Università di Genova

PhD Program in Science and Technology for Electronic and Telecommunication Engineering

Cybersecurity for Distributed Energy Resources: Analysis from Individual Systems to Grid-Scale Communities

Afroz Mokarim

Thesis submitted for the degree of *Doctor of Philosophy* (38° cycle)

06 March 2026

Prof. Mario Marchese	Advisor
Ing. Giovanni Battista Gaggero	Co-Advisor
Oriano Sità	Company Advisor
Prof. Maurizio Valle	Head of the PhD program

Università di Genova | **DITEN** DIPARTIMENTO DI INGEGNERIA NAVALE, ELETTRICA, ELETTRONICA E DELLE TELECOMUNICAZIONI

Cybersecurity for Distributed Energy Resources: Analysis from Individual Systems to Grid-Scale Communities

Afroz Mokarim

⋈

Committee:

President of the committee
Fabio Patrone, Assistant Professor, University of Genoa, Italy

Reviewers
Matteo Repetto, Senior Researcher, Istituto di Matematica Applicata e Tecnologie Informatiche (IMATI), CNR, Genova Italy
Saiful Islam, Full Professor, Department of Computer Engineering, Aligarh Muslim University, India

Advisors
Mario Marchese, Full Professor, University of Genoa, Italy

Co-Advisors
Giovanni Battista Gaggero, Assistant Professor, University of Genoa, Italy
Fabio Patrone, Assistant Professor, University of Genoa, Italy

Company Advisor
Oriano Sità, Program Manager for CyberSecurity OT&IoT, Aizoon S.p.A., Italy

University of Genoa

Afroz Mokarim

Cybersecurity for Distributed Energy Resources: Analysis from Individual Systems to Grid-Scale Communities

xxiii+188 p.

To my mother for her unconditional love and support.

Abstract

Distributed energy resources (DERs) face critical cybersecurity challenges as power grids undergo rapid digitalization. The integration of renewable energy systems, from individual photovoltaic installations to large-scale virtual power plants and energy communities, creates new attack vectors that threaten both system integrity and grid stability. Traditional IT security approaches prove insufficient for these cyber-physical energy systems, necessitating domain-specific solutions.

This thesis presents a comprehensive multi-scale approach to DER cybersecurity through six interconnected studies organized into four main contributions. First, impact assessments quantify cyberattack effects on electric vehicle charging infrastructure and energy communities, revealing voltage excursions exceeding 10% during coordinated generation manipulation attacks on IEEE test feeders. Second, physics-informed neural networks are developed for intrusion detection in PV systems, achieving superior detection accuracy compared to conventional machine learning methods while providing standardized datasets for reproducible research. Third, systematic vulnerability analysis identifies critical attack vectors in virtual power plant ancillary services, particularly in frequency regulation and voltage support mechanisms. Fourth, novel cyber-incident response mechanisms integrate cyberdefense functionalities within electrical protection systems, enabling automated circuit breaker responses that maintain system stability during ongoing attacks.

The research demonstrates through simulation and experimental validation that effective DER protection requires integrated approaches leveraging physics-based constraints and multi-scale threat analysis. This work establishes foundational frameworks for securing increasingly distributed and digitalized grid architectures, advancing both theoretical understanding and practical implementation of cyber-resilient energy systems.

Keywords: Distributed Energy Resources, Cybersecurity, Cyber-Physical Systems, Virtual Power Plants, Physics-Informed Neural Networks, Intrusion Detection, Smart Grid, Energy Communities, Grid Stability, Electric Vehicle Charging, OT Security.

Declaration

I declare that this thesis titled "Cybersecurity for Distributed Energy Resources: Analysis from Individual Systems to Grid-Scale Communities" and the work presented in it are my own. This research was carried out in collaboration with Aizoon S.p.A. Except where explicitly referenced, the content has not been submitted for any other degree or qualification at this or any other institution. I have acknowledged all main sources of assistance and collaboration.

Acknowledgements

This doctoral journey has been a transformative experience, made possible only through the support, guidance, and encouragement of many remarkable individuals and institutions.

I express my profound gratitude to my supervisor, Professor Mario Marchese, whose expertise, patience, and unwavering support have been instrumental throughout this research. I am equally indebted to my co-supervisor, Dr. Giovanni Gaggero, whose keen attention to detail and insightful guidance have greatly enhanced the quality of this work. Your ability to challenge my thinking at critical moments has shaped not only this thesis but also my approach to scientific inquiry.

I am particularly grateful to my company supervisor, Mr. Oriano Sità, for bridging the gap between academic theory and practical application. Your insights into real-world cybersecurity challenges in the energy sector have enriched this work immeasurably.

I am also deeply grateful to Professor Saiful Islam for his invaluable guidance during my research visit abroad. Your expertise in cybersecurity significantly enhanced my understanding of the field, and your warm hospitality made my time both professionally enriching and personally memorable.

My heartfelt appreciation goes to Professor Fabio Patrone for his assistance through various Ph.D. struggles. I extend my sincere thanks to Professor Maurizio Valle, Head of the PhD program in Science and Technology for Electronic and Telecommunication Engineering, for providing an excellent research environment and for fostering a culture of academic excellence within our department.

To my fellow doctoral students and colleagues in the research group, thank you for the stimulating discussions, collaborative spirit, and camaraderie that made the laboratory a place of both productivity and friendship. To my friends, both near and far, thank you for your encouragement, for reminding me of life beyond research, and for providing much-needed moments of laughter and relaxation. Your support has been a source of strength and balance.

On a personal note, I am deeply grateful to my family for their immense love, support, and understanding throughout this demanding journey. To my parents, thank you for instilling in me the value of education and for your sacrifices that made my academic pursuits possible. Your belief in my abilities, even when I doubted myself, has been my anchor. To my husband, Sharjeel, thank you for your patience during countless hours when my attention was consumed by research, for celebrating my small victories, and for providing perspective when challenges seemed insurmountable.

