	Primary information forecasting deviation and acceptable error at time t.

Symbol	Description
$\Delta I^{S}_{t,b}, \tau^{Fr}_{t,b}$	Secondary information forecasting deviation and acceptable error at bus b and time t.
τ_V	Maximum allowable voltage variation under SICA.
M^{FA}	FA historical window.
$\lambda_{t,n}$	Kernel size of the GRBF for variable n at time t.
$\mathbf{1}[\cdot]$	Indicator function.
$a_{\phi,n}, b_{\phi,n}$	Sigmoid slope and offset parameters for classifier ϕ and variable n.
τ^{CS}	Cosine-similarity cutoff threshold for filtering historical FA samples.
κ	Recursive update factor for FA parameter estimation.
c^{e}, c^{q}	Cost coefficients of PtH and GfG units.
c^{g}	Gas supply cost coefficient.
$c^{G,Buy}_{t}, c^{G,Sell}_{t}$	Gas purchasing and selling prices at time t.
$Trade^{G}(\cdot)$	Gas trading cost function.
$\lambda^{PtH}, \lambda^{GfG}$	Overall energy conversion efficiencies of PtH and GfG units.
λ^{HtP}	Overall energy conversion efficiency of HtP units.
$\mathtt{k}^{\mathrm{GC}}, \mathtt{Z}_a$	Gas-compressor unit conversion and compressibility factors.
η^{c}, E_c	Compressor and parasitic efficiencies.
c_k	Gas heat capacity ratio.
c^{H}_{t}	Real-time hydrogen price at time t.
c^{OR}, β^{OR}	OR payment and penalty charges.
λ^{Dsp}	Hydrogen tank dissipation factor.
$\alpha^{OR}_{LB}, \alpha^{OR}_{UB}$	Lower and upper OR reserve margins for hydrogen storage.
S^{OR}_{t}	Binary variable indicating whether an OR signal is active at time t.
$\tau^{(.)}$	Maximum allowable FDIA manipulation ratio.
$c^{SOC/G^{H.D}}$	Attack cost coefficients for hydrogen SoC and hydrogen demand information.
$c^{PtH/HtP/OR}$	Attack cost coefficients for PtH, HtP, and OR information.
$\mathcal{R}(\cdot)$	STFT window function.
W, b	DNN model learnable weight and bias parameters.
ξ	DNN training learning rate.
$\Delta P^{DG}_{t,b}$	Uncertainty bound of Distributed Generation (DG) generation at bus b and time t.
$\Delta P^{D}_{t,b}, \Delta Q^{D}_{t,b}$	Uncertainty bounds of active and reactive demand at bus b and time t.

Variables

Symbol	Description
$P^{D}_{t,b}, Q^{D}_{t,b}$	Active and reactive power demand at bus b and time t.
$P^{G}_{t,b}, Q^{G}_{t,b}$	Active and reactive power generation at bus b and time t.
$P^{RES}_{t,b}, Q^{RES}_{t,b}$	Active and reactive power generation from RES at bus b and time t.
$P^{DG}_{t,b}, Q^{DG}_{t,b}$	Active and reactive power output of DG at bus b and time t.
$P^{Dad}_{t,b}, Q^{Dad}_{t,b}$	Adjustable active and reactive power demand at bus b and time t.
$P^{F}_{t,bb'}, Q^{F}_{t,bb'}$	Active and reactive power flow through transmission line (b, b').
$P^{ch,s}_{t,b}, Q^{ch,s}_{t,b}$	Active and reactive charging power of storage unit s at bus b and time t.
$P^{dch,s}_{t,b}, Q^{dch,s}_{t,b}$	Active and reactive discharging power of storage unit s at bus b and time t.

Symbol	Description
$SoC^{s}_{t,b}$	SoC of storage unit s at bus b and time t.
$P^{XtP}_{t,b}, Q^{XtP}_{t,b}$	Active and reactive power transferred from external energy systems to the power system.
$P^{PtX}_{t,b}, Q^{PtX}_{t,b}$	Active and reactive power transferred from the power system to external energy systems.
$P^{PtH}_{t,b}, Q^{PtH}_{t,b}$	Active and reactive power exchanged by PtH at bus b and time t.
$P^{HtP}_{t,b}, Q^{HtP}_{t,b}$	Active and reactive power exchanged by HtP at bus b and time t.
$P^{GfG}_{t,b}, Q^{GfG}_{t,b}$	Active and reactive power exchanged by GfG at bus b and time t.
$P^{Com}_{t,i,b}$	Active power consumed by gas compressor at node i and bus b at time t.
$\|V_{t,b}\|$	Voltage magnitude at bus b and time t.
$\delta_{t,b}$	Voltage phase angle at bus b and time t.
$\theta_{t,bb'}$	Voltage angle difference between buses b and b' at time t.
$V^{R}_{t,b}, V^{I}_{t,b}$	Real and imaginary voltage components at bus b and time t.
$I^{R}_{t,\beta}, I^{I}_{t,\beta}$	Real and imaginary current components of branch β at time t.
$G^{G}_{t,i}, G^{D}_{t,i}$	Gas generation and demand at node i and time t.
$G^{F}_{t,ii'}$	Gas flow through pipeline (i, i') at time t.
$\Pi_{t,i}$	Gas pressure at node i and time t.
$G^{PtH}_{t,i}, G^{GfG}_{t,i}$	Gas output of PtH and gas input to GfG at node i and time t.
$Com_{t,i}, Vlv_{t,i}$	Compressor and valve operation states at gas node i and time t.
$G^{F}_{\mathrm{Com},l}$	Gas flow through compressor l.
$\Pi^{in}_{t,i}, \Pi^{out}_{t,i}$	Suction and discharge gas pressures at node i and time t.
$T_{t,i}$	Suction gas temperature at node i and time t.
$H^{G}_{t,i}, H^{D}_{t,i}$	Thermal generation and demand at node i and time t.
$G^{PtH}_{t,b}, G^{HtP}_{t,b}$	Hydrogen produced by PtH and consumed by HtP at bus b and time t.
$G^{H,D}_{t,b}$	Hydrogen demand of the HRS at bus b and time t.
$SoC^{H}_{t,b}$	Hydrogen tank state of charge at bus b and time t.
$P^{OR}_{t,b}$	Requested OR power capacity at bus b and time t.
P^{OR}_{t}	Total requested OR capacity at time t.
$P^{OR,PtH}_{t}, P^{OR,HtP}_{t}$	Reserve tracking deviations of PtH and HtP units at time t.
S^{OR}_{t}	Binary variable indicating whether an OR signal is active at time t.
x, x^{*}	State vector and optimal state.
Δx	State correction vector.
$J(x)$	WLS objective function.
r	Measurement residual vector.
$H(x)$	Jacobian matrix of the measurement function.
$G(x)$	Gain matrix.
x'	Basic attack manipulated state.
Δx^{a}	Basic attack state manipulation vector.
$I^{'P}_{t}, I^{'S}_{t}$	Manipulated primary and secondary information vectors at time t.
$\Delta I^{P,a}_{t}, \Delta I^{S,a}_{t}$	Injected attack vectors targeting primary and secondary information at time t.
a_t	Attack vector injected into the measurement vector at time t.
z'_t	Compromised measurement vector at time t.
$P^{'PtH}_{t,b}, G^{'PtH}_{t,i}$	Manipulated electrical and gas setpoints of PtH at time t.
$P^{'GfG}_{t,b}, G^{'GfG}_{t,i}$	Manipulated electrical and gas setpoints of GfG at time t.
$P^{'Com}_{t,i,b}$	Manipulated compressor power setpoint at node i, bus b, and time t.

Symbol	Description
$a_{t,b}^{PtH}, a_{t,b}^{GfG}, a_{t,b}^{Com}$	Attack vectors targeting PtH, GfG, and compressor setpoints.
$a_{t,h}^{SoC}, a_{t,h}^{G^{H.D}}$	Attack vectors targeting hydrogen tank SoC and hydrogen demand of HRS h at time t.
$a_{t,h}^{P^{PtH}}, a_{t,h}^{P^{HtP}}$	Attack vectors targeting PtH and HtP power information.
$a_t^{P^{OR}}$	Attack vector targeting requested OR capacity at time t.
a_t^{DoS}	Set of compromised information by DoS attacks at time t.
ΔRev_i	Percentage revenue loss due to DoS attack.
$x_{t,n}$	FA PSSV n at time t.
$Fg_{\phi(t,n)}$	FA binary flag of classifier ϕ and PSSV n at time t.
$x_{t,n}^{R,min}, x_{t,n}^{R,max}$	Minimum and maximum real bounds of the rectangular classifier for PSSV n at time t.
$x_{t,n}^{I,min}, x_{t,n}^{I,max}$	Minimum and maximum imaginary bounds of the rectangular classifier for PSSV n at time t.
$x_{cen(t,n)}^{R/I}$	Real and imaginary circular classifier center for PSSV n at time t.
$r_{t,n}$	Radius of the circular classifier for PSSV n at time t.
$C_{t,n}^{Ell}$	Center vector of the elliptic classifier for PSSV n at time t.
$A_{t,n}^{Ell}$	Shaping matrix of the elliptic classifier for PSSV n at time t.
$SV_{t,n}^{CH}$	Set of convex-hull boundary vertices for PSSV n at time t.
$\alpha_{\tau,n}$	SVM coefficient of historical sample τ for PSSV n.
$TP_{\phi,n}, FN_{\phi,n}$	TP and FN ratios for classifier ϕ and PSSV n.
$FAUR_{t,\phi}$	FAUR of classifier ϕ at time t.
$f_{i,k}$	Time-frequency feature of information signal i at frequency/time index k.
$\overline{P_{t,h}^{PtH}}, \overline{P_{t,h}^{HtP}}$	Robust maximum admissible power limits of PtH and HtP units at HRS h and time t.
$Fg_{\phi(t,n)}^{sig}$	Sigmoid-expansion flag of classifier ϕ for variable n at time t.
$\gamma_{\phi(t,n)}$	FA expansion factor of classifier ϕ for variable n at time t.
$x_{t,n}^{cnt,R}, x_{t,n}^{cnt,I}$	Real and imaginary centroid coordinates of the convex-hull classifier for variable n at time t.
$x_{t,n}^{itr,R}, x_{t,n}^{itr,I}$	Real and imaginary intersection-point coordinates with the convex-hull boundary.
$x_{t,n}^{out}$	Outer point defining the expansion direction from the convex-hull centroid.
ζ	Interpolation factor between the centroid and outer point.
CS_t^{FA}	Cosine-similarity vector between current and historical primary information over the FA window.

Chapter 1

Introduction

The global push for decarbonization and climate change mitigation has driven policy and governmental initiatives aimed at reducing carbon emissions. These policies have catalyzed the transformation of traditional power systems into what is now known as the Smart Power System (SPS), through two closely interconnected evolutionary transformation [2]. The first transformation involves the physical layer, characterized by the integration of green Renewable Energy Source (RES), Energy Storage System (ESS) technologies, and supportive regulatory frameworks that enables flexible demand-side participation and improved responsiveness to operational conditions [3]. The second transformation pertains to the cyber layer, where the deployment of advanced Information and Communication Technologies (ICT) has enabled fast and real-time monitoring, control, and protection of the SPS by facilitating two-way communication between system components. This holistic integration of physical and cyber components is referred to as a Cyper-Physical Power System (CPPS), where the seamless interaction between both layers introduces substantial operational benefits and paves the way for more efficient, interactive, and intelligent power system.

In parallel with the CPPS, the ongoing push toward decarbonization has driven deep electrification and the integration of various energy systems with the SPS. On one hand, this transition aims to improve overall efficiency, reliability, controllability, and system functionality. On the other hand, the emergence of SPSs and Integrated Energy Systems (IESs) has significantly increased system complexity, required greater integration of ICT to support real-time monitoring, control, and protection, and intensified interdependencies across different energy sectors [4]. Such tightly coupled integration demands innovative frameworks for optimal operation and

management, as well as more advanced regulatory standards and security frameworks, since disturbances or faults in one energy domain can now propagate across multiple energy sectors [5].

1.1 Motivation

The increasing cyber-physical interconnectedness has delivered significant operational benefits; however, it has also introduced a broad spectrum of vulnerabilities and cybersecurity threats, including False Data Injection Attacks (FDIA), Denial-of-Service (DoS) attacks, replay attacks, and other emerging forms of cyber-attacks, such as coordinated cyber-physical attacks. For instance, in November 2022, Russia's Sandworm unit combined physical sabotage with cyberattacks on a Ukrainian substation, remotely tripping breakers and deploying data-wiping malware to obstruct restoration efforts [6].

Moreover, the accelerated push toward decarbonization has driven deep electrification and further strengthened the interconnection of various energy systems with the SPS. While this integration enhances operational performance, it simultaneously creates new opportunities for cyber adversaries. Attackers are increasingly employing advanced strategies to exploit the weakest points within highly integrated systems, deliberately bypassing well-protected components, optimizing attack costs, and potentially triggering severe disruptions to the SPS through external access points. Consequently, this evolution has resulted in a more vulnerable operational landscape, increasing the risk of coordinated and sophisticated cyber-physical threats across both the SPS and the broader IESs [7].

Since the introduction of CPPSs, extensive efforts have been devoted to enhancing their resilience against cyber-attacks. Although many attack attempts have been successfully detected and mitigated, adversaries continue to explore new vulnerabilities by developing advanced strategies targeting both the cyber and physical layers, and by exploiting the increasing integration between the SPS and IESs to launch coordinated multi-energy-domain attacks [8]. The security challenges of SPSs and IESs can be attributed to three primary root causes.

First, the growing uncertainty in both demand and generation profiles, driven by the expansion of RESs and EVs within the SPSs, as well as by the integration of additional energy sectors such as gas, transportation, and heating, has significantly altered the operational characteristics of conventional physical systems [9]. This increased variability creates a wider range of operating

conditions, thereby complicating attack detection. Second, the integration of ICT into the SPS and IES exposes physical infrastructure to cyber threats that can directly compromise system reliability and stability [10]. Third, the non-uniform security standards and regulatory frameworks across different energy sectors create asymmetric protection levels, enabling attackers to exploit interconnections within the IES to propagate attacks into more secure environments. These root causes collectively necessitate substantial upgrades to existing cybersecurity schemes as the SPS and IES continue to expand and incorporate new components.

Addressing the growing cybersecurity threats facing smart power and IESs requires a holistic assessment of their cyber-physical nature, taking into account vulnerabilities across both the cyber and physical layers within the SPS and IESs. In summary, the following research methodology is adopted in this thesis to develop adaptive approaches aimed at enhancing the resilience of smart power and IESs:

1. Accurate modeling of the SPS, capturing the evolving characteristics of CPPSs, and systematically identifying potential vulnerabilities;
2. Investigation of the operational impacts of various cyber-attacks on the SPS, including analysis of their underlying patterns and signatures to reveal system weaknesses;
3. Examination of the effects of IESs integration and newly introduced vulnerabilities on monitoring functions and Energy Management System (EMS) applications;
4. Development of advanced and intelligent cyber-attack strategies capable of bypassing existing cybersecurity mechanisms, infiltrating into the SPS, and manipulating system operations;
5. Evaluation of existing defense mechanisms in terms of their ability to detect and mitigate cyber-attacks, and assessment of their suitability for smart power and IESs;
6. Design of adaptive cybersecurity defense mechanisms that evolve alongside advancements in the SPS, while accounting for the dynamic nature of both CPPSs and IESs;
7. Testing and validation of the proposed defense mechanisms under both standalone SPS conditions and IES environments, followed by the introduction of enhancement approaches to further improve their effectiveness.

The central objective of this thesis is to enhance the cyber-physical security of smart power and IESs against cyber-attacks by developing a novel technique capable of characterizing the

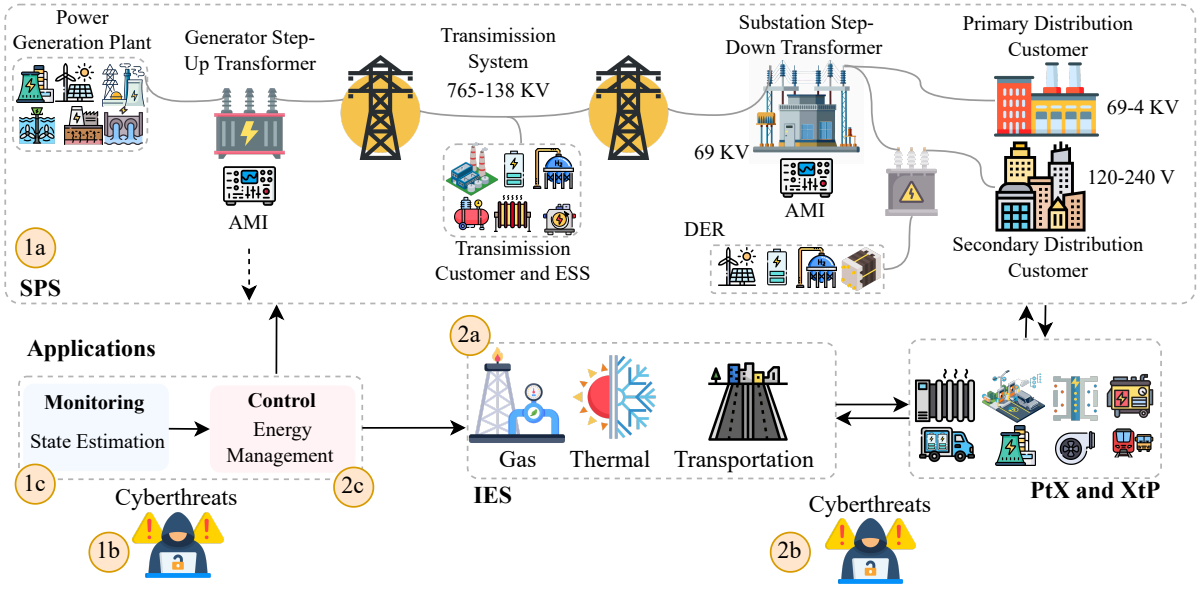


Figure 1.1: Overlay of the cyber-physical methods developed in this thesis for smart power and IESs.

operational behavior of the SPS and detecting abnormal deviations from expected performance under real-world operating conditions. In addition, this thesis proposes an adaptive approach that continuously adjusts its detection capabilities as the system evolves with emerging technologies and increasing electrification efforts.

Specifically, the methodologies developed in this thesis are organized into three primary domains related to smart power and IESs, as illustrated in the overview presented in Figure 1.1. The first domain focuses on the core security of standalone SPSs. Within this domain, ⓵ presents the development of a comprehensive testbed that serves as a benchmark for standalone SPSs, incorporating emerging technologies such as various RESs and ESSs, cybersecurity layers including BDD and advanced cybersecurity layer, and incooperate central control unit functions of monitoring State Estimation (SE) and EMS. Subsequently, ⓵ introduces a new class of stealthy FDIAs, capable of bypassing all existing detection layers, referred to as SICA. Finally, ⓵ proposes a novel FA-based detection approach designed to identify SICAs, which is integrated into the cybersecurity framework to detect compromised operational states of the SPS.

The second domain expands the scope of cybersecurity from standalone SPSs to integrated smart power and IESs. Within this domain, ⓶ presents the development of a comprehensive multi-energy testbed that incorporates power, gas, and transportation sectors within IESs. This

testbed serves as a benchmark platform and integrates Power-to-X (PtX) and X-to-Power (XtP) technologies (where X represents an integrated energy domain such as gas, transportation, or thermal systems). In particular, this domain emphasizes the modeling of coupled power–gas IESs and power–transportation systems within Hydrogen Refueling Stations (HRSs). Subsequently, ②ⓑ investigates various cyber-attack models targeting complex smart power and IESs, including stealthy FDIAs, SICAs, DoS, and coordinated bi-level DDoS cyber-attacks. These attacks are analyzed and executed within control and EMS applications targeting the IES primary information or coupling infrastructure (e.g, Power-to-Gas (PtG)). Finally, ②ⓒ evaluates the effectiveness of the proposed FA-based detection approach in securing SPSs and IESs. This evaluation assesses its capability to block ongoing attacks or detect infiltrated ones, and identifies the necessary adjustments required to enhance security across control layers and introducing a cyber-resilient EMS.

The third domain ③ focuses on advancing the proposed FA-based detection approach to enhance its capability not only to detect cyber-attacks but also to extract their critical features, such as attack localization and magnitude estimation. Furthermore, this domain aims to reinforce the proposed FA-based framework to improve its real-time applicability and strengthen its stochastic performance under high uncertainty conditions. These advancements include extending the proposed FA framework to incorporate both the spatial distribution and temporal correlation properties of system operation, as well as introducing an efficient recursive FA parameter estimation algorithm. The recursive formulation updates the FA parameters using previously estimated values, significantly reducing the computational effort while maintaining estimation accuracy.

1.2 Research Gaps

While both CPPSs architectures, and smart power and IESs provide numerous benefits for efficient energy systems operation, their increased complexity, heightened uncertainties in generation and demand, expanded access to physical infrastructure, and heterogeneous security standards, expose them to a wide range of security and resilience threats. In the context of CPPS within SPSs, numerous studies in the literature have investigated cyber-attacks targeting various monitoring, control, and protection applications under both steady-state and dynamic time-frame conditions. These applications include, but are not limited to (e.g., see Section 2.2), subsystems such as steady-state and dynamic SE, EMS applications (i.e., Economic Dispatch

(ED) and OPF), Automatic Generation Control (AGC), Load Frequency Control (LFC), Voltage Var Control (VVC), Phasor Measurement Unit (PMU) GPS spoofing, Advanced Metering Infrastructure (AMI), protection relays and breakers, as well as Day-Ahead Market (DAM) and Real-Time Market (RTM) [10]–[16]. In particular, these studies examine a range of cyber-physical attack strategies, including data integrity attacks such as FDIAs and replay attacks, which aim to induce incorrect actions in SPSs applications [17], [18]. Additionally, they consider attacks that cause service disruptions at either the cyber or physical layers, such as DoS attacks or physical damage to communication networks and infrastructure components of the SPSs [19], [20]. The development of these attacks can be broadly classified based on their target. In the first category, attackers target ***Primary Information*** by manipulating measurement data, such as weather data, power demand, and energy storage SoC, before it is processed, with the objective of indirectly influencing the operation of SPS subsystem applications [21]–[23]. In the second category, attackers directly target the outputs of subsystem applications, referred to as ***Secondary Information***, such as power dispatch commands and circuit breaker operations [24], [25].

Although several studies have investigated various cyberattack techniques, they generally classify attacks into two categories based on attack sophistication: basic and stealthy cyber-attacks. However, these classifications are primarily defined by the ability to bypass the traditional BDD layer and are largely focused on SE applications. In modern SPS, cybersecurity extends beyond the conventional BDD layer, incorporating dedicated protection mechanisms for both primary and secondary information across different SPS applications [26]. In this context, limiting the analysis to basic and stealthy cyberattacks with respect to traditional defenses and SE applications is no longer sufficient. Instead, it is essential to characterize more advanced cyber-attacks that can bypass multi-layered and advanced defense mechanisms, infiltrate the overall cybersecurity framework of various SPS applications, and ultimately manipulate system operations [24].

To address these gaps, SICA is introduced and investigated to characterize advanced cyber-attacks capable of manipulating the operation of the SPS. To identify the subset of SICA, a comprehensive cybersecurity framework for the SPS is considered, incorporating the BDD, as well as primary and secondary information protection layers. The impact of such cyberattacks is evaluated under different attack vectors with constrained magnitude thresholds. This development establishes the foundation for a new perspective on SPS post-occurrence cybersecurity, where the objective is to estimate and analyze system operation after prevention (pre-occurrence) cy-

bersecurity defenses have been bypassed. To detect SICA, the existing cybersecurity framework is reinforced with additional post-occurrence detection layers. In this context, the FA concept is introduced to characterize abnormal operating conditions within the PSSV resulting from manipulated system states. A set of deterministic and non-deterministic FA classifiers is introduced to characterize the expected operating region of the PSSV based on historical patterns estimated over a defined time window. The resulting FA-based representations of abnormal variations in the PSSV are then used to train a DNN model for the detection of SICA and manipulated system operations. The proposed approach establishes a comprehensive cybersecurity framework that extends beyond the prevention of cyberattacks to include post-occurrence protection, enabling the detection of manipulated SPS operations and facilitating timely corrective actions.

Beyond standalone SPSs, previous studies have investigated the cybersecurity of various IESs, primarily focusing on gas, transportation, and thermal energy systems [7]. Early efforts to address cybersecurity challenges in smart power and IES have focused on power–gas network coupling through PtG (e.g., electrolyzers and PtH) and Gas-to-Power (GtP) technologies (e.g., fuel cells, HtP, and GfG) [27]–[29]. In addition, the cybersecurity of power–transportation integration has been widely studied, particularly in the context of electrified transportation systems, such as trains, buses, and EVs, providing grid services through Vehicle-to-Grid (VtG) and Grid-to-Vehicle (GtV) applications [30]–[32]. However, in the context of power–thermal network integration, limited research has addressed the associated vulnerabilities. Most existing studies focus on the cybersecurity of thermal power plants rather than adopting a comprehensive perspective that considers the integration between district heating networks and the SPS [33], [34].

Despite these efforts, several critical gaps remain. First, existing studies predominantly focus on power–gas integration, with limited attention to transportation systems and district heating networks, and none of the prior works consider the integration of more than two IES. This limitation is primarily due to the complexity of modeling transportation systems (e.g., routing and spatiotemporal optimization) and district heating networks (e.g., nonlinear dynamics and time-varying thermal behavior), which significantly increase computational burden in multi IES system analysis. Second, most studies focus on vulnerabilities within the SPS information layer, such as power demand FDIA targeting the SE subsystem, while largely overlooking the potential for attackers to exploit less secure IES domains to infiltrate and manipulate SPS operations. Third, the majority of existing work is limited to basic and stealthy FDIAs in the context of

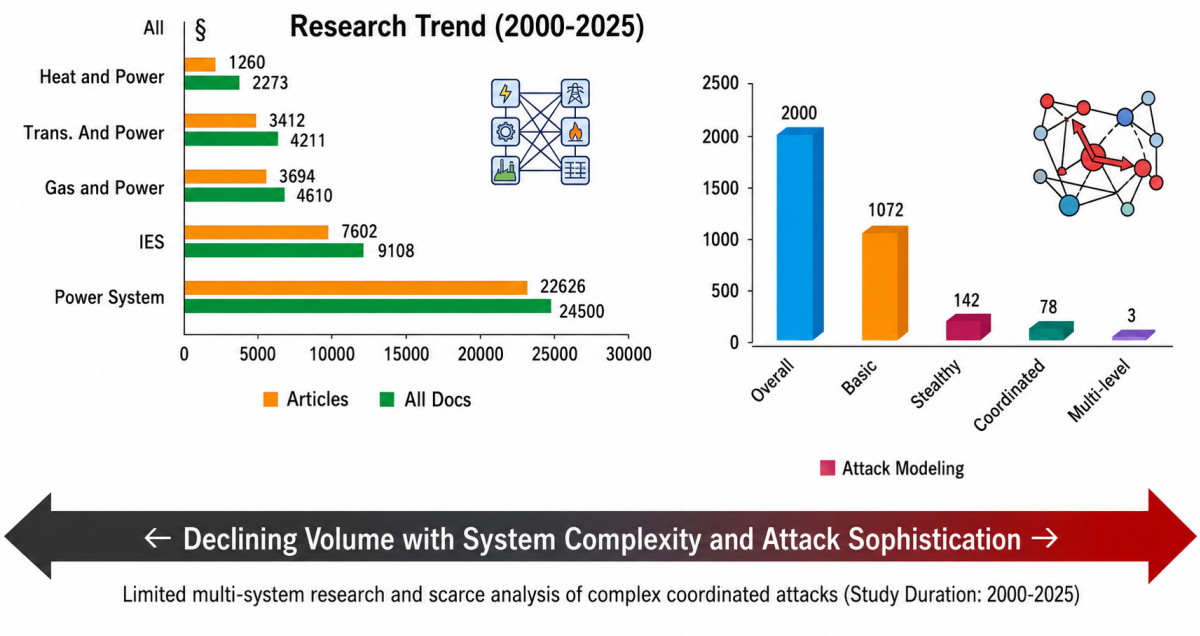


Figure 1.2: Smart power and IES cybersecurity research trends and gaps. Note: "Articles" refers to journal publications released by recognized publishers, whereas "All documents" includes journal articles as well as standards, white papers, and preprints.

SE, with only limited attention given to EMS applications within IESs. Furthermore, advanced coordinated or multi-level attack strategies, where attackers account for operator response and EMS behavior under designed attack scenarios, remain underexplored. In summary, the literature shows limited attention to: 1) transportation and district heating networks within IESs; 2) vulnerabilities originating from external IES domains that can impact SPS operation; and 3) advanced cybersecurity analysis in the context of EMS, including sophisticated multi-level attack strategies that consider operator response dynamics. Figure 1.2 illustrates the number of publications for each topic over the period 2000–2025, highlighting the limited attention given to complex smart power and IES, as well as to sophisticated coordinated and multi-level cyberattacks.

To address these gaps, this thesis first proposes the integration of the FA-based approach within coupled power–gas networks for post-attack detection, evaluating its capability to detect SICA detection on gas network information and coupling units (i.e, PtH and GfG). To extend beyond power–gas integration, the resilience of HRSs, as interconnected systems linking power, transportation, and gas networks, is investigated under various cyber-attack scenarios. In this context, the application of FA as a pre-occurrence cybersecurity layer against FDIAs is

examined at the EMS level of HRSs, with a focus on critical IES information such as hydrogen vehicle demand, hydrogen pricing, and the operational setpoints of PtH and HtP. Furthermore, a class of sophisticated coordinated bi-level DDoS attacks is introduced, where distributed attack strategies are optimally designed to maximize system impact under constrained attack budgets. To counter these threats, a comprehensive cyber-resilience framework that extends beyond traditional FDIA-focused approaches is developed. This framework integrates FA-based detection with convex robust operational strategies to enhance system resilience against diverse attack types. Overall, the proposed approaches ensure secure and resilient operation of HRSs under both FDIAs and DDoS attacks, providing a robust defense across multiple cyber-physical threat scenarios.

In a complementary direction, recent studies have emphasized the need to extend beyond purely detection frameworks toward extracting more informative features of cyber-physical attacks [35]–[37]. Specifically, this line of research aims to accurately identify attack locations, the specific measurements being targeted, and the magnitude of attack. Moving beyond detection enables a more proactive cybersecurity strategy that incorporates attack mitigation and system recovery. Such advancements facilitate corrective actions in several ways. First, knowing which measurements have been compromised allows operators to discard manipulated data, thereby improving SE accuracy. Second, forecasting-based recovery methods can be employed to reconstruct corrupted measurements, ensuring more robust data availability. Third, when the attack magnitude can be estimated, the EMS can be adjusted to account for the associated uncertainty, enabling more secure and resilient operational decisions [38]–[41].

However, the majority of these frameworks are primarily designed for dynamic applications, including AGC [37], LFC [41], and microgrid dynamic operation [39],[40]. In such dynamic settings, observers can be constructed for linear systems using state-space representations, enabling the detection of deviations between expected operation and received measurements. In contrast, this approach faces significant limitations in steady-state applications, whether for SE or EMS, primarily due to two factors: the high nonlinearity of system operation and the introduction of customized operational objectives. This combination results in discrete behavior (i.e., large communication intervals typical of steady-state applications), which, when coupled with high uncertainty, makes it difficult to build a continuous observer capable of extracting cyber-physical attack features. Under this challenge, steady-state applications have largely focused on attack localization using temporal data patterns rather than observer-based methods [35].

To address these gaps, this thesis proposes the integration of both spatial and temporal correlation to develop an advanced FA framework. From the spatial perspective, the FA-based approach is enhanced to not only detect whether the operational state is normal or abnormal, but also to provide a more informative assessment of how close or far each PSSV lies from the expected operational region, considering exact geometric similarity, using spatial distribution feature. Additionally, temporal correlation is incorporated by constructing the FA using historical operating instances that exhibit the highest similarity to the current operating condition. This spatial and temporal information is then fed into a DNN model to deliver critical cyber-attack characteristics: 1) attack location, 2) targeted measurements, and 3) attack magnitude of the manipulated data for SPS OPF. This advancement goes beyond mere localization by providing more valuable information regarding which measurements are attacked and the extent of manipulation. Additionally, to support real-time operation, a recursive FA estimation algorithm is introduced to efficiently update the expected operating region using newly acquired PSSVs. The FA parameters are re-estimated only when the support vectors or boundary points defining the feasible operating region change, and uses previous estimated parameters, reducing the computational effort while preserving estimation accuracy. These two advancements collectively enhance the capabilities of the FA framework and introduce a faster estimation mechanism suitable for dynamic applications.

1.2.1 Thesis Contribution

This thesis develops novel cyber-physical attack detection, characterization, and resiliency approaches using the concept of FA, organized under the three aforementioned domains: CPPSs, smart power and IES, and advanced FA. A summary of the thesis contributions is presented below:

1. A holistic CPPS framework is developed, incorporating both basic BDD and advanced pre-occurrence prevention cybersecurity layers for primary and secondary information.

2. An efficient SICAs model is proposed to extract the most sophisticated stealthy FDIA capable of bypassing all prevention cybersecurity layers and successfully manipulating SPSs operation.

3. The designed SICA attack vector estimation approach identifies the maximum attack magnitude threshold at which prevention layer detection rates degrade, while meeting

specified bypass rates and attack impact requirements. The attack vectors can be tailored to achieve attacker-defined objectives, such as inflicting financial damage (e.g., maximizing cost) or compromising SPSs stability (e.g., voltage regulation and overloading), thereby allowing flexible attack targeting.

4. A novel FA-based detection approach is developed to characterize the normal and healthy operational region of the PSSV using historical operation patterns, and to identify acceptable variations and abnormal operations for each PSSV as well as the overall system region.

5. Using the mathematical model of SPS power flow analysis, a set of FA-classifiers are defined and used as an unsupervised framework to estimate anomaly flags for PSSVs operation. These anomaly flags are then combined with a supervised DNN to extract hidden patterns of total abnormal operation and to detect infiltrated cyberattacks and SICA.

6. The concept of SICAs is extended toward the integration of SPS and IES, considering the impact over integrated power–gas networks, as well as power, gas, and transportation systems within the operation and management of HRSs.

7. The effectiveness of the designed FA framework for both prevention and detection of SICA is investigated over integrated power–gas networks and HRSs, highlighting both the strengths and limitations of the proposed approach.

8. To address the unique nature of coordinated bi-level DDoS attacks, where primary information is disrupted, a cyber-resilience framework is introduced for automatic data recovery using Long short-term memory (LSTM) combined with Time-Frequency Spectrum analysis using Short-Term Fourier Transform (STFT) and TFS to estimate missing information.

9. A new Bi-level DDoS is developed to account for both the attacker and operator perspectives, aiming to minimize attack cost at the upper layer while maximizing impact at the lower layer, thereby strategically maximizing DDoS impact relative to the attack budget.

10. In the context of HRSs, a convex optimal scheduling framework is introduced to ensure optimal operation while accounting for forecasting uncertainty and guaranteeing demand fulfillment and optimal operational under DDoS attacks. This addresses scenarios where the FA framework is insufficient or unable to function due to missing data.

11. An advanced FA framework is introduced to estimate critical attack features by adopting spatial correlation information and the probability that a given PSSV operational state is close to the actual system state. This framework estimates (1) the attack location, (2) the attacked measurements, and (3) the attack magnitude by discovering system state variations from the expected operational state.

12. A recursive FA estimation is developed to improve the estimation time of the expected operational region, thereby enabling the proposed approach to be adapted for dynamic applications.

1.3 Thesis Organization and Layout

The remainder of this thesis is organized into the following chapters:

- **Chapter 2** provides background and a comprehensive review of modern SPSs and their key components, with a particular focus on the integration of cyber-physical layers and the active ICT environment enabled by two-way communication technologies and CPPS. Additionally, it highlights recent advancements in SPS and IES, emphasizing the critical bi-directional interfaces that link the power system with other energy systems. From the cybersecurity perspective, it highlights important reported instances of cyber-physical attacks and presents attack taxonomies. It also highlights the role of SE using non-linear, linear, and hybrid measurement functions, as well as the traditional BDD layer. Furthermore, the chapter provides a comprehensive analysis of different cyber-physical attack types within and beyond SE monitoring, including their mathematical formulations and targets. Finally, it highlights different cybersecurity frameworks, their main strengths and weaknesses, and the test-bed system environment required.

- **Chapter 3** introduces a holistic view of standalone SPS CPPSs, highlighting both the monitoring system (i.e., SE) and the optimal management and control system (i.e., EMS), alongside the cybersecurity layers of BDD, primary information, and secondary information as a prevention (i.e., pre-occurrence) scheme. Additionally, it defines the concept of SICA, along with their mathematical formulation and objectives. The effectiveness of the developed SICA is highlighted in terms of trade-offs between bypass rate, number of attacked measurements, attack magnitude, and final impact. The chapter also introduces

the concept of FA and the mathematical foundation behind the FA classifier used to detect abnormal variation. It further shows how the FA classifier parameters are estimated and calibrated using a historical data window, as well as variations in overall normal operation and PSSV deviation from the expected operational region. Finally, it highlights the utilization of abnormal variations in PSSV normal operation to train a DNN for detecting SICA patterns.

- **Chapter 4** develops the concept of SICA beyond pure SPS into multi-energy system integration, specifically smart power and IES. First, it develops a holistic test-bed of the power-gas IES and tests SICA on their EMS and optimal energy flow, followed by an evaluation of the FA-based detection approach to detect SICA propagated from gas to power systems, thereby examining the effectiveness of the FA-based approach in providing an adaptive cybersecurity scheme for unknown attack propagation over new integrated systems. Additionally, the chapter develops an HRS test-bed in an active grid-service environment, where information from power, gas, and transportation systems are interconnected within the HRSs EMS. This holistic integration provides a strong candidate target for attackers seeking more access points and greater impact. First, a stealthy FDIA model is developed to corrupt both primary and secondary shared information and induce financial damage; then, the FA approach's performance in detecting attacks at the prevention layer (pre-occurrence) is examined. Additionally, the chapter investigates HRSs resilient operation against well-designed bi-level DDoS coordinated attacks. Finally, it introduces a data-forecasting and recovery scheme to recover missing information and provides a convex-decoupled HRS EMS to ensure robust operation, maximizing profit and demand fulfillment. This integration aims to reinforce the FA-based detection approach against attacks where primary information is outdated or missing.

- **Chapter 5** develops a more advanced FA-based detection approach by introducing and incorporating both spatial distribution and temporal correlation within a new FA approach. The spatial distribution is first used to account for the proximity of each PSSV to the expected normal operation region, considering the exact geometry of the FA, which combined with the temporal correlation where most similar operation instance used to ensure accurate estimation of the FA. This integration allows the FA to identify variations in manipulated PSSV data, introduces a more capable approach to detect the location of these variations, highlight the attacked PSSV, and estimate the attack magnitude. This

advancement is followed by a recursive FA parameter estimation algorithm in which FA parameters are estimated using previous information at, and updated when only necessary, thereby meeting real-time requirements and supporting dynamic applications.

- **Chapter 6** summarizes the contribution of this thesis in relation to the target research gaps, and expands on the intention to pursue further work in these areas.

Chapter 2

Literature Survey

In recent years, modern power systems have evolved beyond the traditional uni-directional power flow architecture, where centralized power plants were solely responsible for generation and electric power was transmitted through high-voltage lines to meet consumer demand at the primary and secondary distribution levels. The interactive nature of today's power systems has introduced bi-directional power flows, driven by the integration of Distributed Energy Resources (DERs) and RESs, along with various ESSs deployed across distribution networks. This shift has transformed passive consumers into active prosumers who are capable of participating in energy trading and local generation. This transformation is underpinned by advancements in ICT, which address the growing complexity and uncertainty of modern power systems by enabling fast, accurate, and real-time monitoring, control, and protection. Furthermore, the ongoing electrification trend, motivated by governmental policies and incentive programs aimed at mitigating climate change and improve overall system's efficiency, has added additional layers of complexity to SPSs and IESs. When combined with the CPPS architecture of the power system, this evolution increases operational complexity, introduces widespread communication dependencies, and creates significant challenges for cybersecurity standards aimed at ensuring resilience against both cyber and physical attacks.

This chapter provides background on key concepts in SPSs and their CPPS structure, highlighting generation, storage, and demand roles alongside active information sharing and monitoring, control, and protection functions. It also covers the concept of smart power and IES, emphasizing integration components and cybersecurity aspects. From a cybersecurity perspective, the chapter discusses the taxonomy of cyberattacks from various angles, as well as their mathemati-

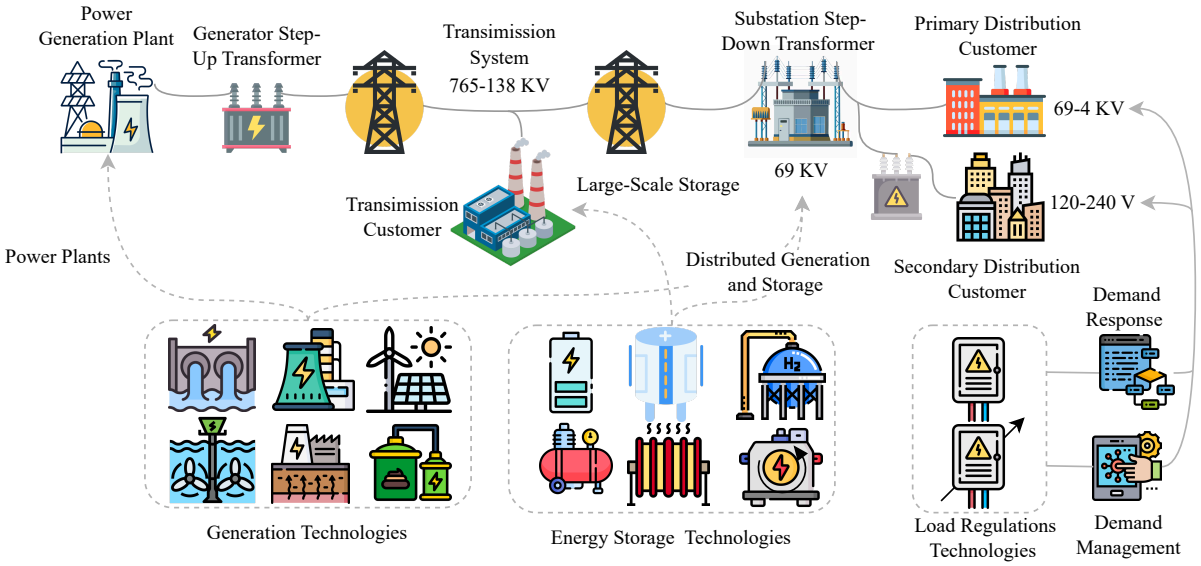


Figure 2.1: Structure of the SPSs and Emerging Technologies.

cal formulation within monitoring and control functions (i.e., SE and EMS). Finally, it provides a comparison of different cybersecurity approaches, evaluating their suitability, strengths and weaknesses, and the common test-bed systems used.

2.1 Electric Power Systems

Electric power systems are large-scale, complex infrastructures designed to generate, transmit, and distribute electrical energy to consumers across wide geographical regions [42]. Electricity generation typically begins at power plants, where generator machines produce electrical power. This power is then passed through step-up transformers to increase the voltage for high-voltage transmission lines, which helps reduce current levels, minimize thermal losses, and lower the infrastructure requirements of wide cross-section transmission lines [43]. Subsequently, electric power is distributed through primary and secondary distribution networks to serve a diverse range of end-users, including industrial, residential, commercial, and institutional sectors [44].

In recent decades, the integration of emerging technologies has significantly transformed traditional electric power systems into what is now referred to as SPS, as illustrated in Figure 2.1 [2]. This transformation includes the adoption of advanced generation technologies that enable the production of clean energy to meet increasing demand, the deployment of ESS to enhance controllability and address uncertainties in both supply and demand, and the imple-

mentation of market-based regulatory mechanisms such as Demand Side Management (DSM) of flexible electric load and Demand Response (DR) programs to incentivize and adapt end-user consumption [45]. These advancements are underpinned by two-way communication infrastructures that collect real-time field data from various measurement devices to the central control systems, and transmit control actions back to the SPS control elements to maintain reliable and efficient system operation [46].

2.1.1 Generation Technologies:

Conventional electric power generation primarily relies on fossil fuels and mature, large-scale technologies. Coal-fired power plants burn pulverized coal to produce high-pressure steam, which drives turbines and typically generates several hundred Megawatts (MW) of power [47]. Natural gas power plants utilize combustion turbines or combined-cycle systems, offering faster startup times and cleaner operation compared to coal-fired plants [48]. Nuclear power plants generate electricity through controlled nuclear fission reactions, which heat water into steam and drive turbines. These facilities produce large amounts of inflexible base-load power, typically between 500 to 1500 MW per unit, with minimal Green House Gas (GHG), though they pose challenges related to radioactive waste management [49]. These conventional generation methods are known for their reliability and are capable of consistently meeting base-load demand. Nuclear power plants serve as the backbone of base-load generation, while the faster ramping capabilities of coal-fired and natural gas plants are used to respond to load variations and operational uncertainties [50].

In contrast, renewable and clean energy generation technologies have emerged as environmentally sustainable alternatives, playing a crucial role in power system decarbonization. This transition is driven by increased global awareness of environmental issues and the need to reduce dependence on GHG-emitting energy sources [51]. Renewable energy technologies utilize naturally replenishing resources with significantly lower environmental impacts. Photovoltaic (PV) systems convert sunlight directly into electricity using semiconductor materials, with applications ranging from small rooftop systems (2–10 kW) to utility-scale solar farms (50–500 MW) [52]. Wind energy systems harness the kinetic energy of moving air; modern wind turbines are typically rated at 2–5 MW each, with large wind farms aggregating hundreds of MW [53]. Similarly, tidal and wave energy systems capture the kinetic energy of ocean water movement [54]. Hydropower systems convert the potential energy of flowing or falling water into

electricity. Large-scale hydropower dams can produce over 2000 MW of base-load power, while small run-of-river installations (1-50 MW) offer lower environmental impact [55]. Geothermal energy harnesses heat from the Earth's interior, typically through underground reservoirs of steam or hot water, to generate electricity via steam turbines [56].

At the distribution level, advancements in renewable and clean energy technologies, along with cost-saving considerations, have driven the widespread deployment of DERs near customer loads. This approach helps avoid the high costs associated with expanding large-scale transmission infrastructure, reduces transmission losses, and enhances the overall efficiency of SPSs [57]. However, this shift has fundamentally transformed the nature of distribution networks, introducing bi-directional power flows and increasing generation uncertainty due to the variable and intermittent behavior of DERs. In addition, the ongoing electrification of various energy systems has led to their large-scale integration with the SPS, introducing yet another layer of uncertainty on the demand side [58].

To maintain the balance between supply and demand in electric power systems and ensure system stability, several strategies have been explored in recent years. These include the hybrid utilization of RESs, curtailment of intermittent generation, integration of ESSs, and the implementation of market-based mechanisms such as DR and DSM. These approaches aim to enhance the flexibility and controllability of the SPS, with each method offering its own set of advantages and limitations [3], [59], [60].

2.1.2 Energy Storage Systems Technologies in Power System

ESSs are essential components in the ongoing transformation of SPS, contributing significantly to improved reliability, grid flexibility, and resilience against both generation and load uncertainties [61]. With the integration of ESSs, the adoption of RESs, frequency regulation, peak load shaving, voltage support, and overall system stability have been substantially enhanced [62]. ESSs technologies can be broadly categorized based on the nature of their energy storage medium into 1) Electrochemical, 2) Chemical, 3) Mechanical, 4) Thermal, and 5) Electromagnetic.

Electrochemical ESSs store energy via reversible chemical reactions and are mainly implemented using battery technologies [63]. Lithium-ion batteries are the most widely deployed due to their high energy density, fast response, and long cycle life, making them suitable for both EVs and large-scale applications. Sodium-sulfur batteries, operating at high temperatures, offer

75%–90% efficiency and are ideal for medium- to long-duration storage. Lead-acid batteries are low-cost and well-established but have shorter lifespans, making them suitable for backup and uninterruptible power supplies. Flow batteries, such as vanadium redox and zinc-bromine, use liquid electrolytes in external tanks, allowing flexible scaling of energy and power. They are suitable for large-scale, long-duration applications, with typical efficiencies of 65%-80%.

Chemical ESS technologies store energy in chemical bonds, typically in the form of gases or synthetic fuels [64]. Hydrogen energy storage converts electricity into hydrogen via electrolysis (i.e, electrolyzer PtH), stores it, and later reconverts it to electricity using fuel cells (i.e, HtP) or turbines (i.e, GfG), which enables integration across multiple energy sectors (i.e, power and gas) [65]. Despite its low round-trip efficiency (30%–50%), hydrogen storage is well-suited for seasonal storage and decarbonizing non-electric sectors, such as transportation through hydrogen-fueled vehicles. PtG systems extend this concept by converting hydrogen and CO_2 into methane via methanation, creating synthetic natural gas compatible with existing gas network infrastructure [66].

Mechanical ESS technologies store energy by converting it into kinetic or potential energy through the movement or positioning of mass [67]. Pumped hydro storage, the most established method, elevates water to store gravitational potential energy, offering high round-trip efficiencies of 70%–85% and suitability for large-scale storage. Compressed air energy storage stores pressurized air in tanks or underground caverns and releases it to drive turbines, with typical efficiencies ranging from 40% to 70% [68]. Flywheel systems store kinetic energy in rotating masses, delivering rapid response and high efficiency (up to 95%), ideal for short-duration applications. Recently, gravity storage systems, also known as gravity batteries, have emerged, storing energy by lifting heavy masses and releasing them to convert potential energy into kinetic energy [69].

Thermal ESS technologies store energy as heat or cold, which can be later converted to electricity or used directly for heating and cooling within IES [70]. Molten salt storage is widely used in concentrated solar power plants, offering efficiencies between 70% and 90%. Phase change materials store latent heat during phase transitions and are commonly applied in building energy management and load shifting [71]. Cryogenic energy storage involves liquefying air at very low temperatures and storing it in insulated tanks; upon regasification, the expanding air drives turbines, achieving efficiency (50%–70%) and are suited for long-duration storage [72].

Electromagnetic ESS technologies store electrical energy directly in electric or magnetic

Table 2.1: Summary of Energy Storage Technologies in Power Systems

Technology	**Energy Carrier**	**Efficiency**	**Response Time**	**Typical Applications**
Lithium-ion Battery	Electrochemical	85–95%	<1 s	EVs, renewables, fast regulation
Sodium-Sulfur Battery	Electrochemical	75–90%	Seconds	Load leveling, renewables
Lead-Acid Battery	Electrochemical	70–85%	Seconds	Backup power, UPS
Flow Battery	Electrochemical	65–80%	Seconds–Minutes	Long-duration storage
Hydrogen Storage	Chemical (Gas)	30–50%	Minutes	Seasonal storage, decarbonization
Methanation (PtG)	Chemical (Gas)	40–60%	Minutes	Synthetic fuel, grid injection
Pumped Hydro Storage	Mechanical (Gravity)	70–85%	Minutes	Bulk energy storage
Compressed Air Storage	Mechanical (Pressure)	40–70%	Minutes	Grid-scale long-duration
Flywheel Storage	Mechanical (Kinetic)	85–95%	<1 s	Frequency regulation
Molten Salt Storage	Thermal (Sensible Heat)	70–90%	Minutes–Hours	CSP, thermal storage
Phase Change Materials	Thermal (Latent Heat)	60–80%	Variable	Cooling, HVAC
Cryogenic Storage	Thermal (Cryogenic)	50–70%	Minutes	Bulk long-duration
Supercapacitor	Electromagnetic	>95%	Milliseconds	Short-term backup, power quality
Superconducting	Electromagnetic	∼95%	Milliseconds	Instantaneous support

fields [73]. Supercapacitors store energy electrostatically in electric field, offering rapid response (milliseconds), high power density, and round-trip efficiencies above 95%. However, their limited energy density restricts them to short-duration, high-power applications. In contrasts, superconducting magnetic uses superconducting coils to store energy in magnetic fields, delivering instant response and high efficiency (95%) [74]. Despite their performance, superconducting ESS are constrained by high costs and the need for cryogenic cooling.

Table 2.1 summarizes the major energy storage technologies, including their energy carriers, efficiencies, response times, and primary applications.

2.1.3 Market Regulations and Demand Side Participation

Alongside ESSs, power system operators increasingly use DSM and DR to improve grid reliability, reduce peak demand, and support RESs integration [75]. Two main demand side participation strategies exist: 1) price-based programs, which influence consumer behavior through dynamic pricing schemes like time-of-use, real-time pricing, or peak charges [76]; and 2) incentive-based programs, where participants are financially rewarded for load reductions during peak or emergency periods via mechanisms such as direct load control, demand bidding and capacity auction, or interruptible load contracts [77].

Effective DR implementation depends on advanced ICT infrastructure, including Intelligent Electronic Devices (IEDs), IoT-enabled devices, and automation platforms. Recently, virtual power plants have emerged, aggregating flexible consumer loads, such as EV chargers or smart thermostats, for coordinated dispatch by grid operators, enabling demand shaping and efficient use of excess renewable generation [78].

2.2 Structure of Cyper-Physical Power Systems

The evolution of SPSs, driven by advancements in generation, storage, and demand-side technologies, has been closely coupled with the development of ICTs over the past decade. The deployment of AMIs and cyber-enabled metering devices established the first communication pathway, enabling real-time data collection and power system SE [10]. This is complemented by a second pathway involving cyber-enabled control devices and actuators, which facilitate remote control and protection functions [79]. Together, these two-way communication channels form the foundation of cyber-physical integration, giving rise to CPPSs.

Figure 2.2 illustrates the general structure of CPPSs, highlighting the interaction between the cyber and physical layers through continuous information exchange [8]. The closed-loop operation of a CPPS involves real-time system monitoring by collecting field data, referred to as *primary information*, essential for system assessment. This includes network topology and parameters, generation and load levels, system limits, electricity prices, and the operational states of RESs and ESSs [80]. These data are transmitted via wired or wireless networks to a central control system, where they are processed for various applications, such as steady-state operations (e.g., OPF) and dynamic control (e.g., AGC) [81]. The resulting optimal decisions, referred to as *secondary information*, are then sent back to the physical layer. Secondary information includes generator setpoints, ESSs charge/discharge schedules, static VAR compensator settings, RESs and DERs curtailments, transformer tap positions, and circuit breaker statuses [79].

From a cybersecurity perspective, two primary threat channels exist within the CPPS architecture. The first targets the primary information, where cyberattacks aim to compromise data collected from the field, leading to incorrect system SE and suboptimal control decisions. The second channel involves attacks on the secondary information as it is transmitted from the cyber layer to physical actuators and control elements. In this case, attackers directly alter op-

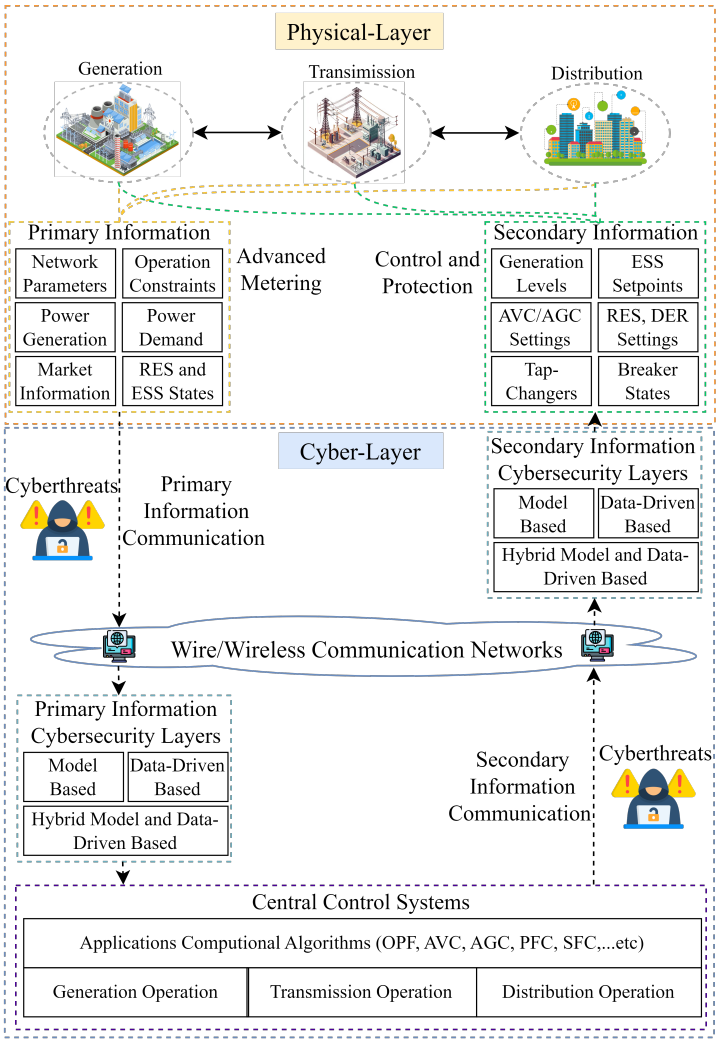


Figure 2.2: Structure of the Cyper-Physical Power Systems.

erational setpoints, potentially causing financial losses or system instability [82]. To safeguard these two-way communications, various cyber defense mechanisms, ranging from model-based to data-driven and hybrid approaches, are integrated within CPPSs. These strategies will be discussed in detail in Section 2.7.

2.2.1 Monitoring System and Advanced Metering Infrastructures

Monitoring the state of SPSs is vital for situational awareness, optimal control, and protection. However, the effectiveness of monitoring systems, particularly their accuracy, quality, and real-time responsiveness, directly influences the performance and decision-making of central con-

trol systems. These factors depend largely on the specifications of deployed field measurement devices and the accuracy of SE algorithms [83]. Commonly collected field data across transmission and distribution networks include voltage, current, active and reactive power, energy consumption, frequency, rate of frequency change, Automatic Generation Control Error (ACE), Total Harmonic Distortion (THD), as well as transient voltage and waveform information, which are collected by different type of measurement devices [84].

In transmission systems, SCADA represented the first centralized monitoring solution, initially relying on Remote Terminal Units (RTUs) installed at generation and substation transformers. These devices reported voltage, active and reactive power injections, and flow measurements every 2–5 seconds [85]. However, RTUs provide unsynchronized measurements, limiting their usefulness for phasor and sequence analysis, particularly under unbalanced conditions. Over time, IEDs emerged as a broader category encompassing any smart field device with embedded processing and bidirectional communication capabilities. These include digital relays, multifunction meters, and smart controllers [86], which have largely replaced RTUs in substations. IEDs are often paired with Merging Units (MUs) capable of reporting voltage and current waveforms at rates up to 80 samples per cycle, enabling detection of electromagnetic transients [87]. Nonetheless, the lack of synchronized measurements still limits their use in local protection and advanced monitoring.

PMUs were later introduced to provide time-synchronized phasor measurements of bus voltages and both injected and branch currents in power systems [88]. Using a universal Global Positioning System (GPS) signal, all PMUs align their measurements to a unified time reference [89]. Typically, PMUs sample waveforms at 48 samples per cycle and report measurements at rates of 0.5–1 report per cycle, where discrete Fourier transform is used to measure the phasor from the current and voltage transducer signals. In addition to voltage and current phasors, they also measure frequency, rate of change of frequency, sequence components, and THD, making them foundational to modern Wide Area Monitoring Systems (WAMSs) and essential for advanced steady-state and dynamic, control and protection applications in SPSs [90].

In distribution systems, Feeder Terminal Units (FTUs), a type of RTUs, are deployed at feeder heads in primary and secondary distribution substations [91]. To enhance network observability, AMIs with Smart Meters (SMs) are widely installed along feeders and transformers, measuring phases, voltages, currents, active/reactive power, and power factor. Although SMs can sample data at 30 Hz, their reporting intervals typically range from 15 to 60 minutes, and

in some cases, once every 24 hours, depending on communication bandwidth and local storage capacity [92].

In 2014, distribution level PMUs, known as μPMUs, were introduced through a collaboration between UC Berkeley and Power Standards Lab [93]. While maintaining the synchronization and phasor measurement capabilities of conventional PMUs, μPMUs offer enhanced performance with a sampling rate of 512 samples per cycle and reporting rates up to 120 measurements per second. They also feature higher resolution 0.01° in angle and phasor magnitude with total vector error under 0.7% [94]. These improvements are tailored for distribution systems, where short line lengths and small voltage drops require high-resolution measurements. Moreover, their high sampling rate enables accurate detection of high-order harmonics, addressing the noise-prone nature of distribution networks and the presence of inverter-based DERs.

Despite the advancement of AMIs and μPMUs, achieving full observability in distribution networks remains challenging due to the high number of nodes, which necessitates deploying a large number of SMs and μPMUs, leading to significant motioning costs [95]. To address this, historical data are often used to generate pseudo-measurements at the load side, which are then integrated into the Distribution System State Estimation (DSSE) algorithm [96]. Additionally, Zero Injection Bus (ZIB) provide virtual measurements of injected power and current to improve observability. More recently, researchers have explored indirect measurements from PMUs and μPMUs, where additional measurements are inferred through iterative application of Ohm's and Kirchhoff's laws across the network, enhancing the overall monitoring quality and SPSs observability [97].

In addition to electrical quantities used in SE, AGC, and protection applications, the monitoring system also collects critical data for other EMS application, such as DERs output, ESSs energy state and SoC, market signals, and other information required by the central control system [98].

2.2.2 Central Control System Applications

The central control system receives primary information from the physical layer via wired or wireless communication. After verifying the data against potential cyberattacks, it is used in various management, control, and protection applications, generally categorized into: 1) steady-state, and 2) dynamic applications [99]. Figure 2.3 summarizes common control and protection functions performed by the central control system.

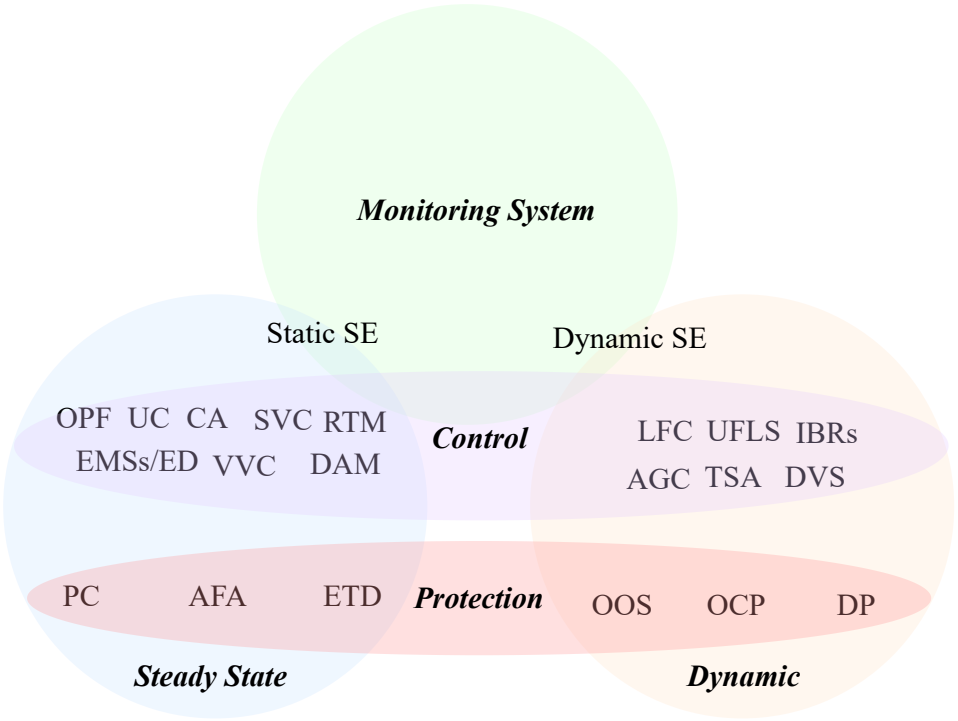


Figure 2.3: List of Steady-State and Dynamic Applications Performed by Central Control Systems.

2.2.2.1 Steady-State Operation

In steady-state operation, SPSs operators focus on optimal system management, including scheduling, capacity limits, voltage regulation, market assessments, and energy imbalance detection, where steady-state energy flow models are utilized [100]. One of the most common steady-state control applications is OPF, which aims to determine the optimal operating state of the power system. This includes identifying optimal setpoints for generators, RESs, storage units, tap changers, and shunt capacitors, as well as estimating the corresponding phasor voltages and currents across buses [101]. ED and EMS are additional applications that coordinate generation, storage, RESs, and flexible loads, often incorporating market analysis to determine the optimal operation of a single system or an IES [102]. While OPF and ED are similar in functionality, the main difference lies in system modeling. ED typically treats the system as a single bus, omitting power flow constraints for simplification, especially when supply and demand are co-located or the grid is spatially compact. One of the most common applications of ED is in the operation and management of μgrids [103].

Similarly, Unit commitment (UC) applications aims to determine the operation scheduling of the power generation, indicating turned on or off scheduling of generator to meet electricity demand over a specific time horizon (typically 24-48 hours), while minimizing the electricity cost. This problem is solved considering the piratical constraints of the generators ramp limits and on/off operation cost, while accounting for maintenance scheduling of the generation units [104]. In addition, Contingency Assessment (CA) aims to analyze the system reliability under $N-1$ contingency of system equipment failure and find the optimal operation strategy such as power system reconfiguration to increase the reliability index [105]. On the other hand, VVC and Secondary Voltage Regulation (SVR) aim to regulate voltage levels by managing reactive power. VVC coordinates devices like capacitor banks, on-load tap changers, shunt reactors, SVCs, STATCOMs, and inverter-based DGs to maintain system voltage within limits [14]. SVR extends VVC with real-time data and communication technologies, enabling adaptive voltage control based on system condition to ensure voltage stability across the SPS [106].

From a market perspective, DAM and RTM are critical clearing mechanisms that optimize the selection of energy resources to meet system demand [107]. The DAM relies on forecasted data for load and RESs generation to schedule energy delivery one day in advance. It allocates contracts to energy providers based on their submitted bids, availability, and capacity, ensuring cost-effective day-ahead scheduling. The RTM, in contrast, operates closer to real-time and addresses discrepancies between forecasted and actual system conditions. It leverages fast-ramping and dispatchable resources, such as gas turbines, hydropower, or battery storage, to rebalance supply and demand, ensuring both market efficiency and operational reliability of SPSs [108]. Together, DAM and RTM facilitate economic operation, price transparency, and grid stability under variable and uncertain conditions.

Steady-state protection applications in the central control system include Protection Coordination (PC), Arc Flash Analysis (AFA), and Energy Thief Detection (ETD). PC determines optimal relay settings an, such as pickup current and coordination between primary and backup zones, to ensure selective fault isolation [109]. AFA assesses fault-related risks, including arc flash detection, severity analysis, and mitigation strategies during abnormal operating conditions [110]. ETD detects energy imbalances caused by electricity theft or abnormal consumption patterns, distinguishing them from high-impedance faults, and supports localization and corrective actions [111].

2.2.2.2 Dynamic Operation

In dynamic operation, SPSs operators focus on maintaining system stability and reliability by managing frequency, voltage, and synchronization during load/generation variations or fault events. These dynamics are typically modeled using state-space representations or high-order transfer functions [112]. AGC and LFC play key roles in regulating system frequency by adjusting generator outputs and tie-line power flows between control areas [113]. When these mechanisms fail to restore frequency within safe margins, Under Frequency Load Shedding (UFLS) is triggered to shed sufficient load in a controlled manner, preventing cascading failures and full system blackout [114].