Afroz Mokarim
Genoa, March 2026

Contents

Appendix

List of Figures

List of Tables

Notations

P	active power (W, kW, MW)
Q	reactive power (VAR, kVAR, MVAR)
S	apparent power (VA, kVA, MVA)
P_{gen}	active power generation
P_{load}	active power load/demand
P_{inj}	active power injection
Q_{gen}	reactive power generation
Q_{load}	reactive power load
ΔP	change in active power
ΔQ	change in reactive power
V	voltage (V, kV)
I	current (A)
V_{rated}	rated voltage
V_{nom}	nominal voltage
I_{rated}	rated current
ΔV	voltage deviation
Z	impedance (Ω)
R	resistance (Ω)
X	reactance (Ω)
f	frequency (Hz)
f_{nom}	nominal frequency
Δf	frequency deviation
ω	angular frequency (rad/s)
E	energy (Wh, kWh, MWh)
T	temperature
Δt	time interval
θ	phase angle
δ	power angle or load angle
φ	phase difference
η	efficiency
λ	Lagrange multiplier or eigenvalue
μ	mean value
σ	standard deviation
σ^2	variance
γ	coefficient
G	solar irradiance (W/m^2)
T_{amb}	ambient temperature ($^\circ$C)

T_{panel}	panel temperature (°C)
SOC	state of charge (%)
DOD	depth of discharge
THD	total harmonic distortion (%)
RMS	root mean square value

Acronyms

A	Ampere
AC	Alternating Current
AES	Advanced Encryption Standard
AES-GMAC	AES-Galois/Counter Mode with Message Authentication Code
aFRR	Automatic Frequency Restoration Reserve
AI	Artificial Intelligence
AMI	Advanced Metering Infrastructure
ANN	Artificial Neural Network
ANSI	American National Standards Institute
API	Application Programming Interface
APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
BESS	Battery Energy Storage System
BMS	Battery Management System
CA	Certificate Authority
CEDS	Cybersecurity for Energy Delivery Systems
CHP	Combined Heat and Power
CIM	Common Information Model
CIP	Critical Infrastructure Protection
CLI	Command Line Interface
CNN	Convolutional Neural Network
CPU	Central Processing Unit
CSF	Cybersecurity Framework
CVPP	Commercial Virtual Power Plant
DC	Direct Current
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DER	Distributed Energy Resource
DL	Deep Learning
DNS	Domain Name System
DoS	Denial of Service
DSO	Distribution System Operator
DT	Decision Tree
ELVTF	European Low-Voltage Test Feeder
EM	Energy Management
EMS	Energy Management System
ENISA	European Union Agency for Cybersecurity

ENTSO-E	European Network of Transmission System Operators for Electricity
EV	Electric Vehicle
EVCS	Electric Vehicle Charging Station
FCR	Frequency Containment Reserve
FDI	False Data Injection
FRR	Frequency Restoration Reserve
G2V	Grid-to-Vehicle
GI	Generation Injection
GOOSE	Generic Object Oriented Substation Event
GRU	Gated Recurrent Unit
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
HV	High Voltage
Hz	Hertz
IACS	Industrial Automation and Control System
ICS	Industrial Control System
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IEA	International Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
KNN	K-Nearest Neighbors
kV	Kilovolt
kW	Kilowatt
kWh	Kilowatt-hour
LCOE	Levelized Cost of Electricity
LLMNR	Link-Local Multicast Name Resolution
LM	Load Manipulation
LSTM	Long Short-Term Memory
LV	Low Voltage
MAC	Media Access Control
mFRR	Manual Frequency Restoration Reserve
MitM	Man-in-the-Middle
ML	Machine Learning
MPPT	Maximum Power Point Tracking
MQTT	Message Queuing Telemetry Transport

MV	Medium Voltage
MW	Megawatt
MWh	Megawatt-hour
NBT-NS	NetBIOS Name Service
NERC	North American Electric Reliability Corporation
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OC-SVM	One-Class Support Vector Machine
OCPP	Open Charge Point Protocol
OPF	Optimal Power Flow
OS	Operating System
OT	Operational Technology
PCA	Principal Component Analysis
PCC	Point of Common Coupling
PF	Power Factor
PKI	Public Key Infrastructure
PV	Photovoltaic
PWM	Pulse Width Modulation
RAM	Random Access Memory
REC	Renewable Energy Community
REST	Representational State Transfer
RF	Random Forest
RMS	Root Mean Square
RNN	Recurrent Neural Network
RP	Reactive Power Manipulation
RSA	Rivest-Shamir-Adleman
SA	Secure Authentication
SCADA	Supervisory Control and Data Acquisition
SOAP	Simple Object Access Protocol
SOC	State of Charge
SOH	State of Health
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SVM	Support Vector Machine
TCP	Transmission Control Protocol
THD	Total Harmonic Distortion
TLS	Transport Layer Security
TSO	Transmission System Operator
TVPP	Technical Virtual Power Plant
UDP	User Datagram Protocol

URL	Uniform Resource Locator
V	Volt
V2G	Vehicle-to-Grid
VPN	Virtual Private Network
VPP	Virtual Power Plant
XML	Extensible Markup Language
XMPP	Extensible Message Presence Protocol
XSS	Cross-Site Scripting

CHAPTER 1

Introduction

1.1 The Evolution of the Smart Grid and Distribution Systems

The modern electrical power system is undergoing a fundamental transformation toward smart grid architectures with distributed energy resources. This evolution, detailed comprehensively in Section 2.1, represents a paradigm shift from centralized to decentralized power generation and bidirectional energy flow. The following section provides context for the cybersecurity challenges this transformation creates.

Several key technological components define this evolution. Solar photovoltaic installations have proliferated from residential rooftops to utility-scale plants, transforming from passive generators into active grid participants. Modern PV systems employ smart inverters that provide voltage regulation, frequency response, and reactive power compensation—functions traditionally reserved for synchronous generators. Battery Energy Storage Systems (BESS) complement this generation capacity by offering fast-responding flexibility for peak shaving, load shifting, and frequency regulation, with response times ranging from milliseconds to seconds for time-critical grid support.

The electrification of transportation introduces Electric Vehicles (EVs) as both significant loads and potential distributed storage resources. Electric Vehicle Charging Stations (EVCSs) span power ratings from AC chargers (up to 22 kW) to DC fast chargers (350 kW and beyond). Through Vehicle-to-Grid (V2G) technology, EVs can discharge stored energy during peak demand periods or provide ancillary services, transforming from mere consumers into flexible grid resources.

These individual technologies increasingly converge within Renewable Energy Communities (RECs), where multiple stakeholders share locally generated renewable energy through sophisticated coordination platforms. At higher aggregation levels, Virtual Power Plants (VPPs) coordinate diverse DER portfolios for market participation and ancillary

service provision comparable to conventional power plants, divided functionally into Commercial VPPs (focused on market optimization) and Technical VPPs (focused on system management within network constraints).

This distributed energy landscape offers substantial benefits: enhanced grid resilience through geographic diversity, improved utilization of renewable resources, reduced transmission losses, and empowerment of prosumers who both produce and consume electricity. However, it also introduces unprecedented operational complexity and—critically for this thesis—significant cybersecurity vulnerabilities.

The fundamental architectural change that enables these benefits is the integration of advanced Information and Communication Technology (ICT) into every aspect of distribution grid operation. Modern DERs are cyber-physical systems integrating sensors, controllers, and communication interfaces. These systems employ various industrial protocols (Modbus, IEC 61850, DNP3) and IoT standards (MQTT, OCPP, ISO 15118) for supervisory control and market interaction. Section 2.1.3 provides comprehensive coverage of DER communication protocols, their security characteristics, and standardization efforts. Chapter 5, Section 5.3 examines protocol-specific vulnerabilities in VPP contexts.

This pervasive connectivity—while essential for coordination, optimization, and market participation—creates multiple attack surfaces that adversaries can exploit to manipulate the physical operation of the power system. Unlike traditional operational technology (OT) that existed in isolated networks, modern DER infrastructure is inherently connected, making it vulnerable to the same classes of cyber threats that have plagued information technology (IT) systems, but with potentially severe physical consequences.

1.2 Problem Statement and Research Gaps

Despite growing recognition of DER cybersecurity challenges, significant gaps remain in both the academic literature and practical implementation approaches. This thesis addresses five critical research gaps that currently limit the power sector's ability to defend against and respond to cyber threats.

1.2.1 Quantitative Impact Analysis of Cyberattacks on Distribution Grids

While the general vulnerability of DER infrastructure is widely acknowledged, there exists a critical shortage of rigorous quantitative analysis examining how cyberattacks manifest

in distribution grid behavior and what magnitude of operational impact they cause. Most existing cybersecurity literature focuses on attack feasibility, vulnerability identification, or conceptual threat models, without systematically quantifying the electrical consequences on real distribution network topologies.

Critical questions remain inadequately addressed. The precise electrical consequences— voltage deviations, current flows, and power imbalances—resulting from manipulation of specific DER types across varying penetration levels lack rigorous quantification.

The differential impacts between low-voltage and medium-voltage distribution systems remain unclear, as do the relative threats posed by different attack vectors: demand inflation, generation injection, or reactive power manipulation.

Most critically, the thresholds separating localized violations from systemic cascading failures have not been systematically characterized, leaving grid operators without clear risk metrics for security investment prioritization.

1.2.2 Standardized Datasets and Benchmarks for DER Cybersecurity Research

The development and validation of cybersecurity detection algorithms requires access to realistic datasets capturing both normal operational behavior and attack scenarios. However, a systematic review of existing cybersecurity datasets reveals critical deficiencies for DER research:

Lack of DER-Specific Datasets: Most publicly available Industrial Control System (ICS) datasets focus on water treatment facilities (SWaT), manufacturing processes (HAI), or generic network traffic (CICIDS-2017). These datasets do not capture the unique electrical parameters, physical relationships, and operational characteristics of photovoltaic systems, battery storage, or other DER technologies.

Absence of Physics-Based Relationships: Existing datasets rarely include sufficient variables to verify physical consistency. For effective physics-informed detection, datasets must include correlated electrical parameters (voltage, current, power, frequency) and environmental variables (irradiance, temperature) that exhibit known physical relationships.

Insufficient Attack Diversity: Many datasets provide limited attack scenario coverage, often focusing on network-level attacks (DoS, port scanning) rather than cyber-physical attacks that manipulate physical process setpoints or measurements.

Lack of Realistic Environmental Conditions: Datasets created under controlled laboratory conditions may not capture the operational variability inherent in real DER deployments—cloud transients affecting solar generation, temperature variations, and normal operational noise—that challenge anomaly detection algorithms in practice.

Reproducibility Challenges: Without open-source simulation models and clearly documented attack implementations, researchers cannot reproduce experiments, validate findings, or extend work to new scenarios.

1.2.3 Physics-Informed Anomaly Detection for DER Cybersecurity

Conventional cybersecurity approaches, developed primarily for IT systems, rely on network traffic analysis, signature-based detection, or purely data-driven machine learning methods. When applied to DER infrastructure, these approaches exhibit significant limitations:

Network-Centric Limitations: Many sophisticated attacks manipulate physical system behavior without producing abnormal network traffic patterns. An attacker who successfully authenticates (using stolen credentials or exploited vulnerabilities) and issues malicious but properly formatted commands will appear as legitimate traffic to network-based intrusion detection systems.

Signature-Based Inadequacy: Signature-based detection requires prior knowledge of attack patterns and fails against novel or adaptive attacks. In the rapidly evolving DER threat landscape, attackers continuously develop new exploitation techniques that evade signature databases.

Data-Driven ML Limitations: While machine learning shows promise for anomaly detection, purely data-driven approaches face several challenges in DER applications:

1. Class imbalance: Normal operation data vastly outnumbers attack samples, degrading supervised learning performance

2. Environmental variability: DER systems experience wide operational variability due to weather (solar irradiance, temperature), user behavior (EV charging patterns), and grid conditions, creating difficulty distinguishing attacks from normal variations

3. Lack of physical consistency: Data-driven models may flag physically plausible anomalies or miss attacks that respect learned statistical patterns but violate physical laws

1.2.4 Systematic Vulnerability and Mitigation Frameworks for VPPs Providing Ancillary Services

Virtual Power Plants represent a critical evolution in grid operations, aggregating distributed resources to provide essential ancillary services including frequency regulation, voltage support, and emergency response. However, VPPs face unique cybersecurity challenges that distinguish them from both traditional power plants and individual DER installations:

Time-Critical Service Requirements: Unlike conventional generation, VPPs providing ancillary services operate under extremely stringent timing constraints. Frequency Containment Reserve (FCR) requires activation within 15-30 seconds with 1-2 second cycle times; Automatic Frequency Restoration Reserve (aFRR) demands 5-15 minute activation with 1-5 second cycles. These tight deadlines create a fundamental tension between security validation time and operational requirements, opening attack windows that adversaries can exploit through latency injection or timing manipulation.