Transient Stability Analysis (TSA) is used to evaluate the transient stability of power systems by analyzing the behavior of synchronous generators during and after disturbances such as short circuits or line faults. It primarily monitors the rotor angle dynamics and critical clearing time to determine whether generators remain synchronized following a disturbance [115]. Traditionally, TSA focused on large synchronous machines; however, with the increasing integration of RESs, DGs, and ESSs, the scope of TSA has expanded to include Inverter-Base Resources (IBRs). These resources lack physical inertia and rely on control-based virtual inertia, requiring adapted TSA methods to assess their contribution to system stability [116]. Meanwhile, Dynamic Voltage Stability (DVS) focuses on evaluating voltage stability during transient events, such as sudden changes in load demand or fault conditions. It aims to determine whether the system can maintain acceptable voltage levels and avoid voltage collapse under dynamic and stressed scenarios [117].

From a protection standpoint, Out-of-Step (OOS) protection is designed to detect generator loss of synchronism by monitoring the phase angle deviation between generators or system areas. Once detected, it initiates controlled islanding or tripping of affected generators or IBRs to prevent cascading failures and ensure system stability [118]. Over Current Protection (OCP), in contrast, focuses on detecting and isolating parallel faults such as phase-to-phase or phase-to-ground short circuits. It operates by identifying abnormal increases in current and sending tripping signals to appropriate protection relays for fault clearance [119]. Additionally, Differential Protection (DP) is employed to protect individual components like power transformers by monitoring differential current, i.e., the difference between incoming and outgoing current, and detecting internal faults or insulation failures. When the differential exceeds a set threshold, a trip signal is issued to isolate the equipment [120].

2.2.3 Power System Control Elements and Actuators:

Once the primary information is processed by the central control system, the decision making is reflected in form of setpoint distributed across the control elements and actuators within the SPSs [121]. In general, actuators within power system can be divided into active power actuators, reactive power actuators, and stability and protection actuators, which aims to ensure the stability of the SPSs frequency, voltage and reliability of the system [122]–[124].

Active power actuators are responsible for regulating active power generation and consumption within the SPSs, playing a critical role in maintaining frequency stability. These actuators include turbine governors in conventional generators, d-axis control in IBRs, output and curtailment control of RESs, and charge/discharge scheduling of ESSs. They also encompass control of energy conversion devices such as PtH and HtP, as well as setpoints determined by market clearing processes in DAM and RTM. Additionally, demand-side controls like DSM and DR enable load shedding and ancillary service participation signals. Collectively, these actuators form the basis of active power control strategies to ensure real-time balance between generation and demand [125].

Reactive power actuators regulate reactive power flow within SPSs, playing a vital role in maintaining voltage stability. These include excitation control in conventional generators, q-axis control in IBRs, on-load tap changers, and passive components such as capacitor banks, shunt capacitors, and reactors. Advanced power electronic devices, including static VAR compensators, static synchronous compensators, and other Flexible AC Transmission System (FACTS) devices, also serve as key reactive power actuators. Together, these elements form the foundation of voltage control strategies to ensure system reliability under varying load and generation conditions [126].

Protection actuators in SPSs are essential for ensuring system reliability, particularly during fault or abnormal operating conditions. These actuators include protection relays and circuit breakers deployed across all system levels including generators, transmission lines, busbars, transformers, and distribution substations. Common protection relays include over/under-frequency, loss of excitation, OOS, distance, overcurrent, differential, directional overcurrent, gas detection, earth fault, busbar differential, over/under-voltage, and rate-ROFC (ROFC) relays. Collectively, these devices implement coordinated protection schemes that isolate faults and preserve system integrity [119].

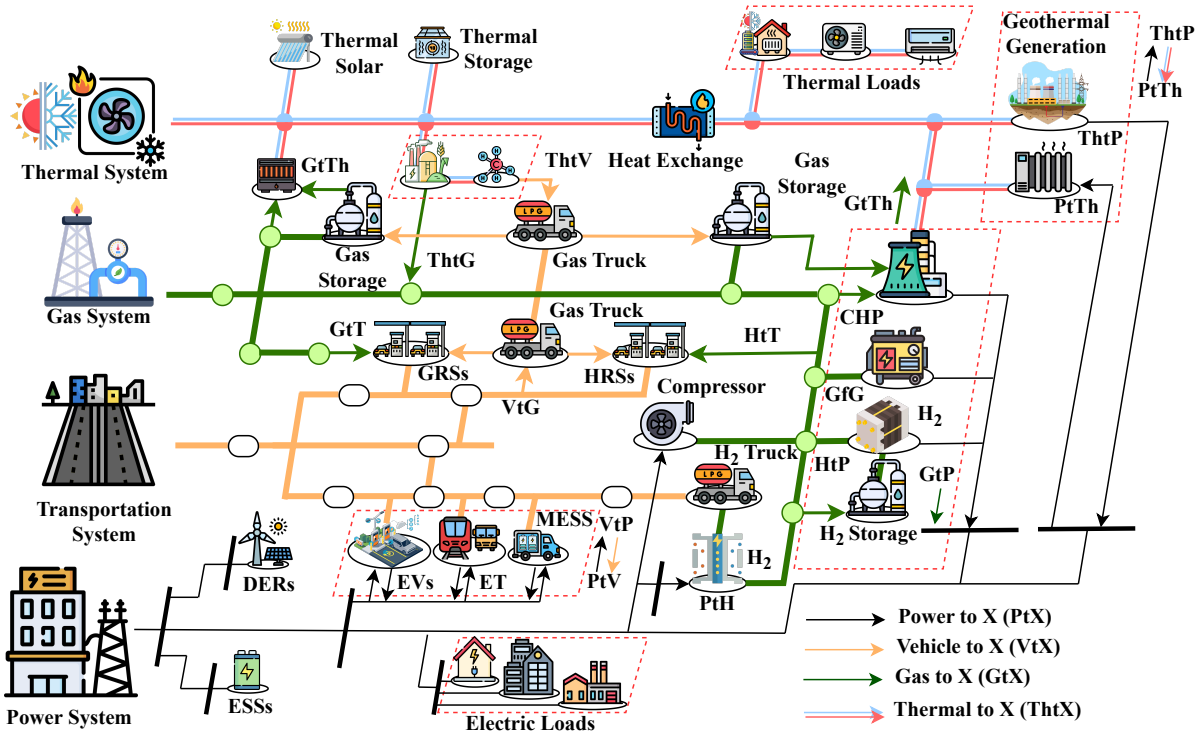


Figure 2.4: Structure of the deep IESs including electric power, transportation, gas, and thermal energy systems.

Together, primary and secondary information constitute the active data exchanged between the cyber and physical layers of SPSs. Securing this bidirectional communication is essential for maintaining overall CPPS security.

2.3 Structure of Integrated Energy Systems

The integration of multiple energy carriers, referred to as IESs, is driven by the urgent need for cleaner, more sustainable energy systems. This integration enhances efficiency, operational flexibility, and reliability while supporting global decarbonization efforts and climate change mitigation [4]. However, it also introduces greater complexity in system management and control. Unlike traditional systems with limited interdependencies, IESs involve deeply interconnected subsystems, requiring enhanced coordination supported by more advanced ICTs infrastructure within the cyber-physical layers [127]. The electric power system serves as the foundational of this integration, playing a central role in decarbonization and supporting the electrification of various energy sectors such as transportation, heating and cooling, gas, and water systems [128].

This integration is facilitated by emerging technologies of PtX and XtP, which enable seamless energy conversion and sector coupling [129].

Figure 2.4 illustrates the deep and complex integration among various energy systems, including electric power, transportation, gas, and thermal networks. These systems are interconnected through emerging technologies that enable X-to-X energy conversion within IESs. Some technologies facilitate unidirectional energy flow, such as PtH, which links the power system to the gas network or transportation via liquid hydrogen [130], while others enable bidirectional flow. For instance, EVs and Electric Transit (ET) allow electric energy to flow from the power system to vehicles in GtV mode and back to the grid in VtG mode, supporting electric grid management applications [131]. Additionally, technologies like Combined Heat and Power (CHP) connect multiple energy carriers simultaneously, linking the gas system with both power and thermal networks [132]. This cross-sector integration significantly alters system-level steady-state energy flow and dynamics, necessitating advanced real-time monitoring, control, and protection mechanisms for reliable and efficient IESs operation [133].

The steady-state operation of IESs can be represented by modeling each constituent system within its domain. The electric power system is modeled using conventional buses, transmission lines, generation units, including both conventional and DER sources, load centers, and storage units that can function as both generators and loads. The transportation system can be represented at varying levels of detail, either as a network of travel nodes and distances or with more granularity by incorporating traffic flow modeling in time domain [134]. The gas system is modeled through gas nodes, pipelines, gas loads, supply nodes, and active lines equipped with compressors for pressure regulation and gas flow control [135]. Meanwhile, the thermal energy system is represented by heating and cooling nodes, thermal loads, thermal storage units, and heat-exchange components [136]. Adopting energy flow models for IESs requires accurate modeling of cross-sector energy conversion technologies **X-to-X** and the development of advanced energy flow analysis tools to address the increasing complexity of these systems. The subsequent sections explore the steady-state energy flow modeling of SPSs, with a focus on the influence of IESs integration from the perspective of the electric power system. Emphasis is placed on the role of PtX and XtP technologies in enabling cross-sector energy interactions.

2.3.1 Electric Smart Power System Model

Electric power systems are typically modeled as interconnected networks comprising set of Buses $\boldsymbol{\mathcal{B}}$, Transmission lines $\boldsymbol{\beta}$, Loads $\boldsymbol{\mathcal{D}}$, generators $\boldsymbol{\mathcal{G}}$, and storage units $\boldsymbol{\mathcal{S}}$. At each bus $b \in \boldsymbol{\mathcal{G}}$ where a generator is located, active power $P^{G}_{t,b}$ and reactive power $Q^{G}_{t,b}$ are injected into the network and transmitted through the lines to supply the active $P^{D}_{t,b'}$ and reactive $Q^{D}_{t,b'}$ power demands at load buses $b^{'} \in \boldsymbol{\mathcal{D}}$. Under a given load and generation condition at time t, the steady-state power flow analysis determines the voltage magnitude $|V_{t,b}|$ and phase angle $\delta_{t,b}$ at each bus under balanced system. The power system can be formulated using the power balance equations given as:

$$\begin{aligned} P^{G}_{t,b} + P^{ch,s}_{t,b} + P^{XtP}_{t,b}\left(\Theta_{P,X}\right) - P^{D}_{t,b} - P^{dch,s}_{t,b} - P^{PtX}_{t,b}(\Theta_{P,X}) = \\ |V_{t,b}| \sum_{b' \in \boldsymbol{\mathcal{B}}} |V_{t,b'}| \left(\mathtt{G}_{bb'} \cos\theta_{t,bb'} + \mathtt{B}_{bb'} \sin\theta_{t,bb'} \right), \forall t \in \boldsymbol{\mathcal{T}} \wedge b, b^{'} \in \mathcal{B} \end{aligned} \tag{2.1}$$

$$\begin{aligned} Q^{G}_{t,b} + Q^{ch,s}_{t,b} + Q^{XtP}_{t,b}\left(\Theta_{P,X}\right) - Q^{D}_{t,b} - Q^{dch,s}_{t,b} - Q^{PtX}_{t,b}(\Theta_{P,X}) = \\ |V_{t,b}| \sum_{b' \in \boldsymbol{\mathcal{B}}} |V_{t,b'}| \left(\mathtt{G}_{bb'} \sin\theta_{t,bb'} - \mathtt{B}_{bb'} \cos\theta_{t,bb'} \right), \forall t \in \boldsymbol{\mathcal{T}} \wedge b, b^{'} \in \mathcal{B} \end{aligned} \tag{2.2}$$

In this context, $P^{\mathrm{ch},s}_{t,b}$ and $Q^{\mathrm{ch},s}_{t,b}$ represent the active and reactive charging power, while $P^{\mathrm{dch},s}_{t,b}$ and $Q^{\mathrm{dch},s}_{t,b}$ denote the discharging active and reactive power of storage system s at bus b. Additionally, $P^{XtP}_{t,b}(\Theta_{P,X})$, $Q^{XtP}_{t,b}(\Theta_{P,X})$, $P^{PtX}_{t,b}(\Theta_{P,X})$, and $Q^{PtX}_{t,b}(\Theta_{P,X})$ represent the active and reactive power exchanged between the power system and another energy system, either from external systems to power (XtP) or from power to external systems (PtX). These power flows are functions of the interdependent system states, denoted by $\Theta_{P,X}$. Also, $\mathtt{G}_{bb'}$ and $\mathtt{B}_{bb'}$ denote the conductance and susceptance, respectively, of the transmission line connecting buses b and $b^{'}$, while $\theta_{t,bb'} = \delta_{t,b} - \delta_{t,b'}$ represents the phase angle difference between them. The power system operation is further constrained by the thermal limits of the transmission lines and the allowable voltage range at each bus, which must be respected to ensure reliable and secure system operation:

$$\underline{P^{F}_{bb'}} \leq P^{F}_{t,bb'} \leq \overline{P^{F}_{bb'}}, \forall t \in \boldsymbol{\mathcal{T}} \wedge b, b^{'} \in \mathcal{B} \tag{2.3}$$

$$\underline{Q^{F}_{bb'}} \leq Q^{F}_{bb'} \leq \overline{Q^{F}_{bb'}}, \forall t \in \boldsymbol{\mathcal{T}} \wedge b, b^{'} \in \mathcal{B} \tag{2.4}$$

$$\underline{V}_{b} \leq V_{t,b} \leq \overline{V}_{b}, \forall t \in \boldsymbol{\mathcal{T}} \wedge b \in \mathcal{B} \tag{2.5}$$

where $(\underline{.})$ and $(\overline{.})$ are notation of minimum and maximum power flow and voltage quantities.

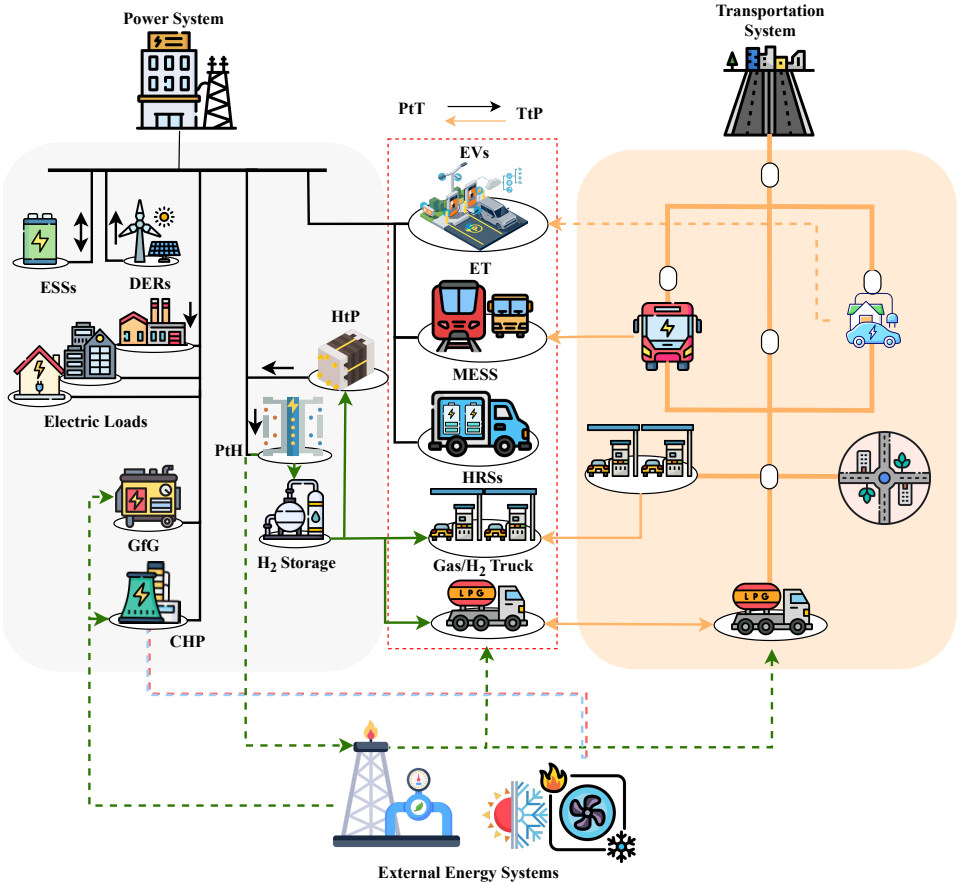


Figure 2.5: Integration of power and transportation systems.

2.3.2 Integrated Power and Transportation System

The integration between the power and transportation systems has significantly increased due to the ongoing electrification of transportation components, including light, medium, and heavy duty vehicles, such as EVs and ET [137]. Although the transportation system is not a distinct energy type system, it functions as a transportation layer that interconnects various IESs, enabling the movement and exchange of energy across different sectors [138]. This integration is facilitated through two primary pathways: 1) direct electric power exchange between the SPS and electrified transportation (e.g., GtV and VtG EVs operation modes), or 2) utilizing gas-based energy carriers as an intermediary medium connecting the two systems [139], as shown in Figure 2.5.

The direct integration between the SPS and the transportation system primarily occurs through the electrification of various classes of vehicles. These include: 1) *Light-duty vehicles*,

such as battery-based EVs, which operate entirely on battery power, and Plug-in Hybrid EVs, which combine battery systems with Internal Combustion Engine (ICE); 2) *Medium-duty vehicles*, including electric delivery vans, buses, and service trucks; and 3) *Heavy-duty vehicles*, such as regional electric trucks designed for medium to long-haul transportation [140]. These electrified transportation systems are primarily considered as dynamic and uncertain electrical loads on the SPS. Their aggregated impact introduces significant operational challenges, especially in terms of demand forecasting, load balancing, and ensuring voltage and frequency stability [141]. To accommodate the power demand of ETs, several charging technologies are deployed. These include Level 1 and Level 2 onboard AC charging, DC fast charging for rapid energy replenishment, battery swapping stations for quick battery replacement, and emerging wireless charging solutions that offer the convenience of contactless energy transfer [142]. Each charging technology, ranging from Level 1 and Level 2 AC charging to DC fast charging and wireless systems, has distinct implications for the grid in terms of energy draw rates, infrastructure planning, and the behavioral patterns of users. The variability in user charging behavior, combined with high spatial and temporal uncertainty in EV deployment, further complicates grid operation and planning [143].

While EVs typically act as electrical loads on the power system during GtV operation mode, their large-scale aggregation in residential areas, commercial buildings, and dedicated charging lots enables them to play a more active role during VtG operations [144]–[146]. In VtG mode, EVs and Mobile Energy Storage Systems (MESSs) can supply power back to the grid, contributing to grid services such as frequency regulation, voltage support, and peak shaving [147]. These services enhance overall grid stability and offer financial incentives to both utilities and EV owners. Nonetheless, the increasing penetration of EVs, coupled with their flexible charging and discharging capabilities, presents both challenges and opportunities. On one hand, uncoordinated charging can exacerbate peak loads, increase transformer aging, and lead to network congestion. On the other hand, coordinated charging strategies, demand response integration, and VtG functionalities transform EVs from passive consumers to active grid assets capable of supporting DERs integration and enhancing system resilience.

In contrast to direct electrification, gas-based transportation provides an alternative mode of integration between the power and transportation systems. In this approach, energy carriers such as hydrogen or natural gas are transported using gas trucks, linking production and consumption sites across different sectors. From the power system perspective, PtH technologies enable the utilization of surplus renewable electricity, especially during off-peak hours or periods

of overgeneration, to produce green hydrogen via electrolysis, thereby reducing renewable energy curtailment [148]. This hydrogen can subsequently be distributed through transportation infrastructure to serve fuel demand for hydrogen-powered vehicles, particularly in industrial, local, or remote mobility applications, representing a decentralized form of power-to-transportation energy integration. Moreover, gas trucks facilitate the reverse energy pathway by delivering hydrogen and natural gas to the power sector through various gas-to-power conversion technologies such as GfG, CHPs, and HtP units [149]. This bidirectional energy exchange strengthens the interdependency between power and transportation system, and highlights the role of the transportation system within the IESs.

2.3.2.1 Energy Conversion Between Power and Transportation Using Node-Based Methods

The energy conversion between the power and transportation systems is primarily represented by the electric demand imposed by EVs and ET on the power grid, and by the hydrogen demand of HRSs derived from power-to-gas conversion processes. In the early stages of integrated planning, the estimation of transportation-induced demand on the power system is often performed by modeling travel behaviors using PDFs [9]. These functions are used to statistically represent daily or weekly travel patterns and energy needs. Node-based methods further enhance this estimation by incorporating the stochastic characteristics of vehicle arrival and departure times, initial and required SoC, or trips energy consumptions, and the number of expected vehicles requiring services throughout the day [97], [150]. By integrating real-world data such as charging station utilization rates and historical charging session profiles, PDFs can be calibrated to reflect realistic transportation demand dynamics. These models are essential for generating representative demand scenarios in stochastic optimization frameworks for planning and operational purposes. Such frameworks can support the optimal siting and sizing of charging infrastructure, determination of the number and types of chargers, charge/discharge scheduling, battery swapping logistics, and hydrogen production sizing for HRSs [151]–[155]. This integrated planning approach ensures not only sufficient energy supply but also improves system reliability, cost-effectiveness, and alignment with renewable energy availability.

In node-based demand analysis, two main principles are commonly adopted for modeling EVs and ET charging behavior. The first is the First-Come, First-Served principle, which is predominantly applied in DC fast charging stations where no coordinated charging strategies

are implemented [156]. Under this approach, the charging demand is determined solely based on the sequential arrival of vehicles and the available charger capacity. In this context, the total energy demand is predefined as the aggregate energy requirements of the arriving vehicles, constrained by the rated power of the chargers and the number of charging lots. The second principle is applied in scenarios where the arrival and departure times of EVs are flexible within a wide time window. In such cases, there is no strict requirement to charge the vehicles in the shortest possible time. Instead, an optimal charging and discharging schedule can be determined through the charging station's EMS [157]. This framework is particularly suitable for commercial and residential buildings, where EVs are typically parked for extended periods. Under these conditions, both GtV and VtG operational modes can be implemented using bidirectional chargers. Consequently, the transportation system's power demand becomes a controllable variable governed by the EMS's charging and discharging decisions, thereby enabling energy exchange between the power and transportation systems [158].

2.3.2.2 Energy Conversion Between Power and Transportation Using Network Flow Models

Node-based methods are generally effective in scenarios with low EVs adoption rates or where charging stations are sparsely distributed and separated by long distances [159]. Under these conditions, spatial correlations between charging stations, charging times, and traffic congestion have minimal influence on drivers' decisions regarding where to charge. However, in urban areas with multiple charging stations offering varying capabilities and pricing schemes, along with dynamic traffic conditions, these factors significantly affect route planning and charging station selection. In such contexts, EVs drivers tend to choose charging locations based on total travel time, comprising both driving and charging durations, and the associated charging cost [160]. To better capture these dynamics, network flow models are employed to estimate the expected vehicle flow across the transportation network, enabling more accurate assessments of EVs demand and aggregation potential [161].

A typical transportation network is represented as a graph $G^T = (\boldsymbol{\mathcal{N}}^T, \boldsymbol{\mathcal{R}}^T)$, where $\boldsymbol{\mathcal{N}}^T$ denotes the set of nodes, such as zones or intersections, and $\boldsymbol{\mathcal{R}}^T$ denotes the set of links or roads within the network. In the transportation network, each vehicle has an origin point o and a destination point d, forming origin-destination pairs $(o, d) \in (\mathcal{O}, \mathcal{D}^T)$. The transportation demand is represented by a matrix $\boldsymbol{\mathcal{Q}} \in \mathbb{R}^{\boldsymbol{\mathcal{N}}^T \times \boldsymbol{\mathcal{N}}^T}$, where each element $q_{o,d}$ denotes the traffic

demand (in vehicles/hour) from origin o to destination d [162]. In such complex network, the actual distribution of traffic flows is predominantly influenced by driver behavior and traffic assignment decisions. Therefore, determining the equilibrium traffic flow requires incorporating user behavior models [163]. Ideally, the transportation network reaches an equilibrium under the *Social Optimum* principle, where the total travel time across the network is minimized, which assumes that all drivers across the transportation network cooperate to reduce overall congestion. Consequently, some drivers may accept longer travel times if doing so leads to a net reduction in total travel time for all users [162], [164]. However, the *Social Optimum* remains largely a theoretical concept, as its realization requires a centralized control mechanism and the full cooperation of all drivers to prioritize collective benefits over individual preferences.

In real-world scenarios, drivers tend to exhibit selfish behavior, where each individual aims to minimize their own travel time. As a result, the transportation system typically reaches a steady state, or an acceptable traffic assignment, when a User Equilibrium (UE) is achieved [165]. The concept of UE is based on the assumption that as long as drivers can reduce their travel time between an origin–destination pair (o, d) by choosing an alternative path $p^{th} \in \boldsymbol{\mathcal{P}}_{o,d}$, the traffic pattern will continue to change dynamically. Equilibrium is only established when no driver can further reduce their travel time by unilaterally switching routes.

2.3.2.3 Cyber-Physical Layers of Integrated Power and Transportation System

To address the complex integration of power and transportation systems, as well as the uncertainties associated with EVs and ET, ICT infrastructures are deployed within the integrated framework. While such information has traditionally been utilized solely by transportation operators, sharing it with SPSs operators has become essential to ensure the reliability, functionality, and stability of the SPS [166]. In this integration, the primary information obtained from the physical power and transportation layers is expanded to include transportation-related information such as: 1) expected arrival and departure times, along with the SoC and required energy demand of EVs; 2) trip schedules of ET; 3) expected hydrogen-powered vehicle demand at HRSs and corresponding hydrogen tank SoC; 4) transportation traffic flow and expected travel times between origin–destination pairs; 5) EVs aggregation capacity for VtG operation mode, as well as owners' willingness to participate; and 6) MESS locations and their available energy levels.

The primary information is then processed within the central control system to determine the optimal set of coordinated actions. For the transportation system elements, these actions

include: charging and discharging schedules of EVs, target departure SoC, battery swapping schedules for ET, setpoints for PtH and HtP operations, as well as trip scheduling and charging/discharging plans for MESSs [167]–[171]. Both primary and secondary information from the transportation system introduce new cybersecurity vulnerabilities that can be exploited by malicious actors to disrupt the operation of both the power and transportation systems. Such cyber-attacks may aim to manipulate traffic flow data, falsify charging/discharging schedules, alter SoC reports, or compromise VtG participation signals, ultimately reducing the profitability, stability, and reliability of both integrated infrastructure.

2.3.3 Integrated Power and Natural Gas System

The integration between the power and gas systems is one of the earliest forms of IESs, originating from the widespread use of conventional natural gas-fired generators to produce electricity [172]. Over time, this interconnection has deepened with the advent of emerging technologies such as PtG and GtP, which enable bidirectional energy conversion between the two systems. When coupled with renewable generation, these technologies facilitate the production of green hydrogen, achieved with zero direct emissions, thereby supporting global decarbonization targets and enhancing system flexibility, long-term energy storage capability, and sector coupling benefits [173].

The integration between power and gas systems is enabled by PtH units, which convert surplus electrical energy into hydrogen, facilitating the power-to-gas pathway. The produced hydrogen can be utilized locally through dedicated storage systems, transported via hydrogen trucks to gas loads, or injected directly into the gas network through interconnected gas nodes [174]. Gas compressors are employed to regulate flow and pressure [175]. Hydrogen may be injected in its original form or further processed via methanation to produce synthetic natural gas, ensuring compatibility with existing natural gas infrastructure. The gas-to-power pathway can follow multiple routes. Pure hydrogen from the gas network can be supplied to HtP units or delivered via hydrogen trucks to local hydrogen storage systems to meet power demands. Alternatively, natural gas, either extracted from pipelines or transported by trucks to local storage, can be used in GfG or CHP units to generate electricity [176].

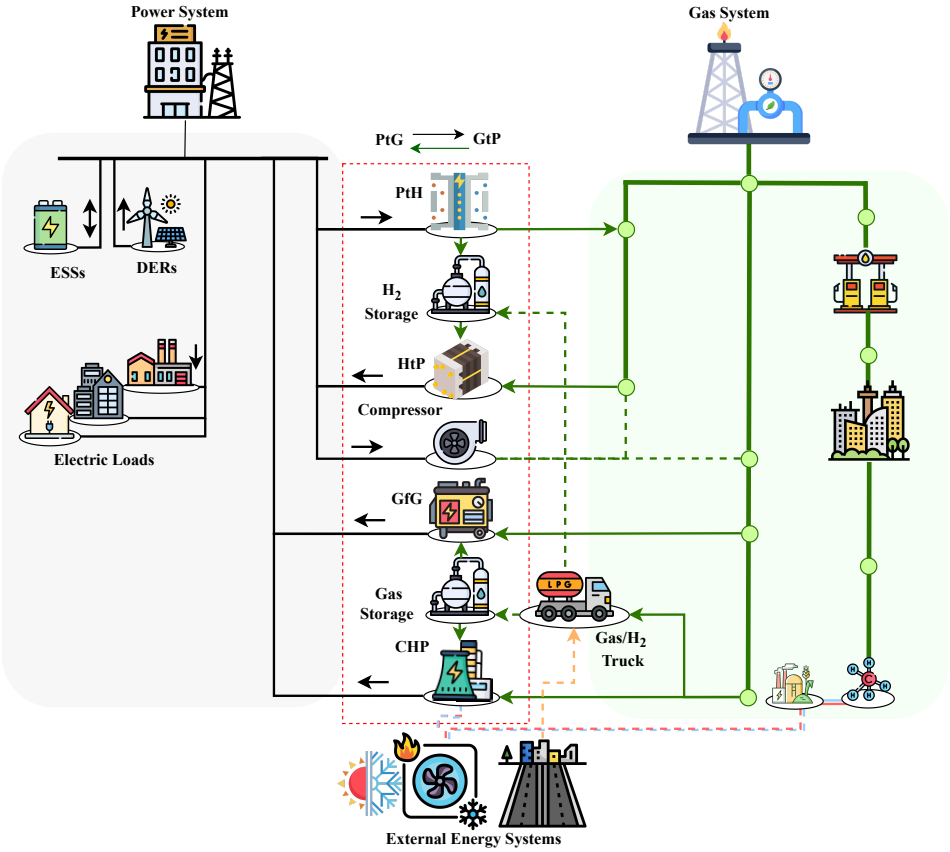


Figure 2.6: Integration of power and gas systems.

2.3.3.1 Energy Conversion Between Power and Gas Systems

Similar to power systems, gas systems can be represented as a graph $G^G = (\boldsymbol{\mathcal{N}}^G, \boldsymbol{\mathcal{L}}^G)$, where $\boldsymbol{\mathcal{N}}^G$ denotes the set of gas nodes interconnected by a set of pipelines $\boldsymbol{\mathcal{L}}^G$. For a given gas node $i \in N^G$, the gas demand is denoted as $G^D_{t,i}$, and the gas supply from wells or injection points is denoted as $G^G_{t,i}$. Gas flow in the network is governed by the nodal pressure $\Pi_{t,i}$, the hydraulic resistance coefficient of the pipeline $\mathcal{C}^2_{ii'}$, and the type of pipeline, either **passive** (natural pressure-driven flow) or **active** (flow assisted by a gas compressor).

The integrated power–gas model considers two coupling mechanisms linking the power to the gas system. The first coupling is achieved through PtH units, which consume electrical energy to produce hydrogen gas. The second coupling involves gas compressors, which draw electric power from designated buses to regulate pressure within active gas pipelines in the gas network. From the gas system is linked to the power system via HtP, GfG, and CHP units. The electric power generated by each unit is represented by their overall energy conversion rate, i.e, the

component efficiency multiplied by the specific energy in MWh/m^3 of the input gas source.

2.3.3.2 Cyber-Physical Layers of Integrated Power and Gas System

The coordinated operation of integrated power and gas systems necessitates continuous information exchange, as well as centralized control and coordination between both infrastructures. Within this integration, optimal operation and control, managed through the EMS, requires acquiring additional key primary information and operational data from the gas network. Such data include the current operational state of the gas grid, i.e, the pressures at gas nodes and the gas flows in pipelines, the SoC of local gas and hydrogen storage tanks, and the temperature and pressure measurements of PtH and HtP units. Furthermore, the operational states of GfG and CHP units, as well as information on the expected arrival times and quantities of gas and hydrogen deliveries from transport trucks, are also used.

Based on these primary information, the central control system and the EMS determine and dispatch optimal control actions to the physical layer of the gas system. These actions include setting the power setpoints for PtH and HtP units, as well as for GfG and CHP units, thereby enabling coordinated power conversion between the two networks. In addition, compressor power setpoints are issued to regulate gas flow within the network, ensuring both safe operation and optimal performance [177]. Both primary and secondary information obtained from the gas system introduce additional cybersecurity vulnerabilities that may be exploited by malicious actors to compromise the coordinated operation of the power and gas networks. Potential cyberattacks could target the manipulation of gas node pressure and pipeline flow measurements, falsification of power conversion setpoints, alteration of storage tank SoC values, or disruption of grid services and DR signals. Such attacks can degrade the profitability, stability, and overall reliability of the IES infrastructure, thereby posing significant risks to its secure and resilient operation.

2.3.4 Integrated Power and Heat System

The integration of power and heat systems is a key component of modern IESs, driven by objectives such as improving overall efficiency, enabling sector coupling, and supporting decarbonization efforts [132]. Traditionally, this integration has been achieved using CHP units, which simultaneously produce electricity and useful heat from a single energy source, thereby increasing total conversion efficiency and reducing GHG emissions. With the growing penetra-

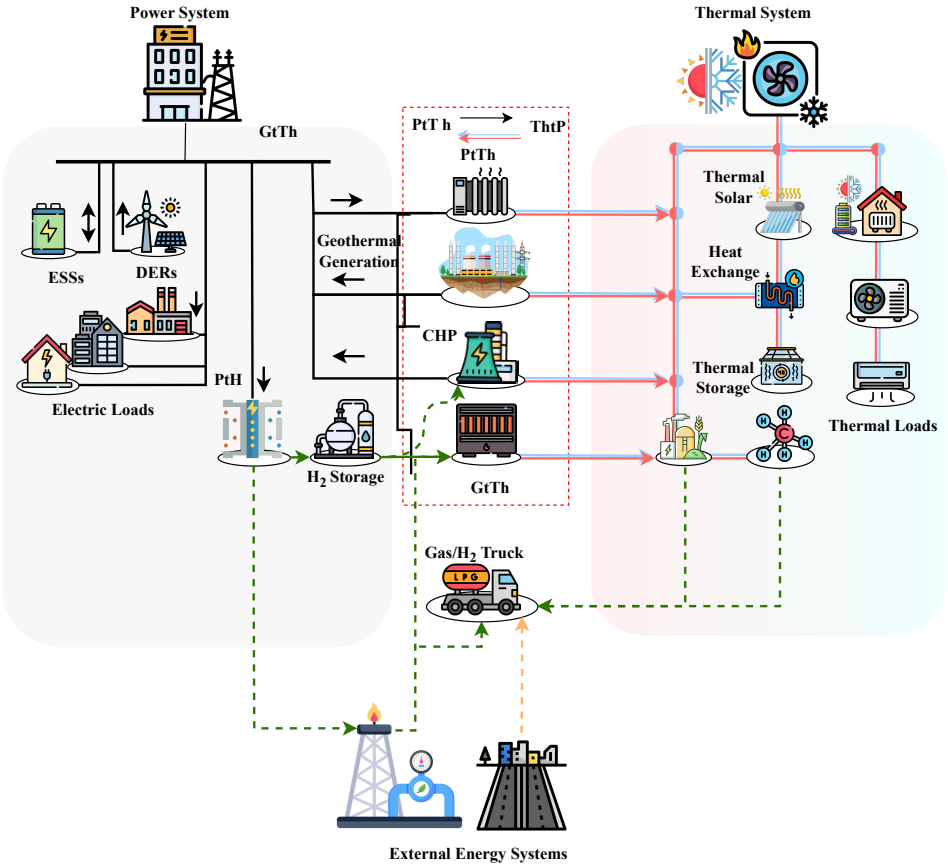


Figure 2.7: Integration of power and heat systems.

tion of renewable energy, emerging technologies such as Power-to-Thermal (PtTh) units and advanced thermal ESSs now facilitate more flexible, bidirectional interactions between the two systems, as illustrated in Figure 2.7.

In the power-to-thermal pathway, surplus electrical energy can be converted into heat using electric boilers, heat pumps, or resistive heating elements. The resulting thermal energy may be directly supplied to district heating networks, stored in thermal tanks, or utilized in industrial heating processes [178]. Conversely, in the thermal-to-power pathway, waste heat from power generation or industrial processes can be upgraded through absorption chillers or heat pumps to meet district heating or other thermal demands, thereby enhancing system efficiency and operational flexibility. Thermal energy storage is pivotal in this coupling, as it decouples heat production from instantaneous demand, enabling load shifting, peak shaving, and improved accommodation of variable renewable generation.

2.3.4.1 Energy Conversion Between Power and Heat Systems

Similar to the modeling of power and gas networks, the district heating system can be represented as a weighted graph $G^H = (\boldsymbol{\mathcal{N}}^H, \boldsymbol{\mathcal{L}}^H)$, where $\boldsymbol{\mathcal{N}}^H$ is the set of heat nodes (e.g., substations, storage units, or consumer locations) and $\boldsymbol{\mathcal{L}}^H$ is the set of pipelines connecting these nodes. For a given heat node $i \in \boldsymbol{\mathcal{N}}^H$, the thermal demand is denoted by $H^D_{t,i}$, while the thermal supply from heat production units or storage facilities is denoted by $H^G_{t,i}$. Heat transfer within the network is governed by temperature differences between nodes, the mass flow rate of the circulating medium, and thermal losses in the pipelines, where nodal heat balance ensures that, for each node, the net heat injection equals the difference between supplied and demanded heat, matching the net inflow from connected pipelines. The coupling between the power and heat systems is primarily realized through CHP units, electric boilers, and heat pumps.

2.3.4.2 Cyber-Physical Layers of Integrated Power and Heat System

The coordinated operation of integrated power and heat systems requires continuous bidirectional energy exchange, as well as centralized control and information sharing between both infrastructures. Within this integration, optimal operation and control, managed through the EMS, necessitates acquiring additional primary information from the district heating network. Such primary information includes the thermal demand at each heat node, water mass flow rates in pipelines, inlet and outlet temperatures at heat exchanger stations, and the thermal storage SoC. Additionally, operational parameters of electric boiler, heat pump, and CHP units, are collected. Weather forecasts, particularly ambient temperature and solar radiation, are also part of the primary information, as they directly influence heating demand and renewable-based thermal generation.

Based on this primary information, the central control system and the EMS compute and dispatch optimal setpoints to the physical layer of the heat system. These control actions include thermal output adjustments for electric boiler, and heat pump units, load allocation for CHP plants, and charging/discharging commands for thermal storage systems. Furthermore, pump speed setpoints and valve positions are optimized to regulate water flow and temperature levels across the heating network, ensuring both efficient operation and service reliability. Secondary information, on the other hand, includes aggregated system performance indicators such as heat-to-power ratios, network thermal losses, and predicted load profiles for different operational scenarios. This processed information supports strategic decision-making and improves

the coordination of both energy networks. However, the reliance on real-time measurements and bidirectional control signals introduces additional cybersecurity risks. Potential cyber-attacks could involve falsifying thermal demand data, altering pipeline flow or temperature measurements, tampering with storage SoC values, or manipulating setpoints for electric boilers, heat pumps and CHP units. Such disruptions could lead to imbalances between power and heat supply, increased operational costs, and reduced system reliability, posing significant threats to the secure and resilient operation of the integrated infrastructure.

2.4 Cyber-Physical Security Background and Taxonomy

The CPSs underlying modern SPSs and IESs rely extensively on ICTs for monitoring, control, and coordination. This heavy dependence on digital infrastructure exposes such integrated systems to a broader spectrum of cyber-attacks and vulnerabilities originating from multiple interconnected domains. Consequently, cybersecurity has emerged as a critical concern for modern SPSs and their cross-sectoral integration. Although established cybersecurity measures exist for SPSs, these protections are primarily designed for the operational characteristics of the power sector alone. As the complexity of IESs continues to grow, driven by the deeper coupling of CPSs components, current security protocols remain largely limited to sector, specific standards, with insufficient adaptation to the interconnected and multi-domain nature of IES infrastructures. This results in a limited understanding and inadequate deployment of advanced cybersecurity strategies capable of addressing the unique threats and interdependencies present in IESs [7].

2.4.1 Cyber-Physical Incidents

Cyberattacks on critical infrastructure IESs, including electric power, transportation, gas, district heating, nuclear facilities, and transportation, have intensified in scale, technical sophistication, and potential societal impact over the past two decades. Documented incidents, both confirmed and suspected, reveal how malicious actors exploit central control systems, communication networks, and operational protocols to disrupt essential services. While some attacks have been purely disruptive, others have damaged equipment, endangered human life, or served as reconnaissance for future campaigns [179].

In early 2024, Ukrainian authorities identified the *FrostyGoop* malware, designed to send

unauthorized Modbus/TCP commands to district heating controllers, which deprived over 600 apartments of heat for 48 hours during subzero weather [180]. In late 2023, U.S. agencies reported that a group Volt Typhoon had compromised routers and gained persistent access to the networks of U.S. power utilities, oil/gas pipeline operators, and transportation hubs, raising concerns of preparatory actions for coordinated disruptions [181]. In November 2022, Russia's Sandworm unit combined physical sabotage with cyberattacks on a Ukrainian substation, remotely tripping breakers and deploying data-wiping malware to hinder restoration efforts [6]. Earlier that year, the Industroyer2 malware, a successor to the 2016 grid, targeting framework, was detected and neutralized before it could disrupt power operations.

In May 2021, the Colonial Pipeline ransomware incident, attributed to the DarkSide group, disrupted the transport of approximately 2.5 million barrels of fuel per day along the U.S. East Coast. The attackers infiltrated the network via stolen VPN credentials, exfiltrated 100 GB of data, and encrypted operational systems, forcing a full shutdown that triggered fuel shortages and price spikes [182]. That same year, Brazilian state utilities Eletrobras and Copel suffered ransomware attacks that temporarily disabled some nuclear power control systems [183]. On March 5, 2019, two U.S. utilities in California and Utah experienced a DDoS attack that disrupted internal IT systems, though power delivery was not affected [184]. In April 2018, cyberattacks on the communication systems of three U.S. natural gas pipeline companies caused multi-day service outages [185].

Transportation has also been targeted by cyber-attacks. In May 2015, a cybersecurity consultant claimed to have accessed a United Airlines 737's flight control systems through its in-flight entertainment interface, allegedly issuing commands that altered engine performance [186]. In December 2015, Ukraine suffered the first publicly confirmed blackout caused by a cyberattack, when BlackEnergy malware remotely opened breakers at three substations, cutting electricity to approximately 225,000 customers and deploying wipers to erase operational data [187]. Earlier that year, a Chatham House report highlighted security risks in civil nuclear plants, including the circumvention of air-gapped systems by temporary network connections left in place by contractors [188].

Nuclear facilities have been long-standing targets. In December 2014, South Korea Hydro and Nuclear Power Company was breached by hackers who exfiltrated sensitive data from its commercial networks, which support 23 nuclear reactors; while no operational disruption occurred, the incident signaled rising extortion attempts in the nuclear sector [189]. In 2010, the Stuxnet

worm exploited multiple zero-day vulnerabilities to infect Iranian nuclear enrichment facilities' programmable logic controllers, delivered via USB drives into air-gapped systems. The malware manipulated centrifuge speeds to induce mechanical stress while feeding false sensor data to operators, ultimately damaging a substantial portion of Iran's enrichment capacity [190]. Beyond energy systems, failures in aviation IT systems have also demonstrated the high impact of cyber incidents, with operational disruptions causing significant economic and logistical consequences [191].

Since the beginning of 2025, more than twenty cyberattacks have been reported against critical infrastructure, while surveys indicate over 900 reported incidents between 2006 and 2025 [179]. The cumulative evidence from these attacks, affecting power grids, gas pipelines, district heating systems, nuclear facilities, and transportation networks, highlights the persistent vulnerability of critical infrastructure to both targeted and opportunistic cyber threats. These incidents reinforce the urgent need for robust, multi-layered cybersecurity strategies that integrate prevention, intrusion detection, and rapid recovery mechanisms, in order to mitigate both immediate operational disruptions and long-term strategic risks.

2.4.2 Cyber-Physical Attacks Taxonomies

Several categories of sophisticated cyber threats exist, including intrusions, FDIA, DoS attacks, malware, insider threats, and other targeted attacks that may establish persistent backdoors for later exploitation [192]. The implementation mechanisms of such attacks are continuously evolving, and the taxonomy of cyber–physical threats varies according to factors such as the type of attacker, the assumed attack model and domain, the intended target, and the potential impact. Regardless of the specific mechanism, the consequences of a cyberattack are ultimately manifested in one or more of the core cybersecurity properties: confidentiality (C), integrity (I), and availability (A), collectively referred to as the CIA triad. In contrast to confidentiality breaches, attacks compromising the integrity or availability of measurement and control data can have a direct and severe impact on the reliability, stability, and security of both SPSs and IESs. Figure 2.8 illustrates the different stages of cyber–physical attacks, where each stage comprises multiple attack types and can be described using different taxonomies.

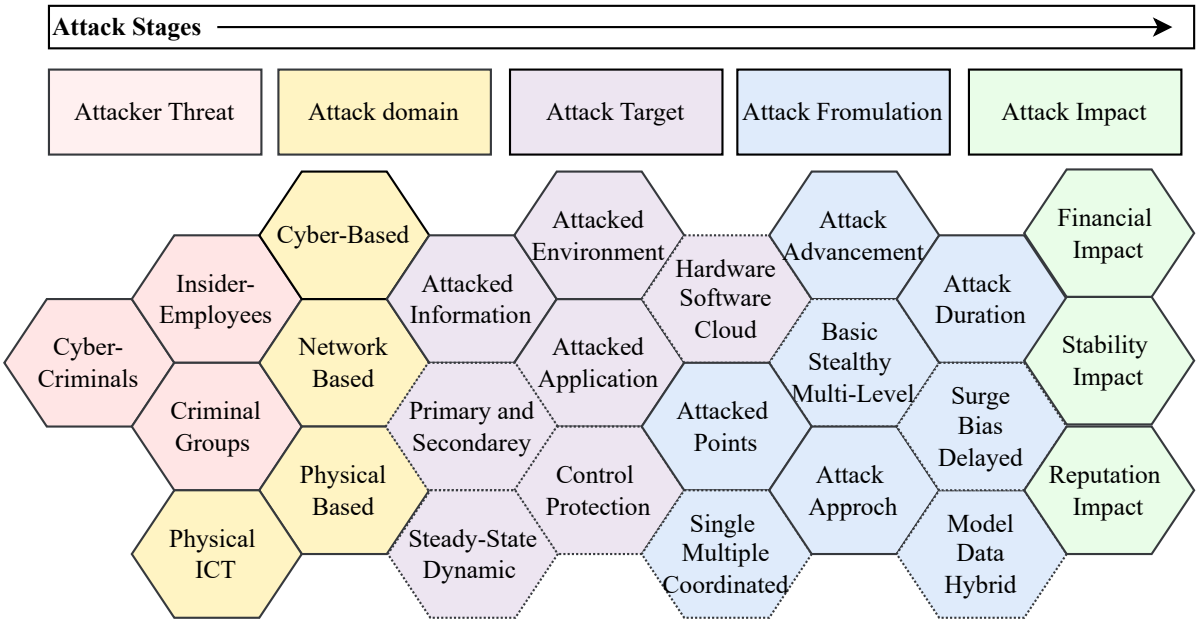


Figure 2.8: Taxonomy of Cyber-Physical Attacks.

2.4.2.1 Threat Actors Taxonomy

Attacker Threat represents the first layer of this taxonomy and begins with identifying threat actors, a crucial step in understanding the overall security risk, the technical and operational capabilities of adversaries, and their potential motives and strategies [193]. A threat actor is any person, group, or entity with malicious intent to compromise the security of IESs and is ultimately responsible for initiating a cybersecurity incident. Threat actors may be internal (insiders) or external to the organization, and they can be classified as follows:

- *Cybercriminals*: Individuals or groups that typically conduct opportunistic attacks against general computer systems without initially targeting cyber–physical infrastructure. For example, deploying malware that infects control software might not specifically aim at disrupting a district heating network; however, once such software is compromised, it can lead to harmful operational impacts across the entire physical system.

- *Disgruntled employees*: Current or former staff members who are dissatisfied and may misuse privileged access to compromise control systems. While the scope of damage from a single insider may be limited compared to coordinated external groups, the risk escalates significantly when these individuals collaborate with outside attackers, enabling deeper system infiltration and exploitation.

- *Terrorists, hacktivists, and organized criminal groups*: Actors who may have ideological, political, or financial motivations and are publicly perceived as major threats to CPS. Cyberattacks in this context are often more attractive than physical assaults because they are less costly, carry reduced personal risk for the attacker, can be executed remotely, and are easier to coordinate across geographic boundaries.

2.4.2.2 Cyber-Physical Attacks Domain Taxonomy

Attack Domain represents the second layer of this taxonomy and focuses on identifying vulnerabilities within the CPS as well as the specific domain, cyber or physical, where an attack can be initiated. In general, cyber–physical attacks on IESs can be executed at the cyber layer, the physical layer, or through combined approaches. Based on the nature of the attack surface, these can be classified into four main groups:

- *Cyber-Based Attacks*: These primarily target the back-end computational functions of the central control system in IESs, with a focus on compromising algorithms, software, or firmware. Common examples include *code manipulation*, where adversaries alter control logic to serve their objectives, and *command manipulation* through malware injection. Another example is *sleep deprivation attacks*, in which devices are prevented from entering low-power modes, causing accelerated resource exhaustion and eventual failure.

- *Network-Based Attacks*: These target the communication processes at the cyber layer by accessing the virtual network without directly altering the software, firmware, or physical communication infrastructure. Examples include DoS and DDoS attacks, black/grey hole attacks (where partial or complete data packets are dropped), FDIA, man-in-the-middle attacks, packet sniffing, rogue node insertion, and fuzzing. The common goal is to disrupt, intercept, or manipulate data flows to degrade system performance or cause incorrect decision-making.

- *Physical Communication-Based Attacks*: These focus on the physical communication links between components without directly interfering with the virtual network layer. They can involve either disrupting the communication channel entirely or injecting falsified data at the physical link. Well-known examples include *GPS spoofing*, where positioning and synchronization signals are manipulated; *message replay attacks*, in which valid data packets are resent to create confusion; and *relay attacks*, which exploit timing and distance, and open/close signals in communication protocols.

- *Physical-Based Attacks*: These directly target the physical components of IESs. While some involve direct physical damage, such as tampering with hardware, others can be executed remotely. For instance, *electromagnetic attacks* such as overvoltage surges or electromagnetic pulses can damage equipment from a distance. Additionally, *emanation-based attacks* exploit unintended emissions such as heat, light, sound, or electromagnetic radiation to infer sensitive information or compromise system integrity.

2.4.2.3 Cyber-Physical Attacks Target Taxonomy

Attack Target represents the third layer of this taxonomy and focuses on defining the specific scope of a cyber–physical attack on the CPS within IESs. The scope can vary depending on whether the attacker aims to compromise information, applications, or the operational environment of the system. These can be categorized into three main groups:

- *Attacked Information*: In this category, cyber–physical attacks are differentiated based on whether they compromise **primary** or **secondary** information. Primary information includes demand and supply measurements, stored network parameters, and the overall operational state of the IES. Attacks on this type of data may indirectly lead to inaccurate decision-making by control systems. Secondary information, on the other hand, relates directly to control and protection decisions, such as optimal power conversion set-points, system reconfiguration parameters, and protection relay actions. Compromising secondary information typically has more immediate and severe consequences.

- *Attacked Applications*: Here, the classification depends on which operational applications are targeted, whether steady-state or dynamic control, energy management, or protection functions. Each application relies on a specific set of primary and secondary information, meaning an attack may focus on one or multiple applications simultaneously. For example, an adversary could target steady-state optimization functions to subtly shift operating points, or interfere with protection algorithms to delay fault isolation, as explained in Section 2.2.2.

- *Attacked Environment*: This category considers the specific environment within the CPS being targeted:

    1. **Hardware environment attacks** include tampering with sensors, actuators, controllers, or other physical control elements.

2. **Software environment attacks** focus on manipulating software functions, either by reverse-engineering (decoding) them or causing interruptions in their execution.
3. **Cloud and data storage environment attacks** aim to steal, alter, or delete critical control system information, such as network parameters, potentially causing widespread disruption. Data exfiltration may also provide attackers with valuable insights into defense layer vulnerabilities, enabling the design of more sophisticated follow-up attacks.

2.4.2.4 Cyber-Physical Attacks Formulation and Model Taxonomy

Attack Model and Strategies represents the fourth layer of this taxonomy and focuses on the development model or the overarching strategy adopted by the attacker to compromise the CPS of IESs. The choice of model and strategy depends on factors such as the attacker's type, the amount of system knowledge obtained, and the level of access to the target infrastructure. Attacks can generally be classified according to their sophistication, targeted points, formulation techniques, and operational time scale, as follows:

- *Attack Sophistication*: This category classifies cyber–physical attacks based on their level of complexity and the amount of system-specific knowledge required to execute them.
    1. **Basic attacks** are relatively simple and can be performed with zero or minimal knowledge of the system's parameters. These are often detectable by traditional BDD mechanisms and may involve straightforward disruption techniques.
    2. **Stealthy attacks** are more advanced and require detailed IES network parameters, along with access to multiple measurement points. The attacker carefully maintains low residuals and preserves physical laws across the system, enabling them to evade detection by conventional BDD schemes.
    3. **Multi-level attacks** represent the most sophisticated category, often structured in hierarchical layers of optimization. For example, a lower layer may simulate EMS optimization under compromised measurements, while an upper layer determines which measurements to attack, balancing cost and impact. Such attacks demand extensive resources, multiple access points, full awareness of the EMS code and network parameters, and continuous interaction with the CPS, and are typically achievable only by highly organized, well-funded groups such as state-sponsored actors.

- *Attack Points*: This category focuses on the number and distribution of system components manipulated to carry out the attack.

    1. **Single-point attacks** target one sensor, actuator, or control signal, with the objective of identifying a location where minimal effort yields maximum disruption.
    2. **Multi-point attacks** affect multiple components within the same layer, type, or application domain.
    3. **Coordinated attacks** are advanced multi-point attacks in which different attack types (e.g., DoS, FDIA), different attack domains (cyber, virtual network, physical communication, and physical hardware), and various sensors (e.g., PMUs, SCADA measurements) are manipulated simultaneously, sometimes across multiple IESs.

- *Attack Techniques*: This category outlines the main methodological approaches used in formulating and implementing attacks:

    1. **Mathematical and optimization-based methods**, which use system models to calculate optimal attack vectors.
    2. **Data-driven, Artificial Intelligence (AI), and Reinforcement Learning (RL) methods**, which leverage historical and real-time data to learn vulnerabilities and predict optimal disruption strategies.
    3. **Hybrid approaches**, which combine model-based and data-driven techniques for greater adaptability and resilience against defense mechanisms.

    The choice of technique depends on the attacker's access level, the amount of data collected, and the availability of a system simulation environment.

- *Attack Duration*: This category refers to the time scale over which the attack is executed and the time required to achieve the intended impact.

    1. **Surge Attacks** are executed immediately after system access is obtained, aiming for rapid and noticeable disruption.
    2. **Bias Attacks** are gradual and discrete, injecting small but persistent deviations into the system over an extended period. For instance, an attacker might slowly alter the acceptable threshold values of the BDD mechanism, causing continuous misclassification of abnormal states as normal operation. Although slower to take effect, such attacks can produce long-term, systemic damage while remaining undetected.

3. **Delayed Impact Attacks** refer to a class of cyber-physical attacks in which the malicious action is executed at a specific time, but its adverse effects on the system only become apparent after a delay. Such attacks are particularly insidious because the system may initially appear to operate normally, reducing the likelihood of early detection. For instance, altering the charging and discharging schedules of ET vehicles, or manipulating the battery swapping timetable, may not immediately disrupt the operation of EVs or electric buses. However, once these vehicles commence their scheduled trips, they may experience unexpected drops in energy levels to critical thresholds or become incapable of reaching their intended destinations, thereby causing significant operational and safety consequences.

2.4.2.5 Cyber-Physical Attacks Impact Taxonomy

Attack Impact represents the final layer of this taxonomy and focuses on the ultimate consequences of cyber-physical attacks on IESs. In other words, it identifies the outcomes that attackers aim to achieve as their primary objectives. These impacts can be broadly classified into three main categories:

- *Financial Impact*: These attacks primarily target the economic performance of the IES operation. In this scenario, attackers avoid inducing abrupt operational changes that might trigger detection systems. Instead, they subtly degrade system efficiency over time, resulting in financial losses while minimizing the risk of detection.
- *Stability Impact*: These attacks focus on compromising the reliability and operational stability of IESs. The primary objective is to destabilize system functions and cause large-scale operational disruptions. For electric power systems, the most severe outcome would be a complete system blackout, representing a critical threat to service continuity.
- *Confidentiality and Reputation Impact*: These attacks aim to undermine the confidentiality, integrity, and public trust associated with IESs. By stealing sensitive data, such as customer information stored on cloud servers, attackers can damage the operator's reputation and erode customer confidence.

2.5 Smart Power Systems Situational Awareness and State Estimations

SE is a fundamental function in SPSs, serving as the core analytical tool for situational awareness in SPS operation. Situational awareness refers to the operator's ability to perceive, comprehend, and project the current and future state of the grid [194]. Accurate SE ensures that control centers maintain a real-time, reliable, and complete view of system operating conditions, even in the presence of measurement errors, missing data, or communication delays. By filtering out noise and identifying bad data in the measurement set and FDIAs, SE provides a coherent and physically consistent representation of the system state, enabling informed decision-making for economic dispatch, contingency analysis, and security assessment.

2.5.1 Role of State Estimations

In steady-state operation, the primary objective of the SE is to determine the system state, typically defined by the voltage magnitudes and phase angles at all buses, or equivalently, by the real and imaginary components of the bus voltages. Direct measurement of these quantities by installing PMUs or IEDs at every bus is generally impractical due to high instrumentation and communication costs. To address this limitation, SE utilizes a redundant set of measurements obtained from SCADA systems, PMUs, and other metering devices, as discussed in Section 2.2.1, to infer the complete state vector.

The main functions of SE can be summarized as follows: 1) *State estimation*: Compute the SPS state, represented by bus phasor voltages either in polar form (magnitude and angle) or in complex form. 2) *Error correction*: Combine information from various measurement devices, each with different levels of trustworthiness and accuracy, to estimate the most probable state that best represents the actual system, thereby mitigating measurement errors. 3) *BDD*: Compare the residuals, defined as the differences between actual measurements and those calculated from the estimated state, against predefined thresholds to detect bad data. Such anomalies may arise from normal sensor degradation or from malicious cyber-physical attacks [195].

The general formulation of SE can be expressed as a least squares optimization problem. First, the measurement model is defined as in (2.6):

$$z = h(x) + e \tag{2.6}$$

where $z \in \mathbb{R}^{\boldsymbol{\mathcal{M}}}$ is the measurement vector, $x \in \mathbb{R}^{2|\boldsymbol{\mathcal{B}}|-1}$ is the vector of state variables to be estimated (e.g., bus voltage phasors in polar or rectangular form), $h(\cdot)$ is the linear or nonlinear measurement function describing the relationship between z and x, and $e \in \mathbb{R}^{\boldsymbol{\mathcal{M}}}$ is the measurement noise vector, typically assumed to follow a Gaussian distribution with zero mean and known covariance R [195].

The WLS method is the most widely used estimation approach, aiming to minimize the weighted sum of squared residuals. Each measurement is assigned a weight reflecting the reliability of the corresponding device, given by $w_m = 1/\sigma_m^2$, where σ_m is the standard deviation of the measurement device error. The objective function of the WLS estimator is thus given by (2.7):

$$\min_x J(x) = [z - h(x)]^T W [z - h(x)] \tag{2.7}$$

Taking the first derivative of $J(x)$ with respect to x (Jacobian) and setting it to zero yields the normal equations:

$$G(x)\,\Delta x = H^T(x) W\, r(x) \tag{2.8}$$

where, $r(x) = z - h(x)$ (residual vector), $H(x) = \frac{\partial h(x)}{\partial x}$ (Jacobian matrix), and $G(x) = H^T(x)WH(x)$ (gain matrix). The solution is then obtained iteratively by updating the state vector according to direction of error minimization using (2.9):

$$x^{(k+1)} = x^{(k)} + \Delta x \tag{2.9}$$

The iterations continue until convergence criteria are satisfied, typically when the norm of Δx or the change in the objective function falls below a predefined threshold ϵ.

The phasor representation of bus voltages, in either polar or rectangular form, is most commonly adopted in the literature [194]. The structure of the measurement vector z determines the form of the measurement function $h(\cdot)$. In particular, active and reactive power measurements (injections and line flows), together with SCADA and IED data, lead to a nonlinear measurement model, commonly referred to as AC SE, regardless of the chosen state representation. In this case, the WLS problem is solved iteratively, with the Jacobian matrix updated at each iteration k, as summarized in Algorithm 1.

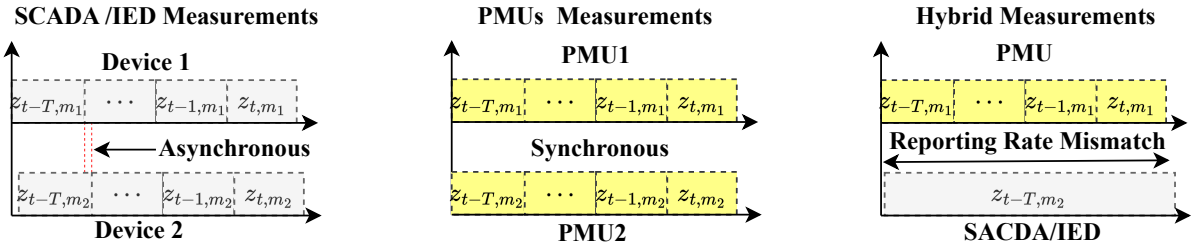


Figure 2.9: SCADA, PMU and hybrid measurements reportingtime frame.

Algorithm 1 Iterative Gauss–Newton WLS Algorithm

Require: Initial guess $x^{(0)}$, measurement vector z, covariance matrix $R = \sigma^2$, where $W = R^{-1}$

Ensure: Estimated state vector x

1: Set iteration counter $k \leftarrow 0$
2: **while** $\|\Delta x^{(k)}\| > \epsilon$ **do**
3: Compute measurement function $h\left(x^{(k)}\right)$
4: Compute residual $r^{(k)} \leftarrow z - h\left(x^{(k)}\right)$
5: Evaluate Jacobian matrix $H\left(x^{(k)}\right)$
6: Form gain matrix $G^{(k)} \leftarrow H^\top W H$
7: Solve $G^{(k)}\Delta x^{(k)} = H^\top W r^{(k)}$, Avoid Singularity by SVD or LU decomposition.
8: Update $x^{(k+1)} \leftarrow x^{(k)} + \Delta x^{(k)}$
9: $k \leftarrow k + 1$
10: **end while**

On the other hand, when voltage phasors are expressed in rectangular coordinates and PMUs are progressively integrated to provide synchronized voltage and current phasor measurements, the SE measurement model becomes linear. This results in a constant Jacobian matrix and typically enhances the accuracy and computational efficiency of state estimation [196]. In this case, the optimal solution admits a closed-form expression due to the linearity of the measurement function, which the optimal state estimate x^* is given by $x^* = \left(H^T W H\right)^{-1} H^T W z$.

2.5.1.1 Hybrid Measurements State Estimation

SE with hybrid measurements integrates both linear and nonlinear measurement functions within a unified estimation framework. PMUs measurements establish linear relationships with the state variables, whereas SCADA measurements are inherently nonlinear functions of the

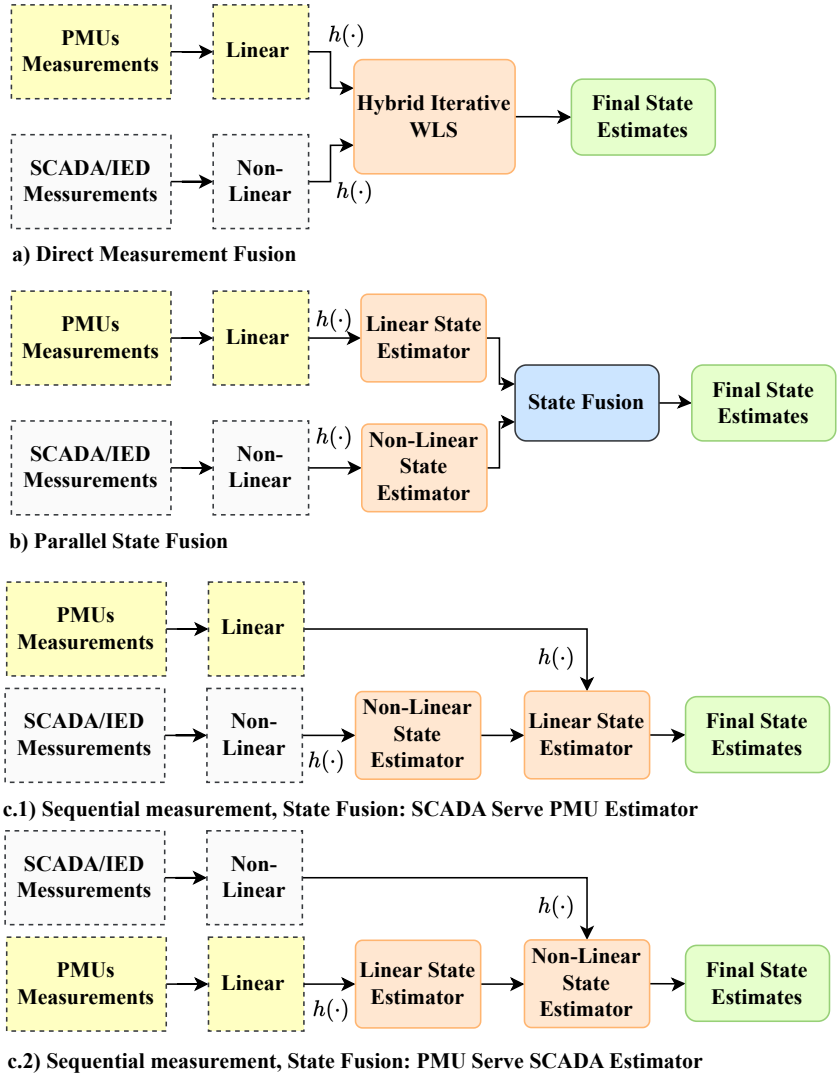


Figure 2.10: Hybrid SE architectures, 1) Direct measurement fusion, 2) parallel state fusion, and 3) sequential measurement-state fusion.

state and require iterative numerical solutions. Furthermore, the differing reporting rates of these devices, combined with the challenge of merging asynchronous measurements with synchronous ones of varying accuracy, make hybrid SE a complex task. For example, while PMU measurements can be updated every cycle, SCADA measurements are typically available at longer intervals and are updated at non-uniform times due to their asynchronous nature, as shown in Figure 2.9. Consequently, although hybrid SE can ensure system observability, it must be carefully designed to address these temporal and accuracy-related discrepancies [197].

In order to address the challenges of Hybrid SE, three main processing architectures have

been proposed in the literature: direct measurement fusion, parallel state fusion, and sequential measurement-state fusion, as illustrated in Figure 2.10. In the direct measurement fusion approach, a single hybrid estimator is employed to process both PMU and SCADA measurements simultaneously at a given time instant. This strategy fully exploits the complementary characteristics of the two data sources but introduces several technical challenges. The measurement function and the associated Jacobian matrix must be reformulated to accommodate the combination of linear PMU measurements and nonlinear SCADA measurements. Furthermore, incorporating current phasor measurements can lead to singularities in the Jacobian matrix under flat start conditions. Another difficulty arises from the large disparity in measurement accuracy and corresponding weights between PMU and SCADA measurements, which may cause ill-conditioning of the gain matrix and, in severe cases, divergence of the WLS solution [198].

In the parallel state fusion architecture, two independent estimators are executed in parallel, one processing SCADA measurements and the other processing PMU measurements. The resulting state estimates from the two estimators are then statistically fused to produce the final SE solution. While this architecture allows independent tuning of each subsystem, it faces challenges related to potential unobservability in the PMU-based estimator, particularly when the PMU network is sparse. Moreover, the time skew between SCADA and PMU datasets, due to differences in reporting rates and synchronization, can further complicate the fusion process. Several strategies have been proposed to mitigate PMU unobservability, including the use of prior information from SCADA-based estimates at previous instants, the inclusion of pseudo-states with large variances, and initialization with arbitrary voltage phasors [199].

The sequential measurement-state fusion approach executes SCADA and PMU estimators in sequence rather than in parallel. Two processing orders are commonly reported. In the first, a nonlinear SCADA-based estimator is executed first to produce SCADA-based SE, which are then transformed into rectangular coordinates and combined with PMU measurements in a subsequent linear estimation stage [200]. In the second, a linear PMU-based estimator is executed first, and its state estimates are subsequently integrated into a nonlinear SCADA-based estimator to obtain the final solution [201]. In the latter case, to avoid unobservability in the PMU-based stage, the estimation in the first step is restricted to state variables corresponding to buses with PMUs or buses directly connected to them.

2.5.2 State Estimation of Integrated Energy Systems

The concept of SE is not exclusive to SPSs; rather, it is a fundamental tool for enhancing situational awareness across all IESs. In recent years, the deployment of joint SEs for integrated monitoring has gained significant attention, driven by the increasingly deep and complex coupling between diverse energy subsystems. For instance, joint SE frameworks have been developed for thermal, hydraulic, and interconnected power networks using direct measurement fusion approaches [202], [203]. Similarly, integrated electric–gas system SE extends the estimation model to incorporate gas node pressures and gas flow measurements, enabling multi-energy domain situational awareness [204], [205]. Furthermore, the scope of SE has been extended to cover integrated electric, gas, and heat systems [206], [207], thereby supporting coordinated operation and improved efficiency across sectors.

However, the integration of heterogeneous energy subsystems introduces additional challenges, including increased measurement dimensionality, mixed linear and nonlinear measurement models, differing time scales of data acquisition, and varying levels of measurement uncertainty. Such complexity can lead to numerical instability or divergence in the estimation process if not properly modeled and regularized. Moreover, joint IES SE remains a relatively nascent research area, with the majority of published work emerging within the last five years. Current approaches often overlook the impact of coordinated cyber-physical attacks and multi-energy domain threat modeling, which represents an important and unexplored dimension for ensuring the resilience and security of future IES.

2.5.3 State Estimation and Bad Data Detection

BDD techniques are employed to detect and remove erroneous measurements that may originate from: 1) meter inaccuracies, 2) unintentional disturbances in the communication channel, or 3) deliberate interference by a malicious adversary. Conventional BDD approaches primarily rely on measurement residual analysis, such as the largest normalized residual test [195]. The measurement residual is given by

$$r = z - h(x^*), \tag{2.10}$$

A widely adopted global detection statistic is the weighted sum-of-squares of the residuals, which corresponds to the WLS objective function $J(x^*)$. Under the null hypothesis of no bad data, assuming the measurement model is accurate, measurement errors are mutually indepen-

dent, and Gaussian-distributed with zero mean and known variance, the statistic $J(\hat{x})$ follows approximately a chi-square distribution, $\chi^2_{|\boldsymbol{\mathcal{M}}|-(2|\boldsymbol{\mathcal{B}}|-1)}$, with $|\boldsymbol{\mathcal{M}}| - (2|\boldsymbol{\mathcal{B}}| - 1)$ degrees of freedom, where $|\boldsymbol{\mathcal{M}}|$ is the number of measurements and $2|\boldsymbol{\mathcal{B}}| - 1$ is the number of states. The global test declares the presence of bad data if:

$$J(\hat{x}) > \tau_{\chi^2}, \tag{2.11}$$

where the threshold τ_{χ^2} is chosen from the χ^2_{m-n} distribution based on a pre-specified false alarm probability. While this residual-based method is effective in detecting gross errors, it is well-known that it can be bypassed by well-structured FDIAs, in which the injected error aligns with the system model and remains hidden within the residual analysis framework.

2.6 Beyond State Estimation, Attack Formulation and Challenges

Traditional BDD methods rely on the residual tests performed within the smart power and IESs SE framework. However, many cyber-physical attacks can entirely evade SE-based detection, particularly when they manipulate data or control signals that lie outside the SE measurement scope. In such cases, the measurement vector before and after the attack remains unchanged, rendering BDD ineffective [5]. These attacks target various categories of primary information utilized within the EMSs of the SPS and IES, which can be summarized as follows:

1. **Stealthy FDIA:** These attacks involve the deliberate injection of false data into the measurement vector z (e.g., voltages, currents, power flows) in a manner consistent with the physical network model. By exploiting knowledge of the measurement matrix and network parameters, the attacker alters the estimated state x while maintaining the residual $\|z - h(x)\|$ below the detection threshold [195]. This makes the attack undetectable to conventional BDD. Notably, stealthy FDIAs are unique among the listed attacks in that they fall within the SE scope yet remain undetected [11], [19].

2. **Weather Primary Information Attacks:** In renewable energy-based systems, weather measurements such as temperature, solar irradiation, and wind speed are critical for estimating the generation from RESs. Attacks targeting weather station data can lead to significant errors in power generation forecasts, ultimately causing suboptimal operational decisions that degrade economic performance and system stability [21].

3. **Storage Systems and SoC Attacks:** In modern grids, the SoC of ESSs is a key parameter in centralized control and decision-making. Cyber-physical manipulation of SoC values can mislead scheduling algorithms without triggering SE-based alarms [22]. Such attacks are increasingly prevalent in IESs and the electrified transportation sector, potentially leading to unsafe overcharging or deep discharging while appearing normal to system operators.

4. **Market Signals Cyber-Physical Attacks:** Real-time market signals, including DR setpoints, grid service commands, and locational marginal prices, are often transmitted via market and SPS operator communication channels. By injecting false price or control data into these channels, attackers can distort market outcomes and operational decisions without altering physical measurements or affecting SE residuals [23].

5. **GPS Spoofing Cyber-Physical Attacks:** PMUs rely on GPS for precise time synchronization. Spoofing attacks introduce false timing signals, which can corrupt phasor measurements, create phase angle errors, cause relay miscoordination, and potentially lead to blackouts [15]. Beyond power systems, GPS spoofing also threatens transportation (e.g., autonomous vehicles, drones) and energy infrastructure, enabling misrouting, collisions, or masking of physical faults.

6. **Secondary Information Cyber-Physical Attacks:** This category involves tampering with secondary control signals issued by the EMS, such as generator setpoints, tap changer positions, breaker operations, or DER dispatch commands. For example, sending a malicious disconnect command to a generator bus can cause a sudden loss of generation without changing the measurements used in SE [24].

7. **Protection-Relay Cyber-Physical Attacks:** These attacks target the configuration or operation of substation protection relays, enabling unauthorized trip commands, disabling fault zones, or modifying breaker logic [25]. Such actions can lead to large-scale outages while leaving system measurements unchanged, making SE-based detection ineffective. These attacks mainly focus on the secondary protection signals in IESs.

2.6.1 Basic Cyber-Physical Attacks

Basic cyberattacks are typically characterized by direct and unsophisticated data manipulation that introduces inconsistencies readily detectable by conventional cybersecurity mechanisms. These attacks may target the SE measurement vector z or extend to auxiliary data

sources such as weather forecasts, market prices, GPS signals, or protection relay commands [208]. A general formulation of such an attack on a signal vector x is given by:

$$x' = x^* + \Delta x^a, \quad \Delta x^a \sim \mathcal{U}(-\Delta x, \Delta x), \tag{2.12}$$

where x' represents the compromised operation state, Δx^a denotes the additive attack-induced perturbation, and $\mathcal{U}(-\Delta x, \Delta x)$ represents a uniform random disturbance over the interval $[-\Delta x, \Delta x]$.

These attacks are usually generated by low-sophistication adversaries with limited knowledge of system topology or operational constraints. Typical examples include unbalanced manipulation of load measurements, zeroing renewable generation under favorable conditions, inducing implausible negative market prices during peak demand, spoofing GPS locations of ET, or introducing abrupt and physically inconsistent coordinate changes. Although disruptive, such alterations generally violate physical or market consistency and are therefore detectable by standard BDD and cybersecurity frameworks.

2.6.2 Stealthy False Data Injection Attacks and Minimal Residual Strategies

In contrast to basic attacks, stealthy cyber-physical attacks are executed by professional adversaries with advanced skills and comprehensive knowledge of the IESs and EMS operation. The objective of such attacks is to minimize the residual between the normal operation state and the state under attack, while maximizing the impact of the manipulated signals. This can be formulated as in (2.13):

$$\text{Minimize} \quad \|h(x^*) - h(x')\| \tag{2.13}$$

$$\text{Subject to:} \quad x' = x^* + \Delta x^a, \quad \Delta x^a \sim \mathcal{U}(-\Delta, \Delta), \quad x' \in \mathbb{P}(x) \tag{2.14}$$

Here, $\mathbb{P}(x)$ defines the PDF of feasible operational space of the SPS and IES. The attacker aims to ensure that x' remains within the expected operational domain while keeping the state deviation $\|h(x^*) - h(x')\|$ small enough to avoid triggering detection mechanisms. This type of attack requires extensive access to system parameters, communication channels, and the capability to manipulate multiple data points simultaneously. Stealthy cyber-physical attacks can target any signal within the SE measurement set or extend beyond it to influence EMS control signals and operational decisions [209].

2.6.3 Multi-level Cyber-Physical Attacks

Multi-level cyber-physical attacks represent a more sophisticated class of threats in which different types of attacks are coordinated across domains, environments, or attack natures, such as combining a DDoS with a FDIA. These attacks are designed as multi-perspective operations that can infiltrate both the decision-making algorithms of the EMS and lower-level cybersecurity layers, while in the upper layer fulfilling requirements such as stealthiness, minimal attack effort, and constrained attack budget [210], [211]. In some cases, multi-level cyber-physical attacks are executed simultaneously across both primary and secondary information channels.

Mathematically, these attacks can be formulated as a bi-level (min–max) optimization problem. The lower-level optimization represents a general EMS of IESs as follows:

$$\text{Minimize:} \quad F_{EMS}(\mathbb{X}, I^P), \ \text{S.t:} \quad L(\mathbb{X}, I^P) \leq 0 \ , \ g(\mathbb{X}, I^P) = 0 \ , \ \underline{\mathbb{X}} \leq \mathbb{X} \leq \overline{\mathbb{X}} \tag{2.15}$$

Here, $F_{EMS}(\mathbb{X}, I^P)$ is the EMS objective function, which aims to minimize capital and operational costs with respect to the primary information signals I^P and the decision and state variables $\mathbb{X}$ of the IES. The functions $L(\mathbb{X}, I^P)$ and $g(\mathbb{X}, I^P)$ represent, respectively, the set of linear inequality constraints (e.g., generator ramp limits, departing SoC limits) and nonlinear equality constraints (e.g., power, gas, and thermal flow balance equations).

The attacker's problem can then be formulated to counteract the IES operator's objectives (i.e., reverse optimization goals) while minimizing attack costs and avoiding detection, as expressed in (2.16).

$$\text{Minimize:} \sum I'^P + \text{Maximize:} F_{EMS}(\mathbb{X}', I'^P) \tag{2.16}$$

$$\text{Subject to:} \quad L(\mathbb{X}', I'^P) \leq 0, \ g(\mathbb{X}', I'^P) = 0, \ \underline{\mathbb{X}} \leq \mathbb{X}' \leq \overline{\mathbb{X}} \tag{2.17}$$

$$I'^P = I^P + \Delta I^{P,a}, \quad \Delta I^{P,a} \sim \mathcal{U}(-\Delta I^{P,a}, \Delta I^{P,a}), \quad I'^P \in \mathbb{P}(I^P) \tag{2.18}$$

This formulation enforces stealthiness and maximizes the attack's adverse impact on the IES with minimal resource use. However, executing such an attack requires extensive system knowledge, including full access to the source code and algorithms of the EMS, as well as broad access to multiple devices across the infrastructure, making it one of the most challenging attacks to implement.

2.6.4 Data-Driven Based Cyber-Physical Attacks

The application of AI techniques, particularly Deep Learning (DL) and RL, has substantially advanced the formulation of cyber-physical attacks in smart power and IESs. Unlike conventional basic, stealthy, or multi-level cyber-physical attacks, AI-driven strategies enable adversaries to learn system dynamics, predict responses, and adapt attack policies to achieve specific operational or economic disruption objectives. One prominent example is the use of generative adversarial networks for constructing stealthy FDIA capable of bypassing BDD mechanisms in SE. In such approaches, the generator is trained to produce measurement perturbations that satisfy the physical constraints of the power flow model while minimizing detection residuals, thereby yielding undetectable yet highly disruptive attack vectors in both transmission and distribution networks [212]. In certain implementations, the discriminator is replaced with a physics-based residual evaluation model to accelerate convergence and improve realism.

Similarly, RL methods, particularly Deep Q-Networks and Proximal Policy Optimization, have been employed to design sequential cyber-physical attacks that exploit temporal dependencies in system operation. For example, RL agents have been trained to manipulate battery ESS SoC measurements over extended periods, inducing operational inefficiencies and economic losses in microgrids and hybrid renewable, and storage systems [213]. The reward functions in such attacks typically aim to maximize system operating cost or voltage deviations while avoiding the activation of protection mechanisms. Predictive attack models based on LSTM networks have also been explored, particularly for manipulating load forecasts or electricity price signals in transactive energy markets. By leveraging historical data patterns, attackers can craft perturbations that influence market clearing prices or alter demand response schedules, ultimately increasing system stress or facilitating economic manipulation [214]. Such predictive approaches are particularly effective in IESs where market and physical layers are tightly integrated.

Moreover, hybrid AI models combining supervised learning for system modeling with RL for decision-making have been proposed for orchestrating coordinated switching attacks on DERs and microgrid interconnections. These attacks can exploit vulnerabilities in inverter controls or grid reconfiguration procedures to destabilize voltage and frequency profiles in both islanded and grid-connected modes [215]. Overall, AI-driven attack formulation marks a shift from static, one-shot data corruption toward adaptive, goal-oriented strategies that leverage system dynamics, control logic, and market mechanisms. The capacity of such methods to model and predict cyber–physical interactions presents a formidable challenge for future grid security, necessitat-

ing equally intelligent and adaptive defense frameworks. However, the implementation of these attacks generally requires full access to system digital twins and simulation environments, enabling continuous learning and pattern recognition by the adversary, making them among most difficult type of cyber-physical attack to be realize in real-life applications.

2.7 Defense Strategies of Cyber-Physical System

Defense strategies for CPSs must address the security of both the physical and cyber layers of the entire system. A holistic view of a CPS is depicted in Figure 2.2. The process layer encompasses actuators, control units, and sensors, whereas the cyber layer consists of monitoring and control software along with the communication networks that interconnect the various hardware components of the smart power and IES. While implementing robust network and information security measures is critical for safeguarding the cyber layer, this alone does not ensure the protection of the physical layer. From the perspective of operational integrity, the physical system is expected to behave according to its modeled dynamics. For example, after an actuator operation, the operator anticipates receiving specific sensor feedback that aligns with the expected physical response. Any deviation from this, whether caused by malicious cyber intrusions, compromised communication, or equipment malfunction, indicates a degradation in the health of the physical system. Consequently, defense mechanisms must not only prevent and detect cyber intrusions but also incorporate process-aware anomaly detection that validates the plausibility of sensor readings against the expected physical behavior.

Apart from information-theoretic defense approaches, numerous mechanisms have been proposed in the literature for safeguarding CPSs against malicious signal injections targeting control systems. These malicious signals, often in the form of falsified sensor data or manipulated control commands, can disrupt the closed-loop operation, degrade performance, or even cause physical damage to the infrastructure. Defense techniques are broadly categorized into *active* and *passive* strategies [216], as summarized in Figure 2.11. In practice, a hybrid defense framework that combines passive monitoring with active intervention is often recommended to address the wide spectrum of cyber-physical threats. Such integration enhances detection robustness while minimizing false alarms, thereby offering a more resilient security posture for IESs.

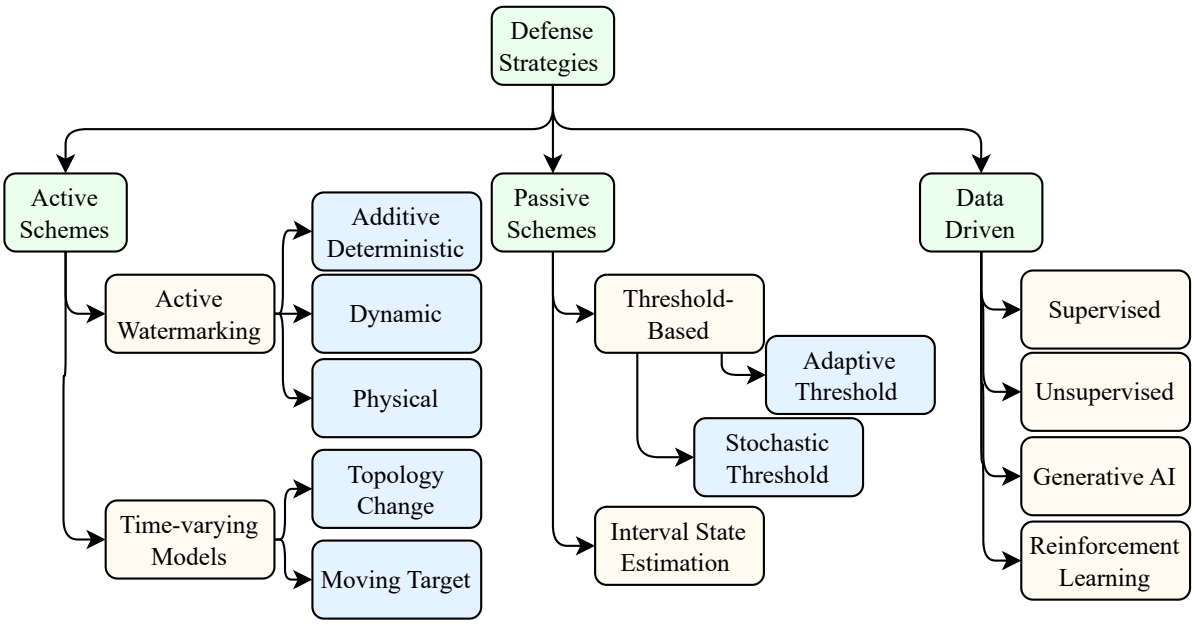


Figure 2.11: Defense strategies against false data in CPSs

2.7.1 Active Schemes

Active defense strategies, deliberately introduce controlled perturbations or diversity into the system to reveal the presence of an attacker. Examples include watermarking control signals, challenge-response authentication, and adaptive reconfiguration of system parameters. By forcing the attacker to respond to unpredictable system changes, active defenses increase the difficulty of maintaining undetectable manipulations. However, their implementation must be carefully designed to avoid compromising system stability or performance.

2.7.1.1 Active Watermarking

Active watermarking involves superimposing a low-amplitude, structured noise or a deterministic signal onto control inputs or sensor outputs. The embedded watermark does not significantly degrade system performance but allows for real-time attack detection by verifying the expected watermark at the receiver. The framework consists of *Watermark Embedding* (adding a secret signal to control actions or expected sensor measurements), *Watermark Detection* (checking received data for the embedded signal using statistical or model-based methods), and *Attack Identification* (detecting cyberattacks through deviations or absence of the expected watermark signal).

Several active watermarking methods have been proposed for securing smart power and IESs, differing in embedding strategies and detection mechanisms [217]. These methods include

1. *Additive Deterministic Watermarks:* These methods embed a known pseudo-random sequence or a sinusoidal signal into control inputs. For instance, in AGC, a cryptographically secure pseudo-random sequence is added to the control signal, and its presence is verified at the generator side [218]. The detection relies on correlation analysis or matched filtering.

2. *Dynamic Watermarking:* Dynamic watermarking superimposes a private random process onto control signals. The detector uses system dynamics to distinguish between legitimate and malicious operations. This method is particularly effective against FDIAs in wide-area monitoring systems [219].

3. *Physical Watermarking:* Some approaches exploit inherent physical properties of the grid, such as the spectral signature of IBRs, to embed watermarks. These techniques are robust against replay attacks as they rely on hardware-specific characteristics [220].

2.7.1.2 Time-Varying Models

Time-varying defense mechanisms in smart power and IESs are designed to continuously alter certain system characteristics, making it more difficult for an adversary to sustain a valid and accurate model of the targeted infrastructure. One such approach involves the *dynamic reconfiguration* of the SPS or IES topology through the use of controllable switching devices. For example, selectively opening or closing transmission lines, or reconfiguring the operational states of DERs, can introduce topological changes that invalidate an attacker's pre-identified network model. Since many cyber-physical attacks rely on an accurate and static representation of the network parameters, such reconfiguration forces the adversary to continuously adapt their strategy, increasing the likelihood of detection [221].

A second time-varying defense strategy involves the *intentional perturbation of network parameters* to modify the underlying measurement functions used in the SE process, known as Moving Target Defense. This can be achieved, for instance, by adjusting reactive power flows or voltage setpoints through FACTS devices, such as static VAR compensators or unified power flow controllers [222]. By introducing controlled and unpredictable variations in the system parameters, any maliciously injected measurements are more likely to produce high residuals in the SE analysis, thereby triggering anomaly detection mechanisms. Importantly, these per-

turbations must be designed such that they do not compromise system stability, operational constraints, or power quality, while still maintaining sufficient unpredictability to disrupt the adversary's model consistency.

2.7.2 Passive Schemes

Passive defense strategies focus on continuously monitoring the system for abnormal patterns without altering the normal operation of the control loop. These include residual-based anomaly detection, model-based fault diagnosis, and data-driven statistical analysis. Such methods generally rely on comparing observed system responses with expected physical behavior to detect inconsistencies. While passive approaches are less intrusive and easier to integrate into existing infrastructure, they may struggle against stealthy attacks specifically designed to mimic legitimate system behavior.

2.7.2.1 Passive Threshold-Based Methods

Passive threshold-based methods constitute the classical paradigm for anomaly detection in SE, as discussed in Section 2.5.3. In these approaches, the residual vector is computed to quantify the mismatch between the measured and estimated quantities. Unlike the basic BDD implementation that applies a fixed threshold, modern variants adopt more sophisticated mechanisms, such as adaptive or dynamic thresholding [223], which adjust the detection limit based on operating conditions. These methods are termed *passive* because they neither modify system operation nor inject deliberate perturbations into the network; instead, they rely exclusively on naturally occurring measurement data. The main advantages of passive threshold-based techniques are their simplicity, low computational requirements, and ease of integration into existing EMS platforms. However, their performance strongly depends on accurate system models and reliable measurements, since detection is based on identifying deviations from expected residual.

2.7.2.2 Interval State Estimation Models

The Interval State Estimation (ISE) framework extends conventional SE by explicitly incorporating measurement and parameter uncertainties into the estimation process. Rather than producing a single point estimate, ISE determines a bounded interval within which the true system state is guaranteed to reside, given known uncertainty bounds in the inputs. This capability

is especially valuable for cybersecurity, as it enables the estimation of the expected maximum state variation under nominal operating conditions [224]. Any measured or estimated state falling outside these bounds is flagged as potentially malicious or erroneous. Mathematically, the deterministic measurement model $z = h(x) + e$ is reformulated in interval form:

$$z \in [\underline{z}, \overline{z}], \quad h(x) \in [\underline{h}(x), \overline{h}(x)] \tag{2.19}$$

where $[\underline{z}, \overline{z}]$ represents the feasible measurement range accounting for sensor tolerances and noise bounds, and $[\underline{h}(x), \overline{h}(x)]$ represents the range of predicted measurements for a given state vector x. These bounds act as adaptive, operating-point-dependent thresholds, mitigating one of the core weaknesses of fixed-threshold approaches.

The integration of *Maximum State Variation Analysis* further improves ISE by detecting stealthy attacks that may not produce significant residuals. This analysis accounts for expected variations caused by load changes, renewable generation fluctuations, and control actions. However, passive methods have several limitations [225]: 1) accurate modeling of complex physical and communication systems is difficult, 2) detection thresholds introduce tolerance margins that attackers can exploit, and 3) they cannot detect attacks that perfectly satisfy system models and statistical assumptions. Nevertheless, passive threshold-based and ISE techniques remain effective for real-time monitoring, particularly when combined with active detection methods.

2.7.3 Data-Driven Based Cyber-Physical Security

Beyond traditional mathematical models, AI and ML techniques have been extensively explored for enhancing the security of CPSs in smart power and IESs [1]. These approaches leverage large volumes of measurement and operational data to detect, classify, and even predict cyber-physical attacks. Their adaptability allows for both known and previously unseen threat scenarios to be addressed. The following subsections outline the principal AI-based methods, emphasizing their detection mechanisms, strengths, and limitations.

1. *Supervised Learning* (training models using labeled normal and attack data): Algorithms such as Logistic Regression, SVM, Random Forests, and Artificial Neural Network (ANN) learn attack patterns from historical data to classify new observations. Their effectiveness depends on the availability and quality of labeled datasets.

2. *Unsupervised Learning* (detecting anomalies without labeled data): Techniques such as Principal Component Analysis, clustering, and autoencoders learn normal operating behavior and

identify deviations as potential attacks. These methods are valuable for detecting unknown threats but may generate higher false alarm rates.

3. *RL* (learning defense strategies through interaction): RL agents continuously interact with the environment to optimize attack detection and mitigation policies. These approaches adapt well to dynamic systems but require extensive training and realistic simulation environments.

4. *Deep Neural Networks* (learning complex spatial and temporal patterns): Models such as LSTM, Convolutional Neural Networks (CNN), and hybrid architectures capture hidden relationships in measurement data, enabling accurate detection of sophisticated attacks. Their main limitations are high computational requirements and tuning complexity.

5. *Graph-Based Methods* (leveraging network topology): Graph Neural Networkss (GNNs) model buses as nodes and network connections as edges, allowing the detection of inconsistencies in both spatial and temporal system behavior. These methods are particularly effective against coordinated multi-point attacks.

Despite their success, AI-based cybersecurity solutions face several challenges, including scalability for large-scale systems, explainability of model decisions, and robustness against adversarial attacks. Emerging approaches such as distributed/federated learning, interpretable AI frameworks, and adversarial training aim to address these limitations [226], [227].

Chapter 3

Stealthy Infiltrated Cyber Attacks and Feasibility Area of Smart Power Systems

The objective of this chapter, and the associated research published in [228], [229], is to develop a holistic representation of the SPS and its testbed environment by integrating the interactions between the cyber and physical layers, while accounting for the cybersecurity of BDD and both primary and secondary. Furthermore, this chapter develops a mathematical framework for designing SICA capable of bypassing existing cybersecurity measures and successfully manipulating SPS operations. Finally, the chapter introduces the concept of the FA, providing the necessary background on FA classifier sets and their theoretical foundations, together with their mathematical formulation and development. The proposed framework is designed to detect abnormal variations in SPS, block SICA, and prevent the propagation of cyberattacks throughout the system.

3.1 Introduction

In the literature survey presented in Section 2.6, the vulnerability of SE within SPS to various cyberattacks, particularly FDIA, has been discussed. These attacks can cause significant damage to the SPS if they succeed in bypassing all cybersecurity layers, including BDD and the cybersecurity mechanisms associated with both primary and secondary information. In response

to escalating cybersecurity threats, governments, academia, and industry have collaborated to strengthen the security and resilience of critical infrastructures and IESs. These efforts have focused on information sharing, privacy protection, and the development of cybersecurity standards and best practices, as reflected in initiatives such as the White House Executive Order 13636 and NIST guidelines [230], [231]. Despite these advancements, the cyber threat landscape continues to intensify, with attacks becoming more frequent and increasingly sophisticated [232]. Modern adversaries employ stealthy techniques capable of bypassing conventional defenses, resulting in low detection rates and prolonged dwell times before compromise is identified and contained [233], [234]. Furthermore, the growing interconnection of IESs has expanded the attack surface, enabling coordinated cross-sector attacks that exploit vulnerabilities across multiple energy domains simultaneously, thereby increasing the potential impact and complexity of detection [235].

Despite considerable advances in securing critical infrastructure and IESs, most existing approaches, as discussed in Section 2.7, focus on preventing and blocking attacks before they affect grid operation, i.e., pre-occurrence cybersecurity measures [236]. Although essential, these methods cannot guarantee complete protection, raising key questions: 1) what happens if a stealthy attack succeeds in compromising smart power and IESs? and 2) how can operators detect, localize, and recover from SICAs after intrusion? These questions highlight the need for *post-occurrence* cybersecurity frameworks capable of early detection and rapid mitigation to limit system impact. A clear example is the December 2015 Kiev blackout, where a SICA targeting the SPS disrupted power supply to over 225,000 customers and caused significant economic losses [237]. In this event, the system operated under manipulated conditions for several minutes before detection and recovery actions were initiated [238]. Such incidents demonstrate that effective post-occurrence detection could significantly reduce outage duration and system-wide damage.

Therefore, this chapter introduces a post-occurrence cybersecurity layer based on a novel FA framework applied to SPS within a CPPS architecture, aimed at detecting sophisticatedly designed SICAs. A CPPS testbed is developed, incorporating the modeling of 1) the physical layer (i.e., generators, loads, and network), 2) the communication layer (i.e., primary and secondary information pathways), 3) the cyber layer (i.e., monitoring functions such as SE, control functions such as OPF, and security mechanisms including BDD and protections for primary and secondary information), and 4) auxiliary functions, including forecasting frameworks and system operation modules. Using the proposed testbed, an SICA development framework is designed, using *Attack-Wait-and-Observe* strategy to bypass all primary and secondary infor-

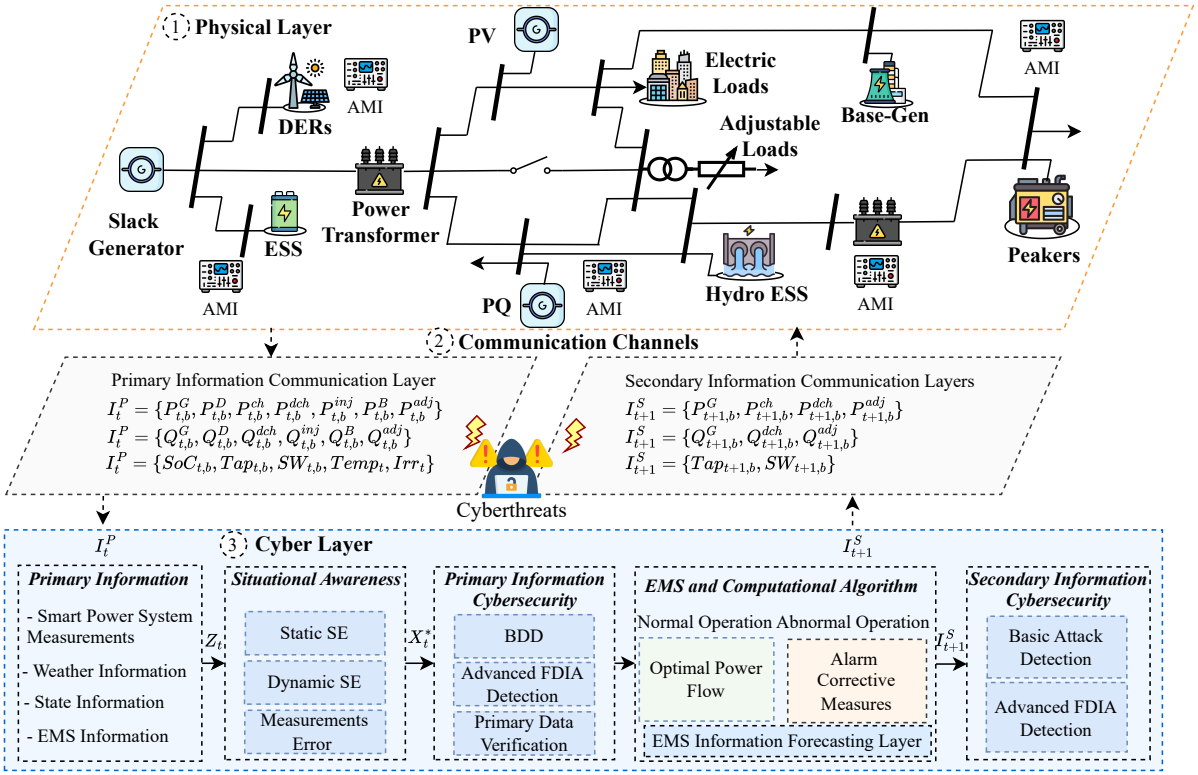


Figure 3.1: Testbed and simulation environment of the SPSs.

mation protection layers, while ensuring a least-effort attack vector formulation. Finally, to detect and mitigate SICA attacks, a novel FA-based framework is developed, consisting of an initial anomaly detection stage using FA-based classifiers (i.e., identifying normal operating conditions of PSSVs), followed by a PRNN that identifies covert SICA patterns.

3.2 Problem Formulation and Preliminaries

3.2.1 Testbed of Smart Power Systems

Figure 3.1 illustrates the testbed and simulation environment of the CPPS for the SPS, highlighting the interaction among the physical, communication, and cyber layers. In the physical layer, the SPS components include generators (i.e., slack, PV, PQ, and fast-dispatchable peaker units), RES generation units, power transformers, circuit breakers, ESS, as well as both flexible and non-flexible demand. These components are coordinated to ensure OPF and to satisfy system demand. For monitoring and situational awareness, a set of AMI devices, including PMU

and SCADA measurements, are deployed throughout the system to guarantee SPS observability. The collected measurements, together with additional primary information, such as weather data and SoC, are transmitted to the central control system via the communication layer.

The primary operational data at time t is transmitted to the cyber layer primary information collection block. At this stage, the data is organized into application-specific categories, including SPS measurement data used for SE, and auxiliary information such as weather data, SoC, and system state information used for EMS and OPF operations. The measurement-based state information of the SPS is processed within the situational awareness module to perform SE, including explicit modeling of measurement device errors. The optimal estimated state x_t^* is then validated against BDD detection schemes, stealthy FDIA detection, and consistency checks using additional primary information such as weather data and ESS state, which lie beyond the direct scope of SE. Finally, in the absence of any cyberattack alarms, the verified data is forwarded to the EMS and control module.

If the estimated SPS state at time t indicates abnormal operating conditions requiring immediate action (e.g., overvoltage or line overloading), the EMS prioritizes corrective actions such as adjusting transformer tap changers or curtailing generator outputs. Otherwise, the EMS proceeds to solve the OPF problem to optimize system operation for the next time step $t+1$. In both normal and abnormal operating scenarios, the EMS and control module generate secondary control signals that are sent back to the physical layer. These signals define the setpoints of SPS actuators, including generator dispatch levels, RES curtailment levels, ESS charging and discharging schedules, transformer tap positions, and circuit breaker statuses. Similar to the primary information, the secondary information is also validated against cyberattacks, particularly FDIA, to ensure the integrity of the control setpoints.

3.2.1.1 Primary Information Module

At each time t, a set of primary information I_t^P is transmitted from the physical layer to the cyber layer through communication channels. This primary information can be classified into four categories: 1) SPS measurements representing AMI data used in the SE process, where z_t includes PMUs and SCADA measurements; 2) state information describing the status of network equipment such as transformer tap positions and circuit breaker states; 3) weather information used for forecasting within the EMS, including solar irradiation and wind speed to estimate PV and wind turbine outputs; and 4) EMS information, which reflects real-time operational data

required for optimal system operation, such as ESS SoC and real-time electricity prices. The primary information vector can be described mathematically by the following set of information:

$$I_t^P = \{z_t^{PMUs}, z_t^{SCADA}, Tp_{t,bb'}, SW_{t,b}, Gs_t, Temp_t, v_t^{wind}, SoC_{t,b}, c_t^{Ele}\} \tag{3.1}$$
$$I_t^P = \{\text{SPS measurements} \wedge \text{State information} \wedge \text{Weather information} \wedge \text{EMS information}\}$$

In this context, cyberattacks targeting the primary information I_t^P aim to indirectly influence SPS operation by misleading the central control unit into taking incorrect actions, such as falsely indicating overvoltage or overloading conditions in the SE results, which may lead to unnecessary generator de-rating or improper tap changer settings. In this case, an attacker may follow two possible pathways: 1) attacking the SPS measurement vector, which requires bypassing the SE cybersecurity layers; or 2) compromising information beyond the SE layer, such as EMS data including SoC and electricity prices, with the objective of manipulating EMS decision-making.

3.2.1.2 State Estimation Situational Awareness Module

The situational awareness module emulates the monitoring functionality of the SPS through the application of SE. The primary objectives of this module are to: 1) estimate the optimal system state, and 2) mitigate the impact of measurement errors in monitoring devices using available AMI and SPS measurements. To achieve this, a hybrid SE model is employed, combining linear PMU measurements (phasor voltages and branch currents) with non-linear SCADA measurements (active and reactive power injections and flows). Using a rectangular phasor representation, the measurement model is expressed as follows:

$$\begin{aligned} z_t = &[h^{V_b^R}(V_t^R, V_t^I)\ h^{V_b^I}(V_t^R, V_t^I)\ h^{I_\beta^R}(V_t^R, V_t^I)\ h^{I_\beta^I}(V_t^R, V_t^I) \\ &h^{P_b}(V_t^R, V_t^I)\ h^{Q_b}(V_t^R, V_t^I)\ h^{P_\beta}(V_t^R, V_t^I)\ h^{Q_\beta}(V_t^R, V_t^I)]^T + e \end{aligned} \tag{3.2}$$

where $h^{V_b^{R,I}}(V_t^R, V_t^I)$ and $h^{I_\beta^{R,I}}(V_t^R, V_t^I)$ denote the measurement functions corresponding to the real and imaginary components of PMU bus voltage and branch current phasors, respectively. Similarly, $h^{P/Q_b}(V_t^R, V_t^I)$ and $h^{P/Q_\beta}(V_t^R, V_t^I)$ represent the measurement functions for bus active/reactive power injections and branch active/reactive power flows, respectively.

The measurement functions can be expressed in terms of the rectangular voltage state vari-

ables V^R and V^I as follows:

$$V_b^R = \{V_b^R\}^{z_m}, \quad h(\cdot) = 1 \text{ since the state and measurement are identical} \tag{3.3}$$

$$V_b^I = \{V_b^I\}^{z_m}, \quad h(\cdot) = 1 \text{ since the state and measurement are identical} \tag{3.4}$$

$$I_{bb'}^R = g_{bb'}(V_b^R - V_{b'}^R) - b_{bb'}(V_b^I - V_{b'}^I) \tag{3.5}$$

$$I_{bb'}^I = g_{bb'}(V_b^I - V_{b'}^I) + b_{bb'}(V_b^R - V_{b'}^R) \tag{3.6}$$

$$P_b = \sum_{b'=1}^{n} \left[V_b^R V_{b'}^R + V_b^I V_{b'}^I\right] G_{bb'} + \sum_{b'=1}^{n} \left[V_b^I V_{b'}^R - V_b^R V_{b'}^I\right] B_{bb'} \tag{3.7}$$

$$Q_b = \sum_{b'=1}^{n} \left[V_b^I V_{b'}^R - V_b^R V_{b'}^I\right] G_{bb'} - \sum_{b'=1}^{n} \left[V_b^R V_{b'}^R + V_b^I V_{b'}^I\right] B_{bb'} \tag{3.8}$$

$$P_{bb'}^F = g_{bb'}\left[(V_b^R)^2 + (V_b^I)^2 - V_b^R V_{b'}^R - V_b^I V_{b'}^I\right] + b_{bb'}\left[V_b^I V_{b'}^R - V_b^R V_{b'}^I\right] \tag{3.9}$$

$$Q_{bb'}^F = -\left(b_{bb'} + b_b^{sh}\right)\left[(V_b^R)^2 + (V_b^I)^2\right] + b_{bb'}\left[V_b^R V_{b'}^R + V_b^I V_{b'}^I\right] + g_{bb'}\left[V_b^I V_{b'}^R - V_b^R V_{b'}^I\right] \tag{3.10}$$

where $G_{bb'}$ and $B_{bb'}$ denote the real and imaginary components of the bus admittance matrix, respectively. Likewise, $g_{bb'}$ and $b_{bb'}$ represent the conductance and susceptance of the series branch connecting buses b and b'. The parameter b_b^{sh} denotes the shunt susceptance associated with the transmission line between buses b and b'.

To account for measurement device errors within the simulation environment, a Gaussian PDF error model is adopted [97]. For PMU phasor measurements, the standard deviation of the magnitude error is assumed to be $\frac{0.7\%}{3}$, while the phase angle error standard deviation is set to $\frac{0.7}{3}$ crad. For SCADA measurements, including branch and injected bus active and reactive power measurements, the standard deviation of the measurement error is assumed to be $\frac{1\%}{3}$. Accordingly, the measurement error samples are generated using (3.11) and (3.12):

$$e^R(PMU)_t = Z_t^{PMUs}\left(1 + |\Delta e_t|\cos(\Delta\delta_t)\right), \quad e^I(PMU)_t = Z_t^{PMUs}\left(1 + |\Delta e_t|\sin(\Delta\delta_t)\right) \tag{3.11}$$

$$\text{where} \quad |\Delta e_t| \sim \mathcal{N}\left(0, \frac{0.7\%}{3}\right), \quad \Delta\delta_t \sim \mathcal{N}\left(0, \frac{0.7 \text{ crad}}{3}\right)$$

$$e^{P/Q}(SCADA)_t = Z_t^{SCADA}\left(1 + |\Delta e_t|\right), \quad \text{where} \quad |\Delta e_t| \sim \mathcal{N}\left(0, \frac{1\%}{3}\right) \tag{3.12}$$

where $|\Delta e_t|$ and $\Delta\delta_t$ denote the sampled magnitude and phase angle errors, respectively, drawn from the corresponding Gaussian distributions. Furthermore, $\mathcal{N}(\mu, \sigma)$ represents a normal PDF with mean μ and standard deviation σ.

To determine the optimal system state x_t^*, the WLS method is employed. The state estimation problem is formulated as the optimization problem given in (3.13) and solved using

Algorithm 1.

$$\min_{x} J(x)_t = [z_t - h(x_t)]^T W [z_t - h(x_t)] \tag{3.13}$$

3.2.1.3 Primary Information Cybersecurity Module

The primary information cybersecurity module serves as both a preventive and post-compromise defense layer against cyberattacks by verifying the integrity of the primary information received from the physical layer. This module consists of three main security mechanisms: 1) a traditional BDD layer, 2) an advanced detection layer designed to identify stealthy FDIA targeting SE results, which may be implemented using either model-based or data-driven techniques, and 3) a forecasting-based detection layer that validates information beyond the scope of SE, such as EMS data and weather information.

1. **BDD Layer:** BDD techniques are employed to detect measurement anomalies caused by meter inaccuracies, unintentional communication channel disturbances, or deliberate manipulation by a cyberattacks, mainly FDIA. When bad data are detected, they must be identified and either removed or corrected to ensure an accurate and unbiased SE process. Conventional BDD methods are primarily based on measurement residual analysis. One of the most widely used approaches is the largest normalized residual test [195], which is defined by (3.14).

   $$J(\hat{x}_t) > \tau_{\chi^2}, \tag{3.14}$$

   In this approach, the threshold τ_{χ^2} is selected as a predefined value used to distinguish normal and abnormal operating conditions.

2. **Advanced Stealthy FDIAs Detection Layer:** A major limitation of traditional BDD methods is their reliance on fixed detection thresholds, which can allow stealthy FDIAs to remain undetected by keeping the residual values within the predefined threshold margin [26]. To address this issue, an adaptive thresholding approach is adopted, where the detection threshold is dynamically updated according to the operating conditions and the incoming measurement data [223]. In this framework, a data-driven model is trained to estimate an acceptable threshold value that is updated at each time step t, denoted by τ_{t,χ^2}. The advanced stealthy FDIA detection criterion is expressed in (3.15):

   $$J(\hat{x}_t) > \tau_{t,\chi^2}, \qquad \text{where} \qquad \tau_{t,\chi^2} = f^{DNN}(\hat{z}_t) \tag{3.15}$$

where $f^{DNN}(\hat{z}_t)$ denotes a trained DNN model that utilizes the SPS measurements and estimated system state to predict an appropriate dynamic detection threshold.

3. **Forecasting-Based Detection Layer:** To detect cyberattacks targeting information beyond the scope of SE, particularly weather and EMS information, a forecasting-based detection layer is employed. This layer compares the received primary information with the corresponding values predicted by forecasting models. A cyberattack alarm is triggered whenever the deviation between the forecasted and received information exceeds the acceptable forecasting error bounds, indicating a potential compromise of data integrity. The forecasting-based detection mechanism can be mathematically formulated using (3.16):

$$\Delta I_t^P > \tau_t^{Fr}, \qquad \text{where} \qquad \Delta I_t^P = I_t^P - f^{LSTM}\left([I_{t'}^P : t' \in M^{His}]\right) \tag{3.16}$$

where ΔI_t^p represents the forecasting deviation, τ_t^{Fr} denotes the acceptable forecasting error threshold, and $f^{LSTM}\left([I_{t'}^P : t' \in M^{His}]\right)$ is a trained LSTM regression model. The model utilizes historical primary information within the forecasting window M^{His} to predict the expected primary information vector at time t. A cyberattack alarm is triggered when the forecasting deviation exceeds the acceptable forecasting error threshold.

3.2.1.4 Energy Management System and Computational Algorithm Module

The EMS module acts as the central control unit of the SPS, with the objective of ensuring reliable, secure, and economically optimal system operation. Although central control systems perform a wide range of functions, as discussed in Section 2.2.2, this module focuses on two key functionalities: 1) OPF during normal operating conditions to achieve optimal system performance, and 2) corrective control actions during abnormal operating conditions, particularly in response to voltage violations and overloading of SPS components. In addition to these two primary functions, an auxiliary forecasting module is incorporated to provide future operating information over a forecasting horizon. This information enables the optimal scheduling of ESS resources, as well as the coordinated management of adjustable loads and generation units of limited generation capacity.

1. **EMS Information Forecasting Layer:** Since the EMS is required to optimize SPS operation not only at the current time instant t but also over future time horizons (particularly for the utilization of ESS capacity and the scheduling of adjustable loads and

generator units), a forecasting layer is essential to provide rolling-horizon predictions of key operational variables, including future demand, RESs generation, and expected electricity prices. Accordingly, a forecasting model is adopted to predict the EMS primary information I_t^P over a future time window M^{Ft} using historical observations within M^{His}. Using an LSTM forecasting approach, the predicted EMS information is expressed as:

$$[I_t^p : t \in M^{Ft}] = f^{LSTM}\left([I_{t'}^P : t' \in M^{His}]\right) \tag{3.17}$$

2. **Normal Operation OPF Layer:** Once the primary information has been verified against potential cyberattacks, and if the SPS operating state at time t is normal (i.e., no over/under-voltage or overloading conditions), the central control unit initiates the OPF to optimize system operation over the future rolling horizon. The objective function of the optimization problem is defined in (3.18):

$$\begin{aligned}
\text{Minimize: } \Delta t \sum_{t \in M^{Ft}} \Bigg(\sum_{b \in \boldsymbol{\mathcal{B}}} \Big[& OPEX(P_{t,b}^G) + OPEX(P_{t,b}^{ch}, P_{t,b}^{dch}) + \\
& OPEX(P_{t,b}^{RES}) + OPEX(P_{t,b}^{Dad}) \Big] \Bigg) \qquad (3.18) \\
& OPEX(P_{t,b}^G) = c_1^g {P_{t,b}^G}^2 + c_2^g P_{t,b}^G + c_3^g, \quad \forall g \in \boldsymbol{\mathcal{G}} \ \wedge \ b \in \boldsymbol{\mathcal{B}} \\
& OPEX(P_{t,b}^{ch}, P_{t,b}^{dch}) = c^s \left(P_{t,b}^{ch} + P_{t,b}^{dch} \right), \quad \forall s \in \boldsymbol{\mathcal{S}} \ \wedge \ b \in \boldsymbol{\mathcal{B}} \\
& OPEX(P_{t,b}^{RES}) = c^f P_{t,b}^{RES}, \quad \forall f \in \boldsymbol{\mathcal{RES}} \ \wedge \ b \in \boldsymbol{\mathcal{B}} \\
& OPEX(P_{t,b}^{Dad}) = c^d P_{t,b}^{Dad}, \quad \forall d \in \boldsymbol{\mathcal{D}^{ad}} \ \wedge \ b \in \boldsymbol{\mathcal{B}}
\end{aligned}$$

where the objective function minimizes the total Operating Expenditure (OPEX) over the forecasting horizon M^{Ft}. The operating cost consists of four components: generation cost, ESS operating cost, renewable energy utilization cost, and the cost associated with adjustable demand. The coefficients c_1^g, c_2^g, and c_3^g represent the generation cost parameters, while c^s, c^f, and c^d denote the cost coefficients associated with ESS operation, RES generation, and adjustable demand, respectively.

The objective in (3.18) is subject to operational constraints on bus voltages and branch power flows, as given in (3.19).

$$\underline{V_b} \leq V_{t,b} \leq \overline{V_b}, \qquad \underline{P_{bb'}^F} \leq P_{t,bb'}^F \leq \overline{P_{bb'}^F}, \quad \forall t \in M^{Ft} \ \wedge \ b \in \boldsymbol{\mathcal{B}} \tag{3.19}$$

In addition, the SPS operation state must satisfy the active and reactive power balance

equations given in (3.20) and (3.21).

$$\begin{aligned} &P^{G}_{t,b} + P^{RES}_{t,b} + P^{dch}_{t,b} - P^{ch}_{t,b} - P^{D}_{t,b} - P^{Dad}_{t,b} = \\ &|V_{t,b}| \sum_{b' \in \boldsymbol{\mathcal{B}}} |V_{t,b'}| \big(G_{bb'} \cos(\theta_{t,bb'}) + B_{bb'} \sin(\theta_{t,bb'})\big) \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \end{aligned} \tag{3.20}$$

$$\begin{aligned} &Q^{G}_{t,b} + Q^{RES}_{t,b} + Q^{dch}_{t,b} - Q^{ch}_{t,b} - Q^{D}_{t,b} - Q^{Dad}_{t,b} = \\ &|V_{t,b}| \sum_{b' \in \boldsymbol{\mathcal{B}}} |V_{t,b'}| \big(G_{bb'} \sin(\theta_{t,bb'}) - B_{bb'} \cos(\theta_{t,bb'})\big) \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \end{aligned} \tag{3.21}$$

The operation of the ESSs is governed by an energy balance constraint, where the SoC evolves over time based on the net charged and discharged energy. At each time step t, the SoC increases due to charging and decreases due to discharging, as described in (3.22):

$$SoC_{t,b} = SoC_{t-1,b} + \left(\eta^{s} P^{ch}_{t,b} - \frac{P^{dch}_{t,b}}{\eta^{s}}\right) \Delta t \quad \forall t \in M^{Ft} \wedge s \in \mathcal{S} \wedge b \in \mathcal{B} \tag{3.22}$$

where η^{s} represents the average charging and discharging efficiency of the ESS s. In addition, certain ESS configurations, which equipped with a single bidirectional converter (e.g, battery ESS), do not allow simultaneous charging and discharging. This operational limitation is enforced through the constraint in (3.23), which ensures mutually exclusive charging and discharging modes, as expressed below.

$$P^{ch}_{t,b} \times P^{dch}_{t,b} = 0 \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \tag{3.23}$$

Furthermore, the adjustable demand is governed by its total energy requirement, while generation units, RES, and ESS are constrained by their operational limits and capacity bounds, as defined in (3.24) and (3.25).

$$\Delta t \sum_{t \in M^{Ft}} P^{Dad}_{t,b} = E^{Dad}_{b} \quad \forall b \in \boldsymbol{\mathcal{B}} \tag{3.24}$$

$$\underline{P^{G}_{b}} \leq P^{G}_{t,b} \leq \overline{P^{G}_{b}}, \quad \underline{P^{RES}_{b}} \leq P^{RES}_{t,b} \leq \overline{P^{RES}_{b}}, \quad \underline{P^{Con}_{b}} \leq P^{ch,dch}_{t,b} \leq \overline{P}^{Con}_{b}, \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \tag{3.25}$$

Here, E^{Dad}_{b} denotes the total energy that must be supplied to the adjustable load at bus b, while P^{Con}_{b} represents the rated capacity of the ESS converter.

3. **Corrective Actions Layer:** The corrective action layer represents the corrective control measures applied to the SPS operation in response to abnormal conditions that may compromise system stability or reliability (e.g, overloading over/under-voltage). In the presence of cyberattacks, a FDIA targeting system stability may manipulate SE outcomes

to falsely indicate abnormal operating conditions, thereby leading to inappropriate and harmful corrective actions. In contrast, FDIA that focus solely on economic objectives manipulate the SE results to increase operational costs without necessarily triggering abnormal stability indications. Unlike OPF, corrective actions must be implemented immediately without waiting for the solution of a complex optimization problem. These corrective measures are defined in terms of system events in (3.26).

$$\begin{cases} \text{Increase } \{P^{G}_{t,b}, P^{RES}_{t,b}, P^{dch}_{t,b}\} \text{ or Decrease } \{P^{ch}_{t,b}, P^{Daj}_{t,b}\} \text{ by } \Delta P & \text{if } V_{t,b} < \underline{V_b} \\ \text{Decrease } \{P^{G}_{t,b}, P^{RES}_{t,b}, P^{dch}_{t,b}\} \text{ or Increase } \{P^{ch}_{t,b}, P^{Daj}_{t,b}\} \text{ by } \Delta P & \text{if } V_{t,b} > \overline{V_b} \\ \text{Set } \{P^{G}_{t,b}, P^{RES}_{t,b}, P^{dch}_{t,b}, P^{ch}_{t,b}, P^{Daj}_{t,b}\} \text{ to } \overline{P^{(\cdot)}_{b}} & \text{under overloading conditions} \end{cases} \tag{3.26}$$

The above logic is designed to 1) mitigate undervoltage conditions by increasing local generation or reducing demand, 2) mitigate overvoltage conditions by decreasing generation or increasing demand, and 3) prevent overloading by limiting any overloaded units to their rated capacity.

3.2.1.5 Secondary Information Module

The output of the EMS module constitutes the secondary information, which corresponds to the OPF setpoints provided to the SPS actuators and the corrective actions at the next time step $t+1$. This secondary information encompasses: 1) generation and demand scheduling, including generator setpoints, RES output, fixable demand profile, and ESS charging/discharging profiles; 2) transformer and circuit breaker statuses, including tap changer positions and switching states (open/close); and 3) corrective action signals.

The secondary information vector can be mathematically represented by as follows:

$$I^{S}_{t} = \{P^{G}_{t,b}, Q^{G}_{t,b}, P^{RES}_{t,b}, Q^{RES}_{t,b}, P^{ch,dch}_{t,b}, Q^{ch,dch}_{t,b}, P^{Dad}_{t,b}, Q^{Dad}_{t,b}, Tp_{t,bb'}, SW_{t,b}\} \tag{3.27}$$

In this context, cyberattacks targeting the secondary information I^{S}_{t} directly aim to influence SPS operation by gaining access to physical-layer setpoints, such as modifying generator dispatch values. Such manipulation can lead to direct and immediate impact on system operation if the security mechanisms protecting the secondary information layer are bypassed.

3.2.1.6 Secondary Information Cybersecurity Module

The secondary information cybersecurity module serves as the final line of defense against cyberattacks targeting the SPS. This module is deployed locally within each SPS component (e.g., generation units, ESS, and controllable loads) and is responsible for verifying the integrity and validity of the received control actions and setpoints before their execution. The module consists of two primary security mechanisms: 1) a basic attack detection layer that identifies logically inconsistent or physically infeasible commands, such as generator setpoints exceeding rated capacity or ESS charging requests that violate safe SoC limits, and 2) an advanced detection layer designed to identify stealthy FDIAs targeting EMS control actions. This advanced layer may employ either model-based or data-driven techniques and utilizes historical equipment setpoints together with local operational measurements to validate the received control signals. A local forecasting-based detection mechanism is employed to verify whether the received setpoint remains within an acceptable operating range. This mechanism combines both the basic and advanced detection layers by checking for violations of operational limits as well as significant deviations from locally forecasted values. This detection logic is expressed by (4.20).

$$\begin{aligned} &\Delta I^S_{t,b} > \tau^{Fr}_{t,b} \text{ or } I^S_{t,b} > \overline{I^S_b} \text{ or } I^S_{t,b} < \underline{I^S_b} \\ &\text{where} \quad \Delta I^S_{t,b} = I^S_{t,b} - f^{LSTM}\left([I^P_{t',b}, I^S_{t',b} : \ t' \in M^{His}]\right) \end{aligned} \tag{3.28}$$

Here, the basic detection layer identifies setpoints that violate predefined operational limits, while the advanced forecasting-based layer detects anomalous control signals by comparing the received setpoint with the value predicted by a local LSTM forecasting model using only local data $I^P_{t,b}, I^S_{t,b}$. An alarm is triggered whenever the deviation exceeds the acceptable forecasting threshold $\tau^{Fr}_{t,b}$.

3.2.2 Primary and Secondary information Basic and Stealthy False Data Injection Attack Modeling

Primary and secondary information are vulnerable to cyberattacks aimed at manipulating the optimal operation and stability of the SPS. Among the various cyber threats, basic and stealthy FDIAs are considered the most prevalent and significant attack vectors in modern CPPSs [208], [239]. Therefore, both attack types are considered representative benchmark cyberattack scenarios for evaluating the security and resilience of the SPS.

3.2.2.1 Basic False Data Injection Attacks on Primary and Secondary Information

Basic cyberattacks are typically launched by adversaries with limited knowledge and access to the SPS. Such limitations may include: 1) restricted access to SPS measurements, and 2) insufficient knowledge of the SPS network parameters and models (i.e., $h(\cdot)$ and $H(\cdot)$). Under these conditions, the attacker injects a random attack vector, $\Delta I_t^{(.),a}$, into either the primary or secondary information with the objective of bypassing cybersecurity defenses and manipulating system operation. The general mathematical formulation of a basic FDIA targeting primary and secondary information is given by (3.29).

$$\begin{aligned} I_t^{'P} &= I_t^P + \Delta I_t^{P,a}, \quad \underline{\Delta I}^{P,a} \leq \Delta I_t^{P,a} \leq \overline{\Delta I}^{P,a} \\ I_t^{'S} &= I_t^S + \Delta I_t^{S,a}, \quad \underline{\Delta I}^{S,a} \leq \Delta I_t^{S,a} \leq \overline{\Delta I}^{S,a} \end{aligned} \tag{3.29}$$

Here, $I_t^{'(\cdot)}$ denotes the manipulated information, while $\Delta I_t^{(\cdot),a}$ represents the injected attack vector. It is worth noting that when the FDIA targets the SE measurement vector z_t, the attack vector is conventionally denoted by a_t, yielding the compromised measurement model $z_t^{'} = z_t + a_t$.

3.2.2.2 Stealthy False Data Injection Attacks on Primary Information

Stealthy FDIAs aim to optimally design the attack vectors $\Delta I_t^{(\cdot),a}$ and a_t to evade both the SE BDD and the forecasting-based detection mechanisms discussed in Section 3.2.1.6. When targeting SE measurements, the primary objective is to compromise the minimum amount of information while ensuring that the resulting SE residual, r, remains below the acceptable BDD threshold [240]. The mathematical formulation of a stealthy FDIA can be expressed as follows:

$$\begin{aligned} &\text{Minimize:} \quad \|a_t\|_0 \\ &\text{Subject to:} \quad |z_t^{'} - h(x_t^*)| \leq \tau_{\chi^2} \end{aligned} \tag{3.30}$$

In addition, the stealthy FDIA formulation may incorporate further constraints reflecting the attacker's intention to trigger inappropriate corrective actions by forcing the estimated optimal state x_t^* to indicate abnormal operating conditions, such as overvoltage, undervoltage, or equipment overloading. This objective can be represented by (3.31).

$$x_{t,b}^* < \underline{x_b} \quad \text{or} \quad x_{t,b}^* > \overline{x_b} \tag{3.31}$$

Similarly, the stealthy FDIA model targeting primary information beyond the SE framework follows the same principles of least-effort manipulation while maintaining the attack within the upper and lower logical limits. This formulation is mathematically described in (3.32).

$$\begin{aligned} &\text{Minimize:} \quad \|\Delta I_t^{P,a}\|_0 \\ &\text{Subject to:} \quad \underline{I_b^P} \leq I_{t,b}^{\prime P} \leq \overline{I_b^P} \end{aligned} \tag{3.32}$$

3.2.2.3 Stealthy False Data Injection Attacks on Secondary Information

Stealthy FDIAs on secondary information aim to optimally design the attack vectors $\Delta I_t^{S,a}$ to evade the basic attack detection layer with attack within acceptable operation margin, while causing economic or stability impact. Such attack can is described by (3.33).

$$\begin{aligned} &\text{Minimize:} \quad \|\Delta I_t^{S,a}\|_0 \\ &\text{Subject to:} \quad \underline{I_b^S} \leq I_{t,b}^{\prime S} \leq \overline{I_b^S} \end{aligned} \tag{3.33}$$

3.3 Proposed Stealthy Infiltrated Cyber Attack Model

Stealthy FDIAs targeting primary and secondary information are typically designed to bypass basic detection mechanisms, such as the BDD in SE and logical consistency checks. However, these attacks do not guarantee successful manipulation of SPS operation, primarily due to the presence of advanced detection layers, including advanced stealthy FDIA detection schemes and forecasting-based anomaly detection methods. Therefore, a more comprehensive attack model is required to effectively evade these advanced cybersecurity layers, leading to the concept of a SICA. This model is designed to ensure successful bypassing of advanced detection mechanisms and to reliably achieve manipulation of SPS operation.

3.3.1 Proposed Model of Stealthy Infiltrated Cyber Attacks on Primary Information

In order to construct a SICA targeting primary information, the designed attack vectors a_t and $\Delta I_t^{P,a}$ must be capable of bypassing both the adaptive FDIA detection threshold within the SE and the forecasting-based detection layer. This can be achieved by explicitly incorporating the responses of these advanced cybersecurity mechanisms into the attack design process, as

formulated in (3.34) and (3.35).

$$\begin{aligned} &\text{Minimize:} \quad \|a_t\|_0 && (3.34)\\ &\text{Subject to:} \quad |z_t^{'} - h(x_t^*)| \leq \tau_{t,\chi^2}, \quad \text{where} \quad \tau_{t,\chi^2} = f^{DNN}(\hat{x}_t) \\ &\text{Minimize:} \quad \|\Delta I_t^{P,a}\|_0 && (3.35)\\ &\text{Subject to:} \quad \left|I_t^P - f^{LSTM}\left([I_{t'}^P : t' \in M^{His}]\right)\right| < \tau_t^{Fr} \end{aligned}$$

3.3.2 Proposed Model of Stealthy Infiltrated Cyber Attacks on Secondary Information

Similarly, to construct a SICA targeting secondary information, the attack vector $\Delta I_t^{S,a}$ must be designed to evade the advanced FDIA detection layer. This objective can be achieved by explicitly incorporating the response of the advanced detection mechanism into the attack formulation, as described in (3.36).

$$\begin{aligned} &\text{Minimize:} \quad \|\Delta I_t^{S,a}\|_0 && (3.36)\\ &\text{Subject to:} \quad \left|I_{t,b}^S - f^{LSTM}\left([I_{t',b}^P, I_{t',b}^S : \ t' \in M^{His}]\right)\right| < \tau_{t,b}^{Fr} \end{aligned}$$

For the OPF application considered in the testbed, the SICA is formulated to maximize the operational objective while remaining undetected by the local forecasting-based cybersecurity layer. The attack model is expressed as follows:

$$\begin{aligned} \text{Maximize:} \quad Obj(3.18) \quad \text{Subject to:} \quad (3.19) - (3.25) \qquad (3.37)\\ |V_{t,b} - \hat{V}_{t,b}| \leq \tau_V, \quad \forall t \in M^{Ft} \ \wedge \ b \in \boldsymbol{\mathcal{B}} \end{aligned}$$

where τ_V denotes the maximum allowable voltage deviation between the actual and manipulated voltage vectors. This constraint ensures that the manipulated operating conditions remain within the acceptable forecasting threshold, thereby reducing the likelihood of detection while maximizing the attack impact on SPS operation.

3.3.3 Implementation Algorithm of Stealthy Infiltrated Cyber Attacks

In order to design a SICA attack vector, $I_t^{(\cdot),a}$, the attacker must possess information regarding the behavior of the advanced cybersecurity layers. While conventional stealthy FDIAs primarily require knowledge of the network model and access to a minimum-effort attack vector, obtaining an accurate representation of the advanced cybersecurity mechanisms is significantly

Algorithm 2 SICA Implementation Algorithm

Require: Initial guess $x_t^{(0)}$, measurement vector z_t, initial thresholds $\tau_{t,\chi^2}^{(0)}$, covariance matrix $R = \sigma^2$

Ensure: Estimated optimal attack vector a_t

Set iteration counter $k \leftarrow 0$
while SICA not successful **do**
  Initiate GA
  while GA did not converge **do**
    for all $p \in$ GA population **do**
      Define the attack vector $a_{t,p}$
      Calculate the residual $r \leftarrow |z_t' - h(x_t')|$ → Apply Algorithm 1
      if $r > \tau_{t,\chi^2}^{(k)}$ **then**
        Set penalty PL
      end if
      Calculate objective $Obj \leftarrow \|a_{t,p}\|_0 + PL$
    end for
  end while
  Apply attack vector a_t → Apply Attack
  if $x_{t+1} \neq x_t'$ → Wait-and-Observe **then**
    $\tau_{t,\chi^2}^{(k+1)} \leftarrow \tau_{t,\chi^2}^{(k)} - \Delta\tau$ → Decrease Threshold
    $k \leftarrow k + 1$
  end if
end while

more challenging, as such information is typically highly confidential. Therefore, an iterative *Attack–Wait–and–Observe* strategy is proposed to implement SICA against SPS measurements z_t, as illustrated in Algorithm 2. The approach employs an iterative optimization process based on Genetic Algorithm (GA) to identify a successful attack vector.