Distributed Architecture Vulnerabilities: VPPs coordinate potentially thousands of DER assets across wide geographic areas, owned by diverse stakeholders (utilities, aggregators, prosumers), communicating through heterogeneous networks, and implementing varied security postures. This distributed architecture creates multiple attack surfaces and coordination challenges absent in centralized facilities.

Market Integration Complexity: VPPs participate in electricity markets, submitting bids, receiving dispatch signals, and settling financial transactions. This market integration introduces additional attack motivations (market manipulation for economic gain) and vulnerabilities (falsification of availability data, bid manipulation).

Despite these unique challenges, existing research has not systematically analyzed VPP vulnerabilities in the context of their operational requirements, nor developed comprehensive mitigation frameworks that address the intersection of time-critical operations, distributed architecture, and market integration.

1.2.5 Automated Cyber-Incident Response Mechanisms for Distributed Systems

Traditional cybersecurity incident response in power systems relies heavily on human operators who, upon detecting an attack or suspicious behavior, manually assess the situation and execute appropriate responses (isolating compromised systems, adjusting

operational setpoints, initiating backup procedures). However, this manual response paradigm is increasingly inadequate for modern DER-intensive distribution grids due to:

Geographic Distribution: With potentially thousands of DER assets distributed across wide areas, centralized manual response cannot react quickly enough to prevent attack propagation or mitigate consequences before damage occurs.

Attack Speed: Cyberattacks execute at digital timescales (milliseconds to seconds), far faster than human reaction times (minutes to hours). By the time operators recognize and respond to an attack, significant damage may already have occurred—equipment may be stressed beyond safe limits, voltage violations may have triggered protective relays, or cascading failures may have initiated.

Operational Complexity: Modern distribution grids exhibit complex interactions between DERs, controllable loads, and network conditions. Determining the optimal response to a detected attack requires rapid assessment of system state, constraint evaluation, and coordination of multiple protective actions—a cognitive load that exceeds human capabilities under time pressure.

Lack of Standardized Response Mechanisms: While electrical protection systems provide automatic response to physical faults (overcurrent, overvoltage, frequency deviation), they generally cannot distinguish between faults caused by equipment failure versus deliberate cyberattacks. Moreover, traditional protections are not designed to respond to intentionally induced dangerous conditions that fall below protection thresholds individually but collectively threaten system stability.

1.3 Thesis Organization and Publications

This thesis is organized into seven chapters that progressively develop the theoretical foundations, methodologies, experimental results, and practical implications of the research.

Chapter 1: Introduction and Context (current chapter) establishes the research motivation by describing the evolution of smart distribution grids, characterizing the cyber-physical threat landscape, identifying critical research gaps, and presenting the five key contributions that address these gaps.

Chapter 2: Background and Cybersecurity Vulnerabilities in DER Infrastructure provides comprehensive background on the technical foundations underlying the research. This chapter reviews DER technologies (EVs, PV systems, BESS), aggregation architectures (RECs, VPPs), and communication protocols (Modbus, IEC 61850, OCPP). It

systematically catalogs known vulnerabilities in EV charging infrastructure, REC platforms, and VPP communication systems, establishing the threat landscape that motivates the research contributions. The chapter concludes with a review of prior work on cyber-physical attacks against power systems, positioning this thesis within the broader cybersecurity literature.

Chapter 3: Quantitative Impact Analysis on Distribution Grids presents detailed simulation studies quantifying how cyberattacks manifest in distribution network behavior. The chapter begins with modeling and simulation methodology (IEEE test feeders, attack implementation in MATLAB/Simulink, Load Manipulation attack models). It then presents experimental results for EVCS attacks on low-voltage grids (examining coordinated charging attacks, V2G reverse power flow scenarios, and voltage/current impacts at various attack magnitudes). The chapter continues with REC attack analysis on both LV and MV systems, demonstrating how active and reactive power manipulation affects voltage profiles and establishing critical attack thresholds. Results establish the quantitative foundation for risk assessment and protection system design addressed in later chapters.

Chapter 4: Physics-Based Anomaly Detection for Photovoltaic Systems develops the novel Physics-Informed Supervised LSTM Encoder-Decoder architecture. The chapter begins with detailed PV system modeling and the creation of the Photo-Set dataset, including comprehensive description of the 22 electrical and environmental features and the 12 attack/fault scenarios. It then presents the proposed detection architecture, explaining the integration of physical constraints into the neural network loss function and the role of LSTM layers in capturing temporal dynamics. Performance evaluation compares the physics-informed approach against baseline methods (autoencoders, LSTM without physics), demonstrating superior detection capabilities particularly for subtle False Data Injection attacks. The chapter concludes with analysis of why physics-informed methods excel and identification of remaining detection challenges.

Chapter 5: Cybersecurity Frameworks and Mitigation Strategies for Virtual Power Plants addresses the unique security challenges of aggregated DER systems providing time-critical ancillary services. The chapter systematically analyzes VPP operational requirements (frequency balance, voltage compensation, supply reconstruction, operational management) and their associated timing constraints. It presents comprehensive threat analysis using the MITRE ATT&CK framework, mapping specific attack techniques to VPP service categories with practical exploitation scenarios. The chapter then develops mitigation strategies aligned with the NIST Cybersecurity Framework, providing specific technical implementations for addressing time-critical vulnerabilities, securing distributed

architectures, and protecting market integration. Real-world deployment guidance and protocol-specific recommendations complete the framework.

Chapter 6: Integrating Cyberdefense into Electrical Power System Protections introduces the concept of automatic cyber-incident response through intelligent protection relays. The chapter establishes the need for subsecond automated response in geographically distributed DER systems where manual operator response is too slow. It presents the proposed architecture combining local Intrusion Detection Systems with circuit breaker control, explaining how cyber threat detection integrates with physical consequence assessment. Validation using massive power injection attack simulations on the IEEE European Low-Voltage Test Feeder demonstrates that automated isolation preserves voltage stability.

Chapter 7: Conclusions and Future Work synthesizes the research contributions, highlighting the key insights and their implications for DER cybersecurity practice. It discusses how the quantitative impact analysis, physics-informed detection methods, standardized datasets, VPP security frameworks, and automated response mechanisms collectively advance the state of the art. The chapter identifies promising directions for future research, including validation in real-world environments, embedded system implementations, extension to additional DER types, and investigation of emerging attack vectors. It concludes with reflections on the broader implications of cyber-physical security for the energy transition.

To summarize the narrative logic, this thesis progresses through four scales of analysis. Chapter 3 examines community-level impacts on EV charging and renewable energy communities to establish the severity and scope of cyber threats. Chapter 4 then develops detection mechanisms for individual PV systems, representing the foundational DER unit. Chapter 5 analyzes vulnerabilities in virtual power plant aggregations where hundreds of DERs coordinate through communication networks. Finally, Chapter 6 integrates these insights into automated protection responses that operate across all scales.

1.4 Research Scope: Cyber-Physical Integration Approach

This thesis adopts a deliberate cyber-physical integration approach that emphasizes power system impacts of cyber compromise over pure IT security analysis. This scoping decision reflects several considerations:

The primary contribution lies in quantifying how cyberattacks translate to physical grid effects—voltage deviations, current flows, frequency excursions, and stability threats. While IT security aspects (network intrusion, malware analysis, authentication bypasses) are acknowledged as attack prerequisites, the research assumes successful cyber compromise has occurred and proceeds to analyze resulting operational impacts.

This approach aligns with the needs of power system operators and protection engineers who must understand attack consequences to design appropriate defensive responses, independent of how attackers initially gained access.

Traditional cybersecurity focuses on preventing unauthorized access (firewalls, intrusion prevention, and access control). This thesis complements that work by addressing the question: "Given that preventive measures failed and an attacker controls DER systems, what happens to the grid?" This consequence-focused perspective informs:

Risk assessment and prioritization

Physical layer defense mechanisms

Resilience strategies assuming compromise

Protection coordination under attack

Comprehensive cyber-forensic analysis of attack vectors, network traffic patterns, and exploitation techniques would require access to operational OT networks and real attack data—resources rarely available in academic research. The thesis instead leverages standard power system simulation tools and datasets, providing reproducible results accessible to the broader research community.

This approach recognizes that effective DER security requires both preventing cyber compromise (IT security domain) and mitigating impacts when prevention fails (power systems domain). This thesis contributes primarily to the latter while acknowledging the essential role of preventive cybersecurity measures.

CHAPTER 2

Literature Review and Theoretical Foundation

The cybersecurity of distributed energy resources (DERs) has emerged as a critical research domain at the intersection of power systems engineering, information security, and cyber-physical systems. As power grids transition from centralized generation paradigms to distributed architectures incorporating renewable energy, electric vehicles, and energy storage systems, the attack surface for malicious actors expands significantly. This chapter provides a comprehensive review of the state of the art in DER cybersecurity, examining the evolution of research from early vulnerability assessments to contemporary physics-informed detection methods and mitigation frameworks.

The structure of this literature review follows the natural progression of cybersecurity research: understanding system architectures and their inherent vulnerabilities (Section 2.2), analyzing documented threats and attack methodologies (Section 2.3), reviewing detection and defense mechanisms (Section 2.4), examining datasets and experimental methodologies (Section 2.5), and surveying standards and regulatory frameworks (Section 2.6). This comprehensive review establishes the context for the research contributions presented in subsequent chapters while identifying critical gaps that this thesis addresses.

2.1 Evolution of Smart Grid and DER Technologies

2.1.1 From Traditional Grids to Smart Grids

The concept of the "smart grid" emerged in the early 2000s as a response to aging infrastructure, increasing demand for reliability, and the need to integrate renewable energy sources. The U.S. Department of Energy's 2003 report "Grid 2030: A National Vision for Electricity's Second 100 Years" articulated the vision of a modernized electrical infrastructure incorporating advanced sensing, communication, and control technologies [1]. The European Technology Platform for SmartGrids, established in 2005, similarly

defined smart grids as electricity networks that can intelligently integrate the actions of all users connected to them to efficiently deliver sustainable, economic, and secure electricity supplies [2].

Amin and Wollenberg (2005) provided one of the early comprehensive frameworks for understanding smart grid security challenges, recognizing that the integration of information technology with operational technology would create new vulnerability classes not present in traditional power systems [3]. Their work presciently identified that "the very features that make the grid 'smart'—widespread sensing, communication, and automated control—also create potential security vulnerabilities."

2.1.2 DER Expansion Drivers

The International Energy Agency (IEA) defines DERs as "small-scale power generation or storage technologies (typically ranging from 1 kW to 10,000 kW) that provide an alternative to or enhancement of the traditional electric power system" [4]. The proliferation of DERs has been driven by multiple converging factors:

The levelized cost of utility-scale solar PV declined approximately 90% between 2010 and 2023, from $0.40/kWh to $0.04/kWh, making distributed solar economically competitive with conventional generation in many markets [5, 6]. These cost reductions, combined with climate policy imperatives under the Paris Agreement and advances in power electronics enabling sophisticated inverter capabilities, have driven exponential growth in distributed generation and storage deployments [7, 8]. Grid codes and interconnection standards have evolved to accommodate and leverage DER capabilities. IEEE Standard 1547-2018 specifies requirements for DER grid integration, including capabilities for voltage and frequency ride-through, dynamic reactive power support, and communication protocols [9].

Distributed Energy Resources (DERs) represent a fundamental shift in power system architecture, moving from the traditional paradigm of centralized generation and unidirectional power flow to a decentralized model characterized by bidirectional energy exchange and active grid participation. This broad represenation encompasses diverse technologies:

Photovoltaic Systems: Teodorescu et al. (2011) provided foundational work on grid converters for photovoltaic systems, establishing the technical requirements for grid integration and control [10]. More recently, Yang et al. (2019) comprehensively surveyed grid codes for photovoltaic integration, documenting how requirements have evolved

to include sophisticated grid support functions such as voltage regulation, frequency response, and fault ride-through capabilities [11].