Algorithm 2 aims to identify a successful attack vector capable of implementing a SICA. Initially, a threshold value is specified that the attack vector a_t must satisfy in order to remain undetected. A GA is then employed to determine a minimum-effort attack vector while penalizing solutions that violate the prescribed threshold. Once a candidate attack vector is obtained through the GA optimization process, it is deployed against the SPS during the *Apply Attack*

stage. Subsequently, the algorithm evaluates whether the resulting state, x_{t+1}, reflects the targeted compromised state x'_t. This step constitutes the *Wait-and-Observe* stage and serves to determine whether the attack has been successful. If the desired system response is not achieved, the GA optimization is reinitiated using a more restrictive threshold value. This iterative process continues until a successful attack vector is identified.

Although Algorithm 2 is presented for attacks targeting the measurement vector z_t, the same *Attack–Wait–and–Observe* concept can be readily extended to SICA implementation against primary information beyond the SE and against secondary information without loss of generality, as going to be discussed in Section 4.2.2.

3.4 Proposed Feasibility Area Approach for Stealthy Infiltrated Cyber Attacks Detection

Data-driven approaches often outperform model-based methods due to their ability to operate without detailed system models, making them more resilient to modeling errors and parameter uncertainties. They also enable fast detection, which is critical for real-time protection against FDIAs, while effectively identifying hidden and abnormal patterns that are difficult to capture using conventional model-based techniques [241]. In this regard, the FA concept can enhance data-driven learning by uncovering hidden patterns for classification tasks and validating the feasibility of predicted solutions in regression models [242]–[246]. Accordingly, FA has been applied to identify operational and economic regions of ESSs [242], guide DNN-based OPF solutions toward feasible and cost-effective operating points [243], and detect failures in SPS equipment [244].

3.4.1 Proposed Feasibility Areas Framework Structure and Preliminaries

3.4.1.1 Exact Feasibility Areas Estimation Using Bi-Level Robust Optimal Power Flows

The FA of the PSSVs represents the normal operating region in which the complex representation of the PSSVs (i.e., their real and imaginary components) are expected to exist within the complex plane. Compared with conventional interval-based SE methods, the proposed FA differs in two fundamental aspects. First, it is formulated using the joint real and imaginary

components of each PSSV, thereby preserving their inherent physical relationship, such as the power factor for active and reactive power measurements, and the phase angle for voltage and current phasors. Second, the FA is constructed based on the optimal operating conditions determined by the OPF, thereby accounting for the influence of the system objective and operational constraints on the expected operating region of the PSSVs. Consequently, the proposed FA framework utilizes the expected outcomes of the EMS, making it directly applicable to both SE monitoring and higher-level EMS applications.

In this case, the estimation of the FA can be formulated as a bi-level optimization problem. The upper-level optimization estimates the maximum feasible operating region for each PSSV, while the lower-level optimization solves a robust OPF that explicitly accounts for forecasting uncertainty in the primary information. The resulting FA can be mathematically formulated as follows:

$$
\begin{aligned}
&Max \sum_{n\in\mathbb{X}} Area(\phi_{t,n}) \\
&Min\ F(\hat{I^P}_t, \mathbb{X}_t),\ \text{Subject to:} \\
&L(\hat{I^P}_t, \mathbb{X}_t) \leq 0, \quad g(\hat{I^P}_t, \mathbb{X}_t) = 0, \quad \underline{\mathbb{X}} \leq \mathbb{X}_t \leq \overline{\mathbb{X}} \\
&\text{Where: } \hat{I^P}_t \in [{I^P}_t - \Delta I^P, {I^P}_t + \Delta I^P]
\end{aligned}
\tag{3.38}
$$

Here, ϕ denotes the FA structure and boundaries, while $\mathbb{X}_t$ represents the set of PSSVs at operating time t, including bus voltages, branch currents, load currents, branch apparent power, and load apparent power. The objective function $F(\hat{I^P}_t, \mathbb{X}_t)$ represents the optimization objective of the power system operator, such as OPF, economic dispatch, stability enhancement, or other operational objectives. This objective depends on both the forecasted primary information $\hat{I^P}_t$ and the resulting system operating state. The forecasted primary information $\hat{I^P}_t$ lies within the expected forecasting interval defined by the uncertainty bound ΔI^P. The functions $L(\hat{I^P}_t, \mathbb{X}_t)$ and $g(\hat{I^P}_t, \mathbb{X}_t)$ represent the linear inequality and nonlinear equality constraints, respectively, including equipment operating limits, network constraints, and power balance equations. Finally, $\underline{\mathbb{X}}$ and $\overline{\mathbb{X}}$ define the minimum and maximum permissible operating limits of each PSSV, including voltage and current constraints.

The proposed bi-level formulation aims to identify the complete feasible operating region by solving the robust OPF over all expected realizations of the forecasted primary information. Consequently, the estimated FA encompasses all normal operating states that may arise due to forecasting uncertainty while satisfying the operational objectives and system constraints. Since

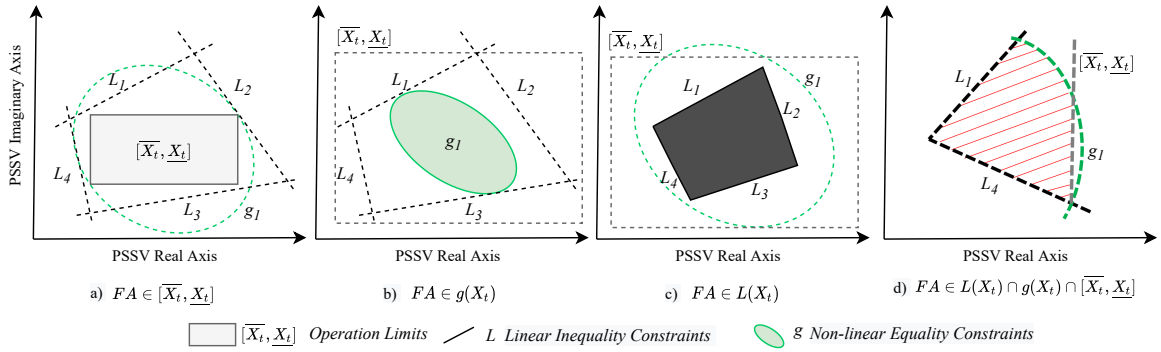


Figure 3.2: Feasibility area structure: (a) Rectangular $FA \in [\underline{X_t}, \overline{X_t}]$, (b) Circular or elliptic $FA \in g(X_t)$, (c) Irregular Convex-Hull polygon $FA \in L(X_t)$, (d) Irregular non-convex shape $FA \in [\underline{X_t}, \overline{X_t}] \cap g(X_t) \cap L(X_t)$.

the primary information is generated through forecasting at the central control unit rather than acquired directly from field measurements, it is assumed to be secure and therefore not directly vulnerable to cyberattacks.

3.4.1.2 Approximate Feasibility Areas Estimation Using Historical Operating Data

A major limitation of the exact FA estimation based on the proposed bi-level optimization framework is its high computational complexity. Estimating the FA boundaries requires repeatedly solving a robust OPF, which is particularly challenging due to the highly nonlinear nature of SPSs. When ESSs and other discrete operational decisions are considered, the problem becomes a robust Mixed-Integer Nonlinear Programming (MINLP) formulation with NP-hard computational complexity. For example, estimating the exact FA for the IEEE 30-bus system using Monte Carlo-based uncertainty analysis requires approximately 8–10 hours of computation. Consequently, the exact formulation becomes impractical for large-scale power systems and unsuitable for real-time cybersecurity applications.

To overcome this limitation, an approximate FA estimation approach is proposed based on historical operating data of the PSSVs. Instead of repeatedly solving the computationally intensive bi-level optimization, the proposed method constructs the expected FA directly from historical operating conditions that represent the normal behavior of the system. The accuracy of this approximation is subsequently validated through comprehensive statistical analysis by comparing the estimated operating boundaries with those obtained from the exact optimization framework. This validation demonstrates that the proposed historical data-driven approach

provides an accurate and computationally efficient approximation of the exact FA, making it suitable for real-time deployment in practical cybersecurity applications.

The computational algorithm searches for the optimal value within the feasible set of $\mathbb{X}_t$. Under the healthy operation, the feasible set represents the domain of healthy operation, and the *mapping of the feasibility set into the complex plane* of the PSSV $x_{t,n}$ represents the FA in which $x_{t,n}$ normally exists under the healthy operation. The structure of the FA relies on the fulfillment of the non-linear equality constraint $g(\hat{I^P}_t, \mathbb{X}_t)$ and falls within the intersection area formed by the linear inequality constraints $L(\hat{I^P}_t, \mathbb{X}_t)$ and the operating constraints $[\underline{\mathbb{X}}, \overline{\mathbb{X}}]$. Formulating a precise mathematical expression for the FA for each PSSV $x_n \in \mathbb{X}$ is highly intricate undertaking owing to the dynamic nature of the system and its dependence on various factors, such as the formulation of the objective function, the constraints imposed, the primary information utilized to establish operating limits, and network parameters, etc [101]. Consequently, the structure of the FA is considered based on possible combinations of the feasible set, and therefore, it is assumed that a combination of Deterministic classifiers Φ_D and Non-Deterministic classifiers Φ_{ND} exist to represent the FA of each PSSV.

Figure 3.2 shows the FA structures based on possible combinations of the feasible sets mapping to the complex plane of the PSSVs as explained hereunder.

- If the operating limits $[\underline{\mathbb{X}}, \overline{\mathbb{X}}]$ of $\mathbb{X}_t$ is a subset of $L(\hat{I^P}_t, \mathbb{X}_t) \leq 0 \cap g(\hat{I^P}_t, \mathbb{X}_t) = 0$, then the FA is represented by rectangular classifier ϕ_{Rec}.

- The FA can also be expressed in a circular form, which occurs when the plane $g(\hat{I^P}_t, \mathbb{X}_t) = 0$ is perpendicular to the complex plane of the PSSV $x_{t,n}^{R,I}$ and satisfies the condition $g(\mathbb{X}_t) = 0 \subseteq L(\hat{I^P}_t, \mathbb{X}_t) \leq 0 \cap [\underline{\mathbb{X}}, \overline{\mathbb{X}}]$. In this scenario, a circular classifier ϕ_{Cir} is employed to represent the FA.

- When the plane $g(\hat{I^P}_t, \mathbb{X}_t) = 0$ is neither parallel nor perpendicular to the complex plane of the PSSV $x_{t,n}^{R,I}$ and satisfies the condition $g(\hat{I^P}_t, \mathbb{X}_t) = 0 \subseteq L(\hat{I^P}_t, \mathbb{X}_t) \leq 0 \cap [\underline{\mathbb{X}}, \overline{\mathbb{X}}]$, an elliptic FA is achieved. In such cases, an elliptic classifier ϕ_{Ell} is utilized to represent the FA. The first three classifiers represent a regular FA and form the deterministic classifiers set $\Phi_D = \{\phi_{Rec}, \phi_{Cir}, \phi_{Ell}\}$.

- The FA can manifest itself in the form of a Convex-Hull polygon, which comprises the intersection of the set of linear inequality constraints $L(\hat{I^P}_t, \mathbb{X}_t) \leq 0$ and fulfills the condition $L(\hat{I^P}_t, \mathbb{X}_t) \leq 0 \subseteq g(\hat{I^P}_t, \mathbb{X}_t) = 0 \cap [\underline{\mathbb{X}}, \overline{\mathbb{X}}]$. Consequently, the FA will be represented by a

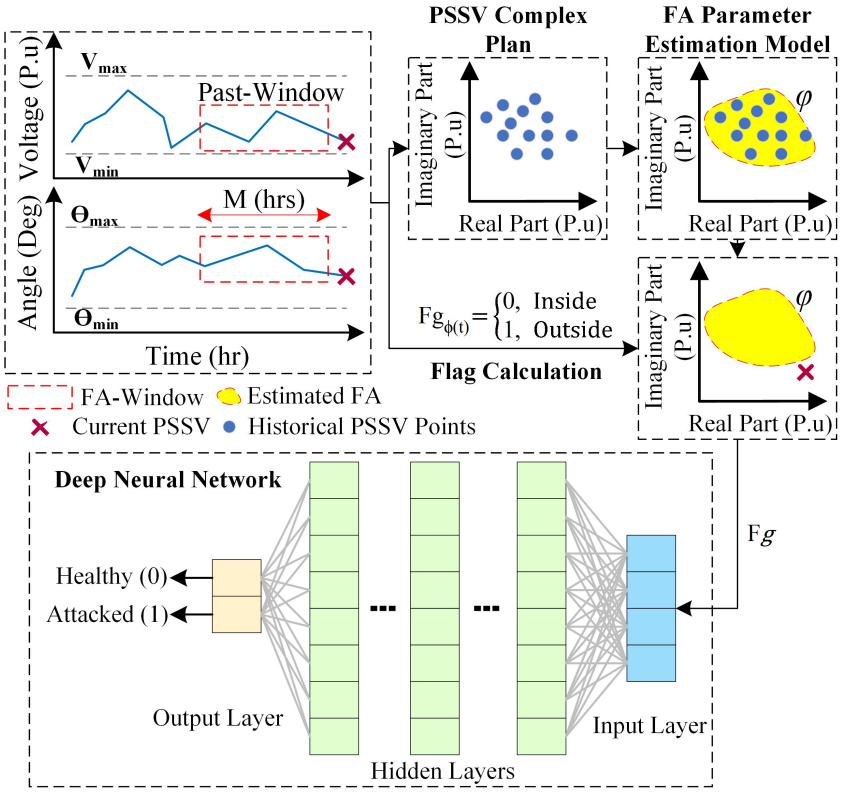


Figure 3.3: High level representation of an FA-based SICA detection framework.

Convex-Hull polygon, and a Convex-Hull classifier, denoted as ϕ_{CH}, is employed to depict the FA.

- In many situations, the FA can arise as the intersection of various constraints $FA = L(\hat{I^P}_t, \mathbb{X}_t) \cap g(\hat{I^P}_t, \mathbb{X}_t) \cap [\underline{\mathbb{X}}, \overline{\mathbb{X}}]$, rather than being a subset of any single constraint. In such cases, the FA takes an irregular and non-convex structure for most of the time. Consequently, there is a requirement for a classifier capable of handling such scenarios. To address this need, a Single-Class SVM classifier is employed, which utilizes the Gaussian Radial Basis Function (GRBF) as kernel. This particular classifier is recognized for its ability to create customized decision boundaries that account for irregular shapes using the kernel trick. Hence, a Single-Class SVM classifier is adapted ϕ_{SVM}. The last two classifiers represent the Non-deterministic classifiers set $\Phi_{ND} = \{\phi_{CH}, \phi_{SVM}\}$, and the overall FA classifier set includes both deterministic and non-deterministic classes $\Phi = \{\Phi_D \cup \Phi_{ND}\}$.

These Φ classifiers derive their name from their role in categorizing the current PSSVs as either (0) inside or (1) outside the FA. Figure 3.3 illustrates the FA-based cybersecurity layer, which

consists of three main stages. Although phasor voltage is used here for illustration, without loss of generality, the same procedure applies to all available PSSVs, including phasor current and apparent power. In the first stage, the PSSV measurements collected over an M^{FA}-hour historical window are plotted in the complex plane according to their real and imaginary components, producing a set of historical samples $\mathcal{S}^{FA}$. These samples serve as input for estimating the parameters of each FA classifier $\phi \in \Phi$. The general estimation criterion for each classifier ϕ is to minimize the enclosed area while ensuring that all historical samples $\mathcal{S}^{FA}$ remain within the FA. In other words, the binary empirical loss over the samples is zero. This can be expressed mathematically as:

$$\text{Minimize Area}(\phi)\ ,\ \text{Subject to: } L_{\mathcal{S}^{FA}}(\phi) = 0, \quad \forall \phi \in \Phi, \tag{3.39}$$

$$\Phi = \{\Phi_D \cup \Phi_{ND}\} \quad \begin{cases} \Phi_D = \{\phi_{Rec}, \phi_{Cir}, \phi_{Ell}\} \\ \Phi_{ND} = \{\phi_{CH}, \phi_{SVM}\} \end{cases}$$

Once the classifier parameters are estimated (e.g., ϕ_{Rec}: rectangular boundaries, ϕ_{Cir}: circular center and radius, ϕ_{Ell}: elliptical center and shape matrix, ϕ_{CH}: convex-hull vertices, and ϕ_{SVM}: kernel coefficients), a binary flag vector Fg_ϕ is generated. This flag vector encodes the position of each PSSV $x_{t,n}$ relative to the FA, as defined in:

$$Fg_{\phi(t,n)} = 1[x_{t,n} \notin \phi], \quad \forall \phi \in \Phi \tag{3.40}$$

Finally, the flag vectors from all classifiers are concatenated to form an *overall flag vector*, which serves as input to a DNN. The DNN identifies covert patterns of stealthy FDIAs by analyzing temporal variations in the PSSV positions. The overall flag vector expressed by (3.41)

$$Fg = \left[Fg_{Rec}^T,\ Fg_{Cir}^T,\ Fg_{Ell}^T,\ Fg_{CH}^T,\ Fg_{SVM}^T\right]^T \tag{3.41}$$

3.4.2 Feasibility Areas Classifiers Parameters Estimation

3.4.2.1 Rectangular Feasibility Area Classifier

The rectangular classifier ϕ_{rec} is determined by estimating the maximum and minimum real and imaginary parts $(x_{t,n}^{R,min}, x_{t,n}^{I,min}, x_{t,n}^{R,max}, x_{t,n}^{I,max})$ from the historical samples $\mathcal{S}^{FA}$ in the past M^{FA}-hour window. The optimization problem for estimating the rectangular parameters is

defined by (3.42).

$$\begin{aligned} &\text{Minimize: } (x_{t,n}^{R,max} - x_{t,n}^{R,min}) \times (x_{t,n}^{I,max} - x_{t,n}^{I,min}) \\ &S.t\ x_{t,n}^{R,min} \leq x_{\tau,n}^{R} \leq x_{t,n}^{R,max}, \quad x_{t,n}^{I,min} \leq x_{\tau,n}^{I} \leq x_{t,n}^{I,max}, \quad \forall n \in \mathbb{X} \wedge \forall\ \tau \in \mathcal{S}^{FA} \end{aligned} \tag{3.42}$$

3.4.2.2 Circular Feasibility Area Classifier

The circular classifier ϕ_{Cir} is determined by estimating the center and radius of the circle. The optimization problem aims to minimize the circle's area, i.e., its radius, while ensuring that all the historical samples $\mathcal{S}^{FA}$ in the past M^{FA}-hour window remain within the boundaries. The optimization problem is defined by (3.43):

$$\begin{aligned} &\text{Minimize: } r_{t,n} \\ &S.t\ (x_{cen(t,n)}^{R} - x_{\tau,n}^{R})^2 + (x_{cen(t,n)}^{I} - x_{\tau,n}^{I})^2 \leq r_{t,n}^2, \quad \forall n \in \mathbb{X} \wedge \forall\ \tau \in \mathcal{S}^{FA} \end{aligned} \tag{3.43}$$

3.4.2.3 Elliptic Feasibility Area Classifier

The elliptic classifier ϕ_{Ell} is determined by both the center vector of the ellipse ($C_{t,n}^{Ell}$), and the shaping matrix ($A_{t,n}^{Ell}$). The optimization problem aims to minimize the ellipse's area, while ensuring that all the historical samples $\mathcal{S}^{FA}$ in the past M^{FA}-hour window remain within the ellipse boundaries. The formulation of the optimization problem is provided in (3.44):

$$\begin{aligned} &\text{Minimize: } \left|(A_{t,n}^{Ell})^{-1}\right| \\ &S.t\ (x_{\tau,n} - C_{t,n}^{Ell})^T A_{t,n}^{Ell} (x_{\tau,n} - C_{t,n}^{Ell}) \leq 1, \quad \forall n \in \mathbb{X} \wedge \forall\ \tau \in \mathcal{S}^{FA}. \end{aligned} \tag{3.44}$$

3.4.2.4 Convex-Hull Feasibility Area Classifier

The convex-hull classifier is constructed by forming a polygon that encloses the historical samples $\mathcal{S}^{FA}$ from the past M^{FA}-hour window. To accurately estimate the convex-hull polygon, this paper utilizes the high-dimensional estimation Graham's scan algorithm, as detailed in [247], and shown by Algorithm 3. The algorithm begins by identifying the lowest point (the point with the minimum imaginary value in the complex plane), which serves as one of the polygon's outliers. It then selects subsequent points to maintain a counterclockwise orientation. The output of the Graham's scan algorithm consists of the convex-hull boundary points $SV_{t,n}^{CH} \in \mathcal{S}^{FA}$.

Algorithm 3 Graham's Scan Convex-Hull Estimation

Require: Sample set $\mathcal{S}^{FA} = \{s_i\}_{i=1}^{N}$

Ensure: Convex-hull support vector set $SV_{t,n}^{CH}$

Find the point $p_0 \in \mathcal{S}^{FA}$ with the minimum imaginary coordinate.
if multiple points satisfy the condition **then**
    Select the point with the minimum real coordinate.
end if
Sort all points according to their polar angle with respect to p_0.
For points with identical polar angles, retain only the farthest point from p_0.
Initialize an empty stack $SV_{t,n}^{CH}$.
for each point p_i in the sorted sequence **do**
    while $|SV_{t,n}^{CH}| > 1$ and $\text{CCW}(\text{NextToTop}(SV_{t,n}^{CH}), \text{Top}(SV_{t,n}^{CH}), p_i) \leq 0$ **do**
        Pop the top point from $SV_{t,n}^{CH}$.
    end while
    Push p_i onto $SV_{t,n}^{CH}$.
end for
return $SV_{t,n}^{CH}$
Function $\text{CCW}(x_1, x_2, x_3)$: → CounterClockWise test
$\text{CCW}(x_1, x_2, x_3) = (x_2^R - x_1^R)(x_3^I - x_1^I) - (x_2^I - x_1^I)(x_3^R - x_1^R)$.
$(\text{CCW} > 0 : \text{ counterclockwise}), \quad (\text{CCW} < 0 : \text{ clockwise}), \quad (\text{CCW} = 0 : \text{ collinear points})$

3.4.2.5 Single-Class Support Vector Machine Feasibility Area Classifier

The SVM classifier is defined in (3.45), where the SVM coefficients are represented by $\alpha_{\tau,n}$, the GRBF is given by $e^{-\lambda_{t,n}|x_{\tau,n}-x|^2}$, and $\lambda_{t,n}$ denotes the kernel size. Increasing the kernel size results in a smoother decision boundary, offering a wider separation between classes, while decreasing the kernel size creates a more complex decision boundary that captures finer patterns in the training data. Typically, the kernel scale value is adjusted during the model training phase to determine the optimal value.

$$\phi_{SVM} = sgn\left(\sum_{\tau,\tau' \in \mathcal{S}^{FA}} \alpha_{\tau,n}.e^{-\lambda_{t,n}|x_{\tau,n}-x_{n,\tau'}|^2}\right) \tag{3.45}$$

The parameters of the classifier ϕ_{SVM} are estimated to ensure that all the historical samples $\mathcal{S}^{FA}$ in the past M^{FA}-hour window are assigned to the same class of healthy operation. The

optimization problem stated in (3.46) is solved to estimate the parameter of the classifier ϕ_{SVM} using quadratic programming, which is efficiently solved using the sequential minimal optimization algorithm [248].

$$min \sum_{\tau,\tau' \in \mathcal{S}^{FA}} \alpha_\tau . \alpha_{\tau'} . e^{-\lambda_{t,n}|x_{\tau,n} - x_{n,\tau'}|^2}, \text{ Subject to: } \sum_{\tau \in \mathcal{S}^{FA}} \alpha_\tau = 0 \tag{3.46}$$

3.4.3 Performance Metrics for the Feasibility Areas-Based SICA Detection

To evaluate the effectiveness of different FA structures in detecting anomalous variations in PSSVs, the TP, FN, and FAUR metrics are defined for each PSSV. The TP metric measures the ability of a classifier $\phi \in \Phi$ to accurately identify healthy PSSV operations that fall within the FA defined by the classifier. The FN metric assesses the classifier's capability to correctly detect abnormal PSSV variations caused by SICA, ensuring these anomalies are identified as residing outside the FA. Using τ^{HL} (healthy dataset) and τ^{A} (attacked dataset), the TP and FN ratios for each PSSV using a given classifier ϕ are calculated by (3.47).

$$TP_{\phi,n} = \frac{\sum_{t=1}^{\tau^{HL}} 1[x_{t,n} \in \phi]}{|\tau^{HL}|}, \; FN_{\phi,n} = \frac{\sum_{t=1}^{\tau^{A}} 1[x_{t,n} \notin \phi]}{|\tau^{A}|} \tag{3.47}$$

The FAUR metric evaluates the presence of SICA by analyzing variations across all PSSVs relative to the FA defined by the classifier ϕ. FAUR is calculated as the ratio of PSSVs located outside the FA of classifier ϕ to the total number of PSSVs. A high FAUR value suggests a higher likelihood of a SICA. Conversely, a low FAUR value indicates a greater probability of normal system operation. The FAUR for a given classifier ϕ at time t is calculated using (3.48).

$$FAUR_{t,\phi} = \frac{\sum_{n=1}^{N} Fg_{\phi(t,n)}}{|N|} \tag{3.48}$$

3.5 Numerical Results

3.5.1 Test System and Simulation Environment

The IEEE 30-bus test system, illustrated in Figure 3.4, is employed as the SPS simulation testbed. The system is simulated over a one-year horizon with a time resolution of $\Delta t = 1$ hour, resulting in a healthy-operation dataset of $\tau^{HL} = 8,760$ samples based on Ontario electricity market data from 2022. The placement of PMUs and their associated measurements is determined using the methodology proposed in [249]. In addition, SCADA measurements

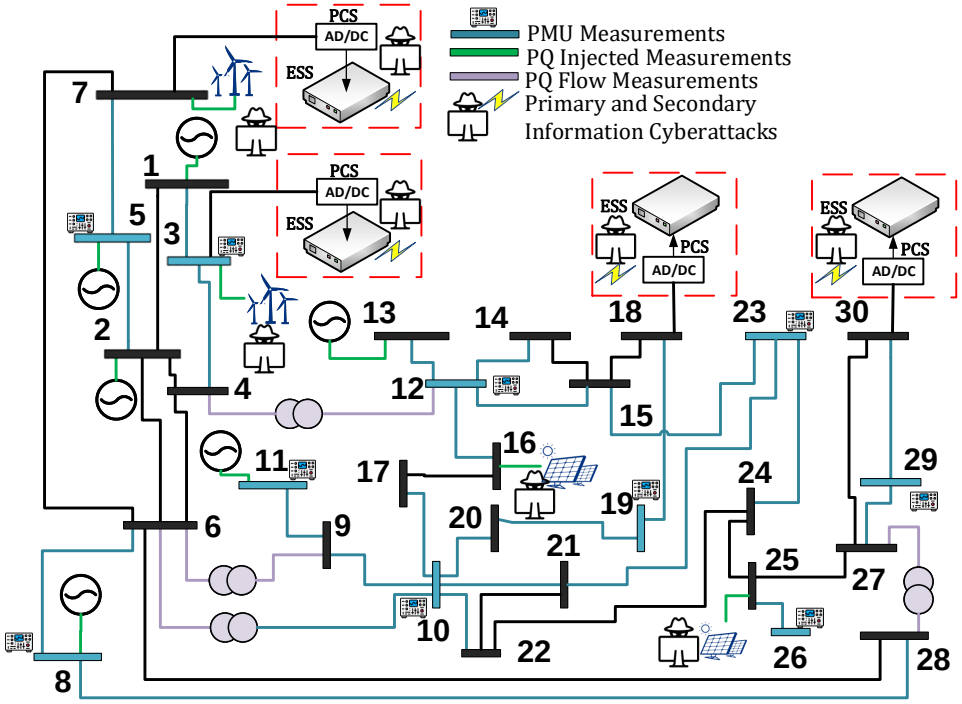


Figure 3.4: The IEEE 30-bus transmission system employed for numerical studies showing PMUs and SCADA measurements, and FDIA of primary and secondary information.

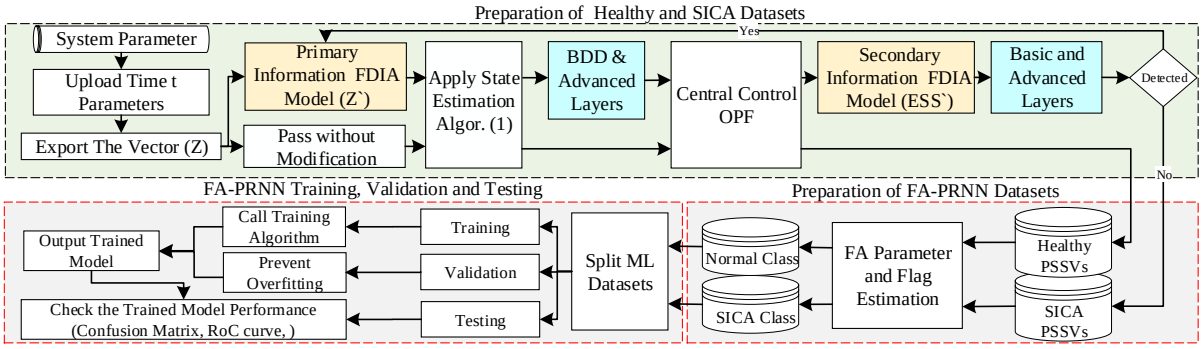


Figure 3.5: Healthy and SICA scenario generation flowchart.

are deployed at critical infrastructure components, including generators for injected apparent power measurements and transformers for branch apparent power monitoring. Primary information cyberattacks, both stealthy FDIAs and SICAs, are designed to maximize the mismatch in RES power generation measurements, thereby misleading the OPF decision-making process and optimality. For secondary information, cyberattacks directly manipulate the ESS charging and discharging setpoints, effectively emulating attacks targeting controllable generation and adjustable demand resources.

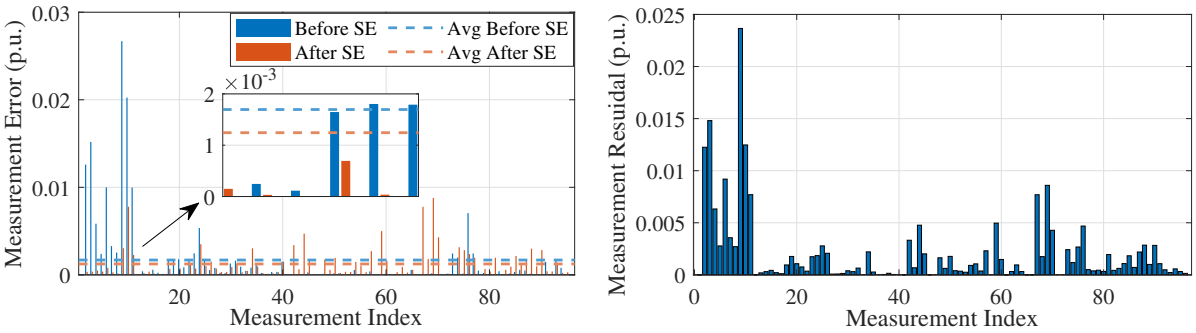


Figure 3.6: Performance of SE in removing measurements error.

Figure 3.5 illustrates the simulation framework and data preparation procedure. At each time step t, the simulation parameters are first loaded, and the healthy PSSV is obtained by applying the unmodified primary information to the computational framework. The resulting outputs are then stored in the healthy PSSV dataset. For the cyberattack scenarios, the primary and secondary SICA models, together with Algorithm 2, are employed to generate manipulated operating conditions. To construct a successful SICA, the manipulated information is iteratively evaluated against the advanced cybersecurity layers described in Section 3.2.1. If the attack is detected by any cybersecurity mechanism, a new attack vector with a reduced manipulation margin is generated following the *Attack–Wait–and–Observe* strategy until all cybersecurity layers are successfully bypassed. The resulting outputs are subsequently stored in the SICA dataset.

For the SPS under study, the bus phasor voltages, injected currents, and injected complex apparent powers at each bus are utilized as PSSVs. For transmission lines, the sending-end and receiving-end currents, together with the corresponding complex apparent power measurements, are used as PSSVs. In total, three and four PSSVs are considered for each bus and transmission line, respectively. All simulations are conducted on an Intel Core i9 (12th Generation, 2.1 GHz) workstation equipped with 32 GB of RAM.

3.5.2 State Estimations and Primary and Secondary Information Cyberattacks

3.5.2.1 Performance of State Estimations

The SE is executed throughout the simulation period to estimate the optimal voltage state vector, x^*. Figure 3.6 compares the measurement error before state estimation, $(z^{act} - z)$, and

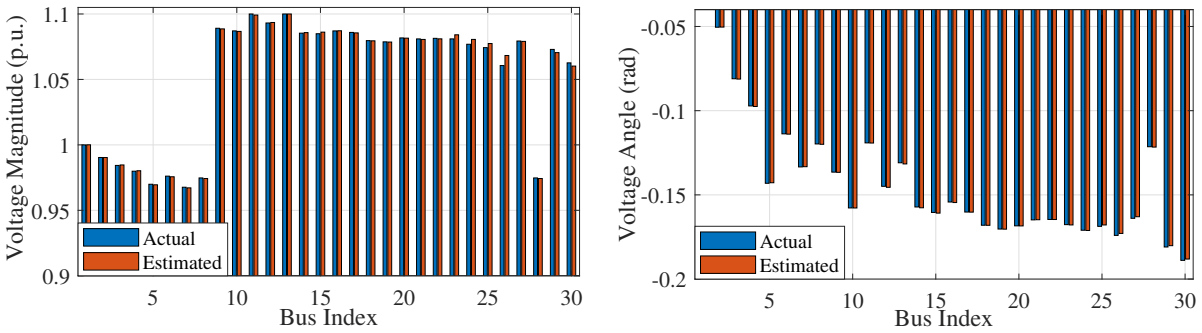


Figure 3.7: SE estimated state x^* and the actual state x^{act}.

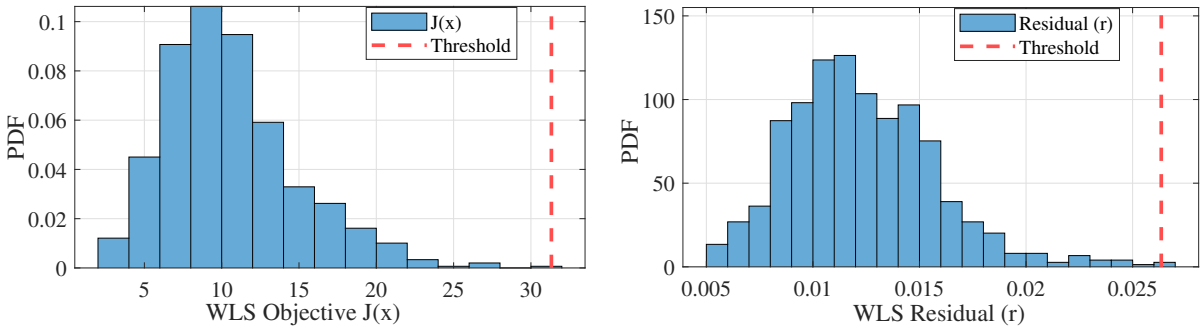


Figure 3.8: SE objective $J(x)$ and residual $r = |z - h(x^*)|$ PDF.

after state estimation, $(z^{act} - h(x^*))$, demonstrating the ability of the SE to provide a more accurate representation of the system state. Note that z^{act} or x^{act}, is only available in the simulation environment, where the true measurements are known before introducing PMU and SCADA measurement errors. The results shows that, the SE reduces the average absolute error from 0.001695 p.u. to 0.0012437 p.u., corresponding to an error reduction of 36.3%. Meanwhile, Figure 3.7 compares the estimated state x^* with the actual state x^{act} (i.e., bus phasor voltages), demonstrating the ability of the SE to accurately estimate the SPS state with minimal deviation.

3.5.2.2 Design and Performance of Bad Data Detection and Advanced False Data Injection Attacks Detection Layers

Figure 3.8 presents the PDF of the SE objective function $J(x)$ and the residual over one year of simulation, used for BDD layer design. The objective function $J(x)$ follows a chi-PDF distribution due to the squared residual structure, while the residual $r = |z - h(x^*)|$ follows a Gaussian PDF, reflecting the measurement error distribution in z. Based on this statistical characterization, two BDD thresholds are defined: 1) $J(x) \leq 31.32$ p.u., and 2) $r \leq 0.0263$ p.u.

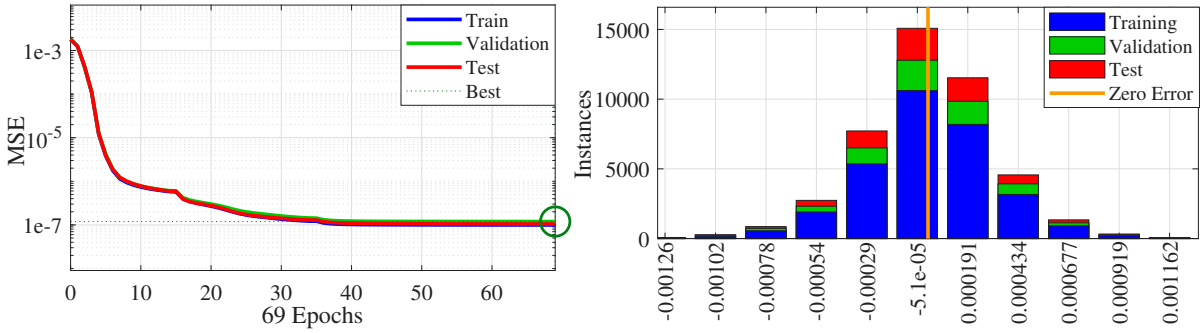


Figure 3.9: Advanced stealthy FDIA forecasting-based detection layer training performance and optimal state x^* forecasting error.

Any SE result exceeding any of these limits triggers a BDD alarm.

For stealthy FDIA detection, an adaptive threshold approach is adopted, where τ_{t,χ^2} is estimated using a DNN, as discussed in Section 3.2.1. To improve robustness and avoid reliance on a specific set of measurements, a dropout layer is incorporated such that a subset of inputs is randomly excluded during each prediction. Figure 3.9 presents the training performance of the DNN in forecasting the optimal state and the corresponding threshold. The model exhibits consistent performance across the training, validation, and testing datasets. As shown by the error histogram, the forecasting error remains small, with a mean error of 0.0071 p.u. and a maximum error of 0.0355 p.u. These results demonstrate the model's ability to accurately predict the expected system state and provide an effective advanced detection layer against stealthy FDIAs.

3.5.2.3 Basic and Stealthy False Data Injection Attacks

For the implementation of basic FDIA, the attacker is assumed to have access only to the measurements it intends to manipulate. Since the attacker lacks knowledge of the SPS model, the attack targets the injected RES power measurements at buses 3, 7, 16, and 25 to cause direct impact. The attack vector a_t is randomly generated with a magnitude ranging from 2.5% to 10% of the measurement value. Due to the inconsistency between the injected attack vector and the underlying SPS model, the estimated state x^* deviates significantly from its true value x^{act}, as shown in Figure 3.10. This inconsistency results in substantial increases in both the WLS objective function $J(x)$ and the residual r, causing them to exceed the BDD thresholds. Consequently, the BDD layer successfully detects all basic FDIAs.

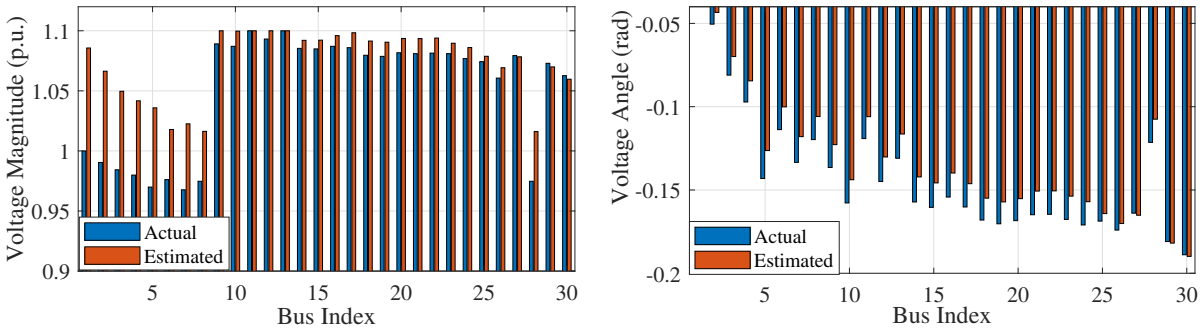


Figure 3.10: SE estimated state x^* and the actual state x^{act} under basic FDIA.

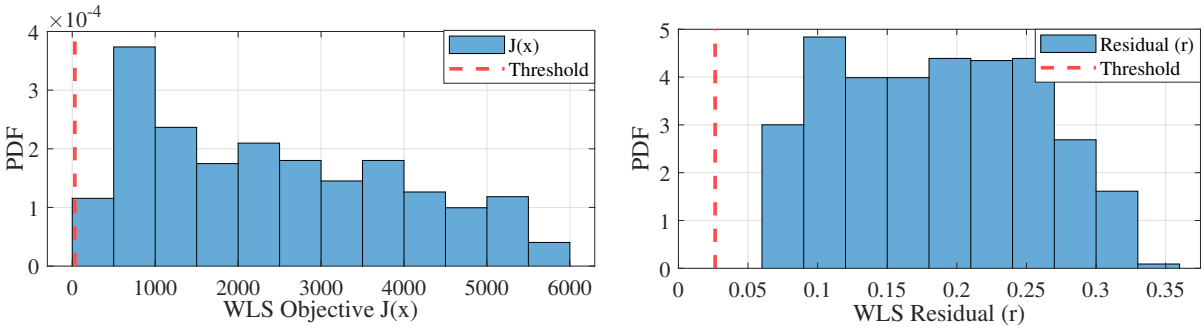


Figure 3.11: SE objective $J(x)$ and residual $r = |z - h(x^*)|$ PDF under basic FDIA.

Unlike basic attacks, stealthy FDIAs are designed with prior knowledge of the SPS model and network parameters. The attacker is assumed to optimize a least-effort attack vector while selecting the measurements to compromise. To maintain stealthiness, the attack magnitude is limited to $\pm 1\%$, keeping the manipulated measurements within the typical accuracy range of PMUs and SCADA. For each steady-state SE and EMS interval, the GA is executed for five minutes to determine the optimal attack vector a_t. Figure 3.12a) demonstrates that the stealthy FDIA successfully bypasses the BDD by maintaining the WLS objective function $J(x)$ below the detection threshold. Figure 3.12b) presents the optimized attack vectors a_t, highlighting the induced mismatch in the targeted RES measurements. Consequently, Figure 3.13 shows a clear deviation between the estimated x^* and actual system states x^{act}, confirming that the attack successfully misleads the SE while remaining undetected by the BDD.

While stealthy FDIAs can bypass the BDD, advanced detection layers employ adaptive thresholds to improve their detection capability. Figure 3.14 compares the forecasted adaptive threshold with the WLS objective function $J(x)$ under stealthy FDIA. Although all attacks evade the conventional BDD, the advanced detection layer successfully identifies 71% of the

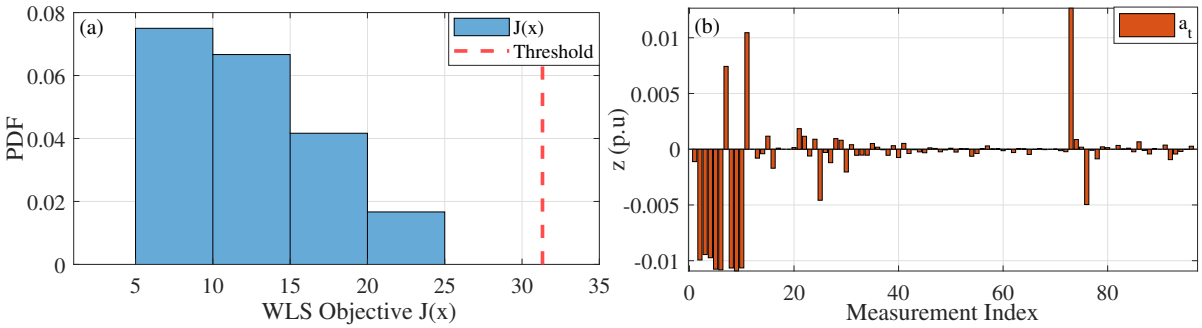


Figure 3.12: Performance of stealthy FDIA a) bypass the BDD layer, and b) optimal designed attack vector a_t.

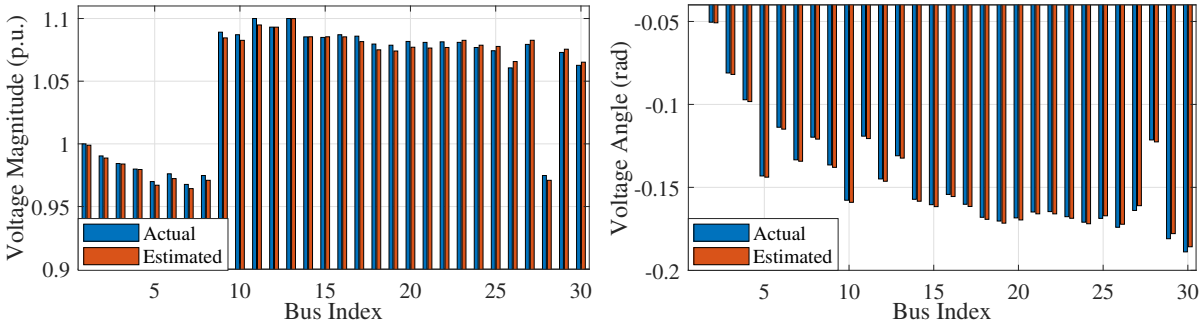


Figure 3.13: SE estimated state x^* and the actual state x^{act} under stealthy FDIA.

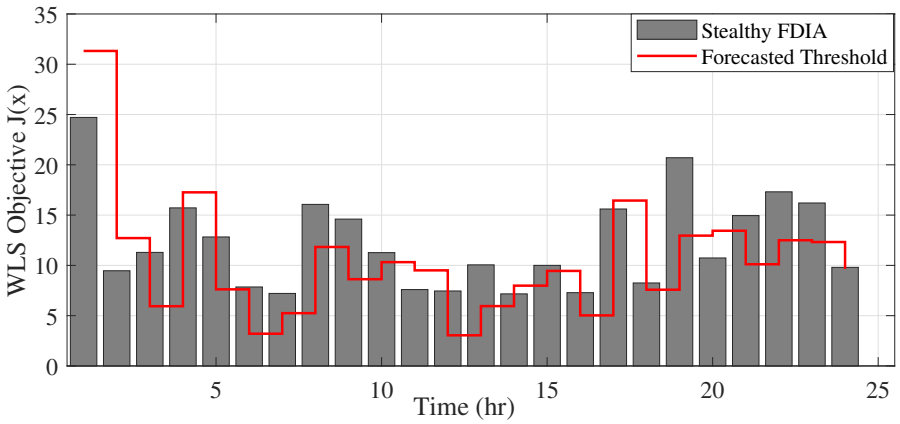


Figure 3.14: WLS objective $J(x)$ under stealthy FDIA and forecasted threshold using advanced stealthy FDIA detection layer.

attacks. The remaining 29% bypass the advanced layer and are therefore classified as SICAs. However, this success rate is relatively low, motivating the development of the proposed SICA implementation to further improve the attack bypass capability.

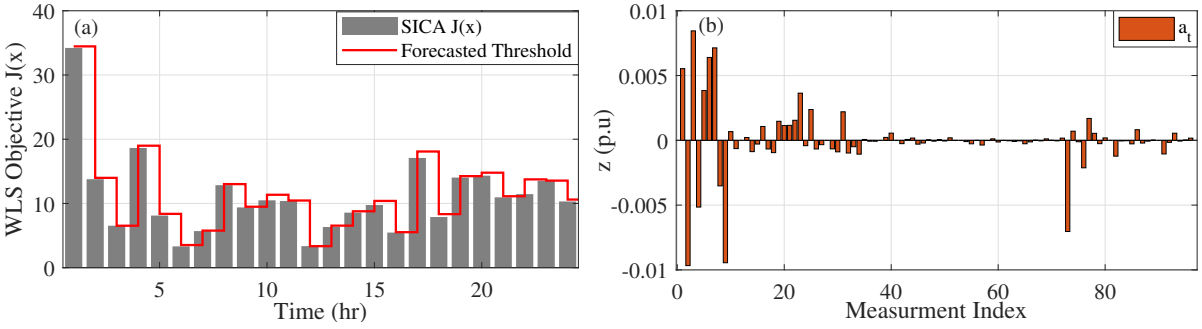


Figure 3.15: Performance of SICA; a) WLS objective $J(x)$ under SICA and forecasted threshold, b) optimal designed attack vector a_t.

3.5.3 Stealthy Infiltrated Cyber Attack Implementation

Unlike stealthy FDIAs, SICA considers both the BDD and the advanced detection layers by employing an *Attack–Wait–and–Observe* strategy to ensure that the designed optimal attack vector a_t bypasses all cybersecurity mechanisms. Figure 3.15a) illustrates the performance of the proposed SICA algorithm, where the attack successfully maintains the WLS objective $J(x)$ below the dynamic SE threshold. Compared to the stealthy FDIA results in Figure 3.14, SICA achieves consistent bypass of the detection thresholds through iterative refinement of a_t. Moreover, due to the adaptive threshold mechanism, SICA maintains $J(x)$ close to the boundary with small deviations, enabling a larger margin for attack optimization and consequently higher impact. This is reflected in Figure 3.15b), where the allowed deviation is effectively exploited to enhance attack effectiveness. As a result, the detection rate of the advanced layer decreases from 71% to only 3%, demonstrating the effectiveness of the proposed SICA in bypassing advanced cybersecurity mechanisms and successfully impacting SPS operation.

It is worth noting that the parameter $\Delta\tau$ (see Algorithm 2) governs the trade-off between the convergence speed toward an acceptable SICA threshold and the number of attack queries issued by the attacker. A larger $\Delta\tau$ accelerates convergence to the desired threshold τ_{t,χ^2}, but may reduce the threshold below an acceptable margin, making it difficult to construct a sufficiently impactful attack.

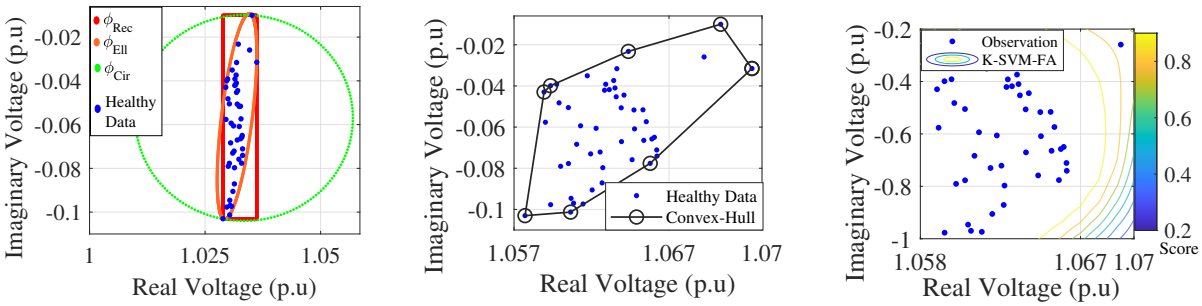


Figure 3.16: Estimated deterministic and non-deterministic FA: a) rectangular, circular, and elliptic classifiers, b) Convex-Hull classifier, c) single-class SVM.

3.5.4 Performance of Feasibility Area-Based for Stealthy Infiltrated Cyber Attack Detection

As shown in the previous section, although the advanced detection layer identifies 71% of stealthy FDIAs, its detection rate drops to only 3% against a well-designed SICA. Therefore, effective SICA detection is essential to prevent attack propagation within the SPS and enable timely corrective actions. To detect SICAs, an FA-based detection layer is employed to identify abnormal variations in the PSSVs caused by the injected optimal attack vector a_t. These variations are quantified by the difference between the estimated healthy state and the estimated attacked state, defined as $\Delta x = x^*|_z - x^*|_{z'}$.

Figure 3.16 provides a visual illustration of the rectangular, circular, elliptical, Convex-Hull, and Single-Class SVM FA classifiers used to characterize the healthy (non-attacked) operating region. The healthy data, represented by blue dots, correspond to the complex phasor voltages over the previous 48 hours. If the estimated phasor voltage at the next time step lies within the FA boundary, it is classified as normal and the detection flag is set to zero; otherwise, it is classified as abnormal and the flag is set to one.

Figure 3.17 illustrates the 2-D complex-plane representation of healthy PSSVs and their corresponding SICAs for the IEEE 30-bus system. As shown in Figure 3.17, healthy PSSVs are enclosed within the corresponding FA. When the attack vector a_t alters the estimated state x_t, the resulting PSSVs deviate from the healthy FA, providing a clear indication of a SICA. Using the examples in Figure 3.17, the proposed approach detects approximately 42.3%–52.1% of SICAs using ϕ_{Rec} for Branch 29–30 and ϕ_{Ell} for the Bus 2 voltage, despite these attacks bypassing the BDD and the advanced detection layers.

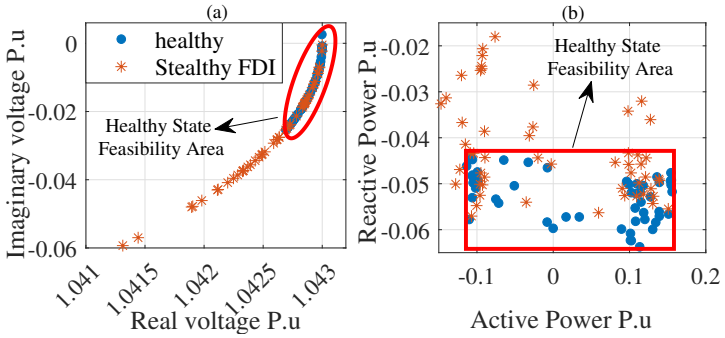


Figure 3.17: Complex plane representation of the PSSV under healthy and SICA; a) Bus 2 real and imaginary voltage values, b) Branch 29-30 active and reactive power values.

3.5.4.1 Individual Performance of Feasibility Area Classifiers

The performance of individual FA classifiers provides essential insight into the suitability of each classifier ϕ in representing the expected normal operation and in statistically characterizing abnormal variations prior to the use of PRNN, ensuring that meaningful learning information is available. Figure 3.18 presents the distributions of TP and FN for PSSVs using the proposed FA classifiers over estimation windows of $M^{FA} = 24$, 48, and 168 hours, covering all PSSVs. A higher mean value indicates a more accurate representation of the FA and improved capability to detect SICAs, while a lower standard deviation reflects better consistency of the classifier ϕ across different PSSVs. In the ideal case, a perfect FA classifier would achieve 100% performance in both TP and FN when no overlap exists between healthy and attacked state spaces. Among the tested methods, ϕ_{Rec} and ϕ_{SVM} achieve the highest TP performance, with mean values of 94–97% and standard deviations of 0.54–1.16%. However, their SICA detection capability remains moderate. In contrast, ϕ_{Ell} and ϕ_{CH} provide more robust separation of the FA, leading to stronger SICA prevention performance, while ϕ_{Cir} shows intermediate behavior across both metrics.

Across all classifiers, the probability of a PSSV falling outside the FA is consistently higher under attack than under normal operation. For example, under healthy conditions, the probability of being outside the ϕ_{SVM} FA is 3%, whereas under SICA it increases to 19.3%. This confirms the effectiveness of the FA-based approach for SICA detection. Finally, increasing the window size M^{FA} increases the number of samples $\mathcal{S}^{FA}$ used to train the classifier ϕ, resulting in a wider FA. This increases the likelihood of overlap between healthy and attacked states,

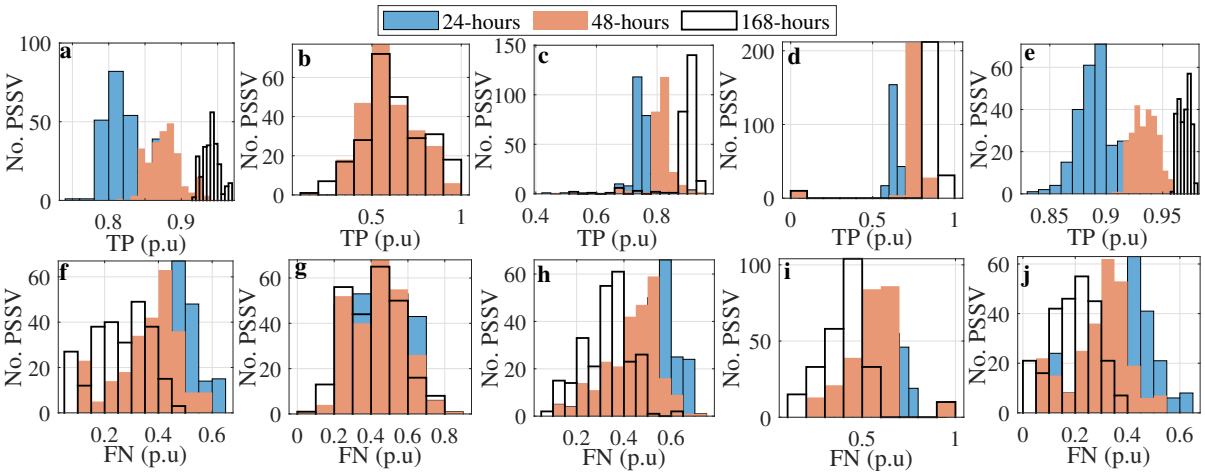


Figure 3.18: TP and FN values for window sizes of 24, 48, and 168 hours: a) $TP_{\phi_{Rec}}$ b) $TP_{\phi_{Cir}}$ c) $TP_{\phi_{Ell}}$ d) $TP_{\phi_{CH}}$ e) $TP_{\phi_{SVM}}$ f) $FN_{\phi_{Rev}}$ g) $FN_{\phi_{Cir}}$ h) $FN_{\phi_{Ell}}$ i) $FN_{\phi_{CH}}$ j) $FN_{\phi_{SVM}}$.

leading to higher TP and lower FN values.

3.5.4.2 Performance of Feasibility Area Across All Power System State Variables

Similar to individual FA classifier performance, the FAUR ($FAUR_{t,\phi}$) metric evaluates the impact of SICAs across all PSSVs, indicating whether the system experiences abnormal deviations in the operating state of the SPS. Figure 3.19 compares FAUR under normal operation and under SICA for different classifiers and window sizes. Across all cases, FAUR consistently increases under attack conditions, indicating a higher number of PSSVs falling outside the FA due to state deviations induced by the attack vector a_t. Notably, in approximately 82.02% of the dataset (about 7,185 hours in a full-year simulation), FAUR is higher under attacks than under normal operation. This confirms the ability of the FA-based framework to capture SICA-induced variations in PSSVs.

3.5.4.3 Performance of Feasibility Area-Based Deep Neural Network Model in Detecting Stealthy Infiltrated Cyber Attacks

To develop a robust SICA detection layer, the outputs of the FA classifiers, specifically the overall flag vector Fg, are used to train a DNN for identifying abnormal variations in PSSVs induced by SICAs. The integration of FA with DNN-based detection is implemented through

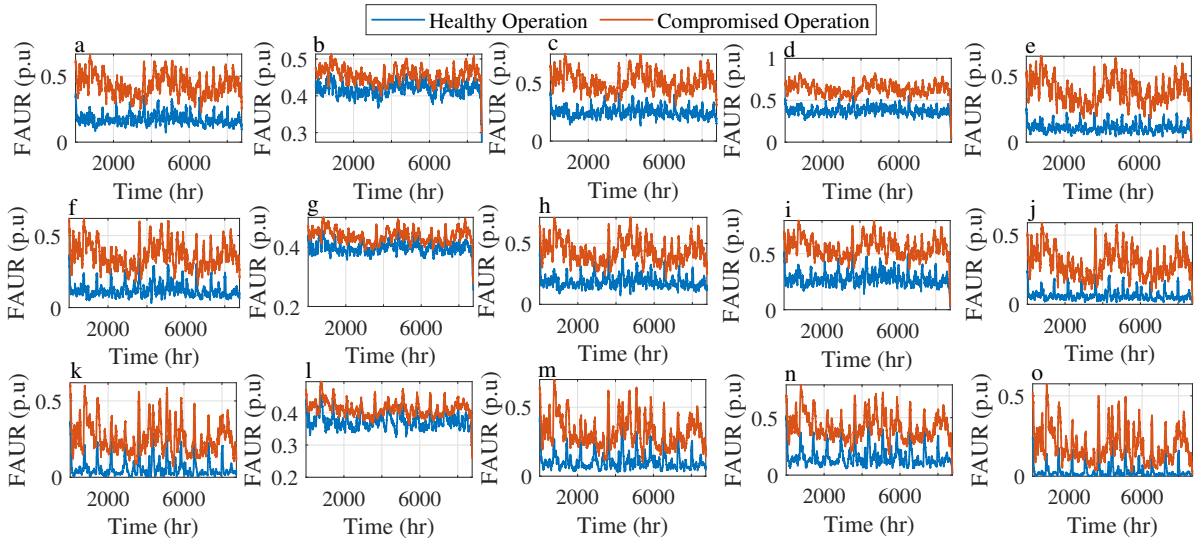
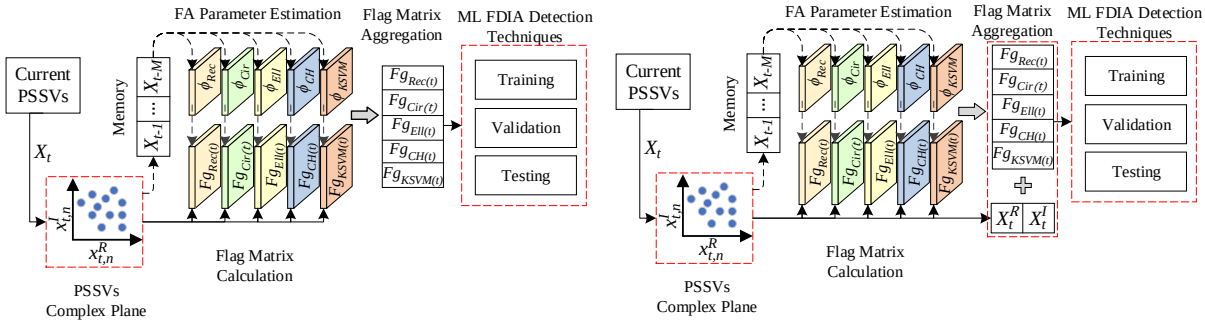


Figure 3.19: FAUR under healthy operation and attacked scenarios



(a) Feedforward FA-Based ML FDIA Detection.

(b) Residual FA-Based ML FDIA Detection.

Figure 3.20: Structure of the FA-based DNN SICA detection.

two structures: Feedforward and Residual FA-based DNN, as shown in Figure 3.20. In the Feedforward structure, PSSVs are first processed by the FA layer to generate the flag vector Fg, which is then used as input to train the DNN independently. In contrast, the Residual structure jointly uses the flag vector and the real and imaginary components of PSSVs. In this case, the DNN is trained on the combined input $[Fg^T, (\mathbb{X}_t^R)^T, (\mathbb{X}_t^I)^T]^T$.

Figure 3.21 summarizes the training and validation performance of the FA-based DNN for SICA detection. Here, the "B term" denotes baseline DNN models without FA integration, the "F term" refers to Feedforward FA-based DNN, and the "R term" corresponds to Residual FA-

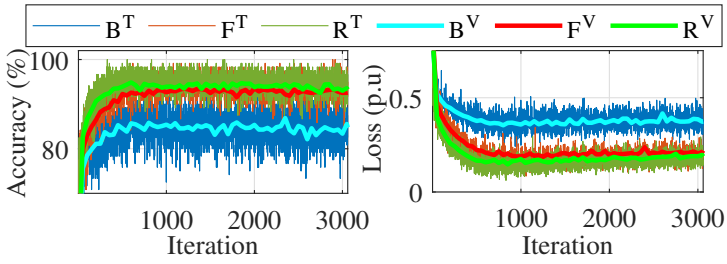


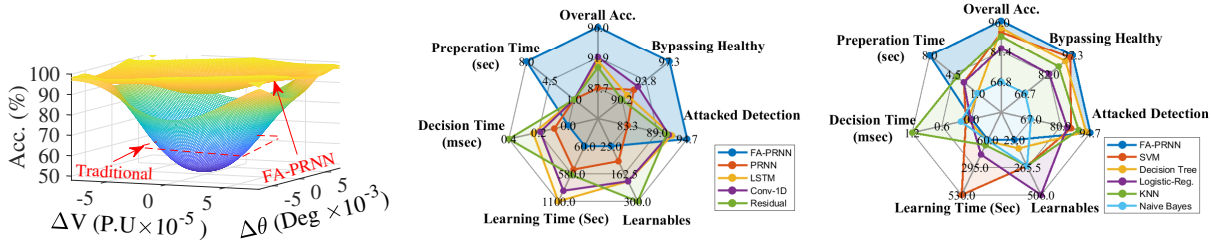
Figure 3.21: Training performance of different DNN structures. B: Basic DNN, F: Feed-forward FA-based DNN, R: Residual FA-based DNN, T: Training, and V: Validation.

based DNN. The results show that integrating the FA layer improves both detection performance and learning stability, reducing loss noise and accelerating convergence. The Residual FA-based DNN consistently achieves the best performance across all cases. Quantitatively, the Feedforward structure improves the basic performance performance by 2.51%–7.38%, while the Residual structure yields higher gains of 6.08%–8.03%.

To capture the temporal patterns of SICAs, a FA-PRNN is proposed, leveraging its memory-based architecture to identify abnormal state variations. Its performance is compared with conventional DNN and ML methods to evaluate its generalization capability. Figure 3.22a shows the detection accuracy as a function of the SPS state deviation (x_t^*) caused by SICAs. As the state deviation decreases, the performance of the conventional PRNN (blue surface) deteriorates significantly. In contrast, the proposed FA-PRNN (yellow surface) maintains consistently high accuracy, demonstrating its ability to detect SICAs even under small PSSV variations.

Figures 3.22b and 3.22c compare the proposed FA-PRNN with conventional DNN and ML methods. The proposed approach achieves an average detection accuracy of 96%, outperforming all benchmark methods by 4%–30%. In addition, it requires a smaller network and fewer learnable parameters, resulting in faster training and inference. The only additional overhead is approximately 8 seconds for FA estimation and flag vector calculation.

It is worth noting that the performance improvement achieved by the proposed FA-PRNN is confirmed to originate from the FA representation rather than the PSSVs themselves. To isolate the contribution of the proposed FA, a feedforward DNN architecture was evaluated using only the FA features as input, thereby eliminating any influence from the raw PSSVs. As shown by the results, the performance improvement remains significant compared with a feedforward network trained directly on the PSSVs, demonstrating that the enhanced detection capability is



(a) (b) (c)

Figure 3.22: Comparison of various performance metrics a) Accuracy with respect to PSSVs variation compared with basic-PRNN, b) proposed Proposed FA-PRNN Vs DNN b) Proposed FA-PRNN Vs common ML methods [1].

primarily attributed to the informative cyber–physical features extracted by the proposed FA. Furthermore, to ensure a fair comparison, each DNN architecture was individually optimized before evaluation, confirming that the observed performance gains are due to the proposed FA representation rather than differences in network structure or hyperparameter selection.

3.5.4.4 Generalization and Adaptation of the Feasibility Area-Based Deep Neural Network Under New Attacks and Normal Operating Disturbances

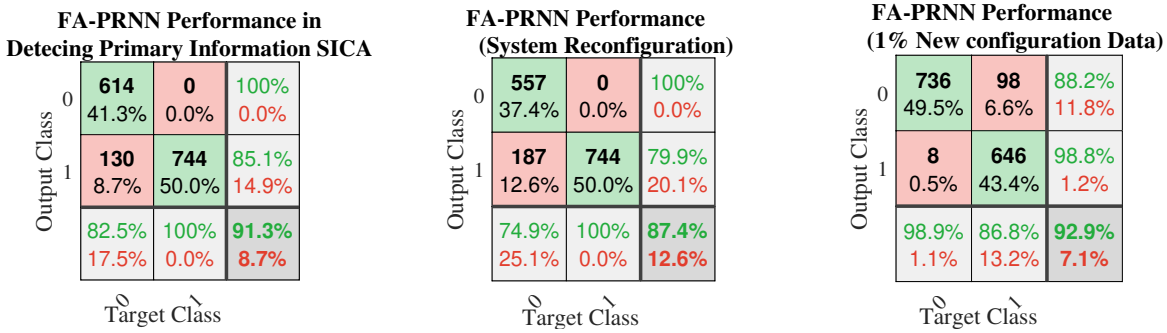
To ensure the practical applicability of the proposed FA-PRNN, the model must demonstrate strong generalization to previously unseen cyberattack scenarios while maintaining robustness against normal operating disturbances. Specifically, the framework should accurately distinguish SICAs from legitimate system events, such as equipment outages, network reconfiguration, and other steady-state operating changes caused by normal system operation or component failures.

To evaluate these capabilities, the proposed FA-PRNN is initially trained using SICAs targeting the secondary information, specifically the setpoints of adjustable generation units. Its generalization performance is then assessed using a previously unseen attack scenario in which the attacker manipulates the primary information instead of the secondary information. In this case, the attacker is assumed to compromise the wind speed measurements associated with the wind farm at Bus 3, thereby altering the estimated wind power generation available to the EMS. The attack is formulated as a sophisticated SICA that adapts its manipulation to evade the existing cybersecurity layers while maximizing its operational impact. To provide a comprehensive evaluation under varying operating conditions, the cyberattack is simulated over 744 operating hours distributed throughout the year.

Figure 3.23a illustrates the performance of the proposed FA-PRNN in detecting the previously unseen SICA targeting the primary information. The results show that the proposed framework successfully detects all attack instances, achieving a true positive rate of 100%. This demonstrates the strong generalization capability of the proposed model, despite being trained exclusively on SICAs targeting the secondary information. The superior generalization arises because the FA-PRNN learns the abnormal deviations of the PSSVs from their normal feasible operating regions rather than memorizing specific operating points or attack patterns. Consequently, the proposed framework captures the underlying cyber–physical behavior of SICAs, enabling accurate detection of previously unseen attack scenarios.

The robustness of the proposed framework under normal operating disturbances was further evaluated using steady-state open circuit fault and network reconfiguration scenarios. The FA-PRNN was initially trained using data collected under the original network topology. Subsequently, several transmission line outages representing normal system reconfiguration and equipment failures were introduced, including the outage of Line 16 connected to the PV farm, the transmission line between Buses 12 and 15, and the transmission line between Buses 21 and 23. A testing dataset consisting of 744 operating hours was then generated for both normal and cyberattacked operating conditions under the modified network configuration. During the first evaluation, only the original network configuration was used for training, while the reconfigured operating data were reserved exclusively for testing.

Figure 3.23b presents the performance of the proposed FA-PRNN without prior exposure to the new network configuration. The model achieved an average detection accuracy of 87.4%, with most misclassifications occurring during normal operating conditions. This performance degradation is primarily attributed to the shift in the operating locations of the PSSVs relative to their previously learned FA boundaries following network reconfiguration. To improve adaptability, a limited amount of operating data from the new network configuration was incorporated into the training process. As illustrated in Figure 3.23c, the detection accuracy increased to approximately 93%, demonstrating that the proposed FA-based features facilitate efficient transfer learning and rapid adaptation to new operating conditions. These results confirm that the proposed framework can effectively accommodate gradual topology changes and normal operating disturbances while preserving its ability to accurately distinguish legitimate system events from stealthy cyberattacks.



(a) (b) (c)

Figure 3.23: Performance of the proposed FA-PRNN under a) unseen type of SICA over the primary information, b) system reconfiguration with no previous knowledge, c) system reconfiguration with 1% retrain on new system configuration.

3.6 Summary and Conclusion

This chapter investigated the cybersecurity of standalone SPSs and addressed one of the primary research gaps identified in this thesis: the inability of existing cybersecurity mechanisms to reliably detect sophisticated stealthy cyberattacks after they successfully bypass conventional protection layers. A comprehensive cyber–physical testbed was first developed, integrating detailed models of the physical SPS, communication channels, SE, EMS, RESs,ESSs, and multi-layered cybersecurity mechanisms. This realistic environment enabled the implementation and evaluation of advanced cyberattacks under practical operating conditions.

Within this framework, a new class of cyberattacks, referred to as SICAs, was introduced using the proposed *Attack–Wait–and–Observe* strategy. Unlike conventional stealthy FDIAs, the proposed attack iteratively adapts its manipulation based on the system response, enabling it to bypass both conventional BDD and advanced adaptive detection mechanisms. The results demonstrated that although adaptive Chi-square thresholding improves the detection of stealthy FDIAs to approximately 71%, the proposed SICAs reduce this detection rate to nearly 3%, highlighting the fundamental limitations of residual-based cybersecurity approaches that rely solely on measurement consistency.

To overcome these limitations, this chapter proposed a novel FA-based cybersecurity framework that shifts the detection paradigm from measurement-space monitoring to operating-state monitoring. Instead of identifying inconsistencies within the measurement vector, the proposed framework characterizes the expected operating region of the PSSVs using multiple comple-

mentary FA classifiers and detects abnormal deviations introduced by stealthy cyberattacks. Statistical analysis demonstrated that although each classifier exhibits different sensitivity characteristics, all FA classifiers consistently provide stronger indications of compromised operation than healthy operation. Moreover, the proposed FAUR metric showed that the number of PSSVs located outside their expected operating regions increases significantly during cyberattacks, providing an informative feature for cybersecurity applications.

The extracted FA features were subsequently integrated with DNN architectures to improve attack detection. The results demonstrated that incorporating FA information not only increases detection accuracy but also accelerates network convergence and improves training stability by providing physically meaningful cyber-physical features. Among the investigated architectures, the proposed FA-PRNN achieved the best overall performance, reaching an average detection accuracy of approximately 96% while requiring fewer learnable parameters than conventional DNN- and machine-learning-based approaches. This demonstrates that embedding system operating knowledge into the learning process is substantially more effective than relying exclusively on data-driven representations.

Overall, this chapter establishes the proposed FA framework as a robust and adaptive cybersecurity solution for standalone SPSs. More importantly, it demonstrates that monitoring the evolution of the system operating state provides a fundamentally stronger defense against advanced stealthy cyberattacks than conventional measurement-based approaches. These findings form the foundation for the subsequent chapters, where the proposed FA framework is extended to interconnected IESs.

Chapter 4

Feasibility Area Applications in Smart Power and Integrated Energy Systems

Building upon the proposed FA framework, this chapter, together with the associated research published in [250]–[253], extends the application of FA beyond standalone SPSs to IESs, with a particular focus on EMS cybersecurity. The proposed FA-based detection framework is applied to: 1) coupled power–gas systems and 2) coupled power–transportation systems interconnected through HRSs. To address cyber threats unique to IES, cyberattacks are designed to compromise the coupling points and manipulate exchanged information while leaving the SPS measurements unaffected (i.e., the SE measurements remain uncompromised). These attacks target the EMS by exploiting the interdependencies between the coupled infrastructures. Finally, to address the limitation of FA under complete information loss, the proposed detection layer is complemented with a resilient EMS capable of maintaining optimal operation under DDoSs. Together, the proposed framework provides comprehensive protection against stealthy FDIAs, SICA, and DDoS.

4.1 Introduction

The literature survey in Section 2.3 discussed the evolution of SPSs toward tightly coupled IESs. While this integration improves operational flexibility, it also increases system complexity and expands the cyberattack surface. The growing uncertainty in generation and demand, extensive integration of ICT, and the heterogeneous standards across IES infrastructures create

opportunities for low-effort, high-impact cyberattacks that exploit insecure coupling points and propagate across interconnected systems [9], [10].

To address these challenges, previous research has focused on securing smart power and IESs, particularly coupled power–gas and power–transportation systems. As discussed in Section 1.2, most studies on power–gas systems concentrate on integrated SE [204], [205] or FDIA detection [27]–[29]. Similarly, research on power–transportation systems has mainly focused on transportation electrification, including trains, buses, and EVs, and their cybersecurity in VtG and GtV applications [30]–[32]. Despite these efforts, several research gaps remain. Existing power–gas studies primarily target FDIA on SPS measurements, with limited attention to gas system information, EMS information, and the coupling points of PtG and GtP. Likewise, cybersecurity and resilient EMS design for HRSs in power–transportation systems remain largely unexplored. Furthermore, most existing works consider only basic or stealthy FDIAs, overlooking coordinated multi-level cyberattacks that simultaneously exploit multiple attack opportunities and accounting for both attacker and EMS operator perspectives.

Therefore, this chapter investigates the application of the FA framework to the cybersecurity of integrated power–gas and power–transportation systems, with a focus on EMS operations. Unlike previous studies, it considers both stealthy FDIA and SICA beyond SPS measurements, targeting gas and transportation primary information I_t^P as well as coupling infrastructure setpoints, including PtG and GtP for power–gas systems, and PtH and HtP for power–transportation systems, captured in the secondary information I_t^S. The proposed stealthy FDIA and SICA models are implemented using the frameworks in Section 3.2.2 and Section 3.3.3. In addition, a two-level DDoS model is introduced to generate coordinated DoS attacks strategies by accounting for both attacker objectives (impact and cost) and operator response. The FA detection framework is then integrated and evaluated against stealthy FDIAs and SICAs to assess its effectiveness in identifying cyber threats originating from IESs toward SPSs. To further address scenarios with information loss, where FA performance depends on available data, a cyber-resilient EMS for HRSs is developed to reconstruct missing information. This includes a convex HRS EMS formulation that accounts for forecasting uncertainty and ensures optimal operation under diverse operating conditions.

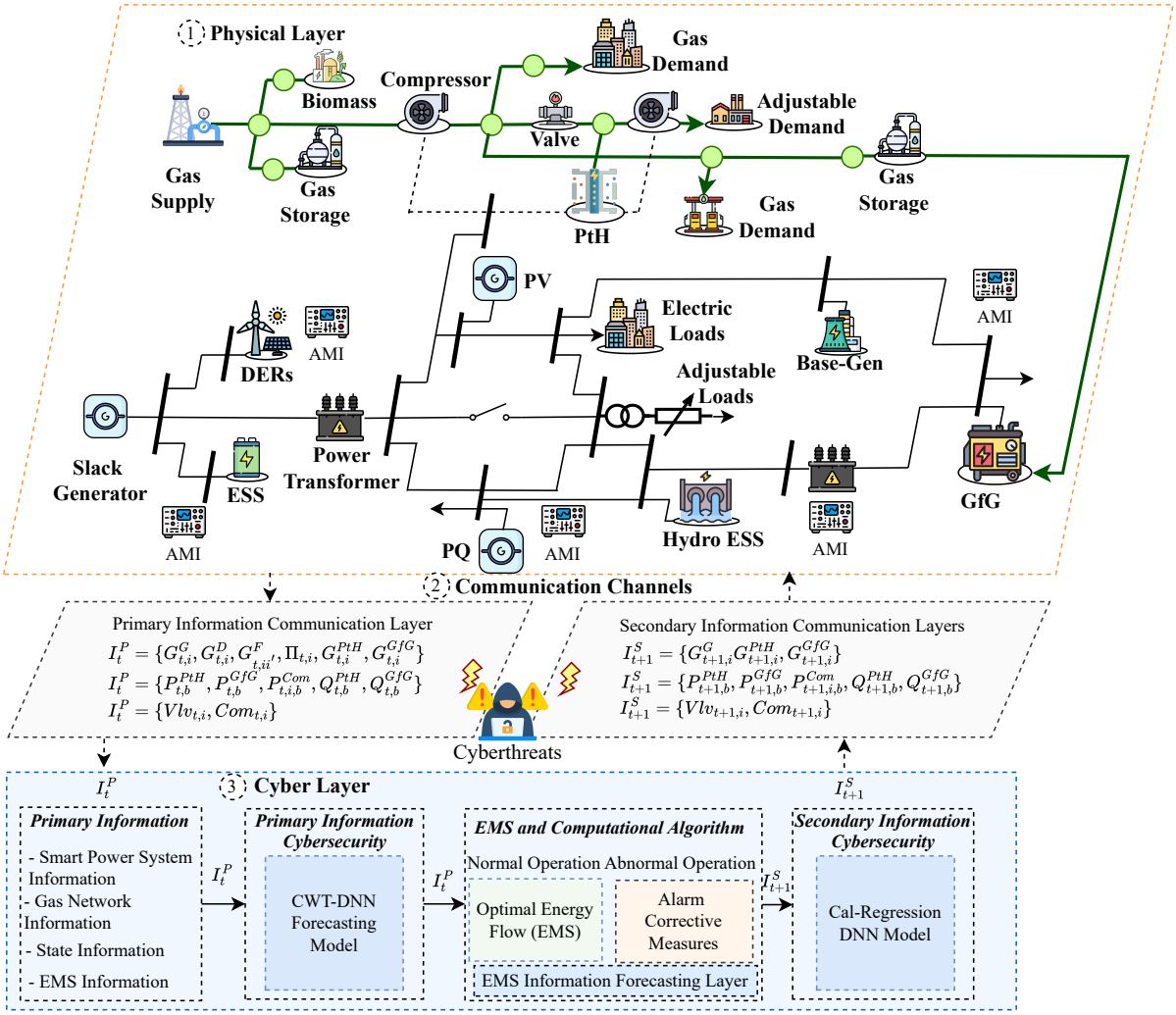


Figure 4.1: Testbed and simulation environment of the power and gas IESs.

4.2 Power and Gas Integrated Energy System Problem Formulation and Preliminaries

4.2.1 Testbed of Power and Gas Integrated Energy System

Figure 4.1 illustrates the simulation testbed of the power-gas IES, highlighting the interactions between the power and gas networks. In addition to the SPS components introduced in Section 3.2.1, the physical layer includes gas sources, biomass generation, gas ESS, and both flexible and non-flexible gas loads. The two systems are coupled through PtH, GfG, and electrically driven gas compressors that regulate gas pressure and flow. These components are

coordinated by the EMS to ensure optimal energy flow while satisfying both system power and gas demands. The gas system primary information at time t consists of measurements of gas generation, demand, flow, nodal pressure, and the operating status of valves and compressors. These measurements are transmitted to the cyber layer through the communication network for monitoring and control.

The received primary information is first verified using forecasting based detection layer using Continuous Wavelet Transform (CWT)-DNN framework. *Since the attacks target information beyond the SPS SE and only focuses on EMS applications*, neither the BDD nor the adaptive threshold detection layers are considered, as the measurement vector z_t remains uncompromised. Once verified, the primary information is processed by the EMS to determine the optimal energy dispatch and generate the secondary information (control setpoints) for time $t+1$. In addition to the SPS control signals, the gas system secondary information includes the setpoints of gas generators, PtH, GfG, gas compressors, and valve switching states. The setpoints are then verified using a combined classification and regression (Cal+Regression)-DNN to detect abnormal settings. The FA framework then monitors the resulting SPS operating state through the PSSVs to detect SICAs, identifying abnormal IES operation through its impact on the SPS.

4.2.1.1 Energy Management System of Power and Gas Integrated Energy System Module

The power-gas IES EMS receives the primary information vector I_t^P from both the power and gas systems through the communication network. The gas system primary information I_t^P is defined using (4.1).

$$I_t^P = \{G_{t,i}^G, G_{t,i}^D, G_{t,ii'}^F, \Pi_{t,i}, G_{t,i}^{PtH}, G_{t,i}^{GfG}, P_{t,b}^{PtH}, P_{t,b}^{GfG}, P_{t,i,b}^{Com}, Q_{t,b}^{PtH}, Q_{t,b}^{GfG}, Com_{t,i}, Vlv_{t,i}\} \tag{4.1}$$

Here, $G_{t,i}^G$, $G_{t,i}^D$, and $G_{t,ii'}^F$ denote the gas generation, demand, and pipeline flow, respectively, while $\Pi_{t,i}$ is the gas pressure at node i. The variables $G_{t,i}^{PtH}$ and $G_{t,i}^{GfG}$ represent the gas output of the PtH and the gas input to the GfG, respectively. The active and reactive power exchanged by these coupling units are denoted by $P_{t,b}^{PtH}$, $Q_{t,b}^{PtH}$, $P_{t,b}^{GfG}$, and $Q_{t,b}^{GfG}$, while $P_{t,i,b}^{Com}$ is the electrical power consumed by the gas compressor. The gas valve state and gas compressor operation state are donated by $Com_{t,i}$ and $Vlv_{t,i}$, respectively. Cyberattacks targeting the gas system primary information I_t^P aim to mislead the EMS into making incorrect operational decisions, resulting in either increased operating costs or compromised IES stability.

Once the primary information is verified, the power and gas data are processed by the central EMS to optimize the operation of the IES over the rolling prediction horizon. The optimization objective is given by (4.2).

$$\begin{aligned}\text{Minimize: } \Delta t \sum_{t\in M^{Ft}} \Bigg(\sum_{b\in\boldsymbol{\mathcal{B}}} \Big[& OPEX(P^{G}_{t,b}) + OPEX(P^{ch}_{t,b}, P^{dch}_{t,b}) + OPEX(P^{RES}_{t,b}) + \\ & OPEX(P^{Dad}_{t,b}) + OPEX(P^{PtH}_{t,b}) + OPEX(P^{GfG}_{t,b}) \Big] + \\ & \sum_{i\in\boldsymbol{\mathcal{N}}^{G}} \Big[OPEX(G^{G}_{t,i}) + Trade^{G}(G^{GfG}_{t,i}, G^{PtH}_{t,i}) \Big] \Bigg) \end{aligned} \tag{4.2}$$

$$OPEX(P^{PtH}_{t,b}) = c^{e} P^{PtH}_{t,b}, \quad \forall e \in \boldsymbol{\mathcal{EL}} \ \wedge \ b \in \boldsymbol{\mathcal{B}}$$

$$OPEX(P^{GfG}_{t,b}) = c^{q} P^{GfG}_{t,b}, \quad \forall q \in \boldsymbol{\mathcal{GFG}} \ \wedge \ b \in \boldsymbol{\mathcal{B}}$$

$$OPEX(G^{G}_{t,i}) = c^{g} G^{G}_{t,i}, \quad \forall g \in \boldsymbol{\mathcal{G}}^{G} \ \wedge \ i \in \boldsymbol{\mathcal{N}}^{G}$$

$$Trade^{G}(G^{GfG}_{t,i}, G^{PtH}_{t,i}) = c^{G,Buy}_{t} G^{GfG}_{t,i} - c^{G,Sell}_{t} G^{PtH}_{t,i}, \quad \forall i \in \boldsymbol{\mathcal{N}}^{G}$$

In addition to the SPS operating cost, (4.2) includes the operating costs of the PtH and GfG units, the gas supply cost, and gas trading transactions. Here, c^{e}, c^{q}, and c^{g} denote the cost coefficients of the PtH, GfG, and gas supply units, respectively, while $c^{G,Buy}_{t}$ and $c^{G,Sell}_{t}$ represent the gas purchasing and selling prices.

The objective function in (4.2) is optimized subject to the SPS constraints in (3.19)-(3.25). The active and reactive power balance constraints in (3.20) and (3.21) are extended to account for the power exchanged by the coupling units (PtH, GfG, and electric compressors), as follows:

$$\begin{aligned} & P^{G}_{t,b} + P^{RES}_{t,b} + P^{dch}_{t,b} - P^{ch}_{t,b} - P^{D}_{t,b} - P^{Dad}_{t,b} + P^{GfG}_{t,b} - P^{PtH}_{t,b} - P^{Com}_{t,i,b} = \\ & |V_{t,b}| \sum_{b'\in\boldsymbol{\mathcal{B}}} |V_{t,b'}| \big(G_{bb'} \cos(\theta_{t,bb'}) + B_{bb'} \sin(\theta_{t,bb'}) \big), \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \end{aligned} \tag{4.3}$$

$$\begin{aligned} & Q^{G}_{t,b} + Q^{RES}_{t,b} + Q^{dch}_{t,b} - Q^{ch}_{t,b} - Q^{D}_{t,b} - Q^{Dad}_{t,b} + Q^{GfG}_{t,b} - Q^{PtH}_{t,b} = \\ & |V_{t,b}| \sum_{b'\in\boldsymbol{\mathcal{B}}} |V_{t,b'}| \big(G_{bb'} \sin(\theta_{t,bb'}) - B_{bb'} \cos(\theta_{t,bb'}) \big), \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \end{aligned} \tag{4.4}$$

To incorporate the gas network dynamics, the objective in (4.2) is constrained by the gas flow relations in passive and active pipelines, defined in (4.5) and (4.6), respectively:

$$G^{F}_{t,ii'} \cdot \left| G^{F}_{t,ii'} \right| = \mathcal{C}^{2}_{ii'} \left(\Pi^{2}_{t,i} - \Pi^{2}_{t,i'} \right), \quad \forall t \in M^{Ft} \wedge (i,i') \in \mathcal{L}_{p} \tag{4.5}$$

$$G^{F}_{t,ii'} \cdot \left| G^{F}_{t,ii'} \right| \geq \mathcal{C}^{2}_{ii'} \left(\Pi^{2}_{t,i} - \Pi^{2}_{t,i'} \right), \quad \forall t \in M^{Ft} \wedge (i,i') \in \mathcal{L}_{a} \tag{4.6}$$

$$G^{F}_{t,ii'} \geq 0, \quad \forall t \in M^{Ft} \wedge (i,i') \in \mathcal{L}_{a} \tag{4.7}$$

Here, $\mathcal{L}_p$ and $\mathcal{L}_a$ denote the sets of passive and active pipelines, respectively, while $\mathcal{C}^2_{ii'}$ is the hydraulic resistance coefficient. Constraint (4.7) enforces unidirectional flow in active pipelines based on compressor operation. The nodal gas balance is given by (4.8), ensuring conservation of mass at each gas node:

$$G^G_{t,i} - G^D_{t,i} + G^{PtH}_{t,i} - G^{GfG}_{t,i} = \sum_{i' \in \boldsymbol{\mathcal{N}}^G} G^F_{t,ii'}, \quad \forall t \in M^{Ft} \wedge \forall i \in \boldsymbol{\mathcal{N}}^G \tag{4.8}$$

Moreover, the gas system operation is restricted by bounds on supply, demand, and pressure:

$$\underline{G^S_i} \leq G^S_{t,i} \leq \overline{G^S_i}, \quad \forall t \in M^{Ft} \wedge i \in \boldsymbol{\mathcal{N}}^G \tag{4.9}$$

$$\underline{G^D_i} \leq G^D_{t,i} \leq \overline{G^D_i}, \quad \forall t \in M^{Ft} \wedge i \in \boldsymbol{\mathcal{N}}^G \tag{4.10}$$

$$\underline{\Pi_i} \leq \Pi_{t,i} \leq \overline{\Pi_i}, \quad \forall t \in M^{Ft} \wedge i \in \boldsymbol{\mathcal{N}}^G \tag{4.11}$$

The coupling between the power and gas systems through the PtH and GfG units is modeled via their overall energy conversion efficiencies, defined as the product of component efficiency and gas energy content ($\mathrm{MWh/m^3}$), which expressed as follow:

$$P^{PtH}_{t,b} = \lambda^{PtH} G^{PtH}_{t,i}, \quad \forall \text{ pair}\{i,b\} \in \{\boldsymbol{\mathcal{N}}^G, \boldsymbol{\mathcal{B}}\} \tag{4.12}$$

$$P^{GfG}_{t,b} = \lambda^{GfG} G^{GfG}_{t,i}, \quad \forall \text{ pair}\{i,b\} \in \{\boldsymbol{\mathcal{N}}^G, \boldsymbol{\mathcal{B}}\} \tag{4.13}$$

where λ^{PtH} and λ^{GfG} denote the overall energy conversion efficiencies of the PtH and GfG units, respectively. The electrical consumption of the gas compressor installed on active pipelines $\mathcal{L}_a$ is given by (4.14) [254]:

$$P^{Com}_{t,i,b} = \mathtt{k}^{\mathrm{GC}} \mathtt{Z}_a G^F_{\mathrm{Com},l} \left[\frac{T_{t,i}}{E_c \eta^c}\right] \left[\frac{c_k}{c_k - 1}\right] \left[\left(\frac{\Pi^{\mathrm{out}}_{t,i}}{\Pi^{\mathrm{in}}_{t,i}}\right)^{\frac{c_k-1}{c_k}} - 1\right], \tag{4.14}$$
$$\forall\, t \in M^{Ft} \wedge \text{pair}\{i,b\} \in \{\boldsymbol{\mathcal{N}}^G, \boldsymbol{\mathcal{B}}\}$$

Here, $G^F_{\mathrm{Com},l}$ is the gas flow through the compressor, Π^{in}_i and Π^{out}_i are the suction and discharge pressures, and T_i is the suction temperature in °R. The parameters $\mathtt{k}^{\mathrm{GC}}$, $\mathtt{Z}_a$, η^c, E_c, and c_k represent the unit conversion factor, compressibility factor, compressor efficiency, parasitic efficiency, and gas heat capacity ratio, respectively.

Finally, all coupling components are constrained by their operating limits:

$$\underline{P^{PtH}_b} \leq P^{PtH}_{t,b} \leq \overline{P^{PtH}_b}, \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \tag{4.15}$$

$$\underline{P^{GfG}_b} \leq P^{GfG}_{t,b} \leq \overline{P^{GfG}_b}, \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \tag{4.16}$$

$$\underline{P^{Com}_b} \leq P^{Com}_{t,b} \leq \overline{P^{Com}_b}, \quad \forall t \in M^{Ft} \wedge b \in \boldsymbol{\mathcal{B}} \tag{4.17}$$

The output of the power and gas IES EMS constitutes the secondary information, representing the optimal energy flow setpoints for both systems at the next time step $t+1$. For the gas network, this includes gas generation, gas exchange with PtH and GfG units, their corresponding power setpoints, compressor electrical consumption, and valve switching states. The secondary information vector is defined by (4.18).

$$I_t^S = \{G_{t,i}^G, G_{t,i}^{PtH}, G_{t,i}^{GfG}, P_{t,b}^{PtH}, P_{t,b}^{GfG}, P_{t,b}^{Com}, Q_{t,b}^{PtH}, Q_{t,b}^{GfG}, Vlv_{t,i}, Com_{t,i}\}. \tag{4.18}$$

Cyberattacks targeting I_t^S directly manipulate the IES operation by altering physical-layer setpoints, particularly those of the PtH and GfG units, affecting both power and gas flows simultaneously. If the secondary information security layer is bypassed, such attacks can cause immediate and direct operational disruptions in the integrated system.

4.2.1.2 Primary and Secondary Information Cybersecurity Module

To detect cyberattacks targeting the primary and secondary information of the IES EMS, a classification and forecasting-based cybersecurity framework is adopted from [24]. For primary information protection, a CWT-CNN detection layer is employed. First, the historical primary information over the window M^{His} is transformed into a three-channel 2-D image using the CWT, capturing the temporal-frequency characteristics of the signals and amplifying subtle variations introduced by FDIAs. The generated image is then classified using a trained CNN. The detection process is given by (4.19).

$$\text{Alarm}_t = CNN(I_t^{2D}), \quad \text{where} \quad I_t^{2D} = CWT\left([I_{t'}^P :\ t' \in M^{His}]\right). \tag{4.19}$$

Here, $CNN(\cdot)$ is the trained CNN classifier, while $CWT(\cdot)$ denotes the continuous wavelet transform applied to the historical primary information.

For secondary information protection, a classification-regression framework is adopted to secure the setpoints of the PtH, GfG, and compressor units using historical data over the window M^{His}. First, a DNN classifier identifies the operating region as: 1) zero-power, 2) maximum-power, or 3) derating. The predicted operating region, together with the historical setpoints, is then used by an LSTM regression model to estimate the expected setpoints. An alarm is triggered when the forecasting error exceeds the allowable threshold or the received setpoint

violates its operating limits as shown by (4.20).

$$\begin{aligned}
&\Delta I^S_{t,b} > \tau^{Fr}_{t,b} \text{ or } I^S_{t,b} > \overline{I^S_b} \text{ or } I^S_{t,b} < \underline{I^S_b} \\
&\text{where } \Delta I^S_{t,b} = I^S_{t,b} - f^{LSTM}\left([P^{PtH}_{t',b}, P^{GfG}_{t',b}, P^{Com}_{t',b}, I^S_{t',b} :\ t' \in M^{His}]\right), \\
&\text{and } \{P^{PtH}_{t',b}, P^{GfG}_{t',b}, P^{Com}_{t',b}\} = f^{DNN}\left([I^S_{t',b} :\ t' \in M^{His}]\right),
\end{aligned} \tag{4.20}$$

where $f^{DNN}(\cdot)$ classifies the operating region and $f^{LSTM}(\cdot)$ predicts the expected secondary information setpoints.

4.2.2 Development of Stealthy Infiltrated Cyber Attacks On Power and Gas Integrated Energy Systems

The proposed SICAs for the power-gas IES target the secondary information of the coupling units, namely the PtH, GfG, and electric compressors. The manipulated secondary information is defined as:

$$I'^S_t = \begin{cases}
P'^{PtH}_{t,b} = P^{PtH}_{t,b} + a^{PtH}_{t,b}, \text{ Such that: } G'^{PtH}_{t,i} = G^{PtH}_{t,i} + \frac{a^{PtH}_{t,b}}{\lambda^{PtH}} \\
P'^{GfG}_{t,b} = P^{GfG}_{t,b} + a^{GfG}_{t,b}, \text{ Such that: } G'^{GfG}_{t,i} = G^{GfG}_{t,i} + \frac{a^{GfG}_{t,b}}{\lambda^{GfG}} \\
P'^{Com}_{t,i,b} = P^{Com}_{t,i,b} + a^{Com}_{t,i,b}
\end{cases} \tag{4.21}$$

Here, $a^{PtH}_{t,b}$, $a^{GfG}_{t,b}$, and $a^{Com}_{t,b}$ are the attack vectors targeting the PtH, GfG, and compressor setpoints, respectively. To preserve physical consistency, the manipulated power and gas setpoints are constrained through the corresponding energy conversion relationships.

For the power–gas IES, the objective of the SICA is to design the attack vector in (4.21) such that it: 1) maximizes the EMS operating cost, 2) bypasses the secondary-information cybersecurity layer by maintaining a small deviation from the actual system state, and 3) ensure physical modeling consistence. These objectives are formulated in (4.22).

$$\begin{aligned}
&\text{Maximize:} \quad Obj(4.2)\big|_{I'^S_t} \quad \text{Subject to:} \quad (3.19) - (3.25) \ \wedge \ (4.3) - (4.17) \\
&\qquad |V_{t,b} - \hat{V}_{t,b}| \le \tau_V, \quad \forall t \in M^{Ft} \ \wedge \ b \in \boldsymbol{\mathcal{B}} \ \wedge \ i \in \boldsymbol{\mathcal{N}}^G.
\end{aligned} \tag{4.22}$$

The optimization maximizes the IES operating cost using the manipulated setpoints while preserving the physical constraints of the integrated power and gas systems and limiting the resulting state deviation. The threshold τ_V is determined iteratively using the proposed *Attack–Wait–and–Observe* strategy in Algorithm 2.

Algorithm 4 Flag Vector Calculation Pseudo Code

Require: Samples: $\mathcal{S}^{FA} \in M^{FA}$, Current PSSVs: $\mathbb{X}_t$.

Ensure: Overall Flag $Fg_t = Fg_{\phi_t}, \forall \phi \in \Phi$.

1: **for** $\phi \in \Phi$ **do**
2: **for** $x_{t,n} \in \mathbb{X}_t$ **do**
3: Upload the healthy window $\{x_{t-1,n} : x_{t-M^{FA},n}\}$ into the complex plane.
4: Estimate the classifier ϕ_t parameters, Minimize Area(ϕ_t), Subject to: $L_{\mathcal{S}^{FA}}(\phi_t) = 0$.
5: Calculate the classifier flag $Fg_{\phi(t,n)} = 1[x_{t,n} \notin \phi_t]$.
6: **end for**
7: **Save**: Store Fg_{ϕ_t}.
8: **end for**

4.2.3 Application of Feasibility Areas On Power and Gas Integrated Energy Systems

To evaluate the applicability of the proposed FA framework beyond standalone SPSs, it is adopted to detect SICAs targeting the power and gas IES. Similar to Section 3.4, the FA classifiers characterize the normal operating region of the SPS by constructing adaptive FA from historical PSSVs within the window M^{FA}. Although the cyberattacks target the gas network and coupling units rather than the SPS measurements, the resulting operational changes propagate through the IES and introduce abnormal deviations in the SPS state, which are reflected in the PSSVs. Consequently, the proposed FA framework detects these indirect impacts by monitoring deviations from the learned feasible operation region. For each classifier $\phi \in \Phi$, an overall flag vector Fg_t is generated to describe the status of all PSSVs relative to their corresponding FA classifiers. Algorithm 4 summarizes the overall flag calculation procedure. Finally, the flag vector is supplied to the trained FA-PRNN, which exploits both the spatial information provided by the FA layer and the temporal evolution of the system to accurately detect SICAs in the power and gas IES.

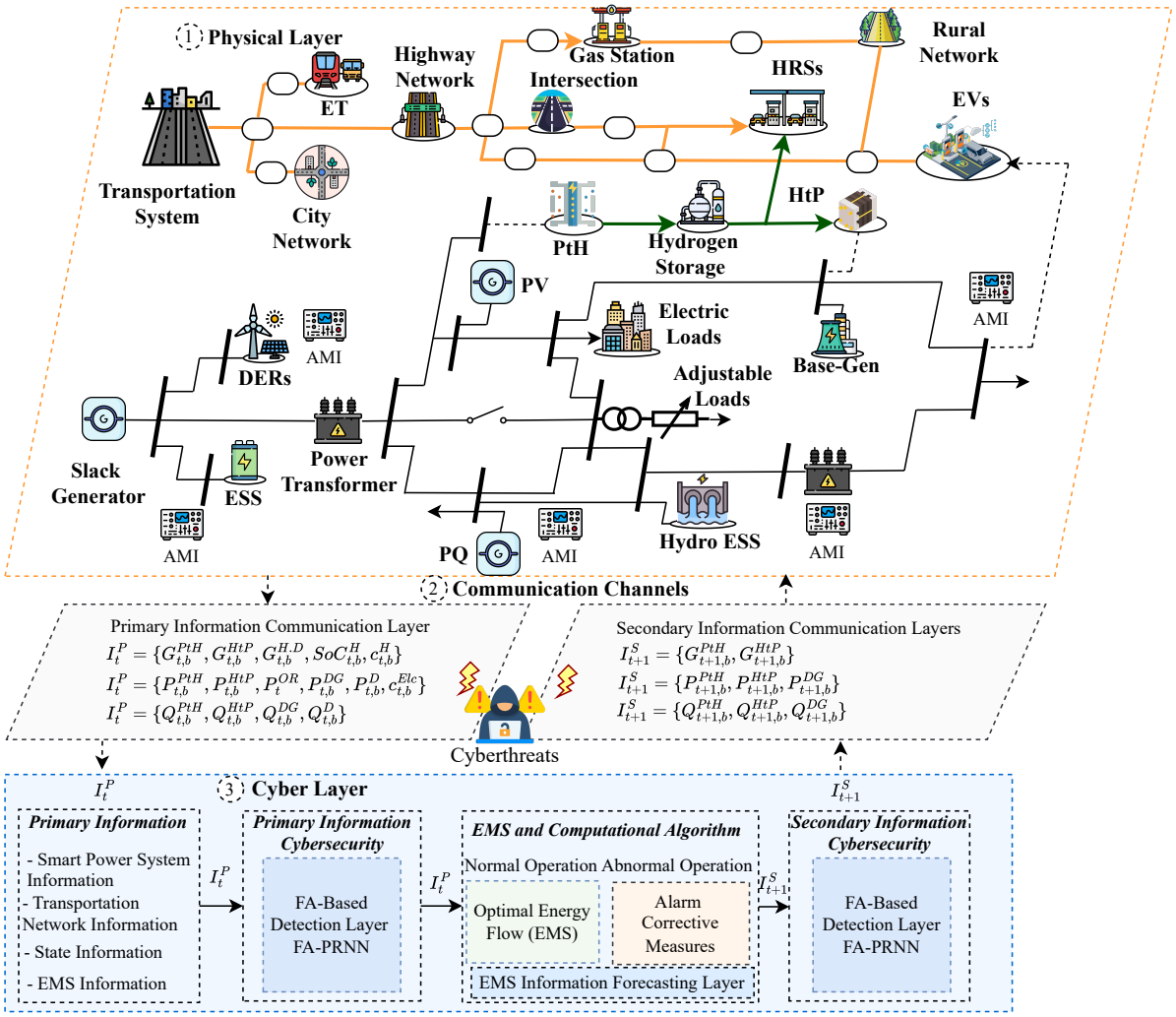


Figure 4.2: Testbed and simulation environment of the power and transportation IESs.

4.3 Power and Transportation Integrated Energy System Problem Formulation and Preliminaries

4.3.1 Testbed of Power and Transportation Integrated Energy System

Figure 4.2 illustrates the simulation testbed of the power and transportation IES, where the two systems are coupled through multiple HRSs. Unlike power and gas IESs, which can be integrated at both transmission and distribution levels, power and transportation integration is primarily realized at the distribution level. In this setup, following similar approach in [255], multiple HRSs is operated by a private entity and incorporates PtH, HtP, and hydrogen ESS,

enabling bi-directional energy exchange with the distribution network while supplying hydrogen-powered vehicles.

The HRS EMS aims to maximize operational profit through electricity price arbitrage, hydrogen trading, and participation in OR services. At each time step t, it receives primary information from the power system, including active and reactive power demand, real-time electricity prices, and OR signals, together with transportation information such as hydrogen demand forecasts, hydrogen storage SoC, and hydrogen market prices. Based on this information, the EMS determines the optimal dispatch of the PtH and HtP units, secondary information, while satisfying hydrogen demand, reserve commitments, hydrogen storage limits, and distribution network operating constraints.

Similar to the previous case study, the proposed FA-PRNN serves as the main cybersecurity layer for both primary and secondary information, in which is used as prevention (pre-occurrence) layer to detect stealthy FDIAs targeting the HRS operation. In this case, PSSV are used directly as the EMS optimal state vector. Although these attacks originate from the transportation subsystem and coupling units, their impact propagates to the power system, causing abnormal variations in the estimated PSSVs. These deviations are captured by the proposed FA framework, enabling early detection before the compromised information affects the physical operation of the IES.

4.3.1.1 Energy Management System of Power and Transportation Integrated Energy System Module

The power and transportation IES EMS receives the primary information vector I_t^P from both the power and transportation systems through the communication network, which is defined by (4.23).

$$\begin{aligned} I_t^P = \{&G_{t,b}^{PtH}, G_{t,b}^{HtP}, G_{t,b}^{H.D}, SoC_{t,b}^{H}, c_t^H, P_{t,b}^{PtH}, P_{t,b}^{HtP}, \\ &Q_{t,b}^{PtH}, Q_{t,b}^{HtP}, P_{t,b}^{OR}, P_{t,b}^{DG}, Q_{t,b}^{DG}, P_{t,b}^{D}, Q_{t,b}^{D}, c_t^{Elc}\}. \end{aligned} \tag{4.23}$$

Here, $G_{t,b}^{HtP}$ and $G_{t,b}^{H.D}$ denote the hydrogen consumption of the HtP unit and the hydrogen demand of the HRS, respectively, while $SoC_{t,b}^{H}$ is the hydrogen tank SoC and c_t^H is the real-time hydrogen price. Similarly, $P_{t,b}^{HtP}$, and $Q_{t,b}^{HtP}$ represent the active and reactive power of the HtP units, respectively. Moreover, $P_{t,b}^{DG}$ and $Q_{t,b}^{DG}$ denote the active and reactive power outputs of the DG, $P_{t,b}^{OR}$ is the requested OR power capacity, and c_t^{Elc} is the real-time electricity price.

Stealthy FDIAs targeting the transportation primary information I_t^P aim to mislead the EMS into determining suboptimal operating schedules, thereby increasing operating costs, reducing market revenues, or compromising the stability of the IES.

Once the primary information has been verified, the power and transportation information are processed by the central HRS EMS to optimize the operation of the IES over the rolling prediction horizon. The optimization objective is defined by (4.24).

$$\text{Maximize: } \sum_{t\in M^{Ft}}\Bigg(\sum_{h\in\boldsymbol{\mathcal{H}}}\big(P_{t,h}^{HtP}-P_{t,h}^{PtH}\big)c_t^{Ele}+\sum_{h\in\boldsymbol{\mathcal{H}}}\big(G_{t,h}^{H,D}-G_{t,h}^{HtP}\big)c_t^{H} + c^{OR}P_t^{OR}-\beta^{OR}\left(P_t^{OR,PtH}+P_t^{OR,HtP}\right)\Bigg)\Delta t. \tag{4.24}$$

Here, c^{OR} and β^{OR} denote the payment and penalty charges associated with OR participation, respectively. Moreover, $P_t^{OR,PtH}$ and $P_t^{OR,HtP}$ represent the reserve tracking deviations under positive and negative OR signals, respectively, where the PtH unit operates as a controllable load and the HtP unit operates as dispatchable generation. The objective in (4.24) maximizes the total operational profit of the HRSs. The first term represents electricity arbitrage through the PtH and HtP units, the second captures the net revenue from hydrogen trading, and the third accounts for OR incentives while penalizing deviations from the requested reserve capacity.

The objective function in (4.24) is subject to the distribution SPS power flow, voltage regulation constraints, and power balance defined in (4.25)–(4.28).

$$P_{t,bb'}\le\overline{P_{bb'}},\quad \underline{V_b}\le V_{t,b}\le\overline{V_b},\quad \forall t\in M^{Ft}\wedge b,b'\in\boldsymbol{\mathcal{B}} \tag{4.25}$$

$$P_{t,b}^{DG}+P_{t,b}^{HtP}-P_{t,b}^{PtH}-P_{t,b}^{D}= \tag{4.26}$$

$$|V_{t,b}|\sum_{b'\in\boldsymbol{\mathcal{B}}}|V_{t,b'}|\big(G_{bb'}\cos(\theta_{t,bb'})+B_{bb'}\sin(\theta_{t,bb'})\big),\ \forall t\in M^{Ft}\wedge b\in\boldsymbol{\mathcal{B}} \tag{4.27}$$

$$Q_{t,b}^{DG}+Q_{t,b}^{HtP}-Q_{t,b}^{PtH}-Q_{t,b}^{D}= \tag{4.28}$$

$$|V_{t,b}|\sum_{b'\in\boldsymbol{\mathcal{B}}}|V_{t,b'}|\big(G_{bb'}\sin(\theta_{t,bb'})-B_{bb'}\cos(\theta_{t,bb'})\big),\ \forall t\in M^{Ft}\wedge b\in\boldsymbol{\mathcal{B}} \tag{4.29}$$

The hydrogen-to-power conversion for PtH and HtP units is defined in (4.30)–(4.31).

$$P_{t,h}^{PtH}=\lambda^{PtH}G_{t,h}^{PtH},\quad \forall t\in M^{Ft}\wedge h\in\boldsymbol{\mathcal{H}} \tag{4.30}$$

$$P_{t,h}^{HtP}=\lambda^{HtP}G_{t,h}^{HtP},\quad \forall t\in M^{Ft}\wedge h\in\boldsymbol{\mathcal{H}} \tag{4.31}$$

where λ^{PtH} and λ^{HtP} denote the hydrogen-to-power conversion factors, given by $(1/360)\,\mathrm{MWh}/m^3$ scaled by the corresponding efficiencies η^{PtH} and η^{HtP}. Additionally, the operating limits of

the PtH and HtP units are enforced by (4.32)–(4.33).

$$\underline{P_h^{PtH}} \leq P_{t,h}^{PtH} \leq \overline{P_h^{PtH}}, \quad \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}} \tag{4.32}$$

$$\underline{P_h^{HtP}} \leq P_{t,h}^{HtP} \leq \overline{P_h^{HtP}}, \quad \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}} \tag{4.33}$$

The objective function is further constrained by the hydrogen storage tank energy balance at each HRS, as defined in (4.34).

$$SOC_{t,h}^{H} - SOC_{t-1,h}^{H} + \left(G_{t,h}^{H,D} + G_{t,h}^{HtP} - G_{t,h}^{PtH} + \lambda^{Dsp} SOC_{t,h}^{H}\right)\Delta t = 0, \ \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}} \tag{4.34}$$

Here, λ^{Dsp} denotes the hydrogen storage dissipation factor. The SoC is constrained within its physical limits as given in (4.35).

$$\underline{SOC_h^H} \leq SOC_{t,h}^{H} \leq \overline{SOC_h^H}, \quad \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}} \tag{4.35}$$

To ensure sufficient reserves for OR provision, the aggregated storage across all HRSs is bounded as in (4.36).

$$|\mathcal{H}|\underline{SOC_h^H}\alpha_{LB}^{OR} \leq \sum_{h \in \boldsymbol{\mathcal{H}}} SOC_{t,h}^{H} \leq |\mathcal{H}|\overline{SOC_h^H}(1 - \alpha_{UB}^{OR}), \quad \forall t \in M^{Ft} \wedge S_t^{OR} = 0 \tag{4.36}$$

Here, $\alpha_{LB}^{OR} > 1$ ensures sufficient hydrogen availability for future negative OR events requiring HtP operation, while $\alpha_{UB}^{OR} < 1$ preserves headroom for positive OR events requiring PtH operation. The binary variable S_t^{OR} indicates whether an OR signal is active.

Finally, the aggregated power response of all PtH and HtP units must track the issued OR signal as specified in (4.37):

$$\begin{aligned} &\sum_{h \in \boldsymbol{\mathcal{H}}} (P_{t,h}^{PtH} - P_{t,h}^{HtP}) = P_t^{OR} + P_t^{OR,HtP} - P_t^{OR,PtH}, \\ &\quad P_t^{OR,PtH}, \ P_t^{OR,HtP} \geq 0, \quad \forall t \in M^{Ft} \wedge S_t^{OR} = 1 \end{aligned} \tag{4.37}$$

where $P_t^{OR,PtH}$ and $P_t^{OR,HtP}$ represent the deviations from the requested OR signal for PtH and HtP aggregations, respectively. These deviations are penalized in (4.24) to enforce compliance with ancillary service requirements.

The output of the power and transportation IES EMS constitutes the secondary information, representing the optimal scheduling of HRSs and the distribution SPS at the next time step $t+1$. This secondary information includes the dispatch setpoints of DGs, PtH, and HtP units, along with their corresponding hydrogen production and consumption levels, as defined in (4.38).

$$I_t^S = \{G_{t,h}^{PtH}, G_{t,h}^{HtP}, P_{t,b}^{PtH}, P_{t,b}^{HtP}, Q_{t,b}^{PtH}, Q_{t,b}^{HtP}, P_{t,b}^{DG}, Q_{t,b}^{DG}\}. \tag{4.38}$$

Cyberattacks targeting I_t^S directly manipulate the operation of the IES by altering physical-layer setpoints, particularly those of the DGs, PtH, and HtP units, thereby affecting both the power system and HRSs simultaneously. If the secondary information security layer is bypassed, such attacks can lead to immediate operational disruptions in the integrated energy system.

4.3.1.2 Primary and Secondary Information Cybersecurity Module

To protect the HRSs EMS against stealthy FDIAs, the proposed FA framework is adopted as a pre-occurrence detection layer to prevent cyberattacks before they impact the IES operation. Unlike the power and gas IES which uses the PSSVs from the IES state measurements, the proposed FA-PRNN utilizes the estimated distribution SPS PSSVs obtained directly from the EMS output to detect abnormal deviations from the learned feasible operating area. The design and implementation of the proposed detection layer follow the same procedure presented in Section 4.2.3.

4.3.2 Development of Cyberattacks On Power and Transportation Integrated Energy Systems

To evaluate the robustness and adaptability of the proposed FA framework in power and transportation IESs, two classes of cyberattacks are developed and implemented. First, stealthy FDIAs are designed to target the transportation side primary information, including hydrogen demand, hydrogen tank SoC, hydrogen market price, and OR signals, as well as the secondary information of the coupling PtH and HtP units. The attacks are implemented in both single-point and coordinated forms to manipulate the EMS. Second, coordinated DDoS attacks are developed to target the same communication channels. Unlike FDIAs, these attacks aim to completely interrupt the transmission of critical information, forcing the EMS to operate using outdated or unavailable data. Both single DoS attacks and coordinated bi-level DDoS attacks are considered. The lower level models the operator's response under partial or complete information loss, while the upper level represents the attacker's objective of maximizing operational disruption while minimizing the attack cost. This coordinated attack framework enables the evaluation of both the prevention capability of the proposed FA-based detection layer against stealthy FDIA and the resilience of the developed EMS under severe communication failures.

4.3.2.1 Proposed False Data Injection Attack on Power and Transportation Integrated Energy System Module

Stealthy FDIAs target the primary information by injecting an attack vector a_t with the objective of causing economic losses or compromising system operation while remaining undetected. In this work, both single-point and coordinated cyberattacks on HRS information are developed, with the primary objective of reducing the operational revenue while maintaining stealthy manipulation limits. The cyberattack model targeting the hydrogen tank SoC is defined by (4.39).

$$a_{t,h}^{SoC} = \begin{cases} SoC_{t-1,h} \times \tau^{SoC}, & \text{if } c_t^{Ele} < Mean(c_t^{Ele}) \\ -SoC_{t-1,h} \times \tau^{SoC}, & \text{if } c_t^{Ele} \geq Mean(c_t^{Ele}) \end{cases}, \quad \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}} \tag{4.39}$$

Here, $a_{t,h}^{SoC}$ denotes the attack vector applied to the hydrogen tank SoC, while τ^{SoC} represents the maximum allowable manipulation ratio selected by the attacker to preserve stealthiness. The attack strategy exploits the electricity price profile to mislead the EMS scheduling decisions. When the real-time electricity price c_t^{Ele} is below its average value, the attacker artificially increases the reported SoC, encouraging the EMS to increase HtP operation instead of storing low-cost electricity as hydrogen. Conversely, when the electricity price is above its average value, the reported SoC is reduced, forcing the EMS to operate the PtH units during high-price periods.

Similarly, stealthy FDIAs targeting the hydrogen demand are modeled by (4.40).

$$a_{t,h}^{G^{H.D}} = \begin{cases} -G_{t,h}^{H.D} \times \tau^{G^{H.D}}, & \text{if } c_t^{Ele} < Mean(c_t^{Ele}) \\ +G_{t,h}^{H.D} \times \tau^{G^{H.D}}, & \text{if } c_t^{Ele} \geq Mean(c_t^{Ele}) \end{cases}, \quad \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}} \tag{4.40}$$

Here, $\tau^{G^{H.D}}$ denotes the maximum allowable attack ratio selected by the attacker to preserve stealthiness. The attack manipulates the reported hydrogen demand according to the electricity price to mislead the EMS scheduling decisions. Specifically, the reported demand is increased during high electricity price periods and decreased during low-price periods, forcing suboptimal operation of the PtH and HtP units. Consequently, the attack reduces the profitability of electricity price arbitrage while maintaining stealthy manipulation limits.

Another critical component of the primary information is the OR signal issued by the distribution SPS operator, which directly governs the operation of all PtH and HtP units through

the equality constraints in (4.37). The corresponding attack model is defined in (4.41).

$$a_t^{P^{OR}} = \begin{cases} Min(P_t^{OR}) \times \tau^{P^{OR}}, & \text{if } c_t^{Ele} < Mean(c_t^{Ele}) \\ Max(P_t^{OR}) \times \tau^{P^{OR}}, & \text{if } c_t^{Ele} \geq Mean(c_t^{Ele}) \\ 0, & \text{if } S_t^{OR} = 1 \end{cases}, \quad \forall t \in M^{Ft} \tag{4.41}$$

Here, $\tau^{P^{OR}}$ represents the maximum allowable manipulation ratio used to preserve stealthiness. The attack injects false OR signals to distort the scheduling decisions of the EMS. It generates negative OR signals during low electricity price periods to encourage HtP operation, and positive OR signals during high-price periods to enforce PtH operation, thereby reducing system revenue. No modification is applied when actual OR signals are issued ($S_t^{OR} = 1$) to prevent easy detection of the manipulated signal.

Using the same concept, cyberattacks targeting the secondary information of the coupling PtH and HtP setpoints are modeled by (4.42).

$$a_{t,h}^{P^{HtP}}, a_{t,h}^{P^{HtP}} = \begin{cases} P_{t,h}^{HtP} \times \tau^{HtP}, & \text{if } c_t^{Ele} < Mean(c_t^{Ele}) \\ P_{t,h}^{PtH} \times \tau^{PtH}, & \text{if } c_t^{Ele} \geq Mean(c_t^{Ele}) \\ 0, & \text{if } S_t^{OR} = 1 \end{cases} \tag{4.42}$$

$$\text{Subject to: } \underline{SOC_h} \leq SOC_{t,h}^{'} \leq \overline{SOC_h}, \quad \forall t \in M^{Ft} \wedge h \in \boldsymbol{\mathcal{H}}$$

Here, τ^{HtP} and τ^{PtH} denote the maximum allowable manipulation ratios ensuring stealthiness. The attack modifies the coupling unit setpoints to force suboptimal energy exchange decisions: increasing HtP operation during low-price periods and increasing PtH operation during high-price periods, thereby degrading arbitrage efficiency. To avoid detection, no manipulation is applied when OR signals are active, and all induced variations are constrained to satisfy the hydrogen storage limits, ensuring physically consistent and stealthy operation over time.

Beyond stealthy FDIAs on individual measurements, coordinated stealthy FDIAs are formulated to simultaneously 1) minimize the attack cost and 2) maximize the operational impact. This leads to the following min–max optimization problem:

$$\begin{aligned} &\text{Min: } \sum_{h \in \boldsymbol{\mathcal{H}}} \left(c^{SOC} \| a_{t,h}^{SoC} \|_0 + c^{G^{H.D}} \| a_{t,h}^{G^{H.D}} \|_0 + c^{PtH} \| a_{t,h}^{P^{PtH}} \|_0 + c^{HtP} \| a_{t,h}^{P^{HtP}} \|_0 \right) + c^{P^{OR}} \| a_t^{P^{OR}} \|_0 \\ &\text{Max: } \sum_{h \in \boldsymbol{\mathcal{H}}} \left(e^{\underline{SOC_h} - SOC_{t,h}^{H}} + e^{SOC_{t,h}^{H} - \overline{SOC_h}} + e^{G_{t,h}^{H.D} - SOC_{t,h}^{H}} \right) + e^{P_t^{OR} - \sum_{h \in \boldsymbol{\mathcal{H}}} (P_{t,h}^{PtH} - P_{t,h}^{HtP})} \\ &\forall\ t \in M^{Ft} \end{aligned} \tag{4.43}$$

where, $c^{(.)}$ represents the cost of the attack on each information. The first term represents the total attack cost, defined as the norm-zero, encouraging the attacker to minimize the number of injected perturbations across primary and secondary information. The second term captures the attack impact by penalizing violations of hydrogen storage limits, hydrogen demand satisfaction, and OR signal consistency, thereby steering the system toward economically suboptimal and physically stressed operating conditions. The exponential functions serve a dual role: they provide a smooth convex surrogate that improves numerical tractability of the optimization, while also amplifying constraint violations to prioritize impactful attack directions. When the system operates within nominal bounds, these terms approach negligible values, whereas deviations lead to rapidly increasing penalties, effectively guiding the attacker toward high-impact.A detailed mathematical foundation of the stealthy FDIA design and its impact on the system objective is provided in [252].

4.3.2.2 Proposed Distributed Denial-of-Service Attacks on Power and Transportation Integrated Energy System Module

Unlike FDIAs, which require access to system measurements and a precise manipulation strategy, DoSs are generally easier to implement as they do not require system state knowledge or measurement alteration. From a cybersecurity perspective, DoS attacks aim to disrupt the delivery of critical information by congesting the communication network, resulting in data unavailability at the EMS. Under such conditions, the EMS operates using the most recently received (outdated) measurements [211]. The DoS attack model targeting the primary information vector $I_t^P = \{SoC_{t,h}, G_{t,h}^{H.D}, P_t^{OR} : \forall h \in \boldsymbol{\mathcal{H}}\}$ is defined in (4.44).

$$I_{t,i}^P = \begin{cases} I_{t,i}^P, & \text{if } i \notin a_t^{DoS} \\ I_{t-1,i}^P, & \text{if } i \in a_t^{DoS} \end{cases} \tag{4.44}$$

Here, a_t^{DoS} denotes the set of compromised primary information channels affected by the DoS attack. The percentage revenue loss in the HRSs caused by a single DoS attack on the communicated signal $I_{t,i}^P$ is then calculated using (4.45).

$$\Delta Rev_i = \frac{Obj(4.24) - Obj(4.24)_{|I_{t,i}^P \in a_t^{DoS}}}{Obj(4.24)}, \ \forall t \in M^{Ft} \tag{4.45}$$

To amplify the attack impact, coordinated bi-level DDoSs are executed by multiple attackers simultaneously targeting different communication channels across the system. The attack is

formulated as a bi-level attack, where the lower level represents the HRS operator's decision-making, aiming to maximize system revenue through optimal scheduling, while the upper level represents the attacker's objective of minimizing the operator's revenue while accounting for attack cost and resource constraints. This hierarchical formulation enables the attacker to anticipate the operator's response to degraded or outdated information and exploit it strategically, leading to a more effective and coordinated disruption. The bi-level DDoSs formulation is expressed in (4.46).

$$\begin{aligned}\text{Min: } & \sum_{h\in\boldsymbol{\mathcal{H}}}\left(c^{SOC}a_{t,h}^{DoS,SoC}+c^{G^{H.D}}a_{t,h}^{DoS,G^{H.D}}\right)+c^{P^{OR}}a_{t}^{DoS,P^{OR}}\\ & +\mathcal{W}^{DoS}\cdot\text{Max: }Obj(4.24)\quad\text{Subject to:}(4.25)-(4.37)\end{aligned}\tag{4.46}$$

Here, $\mathcal{W}^{DoS}$ is a weighting parameter that balances attack cost against and HRSs revenue loss. Unlike FDIAs, which focus solely on measurement manipulation, the proposed bi-level DDoSs explicitly incorporate the operator's response to missing or outdated information, enabling a more realistic attacker–operator interaction model that captures both economic impact and execution cost.

The proposed bi-level DDoS attack model is formulated with the perspective of the HRS operator as lower layer, which assumes several practical conditions. First, such attacks are expected to be launched by well-funded and highly organized adversaries, such as nation-state or advanced persistent threat groups, due to the computational resources and system knowledge required. Second, such attack model depends on the publicly available operational information used by the operator or information can be reasonably inferred. For the HRSs considered in this study, information such as electricity prices, hydrogen prices, hydrogen demand and station capacities is publicly accessible. Therefore, the attacker only requires access to a limited set of local operational variables, namely the hydrogen tank SoC and the operating states of the PtH and HtP units. Even when some of this information is unavailable, the proposed bi-level DDoS can still be formulated under uncertainty by modeling the missing information using stochastic estimates, allowing the attacker to determine attack strategies that remain effective despite incomplete system knowledge.

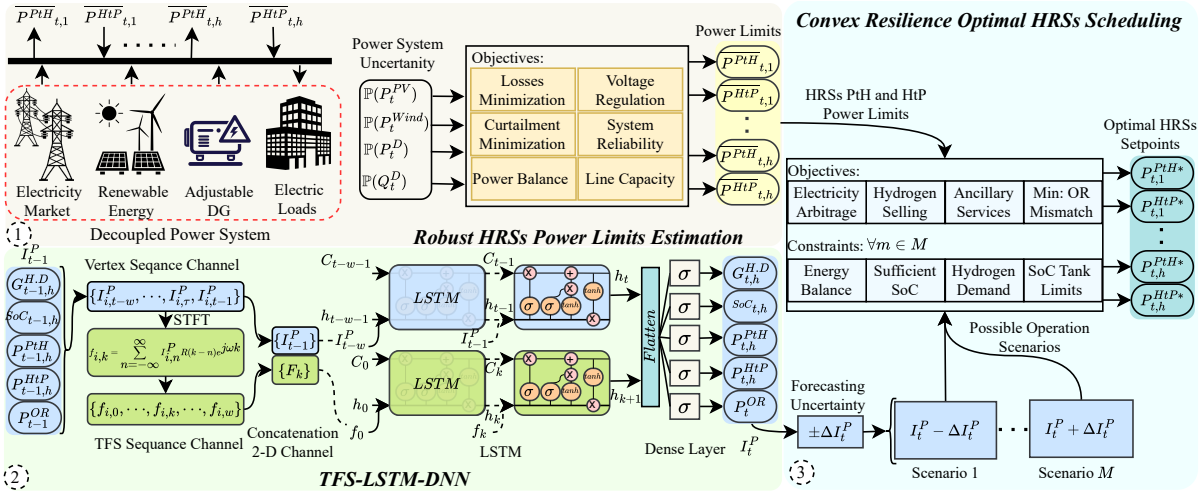


Figure 4.3: Structure of the cyber-resilience EMS against DDoS attacks.

4.3.3 Proposed Cyber Resilience Energy Management System of Power and Transportation IES

One of the main limitations of FA under DDoSs conditions is information unavailability. While the proposed FA framework can effectively detect abnormal variations caused by outdated measurements, its primary role is detection; therefore, recovery from DoSs or coordinated bi-level DDoSs requires additional modifications to the EMS to ensure cyber-resilience.

Figure 4.3 illustrates the proposed cyber-resilient EMS architecture for HRSs, which adopts a two-tier defense strategy. First, a TFS-DNN is used to reconstruct missing or compromised data. The reconstructed signals, together with their associated uncertainty ΔI_t^P, are used to generate a set of possible operating scenarios $\mathbb{M}$. To efficiently handle these scenarios, the coupled power and transportation IES is decomposed into two subproblems, thereby avoiding the non-convexity introduced by distribution network power flow constraints in (4.26) and (4.28).

In the second stage, a robust power limit estimation module determines secure operating bounds for PtH and HtP units while ensuring voltage regulation and feeder capacity constraints. These limits are then integrated into a convex resilience-oriented scheduling framework that maximizes expected revenue across all scenarios in $\mathbb{M}$, while preserving system reliability and operational feasibility under uncertainty and cyber-induced data loss.

4.3.3.1 Time Frequency Spectrum (TFS)-Based Deep Neural Network (DNN)

To reconstruct missing information, a TFS-DNN framework combining STFT with an LSTM-based regression model is employed. Since the original primary information I_t^P in the time domain does not fully capture temporal characteristics, STFT is first applied over a historical window (M^{His}) to extract localized time-frequency features. While the LSTM captures long-term temporal dependencies, the STFT emphasizes short-term dynamics, improving forecasting accuracy and reducing prediction uncertainty [35].

Given the historical sequence $I^P_{t-M^{His}} : I^P_{t-1}$, the STFT of signal I_i^P is computed as follow:

$$f_{i,k} = \sum_{n=-\infty}^{\infty} I^P_{i,n}\, \mathcal{R}(k-n)\, e^{-j\omega k} \tag{4.47}$$

where $\mathcal{R}$ and ω denote the STFT window function and angular frequency, respectively. The resulting magnitude spectrogram $|F_k|$ is concatenated with the historical primary information to form a joint time-frequency representation, shown by (4.48)

$$Z_t = [I^P_{t-1} \;\; |F_k|] \in \mathbb{R}^{w\times 2}, \tag{4.48}$$

which serves as the input to the regression model for reconstructing missing or compromised information. The joint representation Z_t is then provided to a multi-layer LSTM regression network to capture the temporal dependencies of the reconstructed signals. For each time step t and layer l, the forward propagation is computed as follow:

$$f_t^l = \sigma(W_f^l Z_t + U_f^l h_t^{l-1} + b_f^l) \qquad \text{(Forget gate)} \tag{4.49}$$

$$i_t^l = \sigma(W_i^l Z_t + U_i^l h_t^{l-1} + b_i^l) \qquad \text{(Input gate)} \tag{4.50}$$

$$\tilde{c}_t^l = \tanh(W_c^l Z_t + U_c^l h_t^{l-1} + b_c^l) \qquad \text{(Candidate memory)} \tag{4.51}$$

$$c_t^l = f_t^l \odot c_{t-1}^l + i_t^l \odot \tilde{c}_t^l \qquad \text{(Memory update)} \tag{4.52}$$

$$o_t^l = \sigma(W_o^l Z_t + U_o^l h_t^{l-1} + b_o^l) \qquad \text{(Output gate)} \tag{4.53}$$

$$h_t^l = o_t^l \odot \tanh(c_t^l). \tag{4.54}$$

The hidden state of the final LSTM layer, h_t^L, is passed through a fully connected layer with a linear activation function to estimate the reconstructed primary information, as given by

$$\hat{I}_t^P = W_d h_t^L + b_d. \tag{4.55}$$

The TFS-DNN is trained by minimizing the mean squared error between the predicted and actual primary information while applying ℓ_2-regularization to improve generalization:

$$\mathcal{L} = \frac{1}{T}\sum_{t=1}^{T}\left\|\hat{I}_t^P - I_t^P\right\|_2^2 + \lambda\left(\|W\|_2^2 + \|b\|_2^2\right). \tag{4.56}$$

The trainable parameters W and b are updated using stochastic gradient descent during the training process according to (4.57)

$$W \leftarrow W - \xi\frac{\partial\mathcal{L}}{\partial W}, \qquad b \leftarrow b - \xi\frac{\partial\mathcal{L}}{\partial b}, \tag{4.57}$$

where ξ is the learning rate. In contrast to conventional autoregressive, CNN, or LSTM-based forecasting models, the proposed TFS-DNN improves both short- and long-term prediction accuracy by integrating STFT-based time-frequency features with an LSTM regression network. From a signal processing perspective, STFT captures the temporal evolution of the signal's spectral components, highlighting short-term variations, while the LSTM learns long-term temporal dependencies and operational patterns. This complementary representation enables the model to adapt its predictions to recent operating conditions while preserving awareness of long-term system dynamics, resulting in more accurate and robust forecasting [256].