Electric Vehicles and Charging Infrastructure: Kempton and Tomić (2005) introduced the foundational concept of Vehicle-to-Grid (V2G), demonstrating that electric vehicles could provide valuable grid services through bidirectional power flow [12]. Subsequent research by Clement-Nyns et al. (2011) analyzed the impact of uncontrolled EV charging on distribution networks, establishing that coordinated charging strategies are essential for maintaining grid stability with high EV penetration [13]. The development of charging standards, particularly ISO 15118 for automated communication and SAE J1772 for physical connection, has enabled sophisticated interaction between EVs and grid infrastructure [14].

Battery Energy Storage Systems: The role of battery storage in grid applications has been extensively documented by Denholm et al. (2013) in their comprehensive assessment for the U.S. National Renewable Energy Laboratory [15]. They identified multiple value streams including energy arbitrage, frequency regulation, and renewable integration support. The commissioning of utility-scale storage facilities such as the Hornsdale Power Reserve in South Australia (150 MW/194 MWh) provided empirical validation of BESS capabilities for fast frequency response and grid stabilization [16].

Renewable Energy Communities: The European Union's Renewable Energy Directive (EU) 2018/2001 formalized the legal framework for Renewable Energy Communities (RECs), defining them as legal entities where participation is voluntary, members are located in proximity to renewable projects, and primary purpose is community benefit rather than financial profit [17]. Research by Paudel et al. (2019) explored peer-to-peer energy trading within prosumer communities using game-theoretic models, demonstrating the complexity of optimizing collective behavior while respecting individual preferences [18].

Virtual Power Plants: The VPP concept was formalized by Pudjianto et al. (2007), who distinguished between Commercial VPPs focused on market participation and Technical VPPs addressing system management and network constraints [19]. Zamani et al. (2016) developed optimization frameworks for VPP day-ahead resource scheduling, addressing the computational challenges of coordinating heterogeneous DER portfolios [20]. More recent work by Kardakos et al. (2016) addressed optimal bidding strategies for VPPs in electricity markets under uncertainty [21].

2.1.3 Communication Protocols and Standards

The interoperability of DER systems depends critically on standardized communication protocols. Several comprehensive surveys have documented the protocol landscape:

Industrial Control System Protocols: Fang et al. (2012) provided an early comprehensive survey of smart grid communication protocols, covering IEC 61850 for substation automation, DNP3 for SCADA communications, and Modbus for field device control [22]. They identified that many protocols were designed decades ago without security considerations, as systems operated in isolated networks. Cleveland (2008) specifically analyzed IEC 61850, documenting its object-oriented data modeling approach and recognizing early that security extensions would be necessary for smart grid deployment [23].

Internet of Things (IoT) Protocols: The emergence of IoT protocols for smart grid applications was surveyed by Naik (2017), who analyzed MQTT, CoAP, and XMPP for DER communication [24]. Their work highlighted the trade-offs between lightweight protocols suitable for resource-constrained devices and the security requirements of critical infrastructure.

Standards Evolution: The development of the IEC 62351 security standard, which provides security extensions for IEC 61850 and related protocols, has been documented by Fries et al. (2016) [25]. However, deployment of these security extensions remains limited due to performance concerns, backward compatibility requirements, and implementation complexity—challenges that persist in contemporary systems.

2.2 Cybersecurity Vulnerabilities in DER Infrastructure

The cybersecurity risks of smart grid infrastructure were recognized early in the smart grid evolution. The National Institute of Standards and Technology (NIST) Guidelines for Smart Grid Cybersecurity (NISTIR 7628), published in 2010 and revised in 2014, provided the foundational risk assessment framework for smart grid systems [26]. This comprehensive document identified logical interface categories, vulnerability classes, and security requirements, establishing the baseline for subsequent research. The National Electric Sector Cybersecurity Organization Resource (NESCOR) extended NIST's work specifically for distributed energy resources, publishing failure scenarios and security requirements in 2013 [27]. NESCOR identified attack vectors including communication protocol exploitation, data integrity attacks, and denial of service threats specifically relevant to DER systems.

As DER deployment has accelerated, specific vulnerability categories have emerged across different technology domains. In EV charging infrastructure, the security of charging protocols has received significant research attention. Baker and Martinovic (2019) conducted one of the first comprehensive security analyses of ISO 15118 implementations, demonstrating vulnerabilities in certificate validation, TLS implementation, and authentication mechanisms [28]. Their work revealed that despite the protocol specification including security features, real-world implementations often fail to properly implement these protections, enabling man-in-the-middle attacks and credential theft. Lev et al. (2019) focused on the Open Charge Point Protocol (OCPP), widely adopted for communication between charging stations and management systems [29]. Their analysis revealed that OCPP 1.6 implementations frequently lack encryption and authentication, as these security features are optional rather than mandatory in the specification. They demonstrated practical attacks including session hijacking, command injection, and billing fraud.

Johnson et al. (2020) conducted penetration testing on commercial EVCS units, revealing systemic security weaknesses including default credentials, unpatched software vulnerabilities, exposed debug interfaces, and lack of secure firmware update mechanisms [30]. Their findings suggested that charging infrastructure suffers from security issues common to IoT devices generally, where cost pressures and rapid deployment timelines compromise security. Mustafa et al. (2020) specifically analyzed data manipulation attacks targeting EV State of Charge (SOC) communications [31]. They demonstrated that falsified SOC messages could cause overcharging beyond safe limits, create billing fraud opportunities, and enable coordinated attacks where multiple compromised EVs manipulate grid loads through synchronized charging behavior.

The concept of EV botnets capable of grid manipulation was explored by Kang et al. (2017), who analyzed the potential for coordinated load manipulation attacks using compromised charging infrastructure [32]. Their simulations demonstrated that compromising just 1% of EVs in a region could create synchronized demand increases of tens of megawatts, sufficient to cause frequency deviations and voltage instability. This work established that the aggregate impact of distributed attacks could threaten grid stability even when individual compromised devices have limited capacity.