4.3.3.2 Robust Hydrogen Refueling Stations Power Limits Estimation

In the second stage, a decoupled optimization framework is employed to estimate the maximum admissible power limits of the PtH and HtP units while ensuring compliance with distribution network voltage and feeder capacity constraints. Building upon the robust power limit estimation approach proposed in [257], the proposed method additionally considers uncertainties associated with RES generation and electrical demand. The robust optimization problem is formulated as follows:

$$\begin{aligned}\text{Min}\underset{P_{t,b}^{DG},V_{t,b},\delta_{t,b}}{\text{Max}}&\left[\sum_{h\in\boldsymbol{\mathcal{H}}}\left(\overline{P_{t,h}^{PtH}}+\overline{P_{t,h}^{HtP}}\right)\right],\ \text{Subject to: (4.25)}-\text{(4.28)}\\ &\{P_{t,b}^{DG},P_{t,b}^{D},Q_{t,b}^{D}\}\in\{\Delta P_{t,b}^{DG},\Delta P_{t,b}^{D},\Delta Q_{t,b}^{D}\}.\end{aligned} \tag{4.58}$$

Here, $\Delta(\cdot)$ denotes the uncertainty bounds associated with the corresponding variables. The solution of (4.58) provides the robust operating limits $\overline{P_{t,h}^{PtH}}$ and $\overline{P_{t,h}^{HtP}}$, which guarantee distribution network voltage regulation and feeder loading constraints under worst-case operating conditions.

4.3.3.3 Convex Resilience Optimal Hydrogen Refueling Stations Scheduling

After decoupling the power and transportation IES through the estimation of the HRSs power limits, a convex cyber-resilient EMS can be formulated. This is possible because the resulting optimization consists of the convex objective function in (4.24) together with the operational constraints in (4.30)–(4.37), enabling efficient computation and guaranteeing a globally optimal solution. The cyber-resilient EMS receives the estimated power limits ($\overline{P_{t,h}^{PtH}}$, $\overline{P_{t,h}^{HtP}}$), the reconstructed primary information I_t^P, and the associated forecasting uncertainty ΔI_t^P. Based on these inputs, a set of $\mathbb{M}$ operational scenarios is generated to capture the uncertainty in the reconstructed information:

$$I_{t,m}^P \sim \left[I_t^P - \Delta I_t^P,\, I_t^P + \Delta I_t^P\right], \quad \forall m \in \mathbb{M}. \tag{4.59}$$

The objective of the convex-resilient EMS is to compute the optimal PtH and HtP setpoints $\left(P_{t,h}^{PtH*},\, P_{t,h}^{HtP*}\right)$ that maximize the expected revenue over all scenarios in $\mathbb{M}$, while guaranteeing that all HRSs operational constraints are satisfied for each scenario. This optimization problem is formulated as follows:

$$\begin{aligned} &\underset{P_{t,h}^{PtH*},\, P_{t,h}^{HtP*}}{\text{Max}} : \mathbb{E}[\text{Obj}(4.24)] = \sum_{m\in\mathbb{M}} \mathbb{P}(I_{t,m}^P)\, \text{Obj}(4.24)\big|_{I_{t,m}^P} \\ &\text{Subject to: } (4.30) - (4.37), \quad \forall m \in \mathbb{M}. \end{aligned} \tag{4.60}$$

Here, $\mathbb{P}(I_{t,m}^P)$ represents the probability of scenario m, which is derived from the error distribution of the TFS-DNN reconstruction model. When all scenarios are equally likely, the expected value reduces to a simple average over all realizations. Compared to conventional EMS formulations that assume fully reliable data availability, the proposed cyber-resilient framework integrates TFS-DNN-based signal reconstruction, robust power-limit estimation, and convex scenario-based optimal scheduling to ensure feasible and stable operation under severe DoS and DDoS cyberattacks.

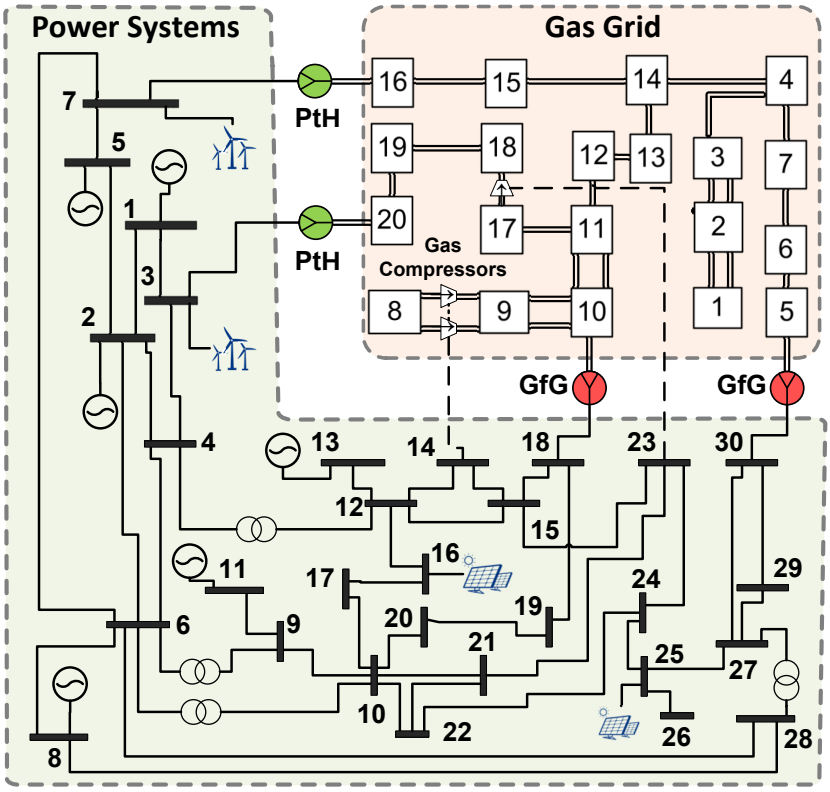


Figure 4.4: The IEEE 30-bus transmission system integrated with a 20–node gas transmission grid employed for numerical analysis.

4.4 Numerical Results of Power and Gas Integrated Energy System

4.4.1 Test System and Simulation Environment

The integrated IEEE 30-bus power system and 20-node gas transmission network, shown in Figure 4.4, is adopted as the simulation testbed for the power and gas IES. The system is simulated over one year with an hourly resolution ($\Delta t = 1$ h), resulting in a healthy-operation dataset of $\tau^{HL} = 8,760$ samples. The simulations are based on Ontario electricity market data from 2022 and gas network data obtained from [24]. The developed SICA targets the secondary information by manipulating the setpoints of the coupling PtH and GfG units, as well as the electric compressors, located at the following power–gas node pairs:

$$\text{PtH}(7,16),\ \text{PtH}(3,20),\ \text{GfG}(18,10),\ \text{GfG}(30,5),\ \text{Com}(14,8\text{–}9),\ \text{Com}(23,17\text{–}18).$$

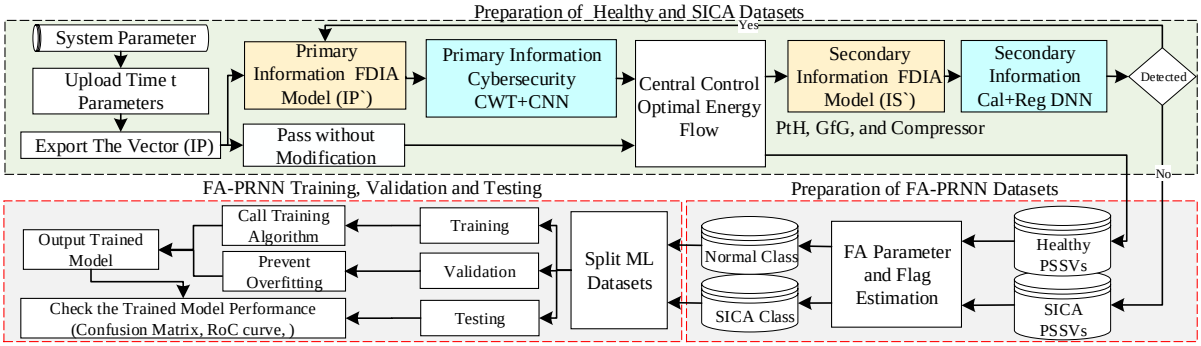


Figure 4.5: Healthy and SICA scenario generation flowchart on power and gas IES.

Figure 4.5 illustrates the simulation framework and data generation procedure. At each time step t, the healthy PSSVs are obtained by applying the unmodified primary information to the IES EMS to compute the optimal energy flow. The resulting operating states are then stored in the healthy PSSV dataset. For the SICA scenarios, the secondary information attack models presented in Section 4.2.2 are applied to generate manipulated operating conditions. To ensure a successful stealthy attack, the manipulated setpoints are iteratively evaluated against the acceptable forecasting error of the Cal-Reg DNN. If the attack is detected, the attack vector is updated by reducing the manipulation magnitude according to the proposed *Attack–Wait–and–Observe* strategy until it successfully bypasses the Cal-Reg DNN cybersecurity layer. The resulting operating states are then stored in the SICA dataset. All simulations were performed on a workstation equipped with a 12th Generation Intel Core i9 processor (2.1 GHz) and 32 GB of RAM.

4.4.2 Power and Gas Integrated Energy System Optimal Energy Flow

Figure 4.6 presents the optimal operating states of the power and gas IES, demonstrating stable and secure operation of both subsystems within their prescribed operating limits. From the SPS perspective, the bus voltage magnitudes and voltage angles remain within the acceptable operating margins. Similarly, the gas network exhibits feasible operating conditions, where the gas node pressures and pipeline gas flows, expressed in Thousand Standard Cubic Meters per Hour (TSCM/h), satisfy all operational constraints without violating pressure or flow limits. Meanwhile, Figure 4.7 illustrates the coordination of PtH and GfG units by the EMS with respect to the overall electricity price of the power and gas IES. Overall, the operation of PtH units is prioritized during periods of high RES generation, when electricity prices are low and

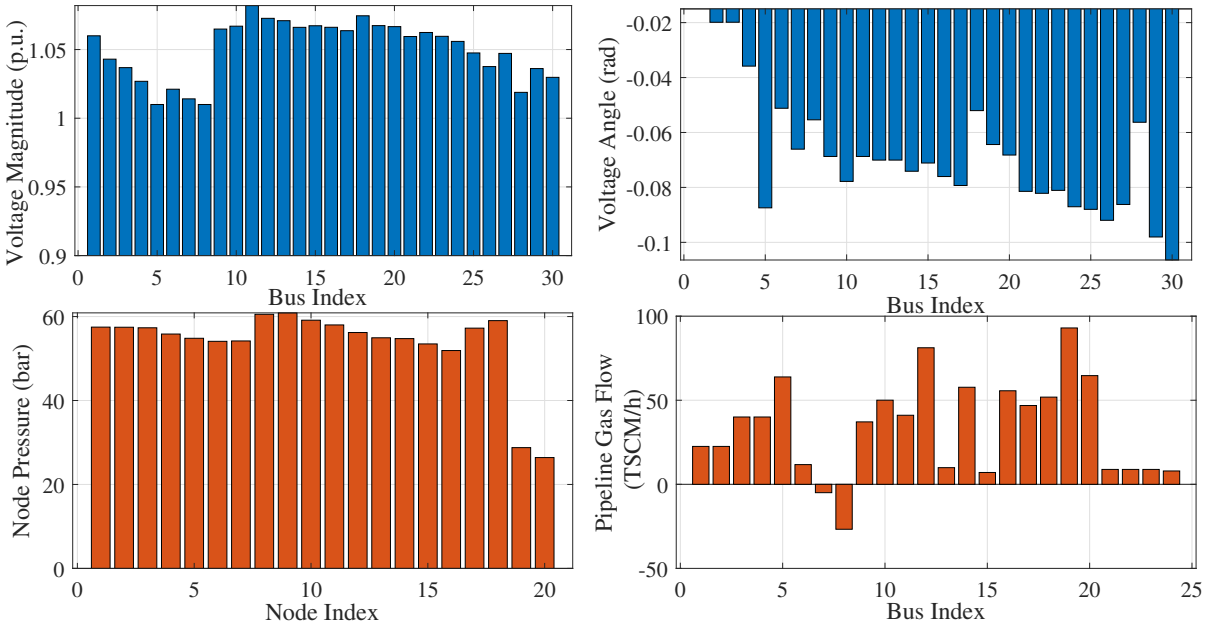


Figure 4.6: Power and gas IES operation state under operation.

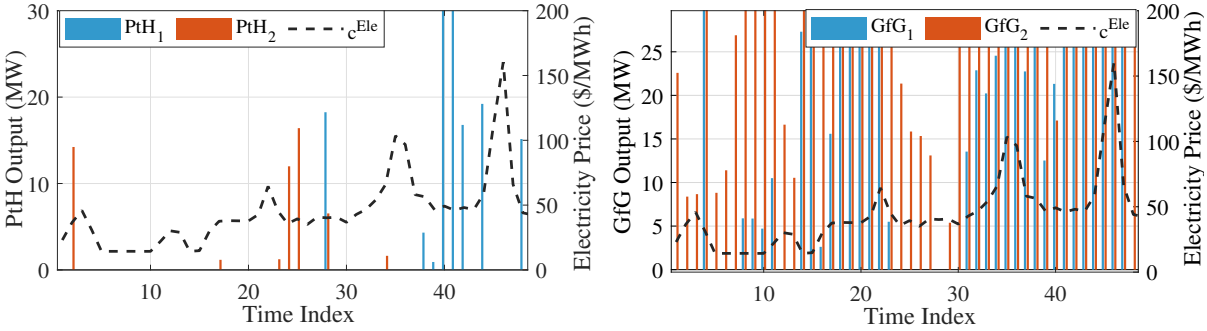


Figure 4.7: PtH and GfG units scheduling with respect to the electricity price.

surplus energy is available on the power side. On the other hand, GfG operation is scheduled during periods of high electricity prices or low RES generation to support the SPS operation. This operation validates the role of the EMS in regulating both the power and gas IES.

4.4.3 Power and Gas Integrated Energy System Secondary Information Cybersecurity Layer

As the SICA targets the secondary information of the gas system, primarily the coupling units of PtH and GfG, the Cal+Regression-DNN proposed in [24] is adopted. Figure 4.8 presents the framework, highlighting the architectures of both the classification DNN and the regres-

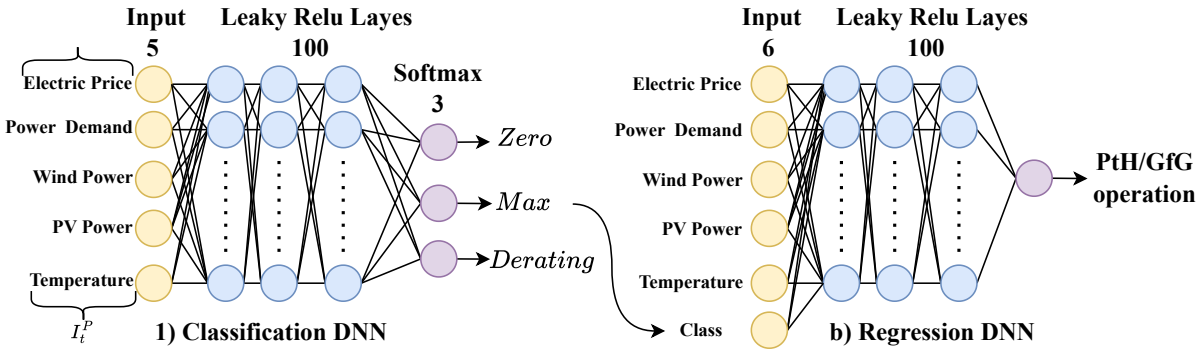


Figure 4.8: Structure of Cal+Regression-DNN secondary information cybersecurity layer.

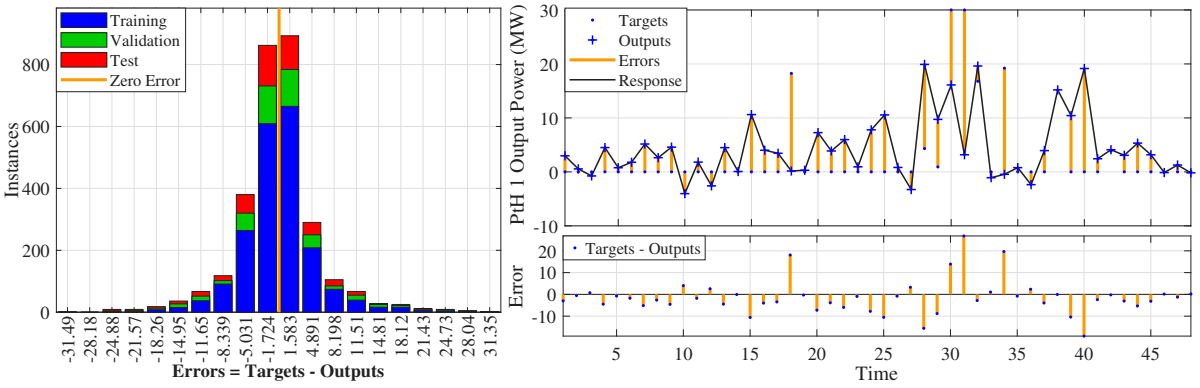


Figure 4.9: Performance of Cal+Regression-DNN in forecasting the setpoints of PtH unit 1.

sion DNN. The classification DNN first determines the operating region of the coupling units, providing a boundary that guides the regression DNN in accurately estimating their expected outputs.

Figure 4.9 presents the performance of the Cal-Regression-DNN in forecasting the setpoint of PtH Unit 1 and summarizes its overall prediction accuracy. The error histogram shows that more than 90% of the forecasting errors are below 8 MW, corresponding to an acceptable forecasting threshold of approximately 26.7%. The 48-hour time-series response further illustrates the forecasting performance at each time step, where larger prediction errors mainly occur during zero-output operating periods. This observation highlights the advantage of the classification stage, which filters these unnecessary regression errors by forcing the predicted setpoint to zero when the operating class is identified as zero-output, or to the rated value when the unit operates at its maximum capacity.

4.4.4 Power and Gas Integrated Energy System Stealthy Infiltrated Cyber Attacks

To evaluate the impact of the proposed SICA on the power and gas IES, coordinated attacks are launched against the secondary information of the PtH and GfG setpoints. Figure 4.10 compares the SPS operating states under healthy conditions and after the SICA successfully bypasses the Cal-Regression-DNN cybersecurity layer. As observed, the SPS operating state, particularly the buses phasor voltage, deviates significantly from the healthy operating condition.

This behavior can be attributed to two main factors. First, unlike attacks targeting SE measurements, where the allowable sensor error is relatively small and any large manipulation is likely to trigger advanced stealthy FDIA detection mechanisms, the secondary information is protected by a forecasting threshold of approximately 26.7% for each controllable unit. This larger tolerance provides the attacker with greater flexibility to coordinate attacks while remaining undetected. The primary reason for the relatively large forecasting uncertainty is that the forecasting model relies solely on local historical information. Consequently, the model cannot exploit additional spatial, meteorological, or system-wide information that could improve forecasting accuracy, resulting in a relatively simple time-series forecasting framework and a wider prediction uncertainty. Second, the strong coupling between the power and gas systems amplifies the attack propagation. Manipulating the setpoints of PtH or GfG units simultaneously affects both energy networks, resulting in system-wide operational deviations rather than localized impacts, as typically observed in standalone SPS. Consequently, even relatively small manipulations of the coupling units can produce significant changes in the overall operating state.

These results demonstrate that cyberattacks on integrated energy systems can have substantially greater system-wide consequences than attacks on standalone infrastructures, highlighting the need for cybersecurity frameworks specifically designed for highly coupled IESs.

4.4.5 Performance of Feasibility Area-Based Deep Neural Network Model in Detecting Stealthy Infiltrated Cyber Attacks on Power and Gas Integrated Energy System

In order to detect SICA in the power and gas IES, the proposed FA framework is adopted, where the objective is to identify the impact of SICA through the resulting SPS PSSVs. Fig-

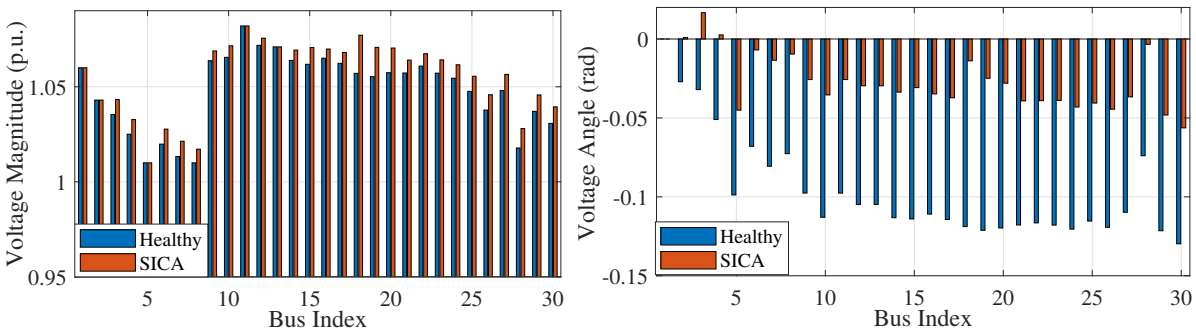


Figure 4.10: SPS operation state under SICA.

ure 4.11 shows the number of effective PSSVs identified using the statistical analysis of the FA framework as the acceptable TP and FN threshold varies ($n \in$ Effective state variables, if $TP_n \geq$ threshold $\wedge$ $FN_n \geq$ threshold). In this context, a threshold of 70% indicates that a given PSSV remains inside the corresponding FA classifier during healthy operation for at least 70% of the samples and is located outside the classifier for at least 70% of the samples under SICA. Therefore, such variables provide reliable indicators for distinguishing between normal and compromised operating conditions.

When a small historical window is used, the Convex-Hull classifier exhibits the lowest performance. However, as the historical window size increases, the number of effective PSSVs associated with ϕ_{CH} increases more rapidly than the other classifiers. This indicates that the Convex-Hull classifier benefits from a larger number of historical operating samples, enabling a more accurate estimation of the healthy operating region. Across all classifiers $\phi \in \Phi$, the maximum simultaneous TP and FN threshold achieved is approximately 70%. Consequently, relying on a single PSSV would still result in nearly a 30% probability of incorrect classification. For this reason, the proposed FA framework combines the information from all PSSVs through the flag vector and the FA-PRNN, significantly improving the overall detection performance. Compared with standalone SPS, the power and gas IES produces larger and more widespread state deviations under SICA due to the propagation of disturbances through the coupling units, allowing a greater number of PSSVs to become effective indicators of cyberattacks.

Figure 4.12 presents the detection performance of the proposed FA-PRNN framework for identifying SICA in the power and gas IES. The proposed method achieves an overall detection accuracy of 95.9%, demonstrating a high detection rate and reliable identification of coordinated cyberattacks.

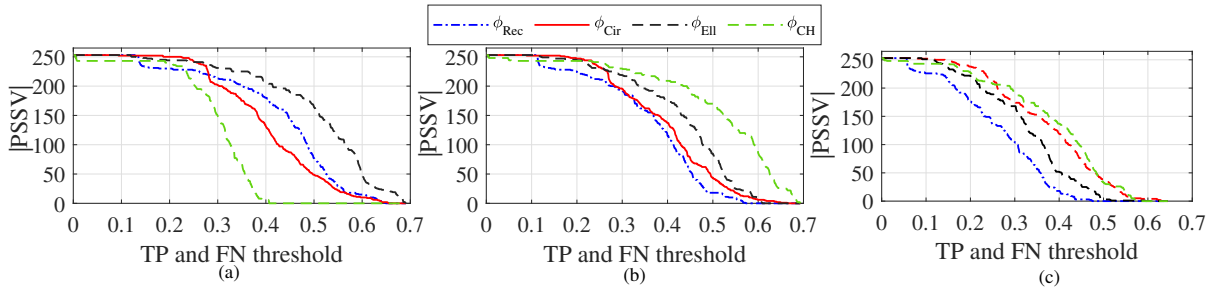


Figure 4.11: The number of effective PSSV for different lengths of historical data window a) M^{FA}=24-hour, b) M^{FA}=48-hour, c) M^{FA}=168-hour.

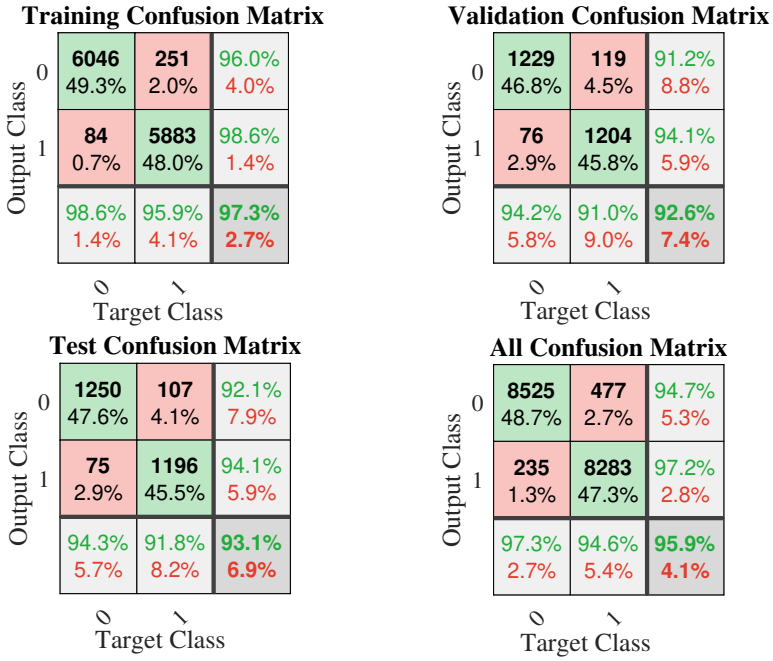


Figure 4.12: Detection performance of the proposed FA-PRNN in the power and gas IES.

It is worth noting that the proposed FA framework detects cyberattacks propagating from the gas network by monitoring only the PSSVs of the SPS. This capability is enabled by the strong physical coupling between the power and gas networks through the interconnected PtH and GfG units, allowing disturbances originating in the gas network to propagate into the electrical system. In principle, an attacker could attempt to design a cyberattack that maintains the coupling-unit setpoints unchanged, thereby confining the attack within the gas network and minimizing its impact on the power system. However, constructing such an attack is highly challenging in practice. Even small manipulations of gas flow or node pressure tend to propagate

throughout the gas network and eventually influence the operating conditions of the coupling units. The simulation results confirm this observation, showing that only a very limited number of operating hours throughout the entire one-year simulation allowed such an attack to remain confined, and even then, the resulting operating-state deviations were minimal.

These findings further highlight an important cybersecurity concern for future IESs: attackers may exploit the weaker cybersecurity of one energy infrastructure to compromise another, more strongly protected system through their physical interconnections. Although this chapter focuses on detecting the propagated impact using the PSSV, the proposed FA concept is equally applicable to the gas network itself. For example, a gas-network FA can be constructed using two interdependent gas-state variables, such as node gas pressure and injected gas flow, as developed in [250]. Such a multi-domain implementation would provide comprehensive cyber-physical monitoring across the entire integrated energy system.

4.5 Numerical Results of Power and Transportation Integrated Energy System

4.5.1 Test System and Simulation Environment

The integrated IEEE 33-bus distribution system coupled with three HRSs, as shown in Figure 4.13, is adopted as the simulation testbed. The system is simulated over a one-year period with an hourly resolution ($\Delta t = 1$ h), resulting in a healthy-operation dataset of $\tau^{HL} = 8,760$ samples. The simulations are based on Ontario electricity market data from 2022 and HRSs operational data obtained from [255]. Three types of cyberattacks are investigated: 1) stealthy FDIA targeting the conventional HRS-EMS, 2) single DoS attacks, and 3) coordinated bi-level DDoS attacks targeting the primary information of the EMS and the coupling PtH and HtP units located at Buses 7, 14, and 29. Figure 4.14 presents the overall simulation framework of the proposed HRS-EMS, highlighting both the cyber-resilient EMS and the proposed FA-PRNN cybersecurity framework. The framework consists of five main components: 1) input data and system operating parameters, 2) robust HRSs power limit estimation, 3) TFS-DNN forecasting, 4) DoS and coordinated bi-level DDoS attack modeling with the cyber-resilient EMS, and 5) the proposed FA-PRNN for stealthy FDIA detection. First, the power limit estimation module receives system uncertainty information and determines the secure operating limits of the PtH and HtP units, which are subsequently supplied to the cyber-resilient EMS, particularly during

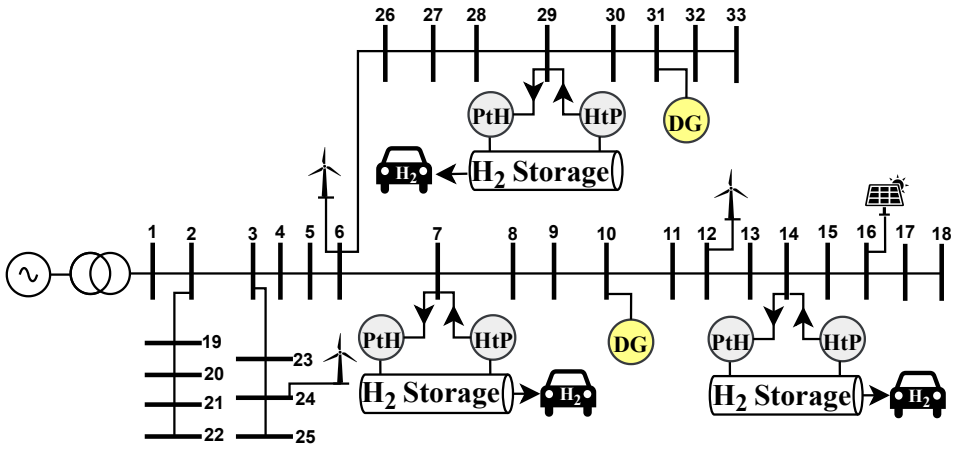


Figure 4.13: IEEE 33-bus distribution system integrated with HRSs and transportation system at Bus 7, Bus 14, and Bus 29 distributed HRSs used for numerical studies.

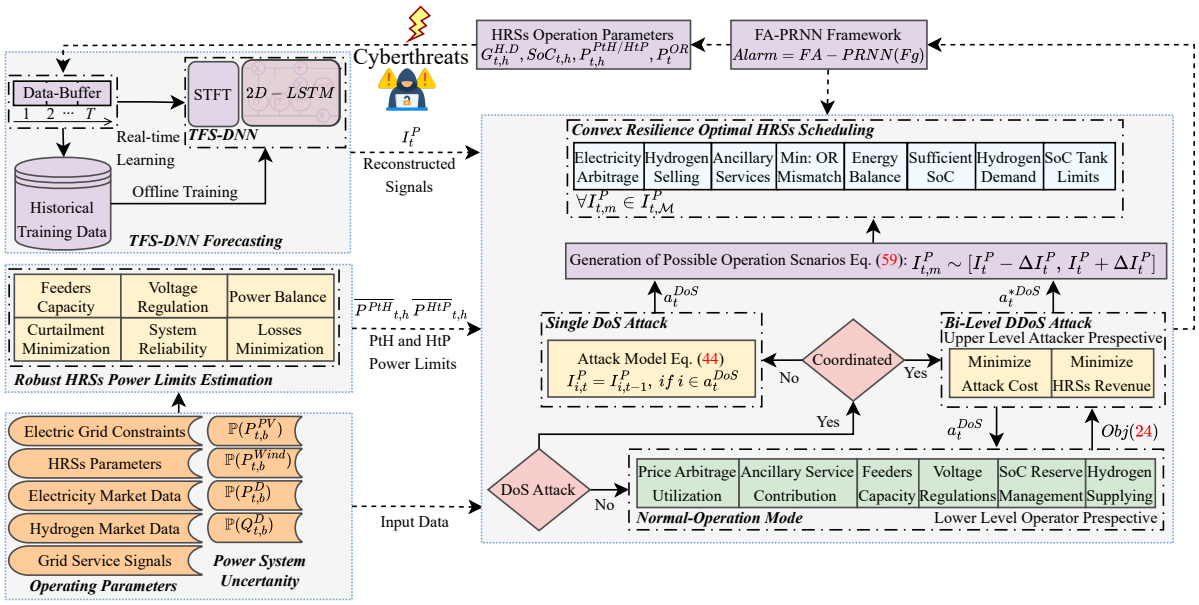


Figure 4.14: Healthy, stealthy FDIA, and DDoS attacks scenario generation flowchart on HRSs power and transportation IES.

cyberattack conditions. Next, the TFS-DNN forecasting module is trained offline using historical HRSs operational data, while an online learning mechanism continuously updates the model using real-time forecasting errors. The forecasted information, together with the estimated power limits and system operating data, is then provided to the EMS. Under normal operating

conditions, or during stealthy FDIA, the conventional EMS performs joint optimization of the coupled power and transportation systems using the received primary information. During a single DoS attack, the affected measurements are modeled according to (4.44). For coordinated bi-level DDoS attacks, the proposed bi-level optimization framework is employed, where the upper level minimizes both the attack cost and the HRSs revenue, while the lower level represents the operator's optimal scheduling response. Once a DoS or DDoS attack is detected, multiple operational scenarios $\mathbb{M}$ are generated using the reconstructed information from the TFS-DNN together with its associated forecasting uncertainty. The convex cyber-resilient HRS scheduling model is then executed to maximize the expected profit across all scenarios while guaranteeing reliable and secure system operation. The proposed framework is implemented in MATLAB and solved using the Gurobi optimizer over a one-week simulation horizon with a rolling (M^{Ft}) 3-hour prediction horizon. All simulations are executed on an Intel Core i9 (12th Generation, 2.1 GHz) workstation equipped with 32 GB of RAM.

4.5.2 Power and Transportation Integrated Energy System Energy Management System

Figure 4.15 illustrates the healthy operation of the HRSs, where the communicated information is free from stealthy FDIA, single DoS, and coordinated bi-level DDoS attacks. Figure 4.15a) presents the instantaneous and cumulative revenue generated from hydrogen sales and participation in the OR market. The instantaneous revenue varies over time according to the electricity price, hydrogen demand, and OR signals, while the cumulative revenue increases steadily throughout the operation. Figure 4.15b) shows the scheduled power setpoints of the PtH and HtP units together with the issued OR signals. The scheduling follows the required positive and negative OR requests while exploiting electricity price arbitrage to maximize profitability. Figure 4.15c) presents the corresponding hydrogen production by the PtH units, hydrogen consumption by the HtP units, and the hydrogen demand at the HRSs. The operating schedules satisfy the transportation demand while coordinating with the electricity market and ancillary service requirements.

Figure 4.15d) illustrates the hydrogen storage SoC for the three HRSs, together with the upper and lower reserve margins. The SoC evolves according to the charging and discharging schedules of the PtH and HtP units while remaining within the prescribed operating limits. During periods without OR requests, the reserve margin is maintained to ensure future oper-

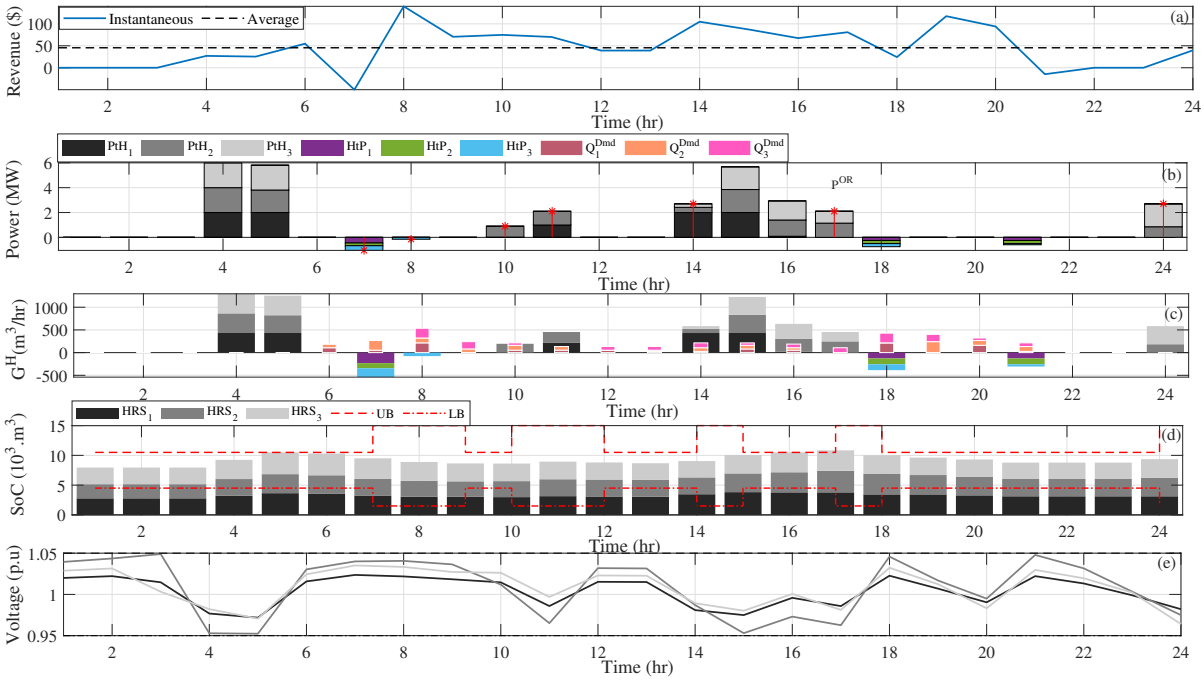


Figure 4.15: Performance of the HRSs under healthy operation; a) Revenue, b) PtH and HtP power setpoints and OR signal, c) PtH and HtP hydrogen flow and HRSs hydrogen demand, d) HRSs hydrogen storage SoC as well as upper bound and lower bound reserve margin, and e) HRSs bus voltage.

ational flexibility. When OR signals are issued, the stored hydrogen is utilized to satisfy the requested ancillary services. Finally, Figure 4.15e) presents the voltage profiles of the buses connected to the three HRSs. The bus voltages remain within the allowable operating range ($\pm 5\%$), confirming that the coordinated operation of the HRSs satisfies the distribution network voltage constraints while maintaining secure and reliable grid operation.

4.5.3 Power and Transportation Integrated Energy System Cyberattacks

4.5.3.1 Power and Transportation Integrated Energy System Stealthy False Data Injection Attack

Stealthy FDIA are conducted to manipulate the HRS EMS. Figure 4.16 presents a representative example of the attack targeting the communicated OR signal. Figure 4.16a) compares the OR signal under healthy and compromised conditions, showing that the stealthy FDIA

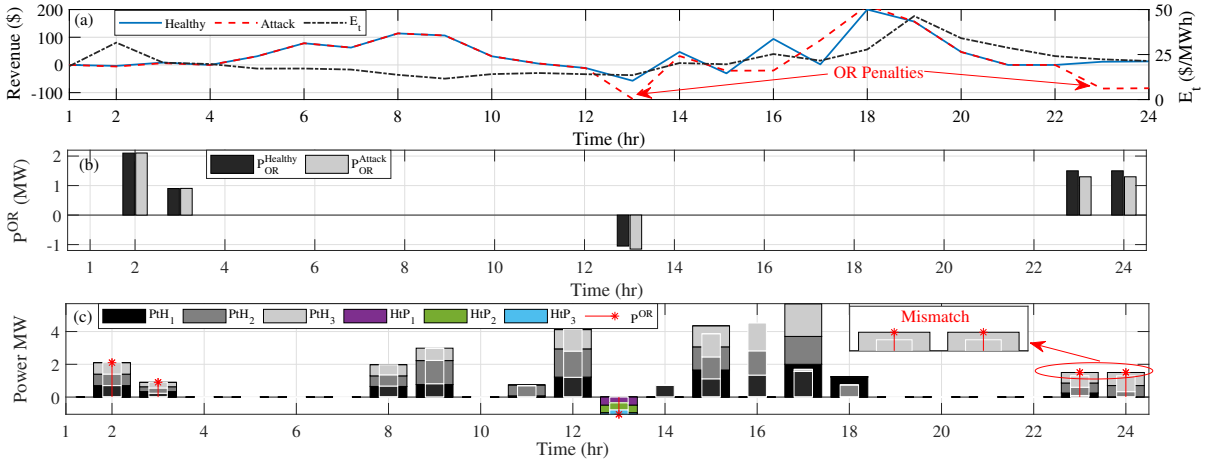


Figure 4.16: Performance of the HRSs under compromise of OR power signal; a) OR signal, b) PtH and HtP power setpoints and the OR signal, c) Revenue.

successfully introduces undetectable deviations in the communicated OR values. Figure 4.16b) illustrates the corresponding PtH and HtP power setpoints, where the thick and thin bars represent the healthy and compromised operating conditions, respectively. The manipulated OR signals cause all HRSs to deviate from their optimal schedules. By injecting false positive or negative OR requirements, the attacker forces the stations to either over-respond or under-respond to the actual ancillary service requests, leading to OR non-compliance and reduced electricity arbitrage opportunities. Figure 4.16c) compares the accumulated revenue under healthy and compromised operating conditions. The manipulated OR signals significantly reduce the HRSs profitability, resulting in an approximately 31% decrease in total revenue compared with healthy operation.

4.5.3.2 Power and Transportation Integrated Energy System Single DoS and Coordinated Bi-Level DDoS Attacks

In the case of DoS and coordinated bi-level DDoS attacks, the attacker aims to force the EMS to operate using outdated information, resulting in suboptimal scheduling of the PtH and HtP units. Representative simulation results are presented in Figure 4.17. Figure 4.17a) illustrates the effect of a single DoS attack on the hydrogen demand signal of HRS 1, where intermittent data blocking leads to outdated or missing information at the EMS.

This disruption leads to two main consequences. First, the system may falsely interpret

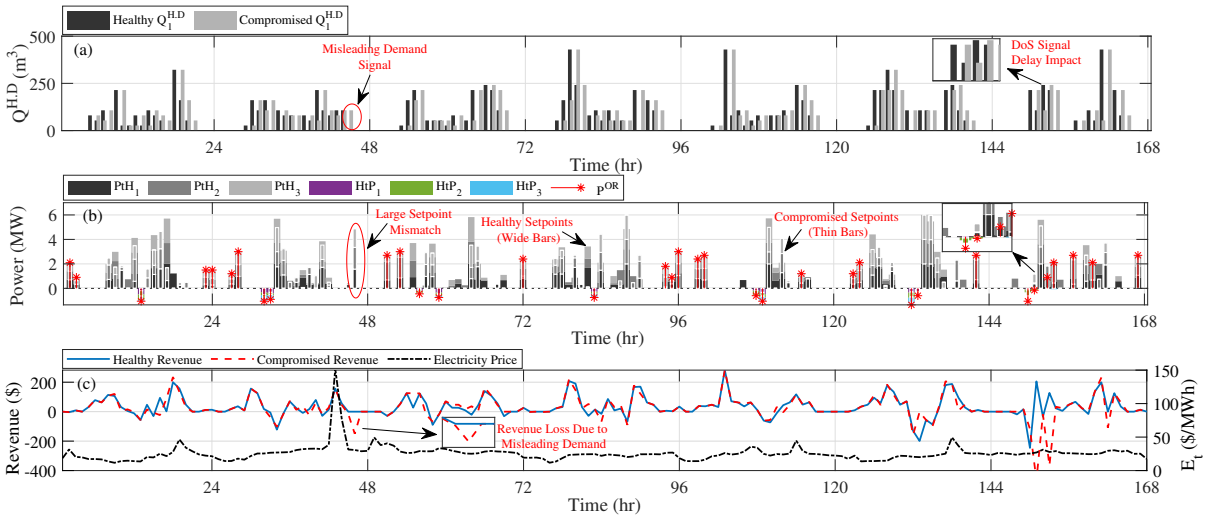


Figure 4.17: Performance of the HRSs EMS under healthy state and DoS for the hydrogen demand ; a) Hydrogen demand , b) PtH and HtP power setpoints and the OR signal, c) Revenue.

elevated hydrogen demand, causing the EMS to schedule excessively high PtH setpoints and consequently purchase electricity during high-price periods, reducing operational profit. This behavior is reflected in Figure 4.17b), where the compromised case (thin bars) deviates significantly from the healthy case (thick bars), particularly around $t = 46$. Second, the overestimated demand signal limits appropriate responses to negative OR events by restricting HtP activation, which further results in penalty costs from the distribution system operator. Figure 4.17c) shows the corresponding revenue comparison, where the weekly profit decreases from \$5.5k under healthy operation to \$4.5k under the DoS attack, corresponding to a 17.63% loss. These results highlight that the impact of DoS attacks is significantly amplified when they interfere with OR participation, leading to additional penalties and degraded economic performance.

Figure 4.18 illustrates the performance of the EMS under the investigated bi-level coordinated DDoS cyberattack. Unlike a conventional DoS attack that persistently targets a single signal, the DDoS attack coordinates disruptions across multiple signals and selectively targets time instances that maximize financial impact, as shown in Figure 4.18a).

Two main attack strategies are considered. First, the attacker disrupts local HRSs signals such as hydrogen demand and station SoC, causing misalignment between PtH and HtP scheduling and the actual OR requirements, without directly modifying the OR signal itself. Second,

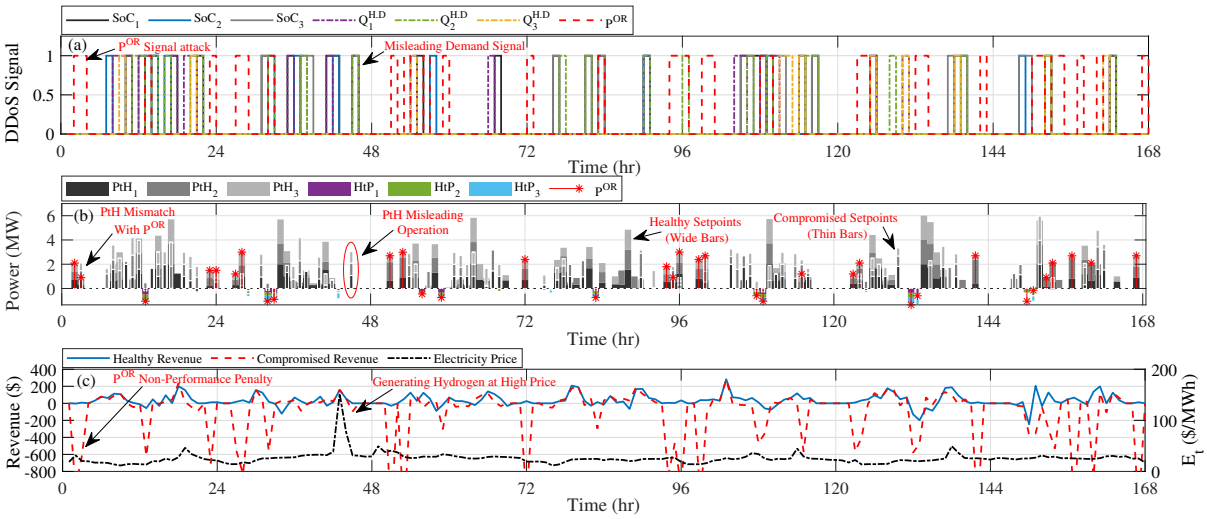


Figure 4.18: Performance of the HRSs EMS under healthy and the investigated Bi-level coordinated DDoS attack; a) DDoS attack vector, b) PtH and HtP power setpoints and the OR signal, c) Revenue.

Table 4.1: Impact of DoS and DDoS Cyberattack

Attack	DoS-SoC			DoS-$Q^{H.D}$			DoS	DDoS	
HRS	1	2	3	1	2	3	P^{OR}	$P^{OR} \notin a^{DoS}$	$P^{OR} \in a^{DoS}$
ΔRev (%)	1	8.1	1	17.6	1	4.16	400	46	438
$\frac{\Delta Rev}{\sum C.a^{DoS}}$	0.1	0.27	0.1	0.58	0.1	0.14	1.31	1.66	5

the attacker directly targets the OR signal to further amplify operational and financial deviations. Both strategies lead to substantial reductions in HRSs revenue. Since the OR signal is typically managed by the distribution system operator and protected using more advanced communication and cybersecurity mechanisms, the coordinated DDoS strategy prioritizes the less protected HRSs side signals, exploiting their vulnerability to indirectly degrade system performance while maximizing economic loss.

Table 4.1 summarizes the impact of DoS and DDoS attacks on HRSs revenue, as well as the attack return from the adversary's perspective. Among all DoS scenarios, manipulation of the SoC signal results in the lowest impact, with an average revenue reduction of only 3.33%. In contrast, attacking the hydrogen demand signal leads to a higher revenue loss of 7.6%. The most severe case occurs when the OR signal is targeted, resulting in an apparent revenue re-

duction exceeding 400%, which reflects negative net profit due to violated OR commitments and associated penalties imposed by the distribution system operator. Under the bi-level DDoS framework, coordinated attacks on HRS-side signals (SoC and hydrogen demand) lead to a significant 46% revenue loss, demonstrating the increased effectiveness of multi-signal coordination. When the OR signal is additionally included in the attack strategy, the revenue loss further escalates to 438%, resulting in sustained negative profitability.

It is also important to note that even in the absence of penalty costs imposed by the distribution system operator, the HRSs would still experience substantial economic degradation, with revenue losses ranging between 27.7% and 48.5% under single DoS and coordinated DDoS attacks. The second row of Table 4.1 reports the attack return, defined as the ratio between the induced revenue loss and the cost of executing the attack. DoS attacks exhibit relatively low returns due to inefficient resource utilization, whereas the bi-level DDoS strategy achieves significantly higher returns by selectively launching attacks only when the expected financial impact exceeds the associated cost. These results highlight the critical vulnerability of HRSs to coordinated cyberattacks and emphasize the need for cyber-resilient EMS frameworks.

4.5.4 Performance of Feasibility Area-Based Deep Neural Network Model in Detecting Stealthy False Data Injection Attacks on Power and Transportation Integrated Energy System

Figure 4.19 illustrates the FA performance in detecing stealthy FDIA. Figure 4.19a) shows that the designed FDIA remains stealthy by closely replicating the healthy operating pattern of the system. As a result, both healthy and compromised data occupy similar operating regions, which makes conventional ML approaches less effective in distinguishing between the two cases due to their high overlap. Figure 4.19b) presents the ratio of PSSVs located outside the FA region under healthy and compromised conditions (FAUR). The results indicate a clear increase in the number of PSSVs outside the FA during attack scenarios, providing a discriminative feature that can be effectively exploited to distinguish healthy and compromised states.

Figure 4.19c) compares the performance of the conventional DNN with the proposed FA-enhanced method for FDIA detection in terms of multiple metrics. First, in terms of accuracy, the traditional DNN achieves 83%, whereas integrating the FA layer improves the accuracy to 94.2%, corresponding to a 13.5% improvement. Second, in terms of training efficiency, the FA-enhanced model converges faster, requiring approximately 1,300 iterations compared to 1,600

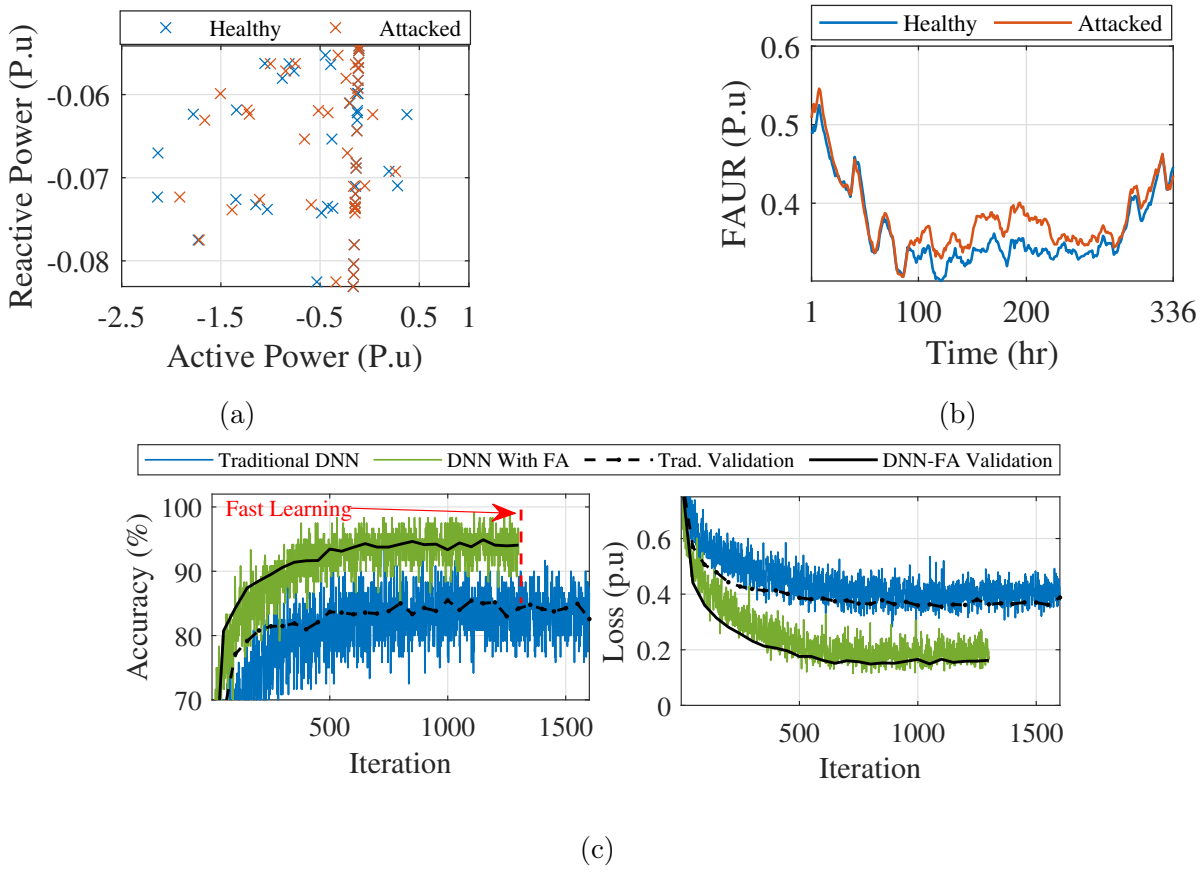
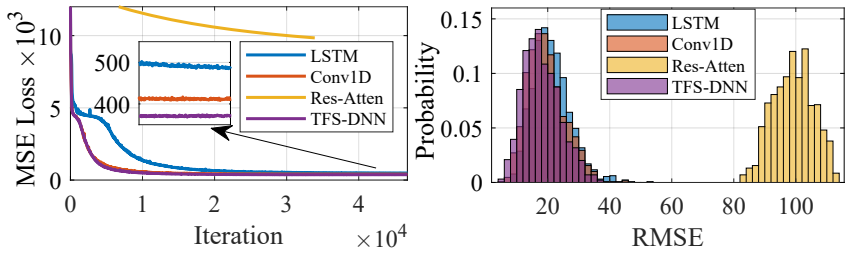


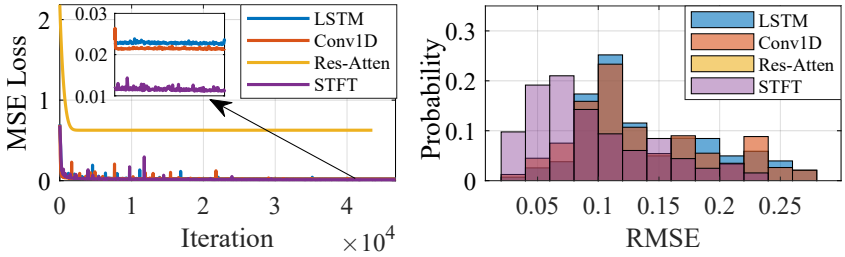
Figure 4.19: The FA's ability to detect attack patterns and DNN training performance; a) PSSV representation in the complex domain showing features overlap, b) FAUR, c) Performance of the DNN.

iterations for the conventional model, reducing training time by about 19%. Third, in terms of training loss, the proposed method achieves approximately 60% lower loss compared to the baseline DNN, demonstrating improved learning stability and robustness against stealthy FDIA.

It is worth noting that the proposed FA framework is capable of detecting both stealthy FDIAs and the abnormal operating-state deviations caused by delayed or outdated information under DoS attacks. Its primary objective, however, is cyberattack detection and operating-state monitoring. Compared with conventional FDIA detection approaches, the proposed FA provides physically meaningful cyber–physical features that significantly improve the learning capability and detection performance of the DNN. Nevertheless, detection alone is insufficient to recover from the operational consequences of cyberattacks. Therefore, a cyber-resilient EMS is integrated with the proposed detection framework, where compromised or missing information is



(a) Hydrogen demand



(b) OR Power signal

Figure 4.20: Training and testing performance of the DNN models in reconstruct the HRSs attacked information.

reconstructed using forecasting models, and a stochastic robust EMS is employed to determine secure operating decisions under uncertainty. This integration enables not only timely attack detection but also effective mitigation and recovery from cyberattack-induced operational disruptions.

4.5.5 Performance of The Proposed Cyber-resilient Hydrogen Refueling Station Energy Management System

To evaluate the proposed cyber-resilient EMS, the performance of the TFS-DNN, the PtH/HtP power limit estimation, and the convex scheduling framework are assessed. Figure 4.20 presents the training validation loss and the testing root mean square error of the proposed TFS-DNN, benchmarked against conventional LSTM, 1-D Convolutional LSTM, Rnet-ALSTM, and autoregressive models. Figure 4.20a shows the hydrogen demand forecasting performance together with the corresponding prediction error distribution. The proposed TFS-DNN achieves the highest forecasting accuracy, with an average error of 18.71 m^3, while also exhibiting the lowest mean and standard deviation on the testing dataset, demonstrating strong generalization capability. Similar performance is observed for OR power forecasting in Figure 4.20b, where the proposed model consistently outperforms the benchmark methods and produces a narrower

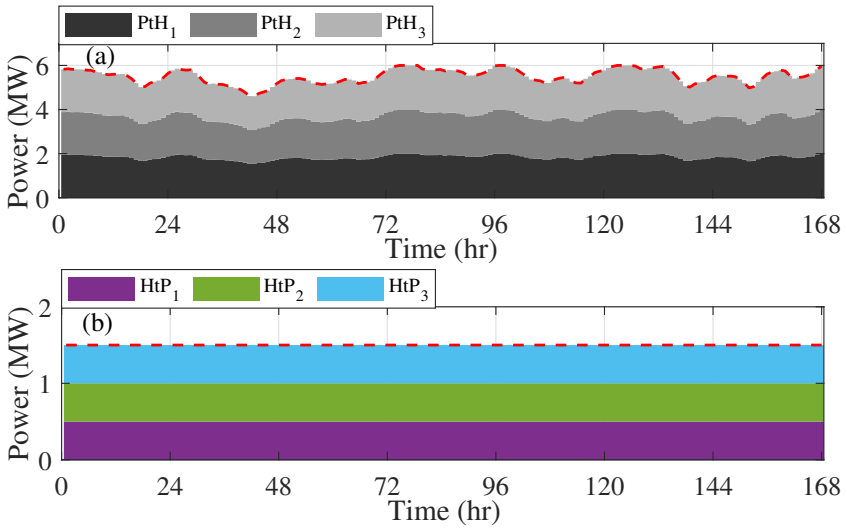


Figure 4.21: Power limits of the HRSs; a) PtH power limits, b) HtP power limits.

prediction error distribution.

Figure 4.21 illustrates the estimated operating limits of the PtH and HtP units obtained using the proposed robust HRSs power limit estimation method, which accounts for DG and demand uncertainties. As shown in Figure 4.21a), the maximum PtH power varies with feeder capacity, DG output, and load demand. During high-demand and low-generation periods, the PtH limit is reduced to satisfy feeder capacity and voltage constraints. In contrast, Figure 4.21b) shows that the HtP unit generally can operates at its rated capacity, since it injects power into the network and supports voltage regulation. The estimated limits are subsequently used as upper bounds in the convex cyber-resilient HRSs scheduling framework. Figure 4.22 illustrates the performance of the proposed convex cyber-resilient HRS EMS under a worst-case coordinated DDoS attack targeting all critical signals. Figure 4.22a) shows the attack instants, where compromised measurements are reconstructed using the proposed TFS-DNN. For each attacked signal, ten operational scenarios are generated to account for forecasting uncertainty, while uncompromised signals are treated deterministically. Figures 4.22b) and 4.22c) present the reconstructed hydrogen demand and SoC, together with their uncertainty bounds. Figure 4.22d) shows the optimal PtH and HtP schedules obtained from the scenario-based optimization while satisfying power limits and OR requirements. Finally, Figure 4.22e) compares the accumulated revenue with healthy operation. Despite the coordinated DDoS attack, the proposed cyber-resilient EMS achieves a revenue of \$5.423K, corresponding to only a 1.36% reduction from the healthy case.

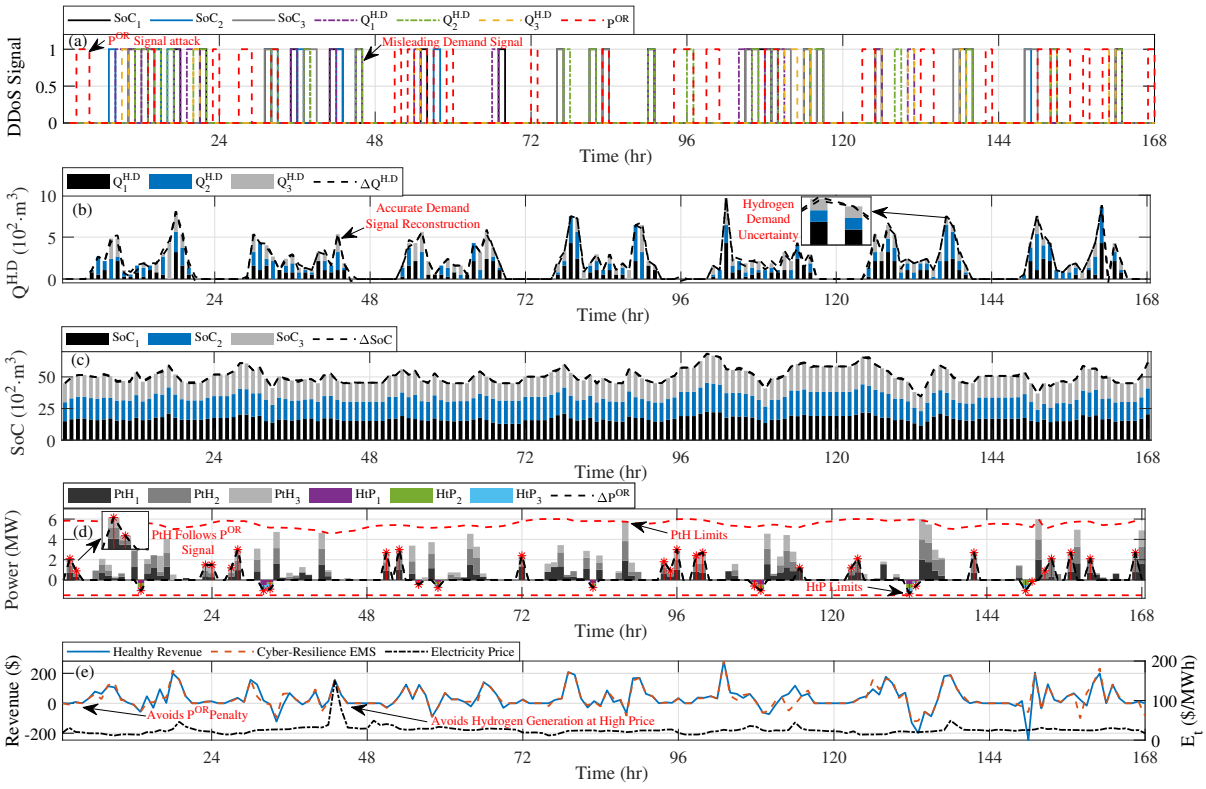


Figure 4.22: Performance of the convex resilience HRSs optimal scheduling; a) DDoS attack vector, b) reconstructed hydrogen demand and its uncertainty, c) reconstructed hydrogen tank SoC and its uncertainty, d) the PtH and HtP power setpoints and power limits beside the OR signal and it uncertainty, c) Revenue.

This demonstrates that the proposed framework reduces the revenue loss from 438% to only 1.36%, substantially improving both system resilience and economic performance.

The overall performance of the proposed cyber-resilient EMS is achieved through the integration of all three proposed components rather than any single module. Each component addresses a different aspect of the cyberattack mitigation problem and collectively enables secure and economically optimal operation under severe coordinated DDoSs. The TFS-DNN forecasting model is responsible for reconstructing compromised or missing signals, thereby providing reliable estimates of the expected operating conditions. Its forecasting accuracy directly influences the uncertainty of the reconstructed information. Higher forecasting errors require a larger set of operating scenarios to adequately represent the uncertainty, which consequently increases the deviation from the ideal optimal operating solution.

The robust estimation of the operating limits for the PtH and HtP units primarily ensures operational security rather than profitability. Although these limits have only a limited direct influence on the economic objective, they prevent the reconstructed operating points from violating distribution network constraints, including feeder capacity and voltage regulation limits, thereby guaranteeing secure system operation under uncertain conditions. Finally, the proposed convex EMS plays a central role in determining the optimal operating strategy. By decoupling the original optimization problem into a convex formulation, the proposed framework can efficiently evaluate a large number of operating scenarios while guaranteeing convergence to the global optimum. This enables the EMS to explicitly account for forecasting uncertainty and cyberattack impacts, resulting in robust operating decisions that simultaneously maximize profitability and maintain secure system operation.

4.6 Summary and Discussion

This chapter extended the proposed FA framework from standalone SPSs to interconnected IESs, addressing the second major research gap of this thesis: the lack of adaptive cybersecurity frameworks capable of protecting highly coupled multi-energy systems against sophisticated cyberattacks. Two representative IES architectures were investigated, namely power–gas and power–transportation systems, providing a comprehensive assessment of cybersecurity challenges arising from cross-sector integration.

For the power–gas IES, the study demonstrated that SICAs can successfully target the secondary information layer, particularly the forecasting-assisted control signals of the coupling PtH and GfG units. Unlike traditional attacks on primary measurements, the uncertainty associated with forecasting models introduces a significantly larger manipulation margin, allowing attackers to design more impactful yet stealthy cyberattacks while remaining within the expected forecasting error. Furthermore, the strong physical coupling between the power and gas infrastructures amplifies the propagation of disturbances, where relatively small manipulations of the coupling units produce substantial deviations throughout the entire integrated system. Although this increased coupling enlarges the cyberattack surface, it also generates stronger cyber-physical signatures that can be exploited by the proposed FA framework. By monitoring only the SPS operating states, the proposed FA-PRNN successfully identified the propagated effects of SICAs, achieving an average detection accuracy of approximately 96%.

The chapter further investigated cybersecurity within power–transportation IESs based on HRSs, where cyberattacks directly target the EMS. The results demonstrated that stealthy FDIAs manipulating HRS information significantly degrade the optimal scheduling of PtH and HtP units, resulting in considerable financial losses. Among the investigated attack vectors, manipulation of the coupling-unit information produced the most severe impact due to penalties associated with ancillary service non-compliance, whereas attacks on the hydrogen storage state of charge exhibited comparatively smaller effects. In contrast, DoS and coordinated bi-level DDoSs exploited information unavailability rather than measurement manipulation, forcing the EMS to operate using outdated information. The proposed bi-level coordinated DDoS further demonstrated that intelligent attackers can strategically schedule attacks by explicitly considering the operator's response, thereby maximizing financial damage while minimizing attack cost. Under severe scenarios, these attacks resulted in revenue losses exceeding 438% and even negative operating profits.

Although the proposed FA framework successfully detected abnormal operating states caused by stealthy FDIAs, DoS, and coordinated DDoSs, this chapter also identified an important limitation of operating-state-based detection: while abnormalities can be detected, missing or unavailable information cannot be recovered solely through the FA. This observation motivated the development of a cyber-resilient EMS capable of maintaining secure operation under severe information loss.

To address this challenge, a comprehensive cyber-resilient EMS was developed by integrating TFS-DNN signal reconstruction, robust estimation of coupling-unit operating limits, and convex multi-scenario scheduling that explicitly accounts for forecasting uncertainty. The proposed resilience framework successfully reconstructed missing information, generated robust operating scenarios, and maintained secure HRS operation despite coordinated cyberattacks. As a result, the maximum revenue loss was reduced from more than 438% under the conventional EMS to only approximately 1.38%, demonstrating that effective cybersecurity for future IESs requires not only accurate attack detection but also resilient operational recovery mechanisms. Overall, this chapter establishes that while IESs introduce new cyber vulnerabilities through their strong physical interdependencies, these same interactions can be leveraged to develop more informative detection features and resilient control strategies capable of ensuring secure and economically efficient operation.

Chapter 5

Advanced Feasibility Area Considering Spatial Distribution and Temporal Correlation Properties

The proposed FA framework has demonstrated the ability to detect stealthy FDIA and SICA in both standalone SPS and IES. However, in its current form, the framework is primarily limited to cyberattack detection. This chapter, together with the associated work published in [258], extends the proposed FA framework beyond detection by introducing attack mitigation capabilities and enabling the extraction of critical cyberattack features.

The proposed framework is enhanced by incorporating two complementary characteristics: 1) the spatial distribution of the SPS operation state and the proximity relationships among state variables within the complex plane, and 2) the temporal correlation between the current SPS operation state and historical operating conditions over a predefined historical window. The temporal correlation filters unrelated or mismatched historical operating states and identifies the most relevant and representative operating patterns. The enhanced FA framework is then applied to a standalone SPS to detect stealthy FDIA and extract the underlying attack vector features targeting the primary information. Moreover, to improve real-time application capabilities, a recursive FA estimation algorithm is proposed, where FA classifier parameters are updated using previous estimation knowledge and only updated when FA parameters change.

5.1 Introduction

The literature survey in Section 2.7 reviewed various cybersecurity approaches developed for CPPS and CPS in IESs. These methods primarily focus on prevention by either increasing the difficulty of launching cyberattacks or detecting attacks and issuing alarms once they occur. However, the evolving nature of coordinated stealthy FDIAs and multi-level cyberattacks enables attackers to optimally coordinate attack vectors across multiple locations. Consequently, although timely attack detection and alarm generation are essential for limiting the impact of cyberattacks, detection alone is insufficient for system recovery, leaving operators without guidance on how to identify compromised measurements or restore normal operation after an attack is detected [35]–[37].

To address these challenges, previous research has emphasized the need to move beyond attack detection toward extracting more informative cyberattack features, including: 1) identifying the compromised primary information, 2) locating the attacked buses or system components, and 3) estimating the number of compromised measurements [38]–[41]. However, the majority of these methods have been developed for dynamic applications, such as AGC [37], LFC [41], and microgrid dynamic operation [39], [40]. In these applications, linear state-space models enable the construction of observers that detect deviations between the expected system dynamics and received measurements. In contrast, extending observer-based techniques to steady-state applications, such as SE and EMS, remains challenging for two main reasons. First, the underlying optimization and power flow models are highly nonlinear. Second, customized operational objectives introduce discrete operating behaviors due to the relatively long communication intervals typical of steady-state applications. Combined with operational uncertainties, these characteristics make it difficult to construct a continuous observer capable of accurately extracting cyberattacks features. Consequently, existing research on steady-state applications has primarily focused on attack localization using temporal data analysis rather than observer-based feature extraction techniques [35].

Therefore, this chapter advances the proposed FA framework beyond attack detection to extract critical features of stealthy FDIAs in SPS. Specifically, the enhanced framework aims to identify: 1) the compromised primary information, 2) the locations of the attacked buses, and 3) the number of compromised measurements. To achieve this objective, two complementary features are incorporated into the FA framework. First, a spatial distribution feature is introduced to quantify the proximity of the current SPS operating state to previous healthy

operating states within the complex plane. This feature assigns a higher probability of normal operation to PSSVs located near densely populated regions of the FA, while PSSVs located farther from these regions are assigned a higher probability of abnormal operation. Second, a temporal correlation feature is developed to determine the contribution of historical operating states in constructing the current FA. This feature evaluates the similarity between the current primary information and historical healthy operating conditions, allowing only the most representative operating states to contribute more significantly to the FA boundary estimation.

To further improve computational efficiency, a recursive FA estimation algorithm is proposed, where the FA parameters are updated only when significant changes in the operating conditions are detected, thereby reducing unnecessary computations. The enhanced FA framework is evaluated using stealthy FDIA scenarios involving single, double, and three bus coordinated attacks with different attack magnitudes. Finally, a classification and regression FA-DNNs framework is developed to extract the key cyberattack features, including the attacked measurements, their locations, and the number of compromised measurements.

5.2 Advanced Feasibility Area Formulation and Preliminaries

5.2.1 Feasibility Area Spatial Distribution Property

The spatial distribution quantifies the proximity of the current PSSV, $x_{t,n}$, to the FA while preserving the exact geometric characteristics of the FA. To incorporate this information, the proposed framework replaces the binary flag vector defined in (3.40) with a continuous flag that reflects the relative distance of the current PSSV from the FA boundary. Consequently, PSSVs located closer to the boundary are assigned different confidence levels than those located farther away. To achieve this, a Sigmoid-expansion flag is proposed, as defined in (5.1).

$$Fg^{sig}_{\phi(t,n)} = \frac{1}{1 + e^{-a_{\phi,n}(\gamma_{\phi(t,n)} - b_{\phi,n})}} \ \forall \phi \in \Phi. \tag{5.1}$$

Here, γ_ϕ denotes the FA expansion factor of classifier ϕ, representing the minimum scaling required for the FA to place the PSSV, $x_{t,n}$, on its boundary while preserving the exact similitude geometry of the classifier. The FA expansion factor is defined by (5.2).

$$\begin{aligned} &\gamma_{\phi(t,n)} = \frac{Area_{\phi(t,n)}|_{x=x_{t,n}}}{Area_{\phi(t,n)}|_{x\in\mathcal{S}^{FA}}} \\ &\text{Such that: } d(f(x^R), f(x^I)) = d(x^R, x^I) \ \forall x \in \mathcal{S}^{FA} \end{aligned} \tag{5.2}$$

where $f(x)$ is a linear transformation function. An expansion factor $\gamma_{\phi(t,n)} > 1$ indicates that the PSSV, $x_{t,n}$, lies outside the expected FA. As $\gamma_{\phi(t,n)}$ increases, the distance from the FA boundary also increases, indicating a higher likelihood of abnormal operation and a potential cyberattack. Conversely, when $\gamma_{\phi(t,n)} < 1$, the PSSV lies within the expected FA, and smaller values of $\gamma_{\phi(t,n)}$ indicate a higher probability of healthy operation. The transition between healthy and attacked states is controlled by the sigmoid-expansion parameters $a_{\phi,n}$ and $b_{\phi,n}$. The estimation of the FA for each classifier ϕ, together with the computation of the corresponding spatial distribution features using the expansion factors, is presented in the following sections.

5.2.1.1 Spatial Distribution of Rectangular Feasibility Area

The rectangular classifier, ϕ_{Rec}, is constructed by estimating the minimum and maximum values of the real and imaginary components ($x_{t,n}^{R,\min}$, $x_{t,n}^{I,\min}$, $x_{t,n}^{R,\max}$, $x_{t,n}^{I,\max}$), as described in Section 3.4.2.1. Once these parameters are obtained, the corresponding expansion factor, $\gamma_{\phi_{Rec}(t,n)}$, for the current PSSV, $x_{t,n}$, is computed as follows:

$$\gamma_{\phi_{Rec}(t,n)} = Max : \begin{cases} \frac{\left|x_{t,n}^{R} - 0.5(x_{t,n}^{R,max} + x_{t,n}^{R,min})\right|}{0.5(x_{t,n}^{R,max} - x_{t,n}^{R,min})} \\ \frac{\left|x_{t,n}^{I} - 0.5(x_{t,n}^{I,max} + x_{t,n}^{I,min})\right|}{0.5(x_{t,n}^{I,max} - x_{t,n}^{I,min})} \end{cases} \tag{5.3}$$

5.2.1.2 Spatial Distribution of Circular Feasibility Area

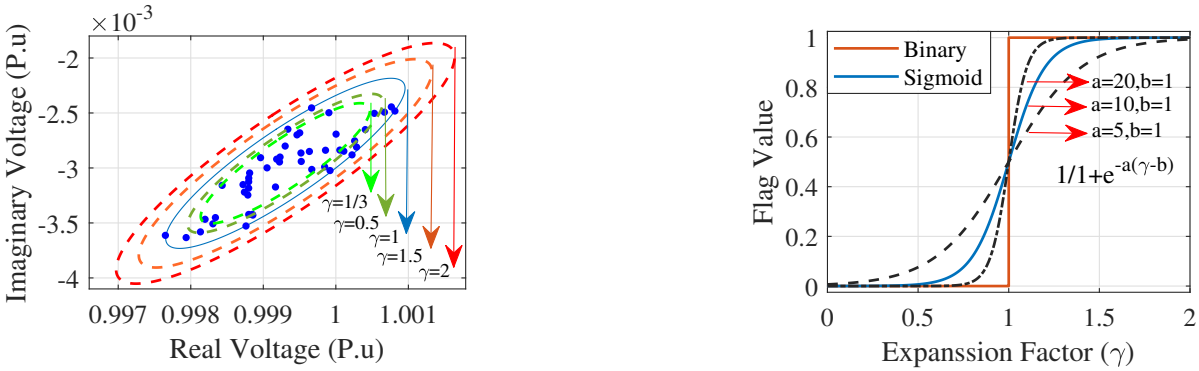
The circular classifier, ϕ_{Cir}, is defined by estimating the center and radius of the circle, as discussed in Section 3.4.2.2. Once these parameters are obtained, the corresponding expansion factor, $\gamma_{\phi_{Cir}(t,n)}$, for the current PSSV, $x_{t,n}$, is computed using (5.4).

$$\gamma_{\phi_{Cir}(t,n)} = \frac{(x_{cen(t,n)}^{R} - x_{t,n}^{R})^2 + (x_{cen(t,n)}^{I} - x_{t,n}^{I})^2}{r_{t,n}^2} \tag{5.4}$$

5.2.1.3 Spatial Distribution of Elliptic Feasibility Area

The elliptic classifier, ϕ_{Ell}, is defined by the center vector of the ellipse, $C_{t,n}^{Ell}$, and the shape matrix, $A_{t,n}^{Ell}$, as discussed in Section 3.4.2.3. Once these parameters are estimated, the corresponding expansion factor, $\gamma_{\phi_{Ell}(t,n)}$, for the current PSSV, $x_{t,n}$, is computed using (5.5).

$$\gamma_{\phi_{Ell}(t,n)} = (x_{t,n} - C_{t,n}^{Ell})^T A_{t,n}^{Ell} (x_{t,n} - C_{t,n}^{Ell}) \tag{5.5}$$



(a) Expansion factor

(b) Sigmoid VS Binary flag

Figure 5.1: Spatial distribution of PSSV using expansion factor and sigmoid-expansion flag.

5.2.1.4 Spatial Distribution of Convex-Hull Feasibility Area

The convex-hull classifier is constructed by generating a polygon that encloses the historical samples $\mathcal{S}^{FA}$ within the past M^{FA}-hour window, as described in Section 3.4.2.4. Once the boundary points of the convex-hull are determined, the corresponding expansion factor, $\gamma_{\phi_{CH}(t,n)}$, for the current PSSV, $x_{t,n}$, is computed using (5.6).

$$\gamma_{\phi_{CH}(t,n)} = \frac{\sqrt{(x_{t,n}^{cnt,R} - x_{t,n}^{R})^2 + (x_{t,n}^{cnt,I} - x_{t,n}^{I})^2}}{\sqrt{(x_{t,n}^{cnt,R} - x_{t,n}^{itr,R})^2 + (x_{t,n}^{cnt,I} - x_{t,n}^{itr,I})^2}} \tag{5.6}$$

Here, $x_{t,n}^{cnt}$ represents the center of gravity (centroid) of the convex-hull polygon, which is calculated using (5.7).

$$\begin{aligned} x_{t,n}^{cnt,R} &= \frac{\sum_{\tau}(x^{R}, n_{\tau} + x_{\tau+1,n}^{R}).(x_{\tau,n}^{R}.x_{\tau+1,n}^{I} - x_{\tau+1,n}^{R}.x_{\tau,n}^{I})}{3\sum_{\tau}(x_{\tau,n}^{R}.x_{\tau+1,n}^{I} - x_{\tau+1,n}^{R}.x_{\tau,n}^{I})} \\ x_{t,n}^{cnt,I} &= \frac{\sum_{\tau}(x_{\tau,n}^{I} + x_{\tau+1,n}^{I}).(x_{\tau,n}^{R}.x_{\tau+1,n}^{I} - x_{\tau+1,n}^{R}.x_{\tau,n}^{I})}{3\sum_{\tau}(x_{\tau,n}^{R}.x_{\tau+1,n}^{I} - x_{\tau+1,n}^{R}.x_{\tau,n}^{I})} \\ \tau &\in \{1, 2, ..., |SV_{t,n}^{CH}| - 1\}. \end{aligned} \tag{5.7}$$

$x_{t,n}^{itr}$ is the intersection point between the line $\overline{x_{t,n}^{cnt} x_{t,n}^{out}}$ and the convex-hull polygon, with both points subject to the following condition.

$$x_{t,n} \in (1-\zeta)x_{t,n}^{cnt} + \zeta x_{t,n}^{out}, \text{ where } 0 \leq \zeta \leq 1 \tag{5.8}$$

5.2.1.5 Spatial Distribution of Single Class SVM Feasibility Area

For the single-class SVM, the model coefficients are represented by $\alpha_{\tau,n}$, as explained in Section 3.4.2.5. The corresponding expansion factor, $\gamma_{\phi_{SVM}(t,n)}$, for the current PSSV, $x_{t,n}$, is

computed using (5.9).

$$\gamma_{\phi_{SVM}(t,n)} = \sum_{\tau \in \mathcal{S}^{FA}} \alpha_{\tau,n}.e^{-\lambda_{t,n}|x_{t,n}-x_{\tau,n}|^2} \tag{5.9}$$

For illustration purposes, Figures 5.1a and 5.1b demonstrate the effect of the expansion factor on an elliptical FA, together with the resulting sigmoid-expansion flag, compared with the conventional binary flag. The healthy samples $\mathcal{S}^{FA}$, shown as blue dots, represent the system voltage phasor measurements generated from the previous 48-hour operating window.

5.2.2 Optimal Tuning of Combined Sigmoid-Expansion Deep Neural Network

The sigmoid-expansion flag parameters, $a_{\phi,n}$ and $b_{\phi,n}$, play a key role in determining the probability of classifying a given PSSV as either healthy or under attack. Since each PSSV exhibits a distinct FA boundary, these parameters are node-specific and must be carefully calibrated. Moreover, they are designed to be compatible with the DNN framework to enable effective learning of hidden patterns associated with stealthy FDIAs. Accordingly, $a_{\phi,n}$ and $b_{\phi,n}$ are jointly optimized with the DNN parameters θ using stochastic gradient descent and backpropagation to ensure stable convergence and improved classification performance.

A general DNN consists of L layers, each defined by a weight matrix W_l and a bias vector b_l, forming the overall parameter set $\theta = \{(W_1, b_1), \ldots, (W_L, b_L)\}$. The training process of the DNN involves four main stages: 1) forward propagation, 2) loss computation, 3) backpropagation, and 4) parameter updates. During forward propagation, the output of each layer l is computed, as mathematically described in (5.10).

$$A_l = \sigma(z_l),\ where\ z_l = W_l A_{l-1} + b_l \tag{5.10}$$

For the input layer, the activated output is $A_0 = Fg_t^{Sig}$, where Fg_t^{Sig} represents the aggregated sigmoid-expansion flag values. The output of the final layer, $A^{(L)}$, yields the predicted state $\hat{\xi}$, indicating whether the system is in a healthy or compromised (attacked) state.

For the classification tasks, the cross-entropy loss function is used to measure the difference between the predicted output $\hat{\xi}$ and the actual target ξ, which defined as follow:

$$L(\xi, \hat{\xi}) = -\sum_{i=1}^{\Xi} \xi_i \log(\hat{\xi}_i) \tag{5.11}$$

Backpropagation is then used to minimize the loss function, by calculating the gradients of the loss with respect to the DNN parameters θ for each layer defined by (5.12)

$$\frac{\partial L}{\partial W_l} = \frac{\partial L}{\partial A_l} \cdot \sigma'(z_l) \cdot A_{l-1}^T, \ \frac{\partial L}{\partial b_l} = \frac{\partial L}{\partial A_l} \cdot \sigma'(z_l) \tag{5.12}$$

Here, $\sigma'(z_l)$ is the derivative of the activation function. The error term for each layer is propagated backward from the output layer to the input layer. Once the gradients have been calculated, the weights and biases are updated using stochastic gradient descent as follow:

$$W_l \leftarrow W_l - \xi \frac{\partial L}{\partial W_l}, \ b_l \leftarrow b_l - \xi \frac{\partial L}{\partial b_l} \tag{5.13}$$

To integrate the tuning of the sigmoid-expansion flag parameters $a_{\phi,n}$ and $b_{\phi,n}$ with the DNN model, the backpropagation process is extended to include the flag equation. This involves calculating how the loss changes with respect to the parameters of the sigmoid-expansion flag by computing the gradients of the loss with respect to $a_{\phi,n}$ and $b_{\phi,n}$, as shown below:

$$\begin{aligned} \frac{\partial L}{\partial a} &= \frac{\partial L}{\partial Fg^{Sig}} \cdot \frac{e^{-a(\gamma-b)} \cdot (\gamma - b)^T}{Fg^{Sig}} \\ \frac{\partial L}{\partial b} &= \frac{\partial L}{\partial Fg^{Sig}} \cdot \frac{-ae^{-a(\gamma-b)}}{Fg^{Sig}} \end{aligned} \tag{5.14}$$

After calculating the gradient of the loss with respect to the sigmoid-expansion flag parameters, these parameters can be updated using stochastic gradient descent to improve the detection performance of the combined sigmoid-expansion flag and DNN. The update is performed as shown in (5.15).

$$a \leftarrow a - \xi \frac{\partial L}{\partial a}, \ b \leftarrow b - \xi \frac{\partial L}{\partial b} \tag{5.15}$$

5.2.3 Feasibility Area Temporal Correlation Property

The temporal correlation quantifies the contribution of previous operating states within the historical window M^{FA} in defining a the FA of the current PSSV, $x_{t,n}$. Under ideal deterministic operation, the EMS and OPF of the central control unit in the SPS should yield identical results when the system operates under identical conditions, including the same demand, the same RES generation, and identical primary information I_t^P. In such cases, similar operating conditions should correspond to similar operation states $\mathbb{X}_t$. Given the periodic nature of SPS demand profiles and the daily load pattern over a 24-hour cycle, not all historical samples in $\mathcal{S}^{FA}$ contribute equally to defining the FA of the current PSSV, $x_{t,n}$. Therefore, instead of assigning uniform weights to all historical states, greater importance is given to samples that exhibit

higher similarity to the current operating condition, improving the representativeness of the FA construction.

To quantify the similarity between the current PSSV and previous operating states, cosine similarity is employed to capture the temporal correlation between the current primary information vector I_t^P and historical samples. Here, I_t^P represents the system operating conditions, including expected generation and demand profiles. The cosine similarity vector over the historical window M^{FA} is defined in (5.16) as follows:

$$CS_t^{FA} = \left[\frac{I_t^P \cdot I_\tau^P}{|I_t^P||I_\tau^P|} : \tau \in M^{FA} \right] \in \mathbb{R}^{1\times|M^{FA}|} \tag{5.16}$$

The temporal correlation is incorporated into the FA estimation by applying a cutoff threshold τ^{CS}, where historical samples with cosine similarity below this threshold are filtered out and removed. This enforces a stricter FA estimation by retaining only samples with sufficiently high similarity to the current operating state.

It is worth noting that the cosine similarity metric is computed using the primary information vectors of the current expected operating condition and historical operating states under the same network configuration. Consequently, the similarity measure and its corresponding threshold are configuration dependent. When the system topology changes due to network reconfiguration or equipment outages, the operating characteristics also change, requiring the cosine similarity threshold to be re-evaluated and updated to accurately reflect the new operating conditions.

5.2.4 Recursive Feasibility Area Estimation Algorithm

One of the main limitations of the proposed FA framework is the computational effort associated with the classifier parameter estimation stage. Although each classifier is estimated by solving a relatively small optimization problem over a limited number of samples, the FA parameters must be computed for every PSSV and for each classifier. Consequently, the overall computational complexity scales approximately linearly with the size of the SPS, primarily with the number of buses and branches.

To improve computational efficiency, two approaches are proposed. First, after training the FA-PRNN, the weights of the DNN input layer are analyzed to identify the set of effective PSSVs. Variables associated with small input weights contribute less to cyberattack detection and can therefore be excluded from the FA estimation process. Second, a recursive FA estimation

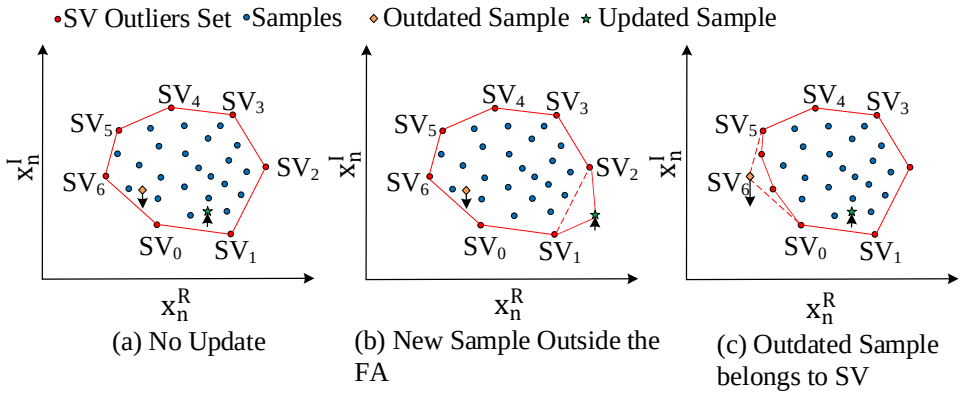


Figure 5.2: Illustration of recursive FA estimation for convex-hull

algorithm is introduced, where the classifier parameters are re-estimated only when significant changes in the operating condition are detected. Otherwise, the current FA parameters are updated recursively from the previous estimate, which is expressed as

$$\phi_{t,n} = \kappa \cdot \phi_{t-1,n} + (1-\kappa) \cdot [x^R_{t,n} \quad x^I_{t,n}]^T \tag{5.17}$$

where κ is the recursive update factor that controls the contribution of the previous FA parameters, $\phi_{t-1,n}$, relative to the current PSSV, $[x^R_{t,n} \quad x^I_{t,n}]^T$. Larger values of κ place greater emphasis on the previous FA estimate, whereas smaller values allow the classifier to adapt more rapidly to changes in the operating condition.

The proposed recursive FA estimation algorithm can be divided into two cases based on the FA classifier. First case, FA estimation based on outliers. This case involves classifiers that mainly defined by their outlier point (i.e, rectangular and convex-hull). Second case is classifiers that depends on the entire distribution of the historical samples $\mathcal{S}^{FA}$. Each algorithm is described within the following section.

5.2.4.1 Outliers-Based Recursive Feasibility Area Estimation Algorithm

Both the rectangular and convex-hull FA classifiers, ϕ_{Rec} and ϕ_{CH}, are defined by their boundary/outliers points (i.e., $x^{R,min}_{t,n}$, $x^{I,min}_{t,n}$, $x^{R,max}_{t,n}$, $x^{I,max}_{t,n}$, and $SV^{CH}_{t,n}$). Consequently, their parameters only need to be updated when these boundary points change. Since the FA is constructed from the historical window M^{FA}, represented by the sample set $\mathcal{S}^{FA}$, each new time step t introduces an updated sample, $s^{Updated} = \{x^R_{t-1,n}, x^I_{t-1,n}\}$, while the oldest sample, $s^{Outdated} = \{x^R_{t-M^{FA}-1,n}, x^I_{t-M^{FA}-1,n}\}$, is removed.

Algorithm 5 Recursive FA Update

1: Obtain $s^{Updated}$ and $s^{Outdated}$
2: **if** $s^{Updated} \notin \phi_{t-1}$ **or** $s^{Outdated}$ is a boundary point of ϕ_{t-1} **then**
3: Initialize the classifier using ϕ_{t-1}
4: Re-estimate the FA parameters
5: **else**
6: Set $\phi_t \leftarrow \phi_{t-1}$
7: **end if**

Accordingly, the rectangular and convex-hull FA parameters are re-estimated only under one of the following conditions:

1. The newly added sample lies outside the previous FA, i.e., $s^{Updated} \notin \phi_{t-1}$, indicating that the classifier boundary must be expanded to include the new operating point.

2. The removed sample is one of the boundary points defining the previous FA, i.e.,

$$s^{Outdated} \in \{x_{t-1,n}^{R,min}, x_{t-1,n}^{I,min}, x_{t-1,n}^{R,max}, x_{t-1,n}^{I,max}\}$$

for the rectangular classifier, or

$$s^{Outdated} \in \{SV_{t-1,n}^{CH}\}$$

for the convex-hull classifier, requiring the boundary to be recomputed.

Figure 5.2 illustrates these update conditions. In case a), both the updated and outdated samples lie inside the FA estimated at time $t-1$, indicating that no parameter update is required. In case b), the newly added sample is located outside the previous FA, requiring the classifier boundary to be expanded to include the new operating point. In case c), the removed sample is one of the boundary points defining the FA, and therefore the classifier parameters must be re-estimated. *It can be observed that the FA geometry changes only locally*, with most modifications occurring around $s^{Updated}$ and $s^{Outdated}$ in the complex plane. *Consequently, a practical implementation is to initialize the FA estimation at time t using the classifier parameters obtained at time* $t-1$, thereby significantly reducing the computational effort. Table 5 shows the recursive update procedure for the rectangular and convex-hull FA classifiers.

5.2.4.2 Samples Distribution-Based Recursive Feasibility Area Estimation Algorithm

In contrast to the outlier-based classifiers, the circular, elliptic, and single-class SVM classifiers, ϕ_{Cir}, ϕ_{Ell}, and ϕ_{SVM}, are defined by the entire distribution of the FA sample set $\mathcal{S}^{FA}$. Consequently, their parameters are influenced by both the newly added and outdated samples, $s^{Updated}$ and $s^{Outdated}$. However, these two samples constitute only a small fraction of the historical dataset, i.e., $\frac{2}{|\mathcal{S}^{FA}|}$, and therefore have a negligible effect on the overall FA geometry. As observed in the previous section, the classifier parameters vary only slightly between consecutive time steps. Accordingly, to reduce the computational burden of solving the optimization problems in (3.43)–(3.46), the FA parameters estimated at time $t-1$ are used as the initial solution for the optimization at time t. Since this initial point is already close to the optimal solution, the optimization converges significantly faster while maintaining the same estimation accuracy.

5.3 Numerical Results

5.3.1 Test System and Simulation Environment

The IEEE 30-bus test system, shown in Figure 5.3, is adopted as the SPS simulation testbed for evaluating the proposed framework under OPF operation. The system is simulated over a one-year period with an hourly resolution ($\Delta t = 1$ h), resulting in a healthy-operation dataset of $\tau^{HL} = 8,760$ samples generated using Ontario electricity market data from 2022. The placement of PMUs and SCADA measurements follows the configuration presented in Section 3.5.1. The proposed advanced FA framework is employed to detect and estimate stealthy FDIAs targeting the primary information of the SE and to assess their impact on the OPF operation. The stealthy FDIAs are designed to maximize the mismatch in RES generation measurements, thereby misleading the OPF decision-making process and degrading its optimality. The attacks primarily target the RES measurements at Buses 3, 7, and 25.

Figure 5.4 illustrates the simulation framework and data preparation procedure. At each time step t, the system operating conditions are first loaded, and the healthy PSSVs are generated by applying the unmodified primary information to the SE and OPF framework. The resulting operating states are stored in the healthy PSSV dataset. For cyberattack scenarios, the primary

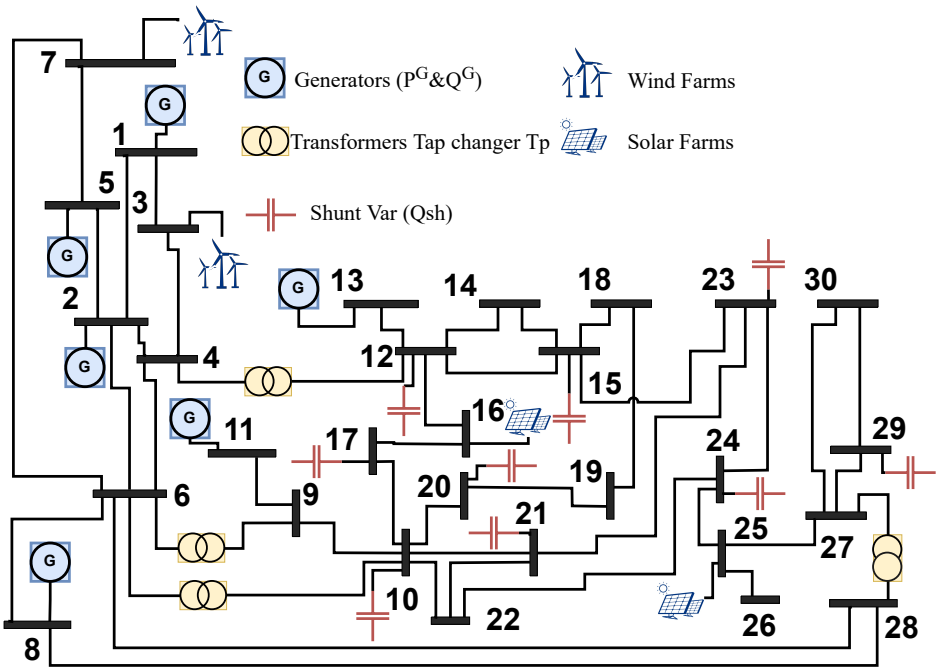


Figure 5.3: The IEEE 30-bus transmission system employed for numerical studies showing OPF control units.

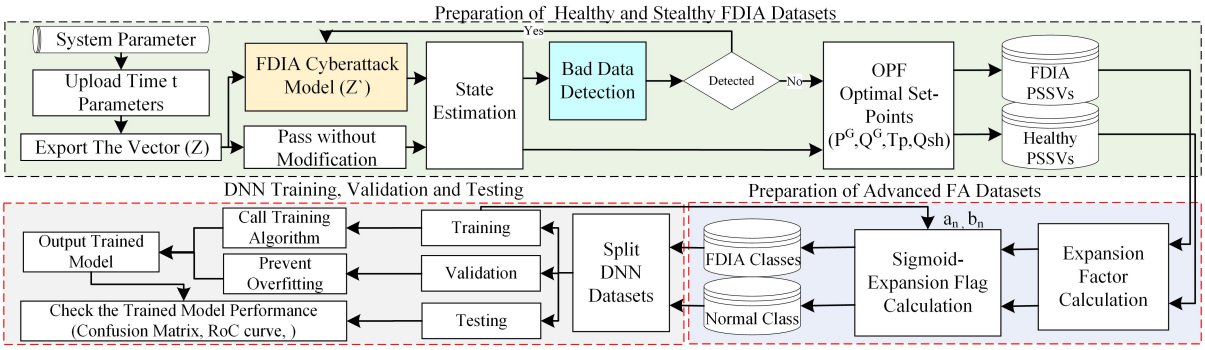


Figure 5.4: Healthy and stealthy FDIAs scenario generation flowchart.

information is manipulated using stealthy FDIAs designed to bypass the BDD while creating misleading operating conditions. If an attack is detected by the BDD, a new attack vector with a reduced manipulation magnitude is generated until a stealthy attack is achieved. A total of 12 stealthy FDIA scenarios are considered, including single-, double-, and triple-bus attacks with manipulation magnitudes ranging from 2.5% to 15%, resulting in an attack dataset of $\tau^A = 14,400$ samples. The corresponding operating states are stored in the compromised PSSV dataset.

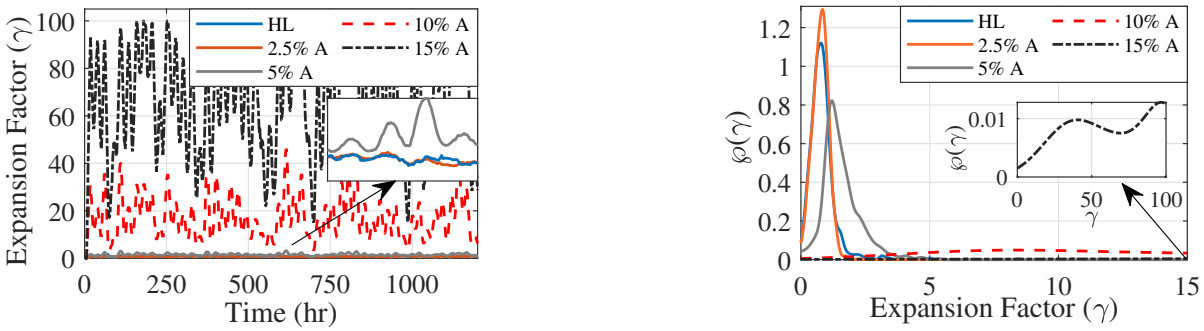
For the studied SPS, the bus voltage phasors, injected currents, and injected complex apparent powers are used as PSSVs. For each transmission line, the sending-end and receiving-end currents, together with the corresponding complex apparent power measurements, are considered. Consequently, three and four PSSVs are defined for each bus and transmission line, respectively. All simulations are performed on an Intel Core i9 (12th Generation, 2.1 GHz) workstation with 32 GB of RAM.

5.3.2 Performance of Advanced Feasibility Area with Spatial Distribution Property

To evaluate the effect of incorporating spatial distribution properties, this section investigates the ability of the expansion factor γ_ϕ to provide information beyond binary detection, particularly its correlation with stealthy FDIA attack vectors.

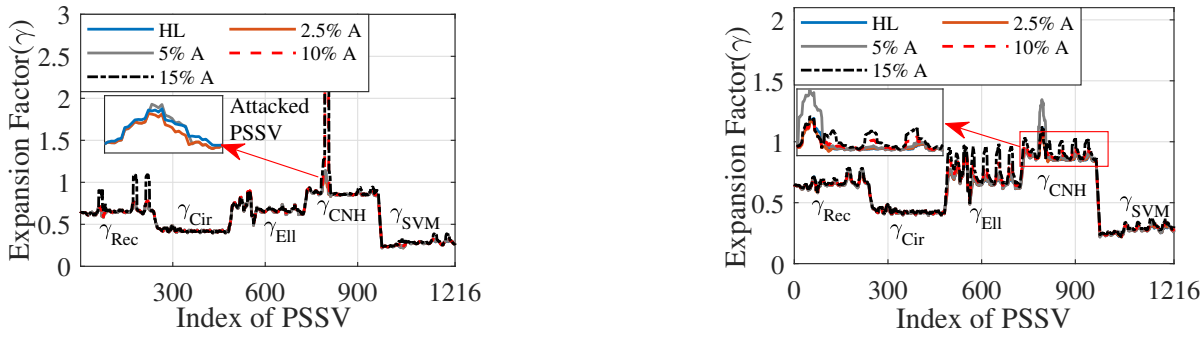
Figure 5.5a shows the evolution of the average expansion factor under different attack magnitudes during system operation. The results indicate that, under stealthy FDIA, the expansion factor increases, reflecting a higher likelihood of classifying the corresponding PSSV as compromised. Moreover, the expansion factor exhibits a monotonic increase with the attack magnitude. This behavior is further confirmed in Fig. 5.5b, which presents the probability density function (PDF) of the expansion flag. During healthy operation, the expansion factor is mainly concentrated between 0 and 1.5, whereas under a 5% single-bus attack, it shifts to the range of 0.5 to 4.5. The mean expansion factor values are 0.8557, 0.86, 1.56, 17, and 66 for healthy operation, and 2.5%, 5%, 10%, and 15% attack scenarios, respectively. Unlike conventional binary flag FA approaches, the proposed spatial distribution-based formulation establishes a strong relationship between the expansion factor magnitude and the attack severity, thereby enhancing the interpretability and characterization of stealthy FDIA attacks.

Figure 5.6 presents the expansion factor values of each PSSV under different classifiers $\phi \in \Phi$ for single- and double-bus attack scenarios across varying attack magnitudes. It is observed that, for all PSSVs, the expansion factor increases under attack conditions regardless of the classifier used. However, the convex-hull FA classifier exhibits the highest sensitivity to cyberattacks, with the most pronounced variations in the expansion factor. Furthermore, compromised PSSVs show distinct peak deviations in the expansion factor, as highlighted in Figure 5.6a. This indicates that the proposed spatial distribution property can effectively localize attacked buses by identifying PSSVs with the largest expansion variations. Figure 5.6b further demonstrates



(a) (b)

Figure 5.5: Variation the expansion factor values under different attack magnitudes. a) Expansion factor versus time of operation b) PDF of the PSSVs expansion factor.

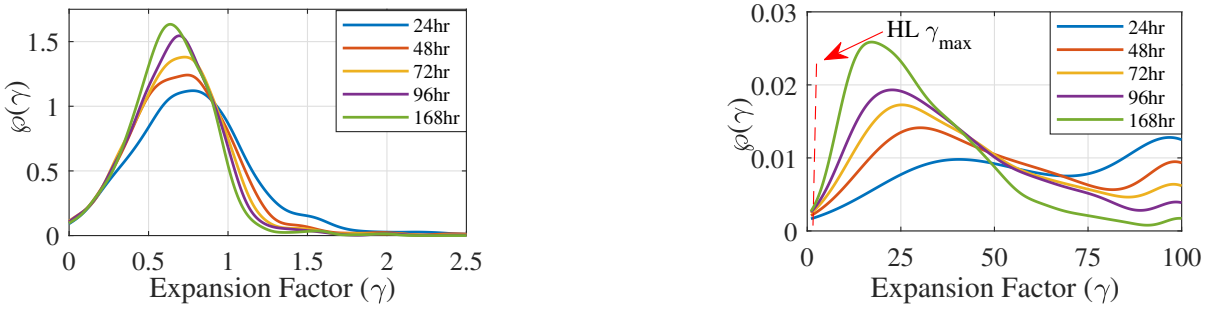


(a) (b)

Figure 5.6: Expansion factor values at different FA classifiers ϕ under a) Single bus attack, and b) Double bus attacks.

that as the number of attacked buses increases, the number of PSSVs exhibiting significant expansion factor deviations also increases. Overall, this capability enables the advanced FA framework to infer both the number and location of attacked buses, thereby providing richer attack characterization compared to traditional detection approaches.

It is worth noting that the selection of the historical window size M^{FA} has a direct impact on both the accuracy of FA representation and the computational burden of FA estimation. From a representation perspective, a small window may fail to capture the underlying historical patterns of the PSSVs, potentially leading to false alarms where normal operating conditions are misclassified as stealthy FDIAs. In contrast, a large window includes outdated operational information, which unnecessarily enlarges the FA boundary, reduces the separability between healthy and attack states, and increases computational complexity during FA estimation. Fig-



(a) Healthy operation

(b) FDIA operation

Figure 5.7: The impact of size of the past M-hours window on the expansion factor.

ure 5.7 illustrates this trade-off by presenting the expected expansion factor under healthy and stealthy FDIA conditions for different window sizes. As the window size increases, the FA becomes less sensitive, resulting in a reduced expansion factor. For excessively large windows, the expansion factor distributions of healthy and attacked cases begin to overlap, reducing the discriminative capability of the DNN. Conversely, very small windows produce overly tight FA boundaries, which can also increase overlap due to elevated expansion factors under normal operation. From a computational perspective, increasing M^{FA} raises the number of constraints involved in FA estimation, thereby increasing computational effort, even though the number of decision variables remains unchanged. Therefore, the optimal window size should maximize the separation margin between healthy and attack expansion factors while preserving computational efficiency. In this work, a window size in the range of 24 to 168 hours is adopted, as it provides a balanced trade-off between detection performance and computational cost.

5.3.3 Performance of Advanced Feasibility Area with Temporal correlation Property

To evaluate the effect of incorporating the temporal correlation property, this section investigates the ability of cosine similarity to identify the most relevant historical operating states for improving the accuracy of the FA.

Figure 5.8 illustrates the temporal correlation obtained using cosine similarity over a 168-hour historical window with respect to the current operating state $x_{t,n}$. The results indicate that previous operating states do not correlate with the current condition, as higher similarity is consistently observed in a clear 24-hour periodic pattern. Specifically, at time t, the maximum

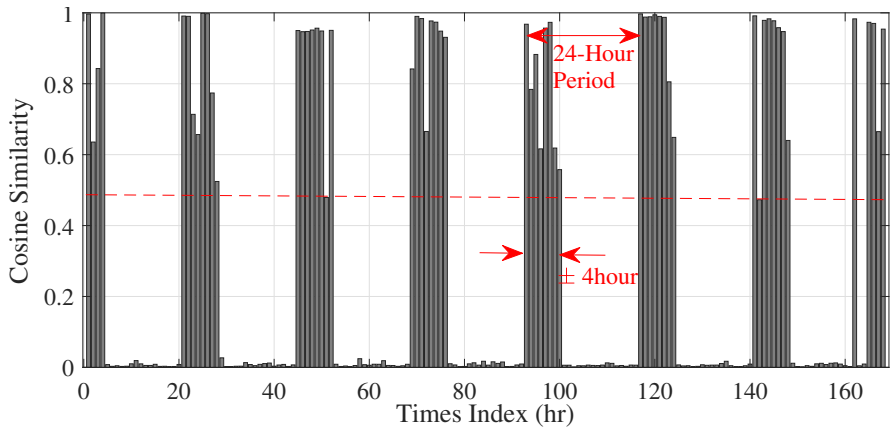


Figure 5.8: Cosine similarity and temporal correlation evaluated over a historical one-week window (168 hours), highlighting the operating states with the highest similarity to the current PSSV.

similarity values occur within the interval $t - 24D - 4$ to $t - 24D + 4$ hours, where D denotes the number of past days. In other words, the strongest correlation is observed between the same time of day across different days, with an effective similarity band of approximately ± 4 hours.

This observation confirms that the temporal structure of the system is highly periodic, and exploiting this property allows the FA framework to assign higher importance to historically aligned operating states, thereby improving boundary estimation and overall detection precision. Figure 5.9 illustrates the complex-plane representation for Bus 2 over a 48-hour historical window. As shown in the left plot, the current operating state (red star) is located closer to previous operating states with higher similarity, primarily due to similar operating conditions, while states with lower similarity are positioned further away in the complex plane. This representation can be extended to a 3D formulation, where the third axis is defined as $1 - CS_t^{FA}$, such that higher similarity points are located closer to the current operating state, and lower similarity points are mapped further away. In this space, the horizontal surface represents the similarity threshold τ^{CS}, which is used to filter low-similarity historical states (i.e., points lying above the threshold plane). Thus, temporal correlation enables the construction of a more precise FA by selecting the most relevant historical samples for FA representation.

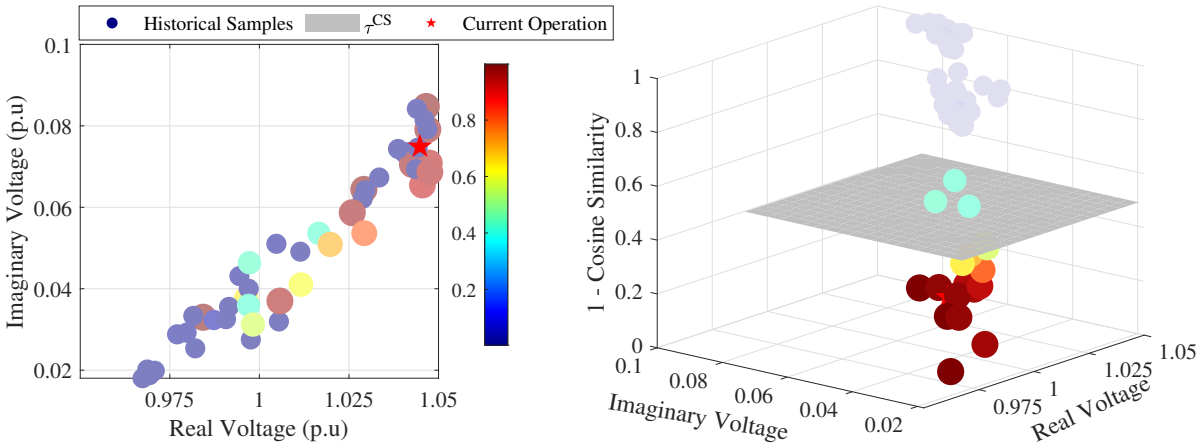


Figure 5.9: Complex plane representation of the PSSV under healthy considering temporal correlation and cosine similarity.

5.3.4 Performance of Recursive Feasibility Area Estimation Algorithm

The proposed recursive FA parameter estimation algorithm is introduced to reduce the computational burden of the FA estimation stage. Table 5.1 compares the average estimation time of each FA classifier with and without the proposed recursive strategy. Without recursion, the average estimation time increases with the FA window size M^{FA}, primarily due to the larger number of constraints associated with the increased number of historical samples $\mathcal{S}^{FA}$. For small window sizes (i.e, 24 hours), all classifiers require approximately 30 ms to estimate the FA for a single PSSV, resulting in a total estimation time of approximately $t_\phi|\Phi||\mathbb{X}|/N^{Cores} = 30 \times 5 \times 254/12 \approx 3$ s.

In contrast, the proposed recursive algorithm reduces the computational time by approximately one order of magnitude (10–12×). This improvement depends on the classifier type. For distribution-based classifiers, the computational time is consistently reduced by nearly a factor of ten across all window sizes, as initializing the optimization with the previous solution enables much faster convergence. For outlier-based classifiers, namely the rectangular and convex-hull classifiers, the computational gain is even greater and scales approximately with the ratio $\frac{|SV|}{|\mathcal{S}^{FA}|}$, where $|SV|$ denotes the number of outlier (support) points. As the historical window increases, the probability that the newly added or removed sample belongs to the set of outlier points becomes progressively smaller. Consequently, FA re-estimation is required less frequently, leading to a substantial reduction in computational effort.

Table 5.1: Computational effort of the FA parameter estimation using traditional and recursive estimation algorithm

Classifier			ϕ_{Rec}	ϕ_{Cir}	ϕ_{Ell}	ϕ_{CH}	ϕ_{SVM}
Computational Effort			$O(n)$	$O(n)$	$O(n)$	$O(nlog(n))$	$O(2n)$
Operation Time (msec)	M^{FA}=24	Traditional	30	30	29.5	29.5	35
		Recursive	1.3	3.2	3	1.4	3.6
	M^{FA}=48	Traditional	34	31.5	31	32	52.5
		Recursive	0.8	3.4	3.3	0.9	6.2
	M^{FA}=168	Traditional	58	61	60	59	94
		Recursive	0.4	5.9	5.7	0.5	9
	Overall Computational Effort (msec)		$N.\sum_{\phi\in\Phi} O(\phi) = N.O(n(5+log(n)))$				

5.3.5 Performance of Stealthy False Data Injection Attack Features Extraction Using Proposed Advanced Feasibility Area

To extract the key characteristics of stealthy FDIAs, two DNN-based approaches are investigated. First, a multi-class classification DNN is developed, where each class represents a specific attack scenario defined by the attack magnitude, the attacked buses, and the number of compromised buses. Second, a regression DNN is designed to estimate the attack magnitude at each bus, directly identifying the attack magnitude, the attacked buses, and the total number of compromised buses. The architectures of both DNN models are illustrated in Figure 5.10.

Figure 5.11 compares the training and validation performance of the DNN using three different input schemes. The first, denoted as W/O FA, directly uses the PSSVs and represents the conventional approach adopted in most previous studies [1]. The second, Traditional FA (TFA), employs the binary flag representation proposed in [229], [246]. The third, the proposed Advanced FA (AFA), uses the sigmoid-expansion flag as the DNN input.

As shown, the detection performance of all three approaches improves as the stealthy FDIA magnitude increases. However, the W/O FA model exhibits poor detection capability for attack magnitudes below 15%. In contrast, both TFA and AFA successfully detect attacks with magnitudes as low as 2.5%, demonstrating their sensitivity to subtle deviations caused by single-bus attacks. Moreover, both FA-based approaches converge significantly faster than the W/O FA model, with AFA achieving the fastest convergence and the highest learning efficiency. The

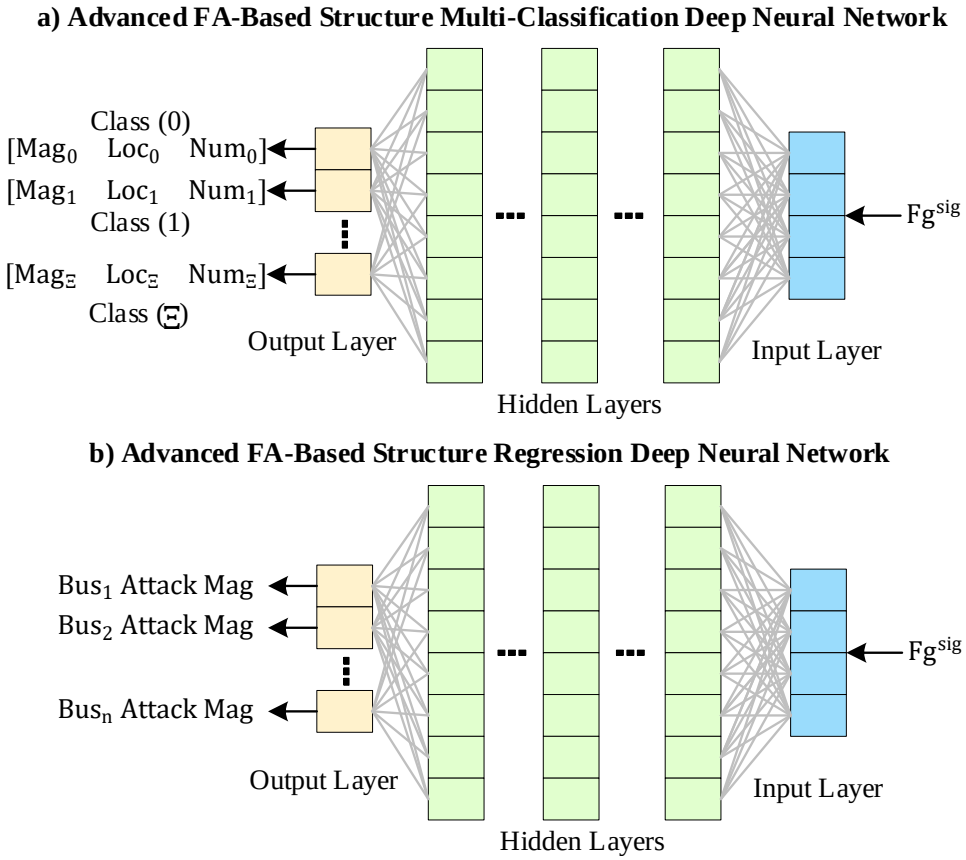
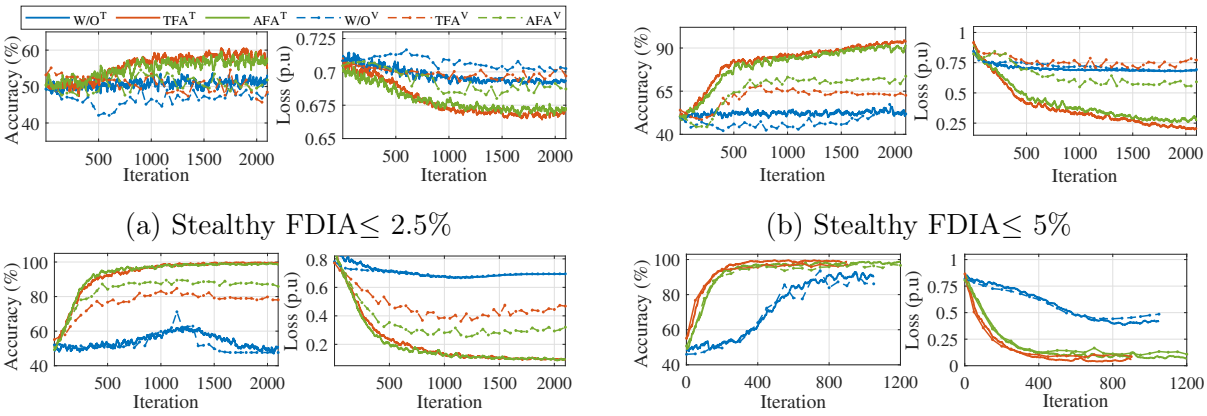


Figure 5.10: Extraction of stealthy FDIA characteristics using a) Multi-classification DNN, b) Regression DNN.

proposed AFA improves the detection accuracy by approximately 11% over TFA for attack magnitudes below 5%. Although this performance gap decreases as the attack magnitude increases, AFA consistently achieves the best overall results.

It is worth noting that for attack magnitudes of $\leq$ 2.5%, the PSSVs under healthy and compromised conditions remain nearly identical and have negligible impact on the OPF. Consequently, neither the raw PSSVs, binary flags, nor sigmoid-expansion flags contain sufficiently discriminative information for the DNN to learn meaningful attack patterns. As a result, the classifier effectively performs random guessing, which is reflected by the validation accuracy oscillating around the 50% baseline in Figure 5.11a. Figure 5.12 presents the confusion matrices of the DNN for distinguishing between healthy operation and different stealthy FDIA scenarios. When the PSSVs are directly used as the DNN input (W/O FA), the model correctly identifies 89.7% of healthy samples but achieves an overall attack classification accuracy of only 71.3%.



(a) Stealthy FDIA≤ 2.5%

(b) Stealthy FDIA≤ 5%

(c) Stealthy FDIA≤ 10%

(d) Stealthy FDIA≤ 15%

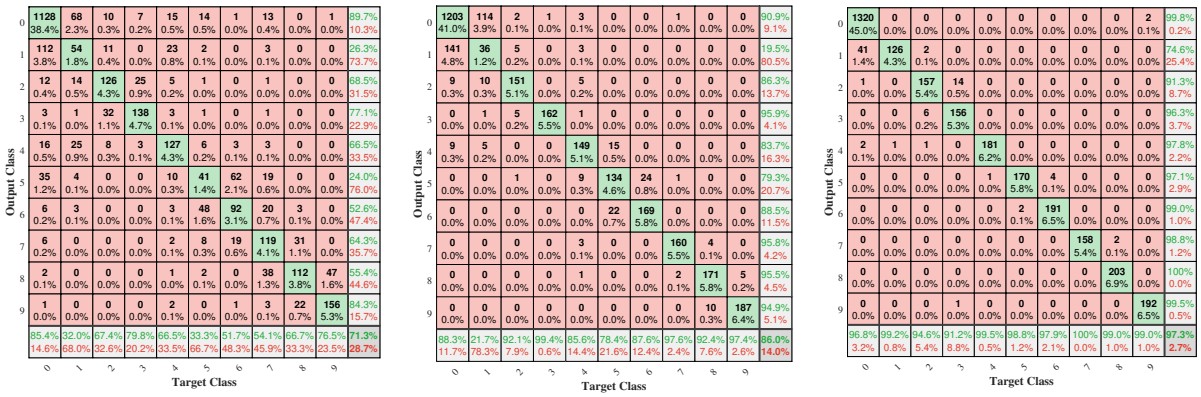
Figure 5.11: DNN training performance for detection of stealthy FDIA using basic PSSVs features (W/O), traditional FA (TFA), and proposed advanced FA (AFA) under different attacks magnitude value. T: training, V: validation.

For example, Class 1 (a single-bus attack with a 5% magnitude) is frequently misclassified as healthy, with a detection accuracy of only 26.3%.

Using the Traditional FA TFA binary flag improves the overall classification accuracy to 86%; however, the model still struggles to distinguish low-magnitude attacks, particularly Class 1, from healthy operation. In contrast, the proposed Advanced FA AFA significantly improves the classification performance, achieving an overall accuracy of 97.3%. It correctly identifies 99.8% of healthy samples while accurately distinguishing between different attack scenarios. This improvement is mainly attributed to the strong correlation between the expansion factor and the underlying attack characteristics. In particular, the detection accuracy of Class 1 increases to 74.6%, demonstrating the ability of the proposed AFA to capture subtle attack signatures that are overlooked by both the conventional PSSVs-based approach and the traditional FA.

Figure 5.13 illustrates the training performance of the regression DNN using the proposed AFA framework and its ability to estimate the magnitude of stealthy FDIAs. Figure 5.13a) demonstrates that the proposed AFA enables efficient model training, achieving a root mean square error below 0.5% in attack magnitude estimation and a mean squared error loss below 0.1%.

Figures 5.13b)–5.13d) evaluate the regression DNN over a 24-hour simulation using an unseen attack dataset. The results show that the proposed framework accurately estimates the attack



(a) W/O FA (b) TFA (c) AFA

Figure 5.12: Performance of multi-class detection of DNN to extract features of the stealthy FDIA without FA and with TFA, and the proposed AFA schemes. Classes number (0:healthy), (1,2,3: single bus attack 5,10,15%), (4,5,6: double bus attack 5,10,15%), (7,8,9: triple bus attack 5,10,15%).

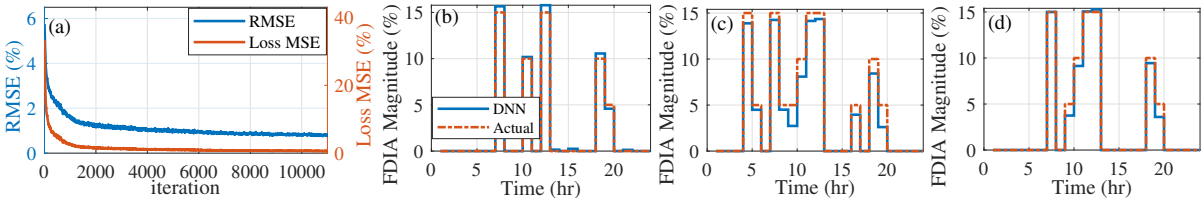


Figure 5.13: Regression DNN performance (a) Training performance (b)-(d) Attack magnitude estimation over Buses 3,7, and 25, respectively.

magnitude at each bus while simultaneously identifying the attacked buses and the total number of compromised buses. These findings demonstrate that integrating spatial distribution and temporal correlation into the advanced FA provides informative features that enable accurate extraction of the stealthy FDIA attack vector.

The capability of the proposed Advanced FA framework to estimate the cyberattack vector is primarily attributed to the introduced spatial distribution property. The proposed expansion factor exhibits a strong correlation with the attack magnitude, while its spatial variation across the PSSVs enables accurate identification of the attacked locations and the number of compromised measurements. In contrast, the temporal correlation property mainly improves the accuracy of the estimated FA by emphasizing historical operating states that closely re-

semble the current operating condition, thereby enhancing the distinction between healthy and attacked operating states. Finally, the proposed recursive FA estimation algorithm significantly reduces the computational effort associated with updating the feasible operating region, enabling efficient real-time implementation without compromising estimation accuracy.

5.4 Summary and Discussion

This chapter advanced the proposed FA framework beyond cyberattack detection toward comprehensive attack characterization, addressing another important research gap identified in this thesis: the limited ability of existing cybersecurity frameworks to extract informative attack features that enable corrective actions after attack detection. While the previous chapters demonstrated the effectiveness of the FA framework in detecting stealthy cyberattacks in both standalone SPSs and interconnected IESs, the framework remained primarily a detection tool. This chapter extended its functionality to estimate critical attack characteristics, including attack magnitude, attack location, the number of compromised measurements, and the corresponding attack vector.

To achieve this objective, two complementary enhancements were introduced into the original FA formulation. First, a spatial distribution property was developed by introducing the expansion factor, which continuously quantifies the distance between the current PSSV and its expected feasible operating region. Unlike the traditional binary FA flag, the expansion factor provides a probabilistic measure of abnormality that preserves valuable information regarding the severity of the operating-state deviation. The results demonstrated a strong monotonic relationship between the expansion factor and attack magnitude, while the largest expansion factor variations accurately identified the attacked PSSVs. Consequently, both the location and the number of compromised measurements could be inferred directly from the operating-state response, enabling attack characterization beyond simple detection.

Second, a temporal correlation mechanism was incorporated to exploit the intrinsic periodic behavior of power system operation. Rather than assigning equal importance to all historical operating samples, cosine similarity was used to identify operating conditions most similar to the current system state based on the primary operating information. The results confirmed a pronounced 24-hour periodic operating pattern, with the highest similarity concentrated within an effective window of approximately ± 4 hours around the corresponding operating instant of

previous days. By emphasizing only the most representative historical samples, the proposed temporal correlation significantly improved the accuracy of the estimated FA, reduced unnecessary expansion of the feasible operating region, and enhanced the separability between healthy and compromised operating states.

The informative features generated by the enhanced FA were subsequently integrated with both multi-classification and regression DNNs. The multi-classification framework successfully distinguished different attack scenarios according to their magnitude, attacked buses, and number of compromised buses, while the regression framework accurately estimated the attack magnitude at each individual bus. Compared with conventional approaches based solely on raw PSSVs or the traditional binary FA, the proposed Advanced FA (AFA) consistently achieved higher detection accuracy, faster convergence, and improved learning efficiency. These results demonstrate that embedding physically meaningful cyber-physical features substantially enhances the ability of deep learning models to understand stealthy cyberattacks rather than merely classify them.

To further support real-time deployment, this chapter also introduced a recursive FA parameter estimation algorithm. Instead of re-estimating the feasible operating region at every sampling instant, the proposed approach updates the FA parameters only when changes in the operating boundary are detected while initializing the optimization using the parameters estimated at the previous time step. Owing to the gradual evolution of system operating conditions, this recursive formulation reduced the computational effort by approximately one order of magnitude (10–12×), significantly improving the scalability of the proposed framework for large-scale smart power systems and future IESs.

Overall, this chapter transformed the proposed FA from a detection-oriented framework into a comprehensive cyber-physical situational awareness tool capable of not only identifying stealthy cyberattacks but also characterizing their critical features in real time. By integrating spatial distribution, temporal correlation, recursive estimation, and deep learning, the proposed Advanced FA establishes a new generation of adaptive cybersecurity frameworks that bridge the gap between cyberattack detection, attack diagnosis, and operational decision support for future smart power systems and integrated energy systems.

Chapter 6

Conclusion and Future Work

6.1 Summary and Conclusions

This thesis developed a comprehensive cybersecurity framework for SPSs and IESs based on the proposed FA concept. The primary objective was to enhance cyber-physical security by addressing several emerging challenges associated with the evolution of modern energy systems. These include: 1) the increasing cyber risks introduced by deep electrification and the growing uncertainties in both demand and renewable generation, which expand the range and sophistication of potential cyberattacks; 2) the strong interdependencies among the cyber and physical layers of interconnected IESs, which enlarge the overall CPS attack surface and create additional entry points for adversaries across multiple infrastructures; and 3) the heterogeneous cybersecurity standards adopted by different IESs, allowing attackers to exploit less secure infrastructures as gateways to compromise otherwise well-protected systems.

The research was further motivated by several limitations of existing cybersecurity approaches. First, most conventional methods are designed primarily to detect basic or stealthy FDIAs within SE applications, with limited applicability to broader cyber-physical operations. Second, current solutions predominantly emphasize attack prevention and detection, providing little support for identifying system manipulation once an attacker has successfully bypassed existing defenses. Third, there is a lack of a unified and adaptive cybersecurity framework capable of addressing the evolving operational characteristics of both standalone SPSs and interconnected IESs. Fourth, existing studies have devoted limited attention to extracting attack characteristics beyond simple detection, such as attack location, magnitude, and affected mea-

surements, which are essential for enabling effective corrective actions. Finally, cyber resilience at the EMS level remains largely unexplored, despite the increasing importance of protecting system operation against sophisticated attacks that extend beyond the scope of traditional SE cybersecurity mechanisms.

To address these challenges, this thesis adopted a comprehensive research methodology spanning from standalone SPSs to integrated smart power and IESs, with particular emphasis on power–gas and power–transportation systems incorporating HRSs. To ensure realistic cyberattack implementation, comprehensive cyber-physical testbeds were developed for both standalone SPSs and IESs. These testbeds incorporate detailed models of the physical infrastructure, communication networks, and cyber-layer components, providing a realistic environment for cybersecurity evaluation. This comprehensive framework enabled the accurate implementation of SICAs, where the proposed *Attack–Wait–and–Observe* strategy was employed to generate successful cyberattacks capable of bypassing all existing cybersecurity layers while remaining stealthy. Within this framework, SICAs were first investigated for standalone SPSs by targeting the primary measurement vector of the SE. The study was subsequently extended to power–gas IESs, where SICAs targeted the secondary information of the gas network, with particular focus on manipulating the setpoints of the coupling PtH and GfG units. For the power–transportation IES, the cybersecurity analysis was extended to the EMS, where stealthy FDIAs, DoS, and coordinated bi-level DDoSs were investigated. These attacks targeted both the primary information of the HRSs and the secondary control setpoints of the coupling PtH and HtP units, enabling a comprehensive assessment of cyberattacks on operational decision-making and energy management.

To detect SICAs and provide an adaptive cybersecurity framework, this thesis proposed a novel FA-based approach, in which a set of complementary FA classifiers is used to characterize the expected operating region of the PSSVs based on historical system behavior. The structure of each classifier is designed according to the underlying operational characteristics of the SPS, enabling an accurate representation of normal operating conditions. Since the FA is continuously estimated using a moving historical window, the proposed framework naturally adapts to recent changes in system dynamics, providing a self-adaptive cybersecurity mechanism. Consequently, the framework is capable of detecting abnormal operating state variations caused by SICAs in post-occurrence applications, as well as identifying the subtle operating state deviations introduced by stealthy FDIAs in pre-occurrence SE cybersecurity applications.

The first part of this thesis demonstrated the effectiveness of the proposed FA framework for standalone SPSs, where it was employed as a post-occurrence cybersecurity mechanism against SICAs. The results showed that conventional cyberattacks are readily detected by the traditional BDD. Although an adaptive Chi-square test significantly improves the detection of stealthy FDIAs, successfully identifying approximately 71% of attacks, the remaining 29% bypass the monitoring framework and become SICAs, demonstrating that even advanced detection schemes cannot guarantee complete protection. Furthermore, when the proposed SICA generation algorithm based on the *Attack–Wait–and–Observe* strategy is adopted, the detection rate of the adaptive Chi-square test decreases to approximately 3%, highlighting the need for a fundamentally different cybersecurity framework based on operating-state monitoring.

The proposed FA framework addresses this challenge by characterizing the normal operating region of the PSSVs. The TP and FN performance indices show that the rectangular and SVM classifiers provide the most accurate representation of healthy operating conditions, whereas the elliptical and convex-hull classifiers generate tighter feasible regions that are more sensitive to abnormal operating-state deviations. Across all classifiers and historical window sizes, the probability of PSSVs remaining inside the FA is consistently higher during healthy operation than under attack conditions, confirming the effectiveness of the proposed framework in distinguishing normal and compromised states. Similarly, the FAUR consistently increases during cyberattacks, indicating that a larger number of PSSVs deviate from their expected operating regions. These complementary features are subsequently integrated into the DNN, improving the overall detection accuracy by approximately 6–8% while significantly enhancing the ability to detect stealthy attacks that produce only minor variations in the PSSVs.