Renewable energy community platforms present another set of vulnerabilities. Liu et al. (2019) conducted security assessments of commercial energy community platforms, identifying common web application vulnerabilities including SQL injection, cross-site scripting, and insufficient authentication controls [33]. Their work highlighted that REC platforms often prioritize ease of use and low deployment cost over security hardening,

inheriting vulnerabilities common to consumer web applications rather than implementing security measures appropriate for critical infrastructure. The security of IoT gateways in smart grid applications was analyzed by Järvinen et al. (2014), who documented the challenges of implementing robust security on resource-constrained devices [34]. Their work identified fundamental tensions between computational limitations (constraining cryptographic capabilities) and security requirements, as well as challenges in maintaining secure firmware across geographically distributed devices.

Man-in-the-middle attacks against smart grid communication were demonstrated by Saxena et al. (2017), showing that attackers positioned on network paths could intercept measurements, modify control commands, and inject false data [35]. Their work emphasized that encryption and authentication must be mandatory rather than optional to prevent these attacks. Molina-Markham et al. (2010) demonstrated that high-resolution energy consumption data reveals sensitive information about household activities, enabling inference of occupancy patterns, appliance usage, and daily routines [36]. This privacy research established that compromised REC platforms expose not only operational risks but also significant privacy violations for community members.

Virtual power plant systems face additional challenges due to their time-critical operational requirements and complex integration. Al-Anbagi et al. (2017) analyzed the impact of communication latency on cyber-physical power grid monitoring systems, demonstrating that delays of even 500ms-2s can compromise time-critical grid services [37]. Their work established that VPPs providing frequency regulation services face fundamental tensions between security validation time and operational deadlines, creating exploitable attack windows. Chen and Abu-Nimeh (2011) provided early analysis of supply chain security risks in smart grid deployments, identifying vulnerabilities introduced during manufacturing, software development, and component integration [38]. More recent supply chain compromises such as the SolarWinds attack (2020) have validated these concerns, demonstrating that sophisticated adversaries target supplier relationships to compromise downstream systems [39].

Communication protocol vulnerabilities represent a particularly significant challenge across all DER types. The security limitations of IEC 61850 were comprehensively analyzed by Falk et al. (2016), who demonstrated attacks against GOOSE (Generic Object Oriented Substation Event) messages and MMS (Manufacturing Message Specification) communications [40]. Their work showed that the lack of authentication and encryption in baseline IEC 61850 implementations enables message spoofing and man-in-the-middle attacks. While IEC 62351 defines security extensions, performance concerns (particularly

for time-critical GOOSE messages) have limited deployment. The security of Modbus protocol, widely deployed in industrial control systems including DER infrastructure, was analyzed by McLaughlin et al. (2016) [41]. They documented that Modbus provides no inherent security features—no authentication, encryption, or integrity protection—making it trivially exploitable by attackers with network access. Andy et al. (2017) surveyed publicly accessible MQTT brokers, discovering over 17,000 instances with no authentication, exposing IoT devices including energy management systems to unauthorized access [42]. Their work highlighted the gap between protocol capabilities (MQTT supports authentication and TLS encryption) and actual deployments (where security features are often disabled for simplicity).

Finally, VPP participation in electricity markets creates additional attack vectors. Xie et al. (2011) analyzed integrity data attacks in power market operations, demonstrating that attackers with access to market systems could manipulate bids, exploit private information, or cause economic harm through strategic bidding [43]. Their work established that VPP participation in electricity markets creates financial incentives for cyber attacks beyond operational disruption.

2.3 Cyber-Physical Attack Research

2.3.1 False Data Injection Attacks

Liu et al. (2011) introduced the foundational theoretical framework for False Data Injection (FDI) attacks against AC power system state estimation [44]. Their seminal work proved that attackers with knowledge of system topology and measurement configuration can construct attack vectors that cause arbitrary errors in state estimates while passing conventional bad data detection tests based on normalized residuals. This work established FDI as a fundamental threat category for power systems, spawning extensive follow-on research.

Subsequent research extended Liu's framework to various attack scenarios. Dán and Sandberg (2010) analyzed FDI attacks with limited attacker resources, demonstrating that strategic selection of compromised measurements can maximize attack impact even with limited access [45]. Kosut et al. (2011) characterized the fundamental limits of attack detectability, proving that certain attack constructions are inherently undetectable without additional physical constraints [46].

Detection approaches for FDI attacks have been extensively studied. Kosut et al. (2011) analyzed the theoretical detection limits, showing that perfect detection is impossible without additional information [47]. Hendrickx et al. (2014) proposed using network topology properties to detect attacks, exploiting the fact that attackers must satisfy physical network constraints [48]. More recently, machine learning approaches have been applied, with Esmalifalak et al. (2014) using support vector machines for FDI detection [49].

2.3.2 Dynamic Load Manipulation and Frequency Attacks

The vulnerability of power system frequency stability to cyber attacks was established through several landmark papers. Soltan et al. (2018) introduced Dynamic Load Altering Attacks (D-LAA), demonstrating that attackers controlling as little as 1% of total load through compromised IoT devices can induce oscillations in grid frequency [50]. Their analysis revealed that timing attacks at the system's natural frequency creates resonance, amplifying small disturbances into large-scale instabilities.

The potential for coordinated EV charging attacks was specifically analyzed by several researchers. Rahman et al. (2014) studied the impact of manipulated EV charging on distribution feeder loading and voltage profiles [51]. Countermeasures for load manipulation attacks have been proposed by several researchers. Amini et al. (2015) developed dynamic load altering attack detection using PMU data and Kalman filtering [52]. Sridhar and Hahn (2012) proposed cyber-physical security testbeds for evaluating attack detection approaches in realistic grid environments [53].

2.3.3 Voltage Stability Attacks

Teymouri et al. (2018) analyzed cyber attacks on solar PV systems with reactive power capability, demonstrating that malicious reactive power injection or absorption can cause voltage violations [54]. Their work established that distribution systems with high PV penetration are particularly vulnerable as numerous distributed inverters can collectively manipulate voltage profiles.

Liu et al. (2017) studied the impact of cyber attacks on microgrid systems including solar PV and energy storage, analyzing how coordinated manipulation of multiple DERs amplifies voltage stability threats [55]. Their simulations showed that attacks timed to coincide with peak loading or high renewable generation variability maximize impact.