The second part of this thesis extended the proposed cybersecurity framework to IESs, including power–gas and power–transportation networks with integrated Hydrogen Refueling Stations. For the power–gas IES, the investigated SICAs successfully bypassed the advanced cybersecurity layer protecting the secondary information. The results demonstrated that system coupling simultaneously increases both vulnerability and detectability. While attackers can exploit the strong interdependencies between the power and gas networks to propagate disturbances and maximize their impact, these same interactions produce distinctive system-wide signatures that can be effectively captured by the proposed FA framework. Several PSSVs exhibited strong sensitivity to SICAs, with effective detection thresholds reaching 70%, indicating that these variables correctly identified approximately 70% of both healthy and compromised operating conditions. By exploiting these operating-state signatures, the proposed FA-PRNN achieved an

average detection accuracy of approximately 96%.

For the power–transportation IES, stealthy FDIAs, DoS, and coordinated bi-level DDoSs were shown to have a significant impact on HRS profitability. Among the investigated FDIAs, attacks targeting the coupling PtH and HtP units produced the largest financial losses, primarily due to penalties associated with non-compliance with operator requirements, whereas attacks on the SoC produced the smallest impact. In contrast, DoS and coordinated bi-level DDoSs, despite being simpler to execute, substantially degraded EMS performance by forcing it to operate using outdated information. This resulted in revenue losses ranging from approximately 1% to negative revenues exceeding 438%. Moreover, the coordinated bi-level DDoSs achieved significantly higher attack return ratios, ranging from 1.66 to 5, demonstrating that intelligent multi-level attackers can strategically launch cyberattacks only when the expected financial damage substantially exceeds the attack cost.

For stealthy FDIAs targeting HRS information, the proposed FA framework achieved a detection accuracy of approximately 99% by identifying abnormal EMS operating states relative to the estimated feasible operating region. However, although the FA framework can successfully detect the abnormal EMS behavior caused by outdated information under DoS and coordinated DDoSs, its capability is inherently limited to detection, as it cannot compensate for missing information or restore normal operation. To overcome this limitation, a cyber-resilient EMS was developed and integrated with the proposed detection framework. The results demonstrated a substantial improvement in operational resilience, reducing the revenue loss under severe coordinated DDoS attacks to only 1.38% compared with healthy operation. This improvement was achieved by integrating TFS-LSTM forecasting for signal reconstruction, robust estimation of the operating limits of the coupling units, and a convex HRS scheduling framework. Together, these components enable the EMS to account for forecasting uncertainty, evaluate multiple operating scenarios, and maintain secure and economically efficient operation despite significant information loss.

The third contribution of this thesis focused on extending the proposed FA framework beyond attack detection toward comprehensive attack vector characterization. Specifically, the framework was enhanced to estimate critical attack features, including the attacked measurements, the number of compromised measurements, the attack location, and the attack magnitude. To achieve this, two complementary properties were introduced: spatial distribution and temporal correlation. The spatial distribution property quantifies the proximity of the current PSSV to

the expected FA through the proposed expansion factor, providing a continuous measure of the probability that an operating state is healthy or compromised. The temporal correlation property exploits the periodic nature of SPSs by weighting historical operating states according to their cosine similarity with the current operating condition, computed from the primary system information. Consequently, operating states with similar demand and generation patterns are given greater importance in defining the feasible operating region.

The results demonstrated that the expansion factor exhibits a strong correlation with attack magnitude, increasing consistently as the attack severity increases. Furthermore, the largest expansion factor deviations accurately identify the attacked PSSVs, while the number of significant peaks corresponds to the number of compromised measurements. The temporal correlation analysis confirmed the existence of a strong 24-hour periodic operating pattern, with the highest similarity concentrated within an effective window of approximately ± 4 hours, beyond which the similarity decreases substantially. Together, these two properties significantly improve the capability of the FA framework to characterize and detect single-, double-, and triple-bus stealthy FDIAs, extending its functionality well beyond binary attack detection.

To further improve the suitability of the proposed framework for real-time applications, a recursive FA parameter estimation algorithm was developed. The proposed algorithm updates the FA parameters only when changes in the feasible operating region are detected, while initializing the estimation process using the parameters obtained from the previous time step, exploiting the gradual evolution of the operating region. This recursive formulation reduces the computational time by approximately one order of magnitude (10–12$\times$), substantially improving the computational efficiency and scalability of the proposed framework for practical real-time deployment.

Overall, the outcomes of this thesis directly address the research gaps and motivations identified at the outset of this work. By moving beyond conventional SE-oriented cybersecurity approaches, the proposed framework provides a unified and adaptive solution applicable to both standalone SPSs and interconnected IESs. The developed methodologies demonstrate that cybersecurity should not be limited to preventing or detecting attacks, but should also include attack characterization, operational recovery, and cyber-resilient control. Through the integration of the proposed FA framework, advanced SICAs, cyber-resilient EMS, and attack feature extraction techniques, this thesis establishes a comprehensive cybersecurity architecture capable of adapting to evolving operating conditions, increasing system uncertainty, and

the growing interdependencies introduced by multi-energy systems. Collectively, these contributions enhance the resilience of modern cyber-physical energy systems against sophisticated stealthy cyberattacks while providing practical tools for real-time monitoring, attack diagnosis, and secure system operation. The proposed framework therefore lays a strong foundation for the next generation of adaptive cybersecurity solutions required for future smart power systems and integrated energy infrastructures.

6.2 Future Work

Although the proposed framework demonstrates strong performance across multiple operating conditions, cyberattack scenarios, and IES configurations, several important research directions remain for future investigation.

The first and most immediate extension is the validation of the proposed framework using real-world operational data and hardware-in-the-loop (HIL) platforms. Although the simulation environments developed in this thesis provide comprehensive cyber–physical representations of standalone SPSs and IESs, practical deployment within utility control centers, digital substations, microgrids, or real-time digital twin platforms would enable evaluation under realistic communication delays, synchronization errors, sensor inaccuracies, missing measurements, equipment failures, and non-ideal operating conditions. Such validation would also facilitate assessment of computational scalability, communication overhead, and integration with existing EMS and SCADA infrastructures.

A second research direction is the development of self-healing cyber-physical energy systems by integrating the proposed FA framework with recent advances in generative AI. Rather than limiting the framework to attack detection and characterization, future intelligent agents could autonomously analyze attack characteristics, generate optimal recovery strategies, recommend corrective operating actions, estimate attack propagation paths, and continuously adapt system operation based on predicted cyber and physical system evolution. Such an architecture would transform the proposed framework from a cybersecurity monitoring tool into an autonomous cyber-resilient operational assistant capable of supporting system operators in real time.

Another promising direction is extending the framework to larger and more diverse IESs. While this thesis considered power–gas and power–transportation systems, future research may investigate integrated electricity, gas, district heating, cooling, hydrogen, water, and indus-

trial energy systems operating simultaneously. Such large-scale multi-energy infrastructures introduce stronger cyber-physical interdependencies, heterogeneous communication architectures, and multiple hierarchical control layers, requiring scalable FA formulations, distributed estimation algorithms, and reduced-order cyber-physical representations capable of maintaining real-time performance.

Future work should also investigate intelligent adversarial scenarios in which attackers explicitly optimize their attack strategies against the proposed FA-based detector. By combining reinforcement learning, generative adversarial networks, or game-theoretic optimization, adaptive attackers could continuously modify their attack vectors to minimize detectability while maximizing operational disruption. Studying these adversarial interactions would facilitate the development of next-generation FA frameworks with adversarial training, online adaptation, and continuously evolving decision boundaries capable of maintaining robustness against intelligent attackers.

Another important extension is expanding the proposed framework beyond cybersecurity toward integrated cyber–physical resilience assessment. Future research may combine the proposed FA with equipment failures, extreme weather events, natural disasters, communication outages, and cascading failures to develop unified resilience metrics that simultaneously quantify cyber, physical, and operational resilience. Such an integrated framework would enable coordinated resilience planning and decision-making for future smart energy infrastructures.

Finally, further improvements in uncertainty modeling represent an important research opportunity. Although this thesis incorporates forecasting uncertainty within the cyber-resilient EMS, future work may develop probabilistic and stochastic FA formulations capable of explicitly modeling uncertainty arising from high RESs penetration, EVs charging behavior, hydrogen demand, communication uncertainty, and forecasting errors. Integrating Bayesian deep learning, probabilistic graphical models, and uncertainty-aware neural networks with the proposed FA framework could further improve both detection reliability and operational robustness under highly dynamic operating conditions, ultimately enabling more trustworthy cybersecurity solutions for future low-carbon cyber-physical energy systems.

List of Publications

Thesis Related Publications:

[1] Ahmed A.A. Elsayed, Hany E.Z. Farag, "On The Resiliency of Hydrogen Refueling Stations in An Integrated Transportation and Electric Power System Against Denial-of-Service Cyberattacks", *IEEE Transactions on Industry Applications*.

[2] H. Khani, Ahmed A. E. Elsayed, H. E. Z. Farag and M. Mohamed, "Adaptive Feasibility Area Estimation to Enhance Cybersecurity of Electrolysis-Based Hydrogen Refueling Stations Integrated With Power Distribution Systems," in *IEEE Transactions on Intelligent Transportation Systems*. Note: Mr. Abdelaziz was responsible for the mathematical modeling, design, and implementation, including the HRS EMS, FDIA modeling, FA framework development, result generation, and implementation. His contribution accounts for more than 60% of the paper.

[3] Ahmed A. E. ElSayed, H. Khani and H. Essa Zidan Farag, "A New Method for Stealthy False Data Injection Attack Detection Using Advanced Feasibility Areas Considering Spatial Distribution," in *IEEE Transactions on Smart Grid*.

[4] Ahmed A. E. Elsayed, H. Khani and H. E. Z. Farag, "A Feasibility Area Approach for Early Stage Detection of Stealthy Infiltrated Cyberattacks in Power Systems," in *IEEE Transactions on Information Forensics and Security*.

[5] Khani, Hadi, Ahmed A. A. Elsayed, Hany EZ Farag, Moataz Mohamed, and Abdelrahman Ayad, "A cyberattack resilient model for battery electric bus transit fleets using real-time adaptive system information.", *Electric Power Systems Research*.

[6] Ahmed A. E. Elsayed and H. E. Z. Farag, "Impact of Denial-of-Service Cyberattacks on Hydrogen Refueling Stations in An Integrated Transportation and Electric Power System,"

2024 6th International Conference on Smart Power & Internet Energy Systems (SPIES), Abu Dhabi, United Arab Emirates.

[7] Ahmed A. E. Elsayed, E. Z. Hany Farag, A. Tauqeer, F. Shahid and A. Asif, "Application of Feasibility Area for Cybersecurity of Electric Power Systems," 2023 IEEE Power & Energy Society General Meeting (PESGM), Orlando, FL, USA, 2023.

[8] Ahmed A. E. Elsayed, H. E. Z. Farag and A. Asif, "Cyber Physical Security of Energy Hubs Using Feasibility Area Estimation," 2023 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 2023, pp. 696-700.

Research Projects Related Publications:

[9] Ahmed A.A Elsayed, A. Alobidi, and Hany E.Z Farag, "Characterization of high-resolution AI data center training workloads on single and multiple GPU nodes", ***Nature Scientific Data***.

[10] Ahmed A.A Elsayed, Hany E.Z Farag, Fahad Mohamed, and Nabil A. Ahmed, "Optimal Design of Fast Charging Stations for Multi-Vehicles Low-density Housing", *IEEE Access*.

[11] Yahia N. Ahmed, Ahmed A.A Elsayed, and Hany E.Z, "Tri-Stage Optimization Framework for Optimal Clustering of Power Distribution Systems into Sustainable Microgrids", *Energies*.

[12] Ahmed A.A Elsayed, S. Saxena and H. E. Z. Farag, "Optimal Design of a Planning and Contracting Framework To Enable Vehicle to Building and Grid Services via Demand Response", *IEEE Transactions on Transportation Electrification*.

[13] Alfarra, Abdelaziz, A., A., El-Hamalawy, A.F., and Farag, H.E., "A Comprehensive Framework for Classifying and Smoothing AI Data Center Power Fluctuations", *Electric Power Systems Research* (Under Review).

[14] Yahia N. Ahmed, Ahmed A.A Elsayed, and Hany E.Z, "Optimal Energy Resource Sizing of Large Energy Facilities Participating in Capacity-Markets Based Demand Response Considering Convex-Relaxed Market Constraints", *IEEE Transactions on Energy Markets, Policy and Regulation - IEEE Power Energy Society* (Under Review).

[15] Waheeb Khan, Ahmed A.A Elsayed, Shivam Saxena, and Hany E.Z Farag, "Optimal Decarbonization of Electric and Transportation Systems in Remote Islanded Microgrids", *IEEE Access* (Under Review).

[16] Ahmed A.A Elsayed, Waheeb Khan, Shivam Saxena and Farag, H.E., 2026. Decarbonization of Electric and Transport Systems in Islanded Remote Communities Using Renewable Energy and Mobile Battery Storage System. In 2026 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1-5). IEEE.

[17] Alfarra, A., El-Hamalawy, A.F., Abdelaziz, A., and Farag, H.E., 2026. Challenges of Centralized Remote Power Smoothing Strategies for AI Data Center Loads. In 2026 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE) (pp. 1-5). IEEE.

[18] Ahmed A.A Elsayed, H. E. Z. Farag and E. F. ElSaadany, "Optimal Load Profile Management in Extensive Agricultural Regions Using Water Storage Systems", PESGM25.

[19] Ahmed A.A Elsayed, and H. E. Z. Farag, "A Novel Optimal Placement of Multi-Type Sensors for Smart Grids Observability Using an Enhanced Graph Theory Search Algorithm", ISIE25.

References

[1] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727–743, 2022.

[2] B. M. Buchholz and Z. Styczynski, *Smart Grids-fundamentals and technologies in electricity networks*. Springer, 2014, vol. 396.

[3] R. Bayindir, I. Colak, G. Fulli, and K. Demirtas, "Smart grid technologies and applications," *Renewable and sustainable energy reviews*, vol. 66, pp. 499–516, 2016.

[4] A. S. Omar and R. El-Shatshat, "A survey on model-based and data-driven operational optimization approaches for integrated energy systems in smart cities," *Electric Power Systems Research*, vol. 249, p. 111946, 2025.

[5] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[6] Industrial Cyber, "Russia-backed Sandworm hackers disrupt Ukraine power grid using novel OT attack techniques," 2023, [Online; accessed 08-04-2025]. [Online]. Available: https://industrialcyber.co/critical-infrastructure/russia-backed-sandworm-hackers-disrupt-ukraine-power-grid-using-novel-ot-attack-techniques/

[7] S. Ding, S. Lu, Y. Xu, M. Korkali, and Y. Cao, "Review of cybersecurity for integrated energy systems with integration of cyber-physical systems," *Energy Conversion and Economics*, vol. 4, no. 5, pp. 334–345, 2023.

[8] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060–1069, 2016.

[9] P. Farhadi, S.-M. Moghaddas-Tafreshi, and A. Shahirinia, "A comprehensive review on stochastic modeling of electric vehicle charging load demand regarding various uncertainties," *Smart Science*, vol. 12, no. 4, pp. 679–714, 2024.

[10] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2831–2848, 2019.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[12] A. S. Musleh, G. Chen, Z. Y. Dong, C. Wang, and S. Chen, "Attack detection in automatic generation control systems using lstm-based stacked autoencoders," *IEEE Trans. Ind. Inform.*, vol. 19, no. 1, pp. 153–165, 2023.

[13] Z. Zhang, R. Deng, and D. K. Y. Yau, "Vulnerability of the load frequency control against the network parameter attack," *IEEE Trans. Smart Grid*, vol. 15, no. 1, pp. 921–933, 2024.

[14] H. Sun, Q. Guo, J. Qi, V. Ajjarapu, R. Bravo, J. Chow, Z. Li, R. Moghe, E. Nasr-Azadani, U. Tamrakar *et al.*, "Review of challenges and research opportunities for voltage control in smart grids," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 2790–2801, 2019.

[15] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to gps spoofing," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3535–3548, 2018.

[16] Q. Zhang, F. Li, and X. Wang, "Cyber-impact analysis for iso revenue adequacy considering fdia in real-time market operations," *IEEE Trans. Power Syst.*, vol. 38, no. 5, pp. 4042–4053, 2023.

[17] Y. Suo, S. Chai, R. Chai, Z.-H. Pang, Y. Xia, and G.-P. Liu, "Security defense of large-scale networks under false data injection attacks: An attack detection scheduling approach," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 1908–1921, 2024.

[18] A. Tahoun and M. Arafa, "Secure control design for nonlinear cyber–physical systems under dos, replay, and deception cyber-attacks with multiple transmission channels," *ISA transactions*, vol. 128, pp. 294–308, 2022.

[19] S. Muangchuen, J. Pahasa, and C. Rakpenthai, "Enhanced resilient model predictive control electrolyzers for frequency regulations under severe denial-of-service attacks," *IEEE Access*, vol. 12, pp. 65 352–65 361, 2024.

[20] E. I. Bilis, W. Kröger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 7, no. 4, pp. 854–865, 2013.

[21] H. Park, S.-O. D. Jung, H. Lee, and H. P. In, "Cyber weather forecasting: Forecasting unknown internet worms using randomness analysis," in *IFIP International Information Security Conference*. Springer, 2012, pp. 376–387.

[22] S. I. Jeong and D.-H. Choi, "Electric vehicle user data-induced cyber attack on electric vehicle charging station," *IEEE Access*, vol. 10, pp. 55 856–55 867, 2022.

[23] R. Dasgupta, A. Sakzad, and C. Rudolph, "Cyber attacks in transactive energy market-based microgrid systems," *Energies*, vol. 14, no. 4, p. 1137, 2021.

[24] A. M. Sawas, H. Khani, and H. E. Farag, "On the resiliency of power and gas integration resources against cyber attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3099–3110, 2020.

[25] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 572–580, 2016.

[26] K.-D. Lu and Z.-G. Wu, "Constrained-differential-evolution-based stealthy sparse cyber-attack and countermeasure in an ac smart grid," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 8, pp. 5275–5285, 2021.

[27] M. Zadsar, A. Abazari, A. Ameli, J. Yan, and M. Ghafouri, "Prevention and detection of coordinated false data injection attacks on integrated power and gas systems," *IEEE Transactions on Power Systems*, vol. 38, no. 5, pp. 4252–4268, 2022.

[28] W. Wang, F. Harrou, B. Bouyeddou, S.-M. Senouci, and Y. Sun, "A stacked deep learning approach to cyber-attacks detection in industrial systems: application to power system and gas pipeline systems," *Cluster Computing*, vol. 25, no. 1, pp. 561–578, 2022.

[29] O. O. Ajayi, C. E. Alozie, and O. A. Abieba, "Enhancing cybersecurity in energy infrastructure: Strategies for safeguarding critical systems in the digital age," *Trends in Renewable Energy*, vol. 11, no. 2, pp. 201–212, 2025.

[30] J. Shi, J. Wu, B. Xu, and Z. Song, "Cybersecurity of hybrid electric city bus with v2c connectivity," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 2, pp. 4070–4084, 2023.

[31] M. A. Razzaque, S. K. Khadem, S. Patra, G. Okwata, and M. Noor-A-Rahim, "Cybersecurity in vehicle-to-grid (v2g) systems: A systematic review," *Applied Energy*, vol. 398, p. 126364, 2025.

[32] H. R. Sayarshad, "Designing vehicle-to-grid (v2g) aggregator fleet capacity for power grid reliability against cyberattacks," *Electric Power Systems Research*, vol. 244, p. 111554, 2025.

[33] N. Tatipatri and S. Arun, "A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security," *IEEe Access*, vol. 12, pp. 18 147–18 167, 2024.

[34] A. Z. Benelhaouare, I. Mellal, M. Saydé, G. Nicolescu, and A. Lakhssassi, "Thermal side-channel threats in densely integrated microarchitectures: A comprehensive review for cyber–physical system security," *Micromachines*, vol. 16, no. 10, p. 1152, 2025.

[35] S. Peng, Z. Zhang, R. Deng, and P. Cheng, "Localizing false data injection attacks in smart grid: A spectrum-based neural network approach," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4827–4838, 2023.

[36] H. Huang, T. Li, B. Li, W. Wang, and Y. Sun, "A bidirectional differential evolution-based unknown cyberattack detection system," *IEEE Transactions on Evolutionary Computation*, vol. 29, no. 2, pp. 459–473, 2025.

[37] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in agc systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 4985–4995, 2019.

[38] Y. Wang, M. M. Amin, J. Fu, and H. B. Moussa, "A novel data analytical approach for false data injection cyber-physical attack mitigation in smart grids," *IEEE Access*, vol. 5, pp. 26 022–26 033, 2017.

[39] A. S. Heikal, I. Mohamed Diaaeldin, N. M. Badra, M. A. Attia, O. A. M. Omar, A. H. El-Ebiary, and H.-S. Kang, "A long short term memory network-based false data injection cyberattack detection and mitigation in dc microgrids," *IEEE Access*, vol. 14, pp. 39 742–39 765, 2026.

[40] M. Liu, X. Zhang, C. Zhao, and R. Deng, "Matrix coding enabled impact mitigation against primary false data injection attacks in cyber-physical microgrids," *IEEE Transactions on Power Systems*, vol. 40, no. 4, pp. 3144–3159, 2025.

[41] X. Zhao, Z. Ma, X. Shi, and S. Zou, "Attack detection and mitigation scheme of load frequency control systems against false data injection attacks," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 8, pp. 9952–9962, 2024.

[42] X.-P. Zhang, "Fundamentals of electric power systems," *Restructured Electric Power Systems: Analysis of Electricity Markets with Equilibrium Models*, pp. 1–52, 2010.

[43] F. Llewellyn, "Some fundamental properties of transmission systems," *Proceedings of the IRE*, vol. 40, no. 3, pp. 271–283, 2007.

[44] F. Shahnia, A. Arefi, and G. Ledwich, *Electric distribution network planning*. Springer, 2018, vol. 400.

[45] W. Shi, N. Li, X. Xie, C.-C. Chu, and R. Gadh, "Optimal residential demand response in distribution networks," *IEEE journal on selected areas in communications*, vol. 32, no. 7, pp. 1441–1450, 2014.

[46] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," *IEEE transactions on Smart Grid*, vol. 4, no. 1, pp. 36–46, 2013.

[47] N. Haneklaus, S. Qvist, P. Gładysz, and Ł. Bartela, "Why coal-fired power plants should get nuclear-ready," *Energy*, vol. 280, p. 128169, 2023.

[48] N. Sipöcz and F. A. Tobiesen, "Natural gas combined cycle power plants with co2 capture–opportunities to reduce cost," *International Journal of Greenhouse Gas Control*, vol. 7, pp. 98–106, 2012.

[49] M. Ho, E. Obbard, P. A. Burr, and G. Yeoh, "A review on the development of nuclear power reactors," *Energy Procedia*, vol. 160, pp. 459–466, 2019.

[50] C. Wang and S. Shahidehpour, "Effects of ramp-rate limits on unit commitment and economic dispatch," *IEEE Transactions on Power Systems*, vol. 8, no. 3, pp. 1341–1350, 2002.

[51] S. M. Jordaan, A. W. Ruttinger, K. Surana, D. Nock, S. M. Miller, and A. P. Ravikumar, "Global mitigation opportunities for the life cycle of natural gas-fired power," *Nature Climate Change*, vol. 12, no. 11, pp. 1059–1067, 2022.

[52] U. K. Das, K. S. Tey, M. Seyedmahmoudian, S. Mekhilef, M. Y. I. Idris, W. Van Deventer, B. Horan, and A. Stojcevski, "Forecasting of photovoltaic power generation and model optimization: A review," *Renewable and Sustainable Energy Reviews*, vol. 81, pp. 912–928, 2018.

[53] S. A. Vargas, G. R. T. Esteves, P. M. Maçaira, B. Q. Bastos, F. L. C. Oliveira, and R. C. Souza, "Wind power generation: A review and a research agenda," *Journal of Cleaner Production*, vol. 218, pp. 850–870, 2019.

[54] M. Melikoglu, "Current status and future of ocean energy sources: A global review," *Ocean Engineering*, vol. 148, pp. 563–573, 2018.

[55] G. Ardizzon, G. Cavazzini, and G. Pavesi, "A new generation of small hydro and pumped-hydro power plants: Advances and future challenges," *Renewable and Sustainable Energy Reviews*, vol. 31, pp. 746–761, 2014.

[56] D. Moya, C. Aldás, and P. Kaparaju, "Geothermal energy: Power plant technology and direct heat applications," *Renewable and Sustainable Energy Reviews*, vol. 94, pp. 889–901, 2018.

[57] E. J. Choi, J. W. Lee, D. Kim, G.-S. Seo, and S. W. Kim, "Quantifying benefit of well-located distributed energy resources," *IEEE Transactions on Energy Markets, Policy and Regulation*, vol. 2, no. 1, pp. 92–106, 2023.

[58] S. Zhou, Y. Han, S. Chen, P. Yang, C. Wang, and A. S. Zalhaf, "Joint expansion planning of distribution network with uncertainty of demand load and renewable energy," *Energy Reports*, vol. 8, pp. 310–319, 2022.

[59] S. K. Rathor and D. Saxena, "Energy management system for smart grid: An overview and key issues," *International Journal of Energy Research*, vol. 44, no. 6, pp. 4067–4109, 2020.

[60] T. Logenthiran, D. Srinivasan, and T. Z. Shun, "Demand side management in smart grid using heuristic optimization," *IEEE transactions on smart grid*, vol. 3, no. 3, pp. 1244–1252, 2012.

[61] P. Breeze, *Power system energy storage technologies*. Academic Press, 2018.

[62] A. Castillo and D. F. Gayme, "Grid-scale energy storage applications in renewable energy integration: A survey," *Energy Conversion and Management*, vol. 87, pp. 885–894, 2014.

[63] Z. Yang, J. Zhang, M. C. Kintner-Meyer, X. Lu, D. Choi, J. P. Lemmon, and J. Liu, "Electrochemical energy storage for green grid," *Chemical reviews*, vol. 111, no. 5, pp. 3577–3613, 2011.

[64] J. W. Ager and A. A. Lapkin, "Chemical storage of renewable energy," *Science*, vol. 360, no. 6390, pp. 707–708, 2018.

[65] F. Zhang, P. Zhao, M. Niu, and J. Maddy, "The survey of key technologies in hydrogen energy storage," *International journal of hydrogen energy*, vol. 41, no. 33, pp. 14 535–14 552, 2016.

[66] J. Gorre, F. Ruoss, H. Karjunen, J. Schaffert, and T. Tynjälä, "Cost benefits of optimizing hydrogen storage and methanation capacities for power-to-gas plants in dynamic operation," *Applied Energy*, vol. 257, p. 113967, 2020.

[67] M. Mahmoud, M. Ramadan, A.-G. Olabi, K. Pullen, and S. Naher, "A review of mechanical energy storage systems combined with wind and solar applications," *Energy Conversion and Management*, vol. 210, p. 112670, 2020.

[68] J. Wang, K. Lu, L. Ma, J. Wang, M. Dooner, S. Miao, J. Li, and D. Wang, "Overview of compressed air energy storage and technology development," *Energies*, vol. 10, no. 7, p. 991, 2017.

[69] F.-F. Li, J.-Z. Xie, Y.-F. Fan, and J. Qiu, "Potential of different forms of gravity energy storage," *Sustainable Energy Technologies and Assessments*, vol. 64, p. 103728, 2024.

[70] G. Li and X. Zheng, "Thermal energy storage system integration forms for a sustainable future," *Renewable and Sustainable Energy Reviews*, vol. 62, pp. 736–757, 2016.

[71] A. Safari, R. Saidur, F. Sulaiman, Y. Xu, and J. Dong, "A review on supercooling of phase change materials in thermal energy storage systems," *Renewable and Sustainable Energy Reviews*, vol. 70, pp. 905–919, 2017.

[72] Y. Li, H. Cao, S. Wang, Y. Jin, D. Li, X. Wang, and Y. Ding, "Load shifting of nuclear power plants using cryogenic energy storage technology," *Applied Energy*, vol. 113, pp. 1710–1716, 2014.

[73] G. Ren, G. Ma, and N. Cong, "Review of electrical energy storage system for vehicular applications," *Renewable and Sustainable Energy Reviews*, vol. 41, pp. 225–236, 2015.

[74] V. S. Vulusala G and S. Madichetty, "Application of superconducting magnetic energy storage in electrical power and energy systems: a review," *International Journal of Energy Research*, vol. 42, no. 2, pp. 358–368, 2018.

[75] G. Strbac, "Demand side management: Benefits and challenges," *Energy policy*, vol. 36, no. 12, pp. 4419–4426, 2008.

[76] Y. Lin, Z. Xiong, and J. Zhu, "Optimization of the electricity consumption behaviors of users under uncertain electricity prices and consumption patterns," *Energy Reports*, vol. 9, pp. 646–657, 2023.

[77] Z. Huang, Y. Liu, K. Li, J. Liu, H. Gao, G. Qiu, X. Shen, and J. Liu, "Evaluating long-term profile of demand response under different market designs: A comparison of scarcity pricing and capacity auction," *Energy*, vol. 282, p. 128096, 2023.

[78] A. Mnatsakanyan and S. W. Kennedy, "A novel demand response model with an application for a virtual power plant," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 230–237, 2014.

[79] T. Samad and A. M. Annaswamy, "Controls for smart grids: Architectures and applications," *Proceedings of the IEEE*, vol. 105, no. 11, pp. 2244–2261, 2017.

[80] G. Rietveld, J.-P. Braun, R. Martin, P. Wright, W. Heins, N. Ell, P. Clarkson, and N. Zisky, "Measurement infrastructure to support the reliable operation of smart electrical grids," *IEEE Transactions on Instrumentation and Measurement*, vol. 64, no. 6, pp. 1355–1363, 2015.

[81] G. Dileep, "A survey on smart grid technologies and applications," *Renewable energy*, vol. 146, pp. 2589–2625, 2020.

[82] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.

[83] H. Bevrani, M. Watanabe, and Y. Mitani, *Power system monitoring and control*. John Wiley & Sons, 2014.

[84] J. Arrillaga, N. R. Watson, and S. Chen, *Power system quality assessment*. John Wiley & Sons, 2000.

[85] I. PES, "Ieee standard for scada and automation systems," *vol. IEEE Std C*, vol. 37, 2008.

[86] J. D. McDonald, "Substation automation. ied integration and availability of information," *IEEE Power and Energy magazine*, vol. 1, no. 2, pp. 22–31, 2003.

[87] A. S. Meliopoulos, G. J. Cokkinides, P. Myrda, Y. Liu, R. Fan, L. Sun, R. Huang, and Z. Tan, "Dynamic state estimation-based protection: Status and promise," *IEEE Transactions on Power Delivery*, vol. 32, no. 1, pp. 320–330, 2016.

[88] M. Hadley, J. McBride, T. Edgar, L. O'Neil, and J. Johnson, "Securing wide area measurement systems," *US Department of Energy*, 2007.

[89] A. G. Phadke and J. S. Thorp, *Synchronized phasor measurements and their applications*. Springer, 2008, vol. 1, no. 2017.

[90] A. G. Phadke and T. Bi, "Phasor measurement units, wams, and their applications in protection and control of power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 619–629, 2018.

[91] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, "A survey on state estimation techniques and challenges in smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2312–2322, 2018.

[92] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Transactions on smart Grid*, vol. 10, no. 3, pp. 3125–3148, 2018.

[93] A. Von Meier, D. Culler, A. McEachern, and R. Arghandeh, "Micro-synchrophasors for distribution systems," in *ISGT 2014*. IEEE, 2014, pp. 1–5.

[94] A. A. E. Elsayed, M. A. Mohamed, M. Abdelraheem, and M. A. Nayel, "Optimal μpmu placement based on hybrid current channels selection for distribution grids," *IEEE Transactions on Industry Applications*, vol. 56, no. 6, pp. 6871–6881, 2020.

[95] M. P. Anguswamy, M. Datta, L. Meegahapola, and A. Vahidnia, "Optimal micro-pmu placement in distribution networks considering usable zero-injection phase strings," *IEEE Transactions On smart grid*, vol. 13, no. 5, pp. 3662–3675, 2022.

[96] Y. Ju, X. Jia, and B. Wang, "Review of dataset and algorithms for distribution network pseudo measurement," *Energy Internet*, vol. 2, no. 1, pp. 1–12, 2025.

[97] A. A. E. Elsayed, M. Khalaf, M. A. Mohamed, M. A. E. Nayel, and D. Kundur, "Optimal multi-type sensor placement using hybrid graph theory and numerical observability analysis for system observability and cybersecurity enhancement," *Electric Power Systems Research*, vol. 241, p. 111361, 2025.

[98] M. Rezaeimozafar, R. F. Monaghan, E. Barrett, and M. Duffy, "A review of behind-the-meter energy storage systems in smart grids," *Renewable and Sustainable Energy Reviews*, vol. 164, p. 112573, 2022.

[99] H. Lee, Tushar, B. Cui, A. Mallikeswaran, P. Banerjee, and A. Srivastava, "A review of synchrophasor applications in smart electric grid," *Wiley Interdisciplinary Reviews: Energy and Environment*, vol. 6, no. 3, p. e223, 2017.

[100] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on power systems*, vol. 26, no. 1, pp. 12–19, 2010.

[101] Y. Tang, K. Dvijotham, and S. Low, "Real-time optimal power flow," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2963–2973, 2017.

[102] S. F. Rafique and Z. Jianhua, "Energy management system, generation and demand predictors: a review," *IET Generation, Transmission & Distribution*, vol. 12, no. 3, pp. 519–530, 2018.

[103] S. A. Gopalan, V. Sreeram, and H. H. Iu, "A review of coordination strategies and protection schemes for microgrids," *Renewable and Sustainable Energy Reviews*, vol. 32, pp. 222–228, 2014.

[104] Q. P. Zheng, J. Wang, and A. L. Liu, "Stochastic optimization for unit commitment—a review," *IEEE Transactions on Power Systems*, vol. 30, no. 4, pp. 1913–1924, 2014.

[105] T. Aziz, Z. Lin, M. Waseem, and S. Liu, "Review on optimization methodologies in transmission network reconfiguration of power systems for grid resilience," *International Transactions on Electrical Energy Systems*, vol. 31, no. 3, p. e12704, 2021.

[106] L. Yu, D. Czarkowski, and F. De León, "Optimal distributed voltage regulation for secondary networks with dgs," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 959–967, 2012.

[107] S. S. Reddy, P. Bijwe, and A. R. Abhyankar, "Optimal posturing in day-ahead market clearing for uncertainties considering anticipated real-time adjustment costs," *IEEE Systems Journal*, vol. 9, no. 1, pp. 177–190, 2013.

[108] J. Nutaro and V. Protopopescu, "The impact of market clearing time and price signal delay on the stability of electric power markets," *IEEE Transactions on power systems*, vol. 24, no. 3, pp. 1337–1345, 2009.

[109] M. Singh, T. Vishnuvardhan, and S. Srivani, "Adaptive protection coordination scheme for power networks under penetration of distributed energy resources," *IET Generation, Transmission & Distribution*, vol. 10, no. 15, pp. 3919–3929, 2016.

[110] Z. Wang and R. S. Balog, "Arc fault and flash signal analysis in dc distribution systems using wavelet transformation," *IEEE Transactions on Smart Grid*, vol. 6, no. 4, pp. 1955–1963, 2015.

[111] Z. Yan and H. Wen, "Performance analysis of electricity theft detection for the smart grid: An overview," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–28, 2021.

[112] A. M. Ersdal, L. Imsland, and K. Uhlen, "Model predictive load-frequency control," *IEEE Transactions on Power Systems*, vol. 31, no. 1, pp. 777–785, 2015.

[113] R. Patel, C. Li, L. Meegahapola, B. McGrath, and X. Yu, "Enhancing optimal automatic generation control in a multi-area power system with diverse energy resources," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3465–3475, 2019.

[114] C. Li, Y. Wu, Y. Sun, H. Zhang, Y. Liu, Y. Liu, and V. Terzija, "Continuous under-frequency load shedding scheme for power system adaptive frequency control," *IEEE Transactions on Power Systems*, vol. 35, no. 2, pp. 950–961, 2019.

[115] Z. Qiu, C. Duan, W. Yao, P. Zeng, and L. Jiang, "Adaptive lyapunov function method for power system transient stability analysis," *IEEE Transactions on Power Systems*, vol. 38, no. 4, pp. 3331–3344, 2022.

[116] Y. Tang, Z. Tian, X. Zha, X. Li, M. Huang, and J. Sun, "An improved equal area criterion for transient stability analysis of converter-based microgrid considering nonlinear damping effect," *IEEE Transactions on Power Electronics*, vol. 37, no. 9, pp. 11 272–11 284, 2022.

[117] N. Hosseinzadeh, A. Aziz, A. Mahmud, A. Gargoom, and M. Rabbani, "Voltage stability of power systems with renewable-energy inverter-based generators: A review," *Electronics*, vol. 10, no. 2, p. 115, 2021.

[118] N. S. Ugwuanyi, X. Kestelyn, O. Thomas, B. Marinescu, and B. Wang, "A normal form-based power system out-of-step protection," *Electric Power Systems Research*, vol. 208, p. 107873, 2022.

[119] K. Islam, D. Kim, and A. Abu-Siada, "A review on adaptive power system protection schemes for future smart and micro grids, challenges and opportunities," *Electric Power Systems Research*, vol. 230, p. 110241, 2024.

[120] L. A. Kojovic, M. T. Bishop, and D. Sharma, "Innovative differential protection of power transformers using low-energy current sensors," *IEEE transactions on Industry Applications*, vol. 49, no. 5, pp. 1971–1978, 2013.

[121] S. Anttila, J. S. Döhler, J. G. Oliveira, and C. Boström, "Grid forming inverters: A review of the state of the art of key elements for microgrid operation," *Energies*, vol. 15, no. 15, p. 5517, 2022.

[122] M. R. Tur and R. Bayindir, "A review of active power and frequency control in smart grid," in *2019 1st Global Power, Energy and Communication Conference (GPECOM)*. IEEE, 2019, pp. 483–488.

[123] M. N. I. Sarkar, L. G. Meegahapola, and M. Datta, "Reactive power management in renewable rich power grids: A review of grid-codes, renewable generators, support devices, control strategies and optimization algorithms," *Ieee Access*, vol. 6, pp. 41 458–41 489, 2018.

[124] I. Alhamrouni, N. H. Abdul Kahar, M. Salem, M. Swadi, Y. Zahroui, D. J. Kadhim, F. A. Mohamed, and M. Alhuyi Nazari, "A comprehensive review on the role of artificial intelligence in power system stability, control, and protection: Insights and future directions," *Applied Sciences*, vol. 14, no. 14, p. 6214, 2024.

[125] Z. A. Obaid, L. M. Cipcigan, L. Abrahim, and M. T. Muhssin, "Frequency control of future power systems: reviewing and evaluating challenges and new control methods," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 1, pp. 9–25, 2019.

[126] S. M. Mohseni-Bonab and A. Rabiee, "Optimal reactive power dispatch: a review, and a new stochastic voltage stability constrained multi-objective model at the presence of uncertain wind power generation," *IET Generation, Transmission & Distribution*, vol. 11, no. 4, pp. 815–829, 2017.

[127] T. Mai, D. Steinberg, J. Logan, D. Bielen, K. Eurek, and C. McMillan, "An electrified future: initial scenarios and future research for us energy and electricity systems," *IEEE Power and Energy Magazine*, vol. 16, no. 4, pp. 34–47, 2018.

[128] R. Daiyan, I. MacGill, and R. Amal, "Opportunities and challenges for renewable power-to-x," 2020.

[129] G. Buffo, P. Marocco, D. Ferrero, A. Lanzini, and M. Santarelli, "Power-to-x and power-to-power routes," in *Solar hydrogen production*. Elsevier, 2019, pp. 529–557.

[130] B. Widera, "Renewable hydrogen implementations for combined energy storage, transportation and stationary applications," *Thermal Science and Engineering Progress*, vol. 16, p. 100460, 2020.

[131] R. P. Upputuri and B. Subudhi, "A comprehensive review and performance evaluation of bidirectional charger topologies for v2g/g2v operations in ev applications," *IEEE Transactions on Transportation Electrification*, vol. 10, no. 1, pp. 583–595, 2023.

[132] H. Liu, X. Liu, C. Cai, and Q. Jin, "A new power flow model for combined heat and electricity analysis in an integrated energy system," *Applied Thermal Engineering*, vol. 219, p. 119597, 2023.

[133] H. Chen, H. Yan, and G. He, *Integrated Energy System Modeling and Simulation*. Springer, 2025.

[134] W. Wei, S. Mei, L. Wu, M. Shahidehpour, and Y. Fang, "Optimal traffic-power flow in urban electrified transportation networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 84–95, 2016.

[135] Y. Zhou, C. Gu, H. Wu, and Y. Song, "An equivalent model of gas networks for dynamic analysis of gas-electricity systems," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4255–4264, 2017.

[136] S. Lu, W. Gu, J. Zhou, X. Zhang, and C. Wu, "Coordinated dispatch of multi-energy system with district heating network: Modeling and solution strategy," *Energy*, vol. 152, pp. 358–370, 2018.

[137] M. H. Amini and O. Karabasoglu, "Optimal operation of interdependent power systems and electrified transportation networks," *Energies*, vol. 11, no. 1, p. 196, 2018.

[138] W. Wei, W. Danman, W. Qiuwei, M. Shafie-Khah, and J. P. Catalão, "Interdependence between transportation system and power distribution system: A comprehensive review on models and applications," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 433–448, 2019.

[139] M. Genovese and P. Fragiacomo, "Hydrogen refueling station: Overview of the technological status and research enhancement," *Journal of Energy Storage*, vol. 61, p. 106758, 2023.

[140] J. A. Sanguesa, V. Torres-Sanz, P. Garrido, F. J. Martinez, and J. M. Marquez-Barja, "A review on electric vehicles: Technologies and challenges," *Smart Cities*, vol. 4, no. 1, pp. 372–404, 2021.

[141] J. C. Lopes, T. Sousa, and J. D. Melo, "Demand estimation for electric vehicle charging infrastructure: an extensive approach method," *IEEE Access*, 2024.

[142] S. Hemavathi and A. Shinisha, "A study on trends and developments in electric vehicle charging technologies," *Journal of energy storage*, vol. 52, p. 105013, 2022.

[143] N. Panossian, M. Muratori, B. Palmintier, A. Meintz, T. Lipman, and K. Moffat, "Challenges and opportunities of integrating electric vehicles in electricity distribution systems," *Current sustainable/renewable energy reports*, vol. 9, no. 2, pp. 27–40, 2022.

[144] H. Turker and S. Bacha, "Smart charging of plug-in electric vehicles (pevs) in residential areas: Vehicle-to-home (v2h) and vehicle-to-grid (v2g) concepts," *International Journal of Renewable Energy Research*, vol. 4, no. 4, pp. 859–871, 2014.

[145] Z. He, J. Khazaei, and J. D. Freihaut, "Optimal integration of vehicle to building (v2b) and building to vehicle (b2v) technologies for commercial buildings," *Sustainable Energy, Grids and Networks*, vol. 32, p. 100921, 2022.

[146] A. A. Al-obaidi and H. E. Farag, "Optimal design of v2g incentives and v2g-capable electric vehicles parking lots considering cost-benefit financial analysis and user participation," *IEEE Transactions on Sustainable Energy*, vol. 15, no. 1, pp. 454–465, 2023.

[147] H. H. Abdeltawab and Y. A.-R. I. Mohamed, "Mobile energy storage scheduling and operation in active distribution systems," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 9, pp. 6828–6840, 2017.

[148] Z. Tian, H. Lv, W. Zhou, C. Zhang, and P. He, "Review on equipment configuration and operation process optimization of hydrogen refueling station," *International Journal of Hydrogen Energy*, vol. 47, no. 5, pp. 3033–3053, 2022.

[149] C. Shao, M. Shahidehpour, X. Wang, X. Wang, and B. Wang, "Integrated planning of electricity and natural gas transportation systems for enhancing the power grid resilience," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4418–4429, 2017.

[150] T. Shun, L. Kunyu, X. Xiangning, W. Jianfeng, Y. Yang, and Z. Jian, "Charging demand for electric vehicle based on stochastic analysis of trip chain," *IET Generation, Transmission & Distribution*, vol. 10, no. 11, pp. 2689–2698, 2016.

[151] J. Asamer, A. Graser, B. Heilmann, and M. Ruthmair, "Sensitivity analysis for energy demand estimation of electric vehicles," *Transportation Research Part D: Transport and Environment*, vol. 46, pp. 182–199, 2016.

[152] S. Wang, Z. Y. Dong, F. Luo, K. Meng, and Y. Zhang, "Stochastic collaborative planning of electric vehicle charging stations and power distribution system," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 1, pp. 321–331, 2017.

[153] D. Yang, N. J. Sarma, M. F. Hyland, and R. Jayakrishnan, "Dynamic modeling and real-time management of a system of ev fast-charging stations," *Transportation Research Part C: Emerging Technologies*, vol. 128, p. 103186, 2021.

[154] A. Ayad, N. A. El-Taweel, and H. E. Farag, "Optimal design of battery swapping-based electrified public bus transit systems," *IEEE Transactions on Transportation Electrification*, vol. 7, no. 4, pp. 2390–2401, 2021.

[155] M. Gökçek and C. Kale, "Optimal design of a hydrogen refuelling station (hrfs) powered by hybrid power system," *Energy Conversion and Management*, vol. 161, pp. 215–224, 2018.

[156] I. Zenginis, J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "Analysis and quality of service evaluation of a fast charging station for electric vehicles," *Energy*, vol. 112, pp. 669–678, 2016.

[157] B. Zhou, K. Zhang, K. W. Chan, C. Li, X. Lu, S. Bu, and X. Gao, "Optimal coordination of electric vehicles for virtual power plants with dynamic communication spectrum allocation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 450–462, 2020.

[158] Z. Jia, J. Li, X.-P. Zhang, and R. Zhang, "Review on optimization of forecasting and coordination strategies for electric vehicle charging," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 2, pp. 389–400, 2022.

[159] Z. Tan, F. Liu, H. K. Chan, and H. O. Gao, "Transportation systems management considering dynamic wireless charging electric vehicles: Review and prospects," *Transportation Research Part E: Logistics and Transportation Review*, vol. 163, p. 102761, 2022.

[160] C. Marmaras, E. Xydas, and L. Cipcigan, "Simulation of electric vehicle driver behaviour in road transport and electric power networks," *Transportation Research Part C: Emerging Technologies*, vol. 80, pp. 239–256, 2017.

[161] E. Elghanam, A. Abdelfatah, M. S. Hassan, and A. H. Osman, "Optimization techniques in electric vehicle charging scheduling, routing and spatio-temporal demand coordination: A systematic review," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 1294–1313, 2024.

[162] Y. Sheffi, *Urban transportation networks*. Prentice-Hall, Englewood Cliffs, NJ, 1985, vol. 6.

[163] V. Morandi, "Bridging the user equilibrium and the system optimum in static traffic assignment: a review," *4or*, vol. 22, no. 1, pp. 89–119, 2024.

[164] E. M. Daly and M. Haahr, "Social network analysis for information flow in disconnected delay-tolerant manets," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, pp. 606–621, 2008.

[165] T. L. Friesz and K. Han, *Dynamic network user equilibrium*. Springer, 2022, vol. 363.

[166] Q. Xu, X. Li, Y. Jiang, S. Zhu, B. Yang, C. Chen, S. Duan, and X. Guan, "Transportation-energy-communication integrated management of ship cyber-physical systems against cyber attacks," *IEEE Transactions on Smart Grid*, 2025.

[167] O. Hafez and K. Bhattacharya, "Optimal design of electric vehicle charging stations considering various energy resources," *Renewable energy*, vol. 107, pp. 576–589, 2017.

[168] N. A. El-Taweel, A. Ayad, H. E. Farag, and M. Mohamed, "Optimal energy management for battery swapping based electric bus fleets with consideration of grid ancillary services provision," *IEEE Transactions on Sustainable Energy*, vol. 14, no. 2, pp. 1024–1036, 2022.

[169] R. Caponi, E. Bocci, and L. Del Zotto, "On-site hydrogen refuelling station techno-economic model for a fleet of fuel cell buses," *International Journal of Hydrogen Energy*, vol. 71, pp. 691–700, 2024.

[170] J. Geske and D. Schumann, "Willing to participate in vehicle-to-grid (v2g)? why not!" *Energy Policy*, vol. 120, pp. 392–401, 2018.

[171] R. Alonso and A. Z. de Souza, "Resilience of active networks with optimal mobile energy storage systems management," *Electric Power Systems Research*, vol. 217, p. 109152, 2023.

[172] I. Khan, "Greenhouse gas emission accounting approaches in electricity generation systems: A review," *Atmospheric Environment*, vol. 200, pp. 131–141, 2019.

[173] D. Parra, L. Valverde, F. J. Pino, and M. K. Patel, "A review on the role, cost and value of hydrogen energy systems for deep decarbonisation," *Renewable and Sustainable Energy Reviews*, vol. 101, pp. 279–294, 2019.

[174] X. Xing, J. Lin, Y. Song, Y. Zhou, S. Mu, and Q. Hu, "Modeling and operation of the power-to-gas system for renewables integration: a review," *CSEE Journal of Power and Energy Systems*, vol. 4, no. 2, pp. 168–178, 2018.

[175] M.-R. Tahan, "Recent advances in hydrogen compressors for use in large-scale renewable energy integration," *International Journal of Hydrogen Energy*, vol. 47, no. 83, pp. 35 275–35 292, 2022.

[176] L. Jianlin, L. Guanghui, M. Suliang, and S. Jie, "An overview on hydrogen energy storage and transportation technology and its typical application in power system," *Modern Electric Power*, vol. 38, no. 5, pp. 535–545, 2021.

[177] T. Ding, W. Jia, M. Shahidehpour, O. Han, Y. Sun, and Z. Zhang, "Review of optimization methods for energy hub planning, operation, trading, and control," *IEEE Transactions on Sustainable Energy*, vol. 13, no. 3, pp. 1802–1818, 2022.

[178] J.-K. Kim, H. Son, and S. Yun, "Heat integration of power-to-heat technologies: case studies on heat recovery systems subject to electrified heating," *Journal of Cleaner Production*, vol. 331, p. 130002, 2022.

[179] Center for Strategic and International Studies, "Significant Cyber Incidents," 2025, [Online; accessed 01-08-2025]. [Online]. Available: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[180] Dean Parsons, "What's the Scoop on FrostyGoop: The Latest ICS Malware and ICS Controls Considerations," 2024, [Online; accessed 01-12-2024]. [Online]. Available: https://www.sans.org/blog/whats-the-scoop-on-frostygoop-the-latest-ics-malware-and-ics-controls-considerations

[181] Cybersecurity and Infrastructure security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," 2024, [Online; accessed 08-01-2025]. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[182] Cybersecurity and Infrastructure security Agency, "The Attack on Colonial Pipeline: What We've Learned What We've Done Over the Past Two Years," 2023, [Online; accessed 08-03-2025]. [Online]. Available: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[183] CybersecurityHelp, "Major Brazilian energy firms suffer ransomware attacks," 2021, [Online; accessed 014-05-2025]. [Online]. Available: https://www.cybersecurity-help.cz/blog/1915.html#:~:text=Two%20Brazilian%20state%2Downed%20utility,the%20attack%20might%20have%20been.

[184] K. Fazzini and T. DiChristopher. (2019, 5) An alarmingly simple cyberattack hit electrical systems serving la and salt lake, but power never went down. [Online]. Available: https://www.cnbc.com/2019/05/02/ddos-attack-caused-interruptions-in-power-system-operations-doe.html

[185] N. S. Malik, R. Collins, and M. Vamburkar. (2018, 4) Cyber-attack pings data systems of at least four gas networks. [Online]. Available: https://www.bloomberg.com/news/articles/2018-04-03/day-after-cyber-attack-a-third-gas-pipeline-data-system-shuts

[186] BBC News. (2015, 5) Fbi flight hacker claims queried by security experts. [Online]. Available: https://www.bbc.com/news/technology-32780513

[187] E. Nakashima. (2016, 1) Russian hackers suspected in attack that blacked out parts of ukraine. [Online]. Available: https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html

[188] Chatham House. (2015, 10) Cyber security at civil nuclear facilities: Understanding the risks. [Online]. Available: https://www.chathamhouse.org/sites/default/files/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf

[189] Reuters. (2014, 12) South korea nuclear operator says cyberattacks continue, reactors safe. [Online]. Available: https://www.reuters.com/article/us-southkorea-cybersecurity-nuclear/south-korea-nuclear-operator-says-cyberattacks-continue-reactors-safe-idUSKBN0K603320141228

[190] N. Falliere. (2010, 8) Stuxnet introduces the first known rootkit for industrial control systems. [Online]. Available: https://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

[191] The Washington Post. (2016, 7) Southwest airlines computer glitch causes cancellations, delays for third day. [Online]. Available: https://www.washingtonpost.com/news/dr-gridlock/wp/2016/07/21/long-lines-for-southwest-airlines-passengers-at-area-airports/

[192] A. E. Elhabashy, L. J. Wells, J. A. Camelio, and W. H. Woodall, "A cyber-physical attack taxonomy for production systems: a quality control perspective," *Journal of Intelligent Manufacturing*, vol. 30, no. 6, pp. 2489–2504, 2019.

[193] M. H. Rahman, R. Cassandro, T. Wuest, and M. Shafae, "Taxonomy for cybersecurity threat attributes and countermeasures in smart manufacturing systems," *arXiv preprint arXiv:2401.01374*, 2023.

[194] G. Cheng, Y. Lin, A. Abur, A. Gómez-Expósito, and W. Wu, "A survey of power system state estimation using multiple data sources: Pmus, scada, ami, and beyond," *IEEE Transactions on Smart Grid*, vol. 15, no. 1, pp. 1129–1151, 2023.

[195] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[196] A. Primadianto and C.-N. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, 2016.

[197] I. Džafić, R. A. Jabr, and T. Hrnjić, "Hybrid state estimation in complex variables," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5288–5296, 2018.

[198] Z. Lu, Z. Wei, and Y. Sun, "Power system dynamic state estimation considering correlation of measurement error from pmu and scada," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 10, p. e4726, 2019.

[199] L. B. Ascari, A. S. Costa, and V. Miranda, "Correntropy-based fusion strategy for incorporating pmu measurements into power system state estimation," in *2019 IEEE Milan PowerTech*. IEEE, 2019, pp. 1–6.

[200] D. M. Bez, A. S. Costa, L. B. Ascari, and E. Z. Junior, "A block version of orthogonal rotations for improving the accuracy of hybrid state estimators," *IEEE Transactions on Power Systems*, vol. 35, no. 6, pp. 4432–4444, 2020.

[201] V. Kirincic, S. Skok, and V. Terzija, "A two-step hybrid power system state estimator," *International Transactions on Electrical Energy Systems*, vol. 25, no. 7, pp. 1158–1172, 2015.

[202] Y. Chen, Y. Yao, and Y. Zhang, "A robust state estimation method based on socp for integrated electricity-heat system," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 810–820, 2020.

[203] T. Sheng, G. Yin, Q. Guo, H. Sun, and Z. Pan, "A hybrid state estimation approach for integrated heat and electricity networks considering time-scale characteristics," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 636–645, 2020.

[204] P. Lan, D. Han, X. Xu, Z. Yan, X. Ren, and S. Xia, "Data-driven state estimation of integrated electric-gas energy system," *Energy*, vol. 252, p. 124049, 2022.

[205] H. Zang, M. Geng, M. Huang, Z. Wei, S. Chen, and G. Sun, "Asynchronous and adaptive state estimation of integrated electricity–gas energy systems," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7636–7644, 2022.

[206] Q. Chen, D. Yang, Y. Wang, C. Rehtanz, and H. Pandžić, "Robust state estimation of electricity-gas-heat integrated energy system based on the bilinear transformations," *IET Generation, Transmission & Distribution*, vol. 15, no. 1, pp. 149–163, 2021.

[207] Y. Du, W. Zhang, and T. Zhang, "Admm-based distributed state estimation for integrated energy system," *CSEE Journal of Power and Energy Systems*, vol. 5, no. 2, pp. 275–283, 2019.

[208] S. Tan, J. M. Guerrero, P. Xie, R. Han, and J. C. Vasquez, "Brief survey on attack detection methods for cyber-physical systems," *IEEE Systems Journal*, vol. 14, no. 4, pp. 5329–5339, 2020.

[209] Z. Yang, H. Liu, T. Bi, and Q. Yang, "Bad data detection algorithm for pmu based on spectral clustering," *Journal of Modern Power Systems and clean energy*, vol. 8, no. 3, pp. 473–483, 2020.

[210] C. Huang, S. Fu, M. Hong, and S. Deng, "Optimal cooperative cyber–physical attack strategy against gas–electricity interconnected system," *Energy*, vol. 285, p. 128513, 2023.

[211] Y. Zhang, X. Tu, W. Fu, Y. Gao, X. Chen, and L. Zhang, "A novel collusion combination cyberattack strategy against integrated energy system," *IEEE Transactions on Industrial Informatics*, 2024.

[212] R. Nawaz, R. Akhtar, S. U. Khan, S. Bu, and M. H. Mahmood, "Generative adversarial networks-based false data injection: A concern for data integrity of power networks," *IEEE Transactions on Power Systems*, 2025.

[213] S. H. Oh, J. Kim, J. H. Nah, and J. Park, "Employing deep reinforcement learning to cyber-attack simulation for enhancing cybersecurity," *Electronics*, vol. 13, no. 3, p. 555, 2024.

[214] K. Zarzycki, P. Chaber, K. Cabaj, M. Ławryńczuk, P. Marusak, R. Nebeluk, S. Plamowski, and A. Wojtulewicz, "Forgery cyber-attack supported by lstm neural network: an experimental case study," *Sensors*, vol. 23, no. 15, p. 6778, 2023.

[215] S. Suprabhath Koduru, V. S. P. Machina, and S. Madichetty, "Cyber attacks in cyber-physical microgrid systems: A comprehensive review," *Energies*, vol. 16, no. 12, p. 4573, 2023.

[216] P. Griffioen, S. Weerakkody, B. Sinopoli, O. Ozel, and Y. Mo, "A tutorial on detecting security attacks on cyber-physical systems," in *2019 18th European control conference (ECC)*. IEEE, 2019, pp. 979–984.

[217] W.-H. Ko, J. A. Ramos-Ruiz, T. Huang, J. Kim, H. Ibrahim, P. N. Enjeti, P. Kumar, and L. Xie, "Robust dynamic watermarking for cyber-physical security of inverter-based resources in power distribution systems," *IEEE Transactions on Industrial Electronics*, vol. 71, no. 7, pp. 7106–7116, 2023.

[218] S. D. Roy and S. Debbarma, "Enhancing cyber-resilience of power systems' agc sensor data by time series to image domain encoding," *IEEE Transactions on Smart Grid*, vol. 15, no. 4, pp. 4159–4169, 2024.

[219] X. Li, Z. Wang, C. Zhang, D. Du, and M. Fei, "A novel dynamic watermarking-based ekf detection method for fdias in smart grid," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 7, pp. 1319–1322, 2022.

[220] M. Liu, X. Zhang, H. Zhu, Z. Zhang, and R. Deng, "Physics-aware watermarking embedded in unknown input observers for false data injection attack detection in cyber-physical microgrids," *IEEE Transactions on Information Forensics and Security*, 2024.

[221] J. Callenes and M. Poshtan, "Dynamic reconfiguration for resilient state estimation against cyber attacks," *IEEE Transactions on Emerging Topics in Computing*, vol. 12, no. 2, pp. 559–571, 2023.

[222] P. Griffioen, S. Weerakkody, and B. Sinopoli, "A moving target defense for securing cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2016–2031, 2020.

[223] X. Zhang, W. Yan, and H. Li, "False data injection attacks detection and state restoration based on power system interval dynamic state estimation," *Computers and Electrical Engineering*, vol. 118, p. 109347, 2024.

[224] Y. Zhang, J. Wang, and Z. Li, "Interval state estimation with uncertainty of distributed generation and line parameters in unbalanced distribution systems," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 762–772, 2019.

[225] J. Yang, C. Zhou, S. Yang, H. Xu, and B. Hu, "Anomaly detection based on zone partition for security protection of industrial cyber-physical systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 5, pp. 4257–4267, 2017.

[226] J. Liu, J. Huang, Y. Zhou, X. Li, S. Ji, H. Xiong, and D. Dou, "From distributed machine learning to federated learning: A survey," *Knowledge and information systems*, vol. 64, no. 4, pp. 885–917, 2022.

[227] J. Li, Y. Yang, J. S. Sun, K. Tomsovic, and H. Qi, "Towards adversarial-resilient deep neural networks for false data injection attack detection in power grids," in *2023 32nd International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2023, pp. 1–10.

[228] A. A. E. Elsayed, E. H. Farag, A. Tauqeer, F. Shahid, and A. Asif, "Application of feasibility area for cybersecurity of electric power systems," in *2023 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2023, pp. 1–5.

[229] A. A. E. Elsayed, H. Khani, and H. E. Z. Farag, "A feasibility area approach for early stage detection of stealthy infiltrated cyberattacks in power systems," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 6455–6470, 2024.

[230] E. O. B. O. President, "Improving critical infrastructure cybersecurity," https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636, 19 February 2013, [Accessed 1-09-2024].

[231] N. I. o. S. Victoria Y. Pillitteri, Tanya L. Brewer and Technology, "Guidelines for smart grid cybersecurity," https://www.nist.gov/publications/guidelines-smart-grid-cybersecurity, 25 Septemper 2014, [Accessed 10-09-2024].

[232] G. K. CROWDSTRIKE, "Crowdstrike 2024 global threat report," https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf, 1 March 2024, [Accessed 15-09-2024].

[233] EMBROKER, "2024 must-know cyber attack statistics and trends," https://www.embroker.com/blog/cyber-attack-statistics/, 4 January 2024, [Accessed 1-09-2024].

[234] I. B. M. (IBM), "Cost of a data breach report 2024," https://www.ibm.com/reports/data-breach, 1 Febuerary 2024, [Accessed 10-08-2024].

[235] P. Zhao, C. Gu, and D. Huo, "Coordinated risk mitigation strategy for integrated energy systems under cyber-attacks," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 4014–4025, 2020.

[236] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, 2019.

[237] J. Condliffe, "Ukraine's power grid gets hacked again, a worrying sign for infrastructure attacks," *MIT Technology Review*, 2016.

[238] C.-W. Ten, K. Yamashita, Z. Yang, A. V. Vasilakos, and A. Ginter, "Impact assessment of hypothesized cyberattacks on interconnected bulk power systems," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4405–4425, 2017.

[239] J. Shi, S. Liu, B. Chen, and L. Yu, "Distributed data-driven intrusion detection for sparse stealthy fdi attacks in smart grids," *IEEE Trans. Circuits Syst. II: search Express Br.*, vol. 68, no. 3, pp. 993–997, 2020.

[240] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306–1318, 2013.

[241] M. Sulaiman, M. Waseem, A. N. Ali, G. Laouini, and F. S. Alshammari, "Defense strategies for epidemic cyber security threats: modeling and analysis by using a machine learning approach," *IEEE Access*, vol. 12, pp. 4958–4984, 2024.

[242] H. Khani, H. E. Farag, and E. F. El-Saadany, "Operational and economic feasibility area estimation for peer-to-peer consortium of storage systems in a blockchain framework," *IEEE Syst. J.*, vol. 15, no. 1, pp. 423–434, 2020.

[243] J. Wang and P. Srikantha, "Fast optimal power flow with guarantees via an unsupervised generative model," *IEEE Trans. Power Syst.*, 2022.

[244] A. S. Mogos, X. Liang, and C. Y. Chung, "Distribution transformer failure prediction for predictive maintenance using hybrid one-class deep svdd classification and lightning strike failures data," *IEEE Transactions on Power Delivery*, vol. 38, no. 5, pp. 3250–3261, 2023.

[245] A. M. Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin, and E. F. El-Saadany, "Anomaly-based detection of cyberattacks on line current differential relays," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4787–4800, 2022.

[246] H. Khani, H. E. Farag, and E. F. El-Saadany, "Post-occurrence cybersecurity of power-to-gas hydrogen-based energy hubs using real-time optimal adaptive feasibility area estimation," *International Journal of Hydrogen Energy*, vol. 72, pp. 297–306, 2024.

[247] F. Cheng, S. Shu, L. Zhang, M. Tan, and J. Qiu, "An evolutionary multitasking method for high-dimensional receiver operating characteristic convex hull maximization," *IEEE Trans. Emerg. Top. Comput. Intell.*, pp. 1–15, 2024.

[248] T.-W. Kuan, J.-F. Wang, J.-C. Wang, P.-C. Lin, and G.-H. Gu, "Vlsi design of an svm learning core on sequential minimal optimization algorithm," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 4, pp. 673–683, 2011.

[249] A. A. E. Elsayed and H. E. Farag, "A novel optimal placement of multi-type sensors for smart grids observability using an enhanced graph theory search algorithm," in *2025 IEEE 34th International Symposium on Industrial Electronics (ISIE)*. IEEE, 2025, pp. 1–6.

[250] A. A. E. Elsayed, H. E. Farag, and A. Asif, "Cyber physical security of energy hubs using feasibility area estimation," in *2023 International Telecommunications Conference (ITC-Egypt)*. IEEE, 2023, pp. 696–700.

[251] H. Khani, A. A. E. Elsayed, H. E. Farag, M. Mohamed, and A. Ayad, "A cyberattack resilient model for battery electric bus transit fleets using real-time adaptive system information," *Electric Power Systems Research*, vol. 231, p. 110321, 2024.

[252] H. Khani, A. A. E. Elsayed, H. E. Farag, and M. Mohamed, "Adaptive feasibility area estimation to enhance cybersecurity of electrolysis-based hydrogen refueling stations integrated with power distribution systems," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[253] A. A. E. Elsayed and H. E. Z. Farag, "On the resiliency of grid-connected hydrogen refueling stations against distributed denial-of-service cyberattacks," *IEEE Transactions on Industry Applications*, 2026.

[254] S. Mokhatab, W. A. Poe, and J. Y. Mak, *Handbook of natural gas transmission and processing: principles and practices*. Gulf professional publishing, 2018.

[255] H. Khani, N. A. El-Taweel, and H. E. Z. Farag, "Supervisory scheduling of storage-based hydrogen fueling stations for transportation sector and distributed operating reserve in electricity markets," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1529–1538, 2019.

[256] S. Murali, P. Saini, K. Abhinav, R. Shankar, and S. Parida, "Improved lstm-based load forecasting embedded 3dof (fopi)-fopd controller for proactive frequency regulation in power system," *IEEE Trans. Ind. Appl.*, vol. 60, no. 6, pp. 8213–8227, 2024.

[257] K. Petrou, A. T. Procopiou, L. Gutierrez-Lagos, M. Z. Liu, L. F. Ochoa, T. Langstaff, and J. M. Theunissen, "Ensuring distribution network integrity using dynamic operating limits for prosumers," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 3877–3888, 2021.

[258] A. A. E. ElSayed, H. Khani, and H. E. Z. Farag, "A new method for stealthy false data injection attack detection using advanced feasibility areas considering spatial distribution," *IEEE Transactions on Smart Grid*, vol. 16, no. 4, pp. 3346–3358, 2025.