Rahman et al. (2016) investigated attacks targeting power quality through harmonic injection from maliciously controlled inverters [56]. They demonstrated that coordinated harmonic injection can exceed IEEE 519 limits, degrade power factor, and interfere with protective relay operation.

2.3.4 Protection System Attacks

Hong et al. (2014) demonstrated attacks modifying protective relay settings to disable protections or cause miscoordination [57]. Their work showed that attackers gaining access to relay configuration interfaces can prevent operation during actual faults or trigger unnecessary trips, creating reliability risks.

The vulnerability of protection systems to false trip commands via protocols like IEC 61850 GOOSE was demonstrated by Falk et al. (2016) [40]. They showed that the lack of authentication in GOOSE messages enables attackers to inject false trip commands, potentially causing cascading outages through protection miscoordination.

2.3.5 Market Manipulation Attacks

Xie et al. (2011) analyzed how cyber espionage enabling access to confidential bidding information could facilitate market manipulation [43]. Their work established that information asymmetry created by cyber attacks introduces economic incentives beyond operational disruption.

Tan et al. (2017) investigated attacks where DER aggregators falsify availability claims to collect capacity payments without delivering services [58]. This work highlighted reliability risks when system operators depend on unavailable resources during emergencies.

2.4 Detection and Defense Mechanisms

2.4.1 Network-Based Intrusion Detection

SCADA Network Monitoring: Traditional network-based intrusion detection for SCADA systems was surveyed by Zhu et al. (2011), who reviewed signature-based and anomaly-based approaches [59]. However, their work acknowledged fundamental limitations: sophisticated attacks that manipulate physical processes while generating legitimate-appearing network traffic can evade network-based detection.

Protocol Anomaly Detection: Lin and Nadjm-Tehrani (2019) developed timing pattern analysis for SCADA traffic, exploiting the fact that industrial protocols exhibit predictable communication patterns [60]. Deviations from expected timing, message sequences, or data values can indicate attacks. However, this approach requires extensive training data and struggles with novel attack variants.

2.4.2 Physics-Based Anomaly Detection

Conceptual Foundations: The paradigm of physics-based anomaly detection for cyber-physical systems was articulated by Giraldo et al. (2018) in their comprehensive survey [61]. They established that cyber attacks targeting physical processes must ultimately violate physical laws or create implausible system states, providing detection opportunities unavailable to purely network-based approaches.

State Estimation Approaches: Hendrickx et al. (2014) proposed using network topology constraints to detect FDI attacks, exploiting the fact that attackers must satisfy power flow equations [48]. Their work demonstrated that incorporating physical constraints strengthens detection compared to statistical residual-based approaches.

Model-Based Detection: Pasqualetti et al. (2013) developed theoretical frameworks for attack detection using dynamic system models [62]. Their work characterized fundamental detectability limits based on system observability and attack subspace properties.

Data-Driven Physics-Informed Methods: More recent work has combined machine learning with physical constraints. Kosut et al. (2011) used hypothesis testing with physical models [46]. Esmalifalak et al. (2014) applied support vector machines incorporating power flow constraints [49]. However, a comprehensive physics-informed deep learning approach specifically for DER cybersecurity remained an open research question that this thesis addresses.

2.4.3 Machine Learning for Cybersecurity

Deep Learning Applications: The application of deep learning to smart grid cybersecurity has been surveyed by He et al. (2020), who reviewed neural networks, recurrent architectures, and autoencoders for anomaly detection [63]. However, their survey identified that most approaches are purely data-driven without incorporating domain-specific physical knowledge.

Autoencoder Approaches: Autoencoders have been widely applied to anomaly detection in industrial systems. Sakurada and Yairi (2014) demonstrated autoencoders for spacecraft telemetry anomaly detection [64]. Malhotra et al. (2016) applied LSTM autoencoders to time-series anomaly detection [65]. However, these approaches lack explicit physics integration, limiting their effectiveness for subtle cyber-physical attacks.

Challenges and Limitations: Luo et al. (2021) surveyed deep learning-based anomaly detection in cyber-physical systems, identifying critical challenges including class imbalance (normal data vastly outnumbers attack samples), environmental variability (legitimate operational variations can appear anomalous), and adversarial robustness (attackers may craft attacks to evade detection) [66].

2.4.4 Blockchain and Distributed Security

Blockchain for Grid Security: The potential application of blockchain technology to smart grid security has been explored by multiple researchers. Gai et al. (2018) proposed blockchain-based access control for smart grids [67]. Aitzhan and Svetinovic (2018) developed blockchain-based security and privacy for decentralized energy trading [68]. However, blockchain approaches face challenges including scalability (transaction throughput insufficient for real-time grid operations), latency (block confirmation times incompatible with time-critical services), and energy consumption (proof-of-work consensus mechanisms contradicting sustainability goals).

Distributed Intrusion Detection: Collaborative intrusion detection distributing security monitoring across multiple nodes was proposed by Faisal et al. (2012) [69]. Their approach addresses single-point-of-failure risks inherent in centralized security monitoring but introduces challenges in consensus and coordination under attack.

2.5 Digital Twin Technology for DER Cybersecurity

Digital twin technology represents an emerging approach in cyber-physical security for distributed energy resources. A digital twin is a virtual replica of a physical system that maintains synchronized state through continuous data exchange, enabling real-time monitoring, simulation, and prediction without affecting physical operations [70].

2.5.1 Relevance to DER Cybersecurity

For DER security, digital twins provide anomaly detection capabilities by maintaining expected system states based on current environmental conditions (irradiance, temperature), historical performance patterns, and physical constraints [71]. Deviations between measured behavior and twin predictions indicate potential equipment malfunction, sensor compromise, control system attacks, or data poisoning.

The key advantage over threshold-based detection is context awareness—the same measurement may be normal under certain conditions but anomalous under others. Digital twins can also simulate attack propagation effects and evaluate mitigation strategies before deployment, addressing the inability to safely test defensive responses in operational environments.

2.5.2 Implementation Challenges

Despite promising potential, digital twin deployment faces several barriers:

- Model fidelity requirements: High-accuracy models need detailed system parameters often unavailable for commercial DER equipment due to proprietary constraints

- Computational costs: Real-time simulation for distribution networks is computationally intensive, limiting scalability beyond single installations

- Synchronization issues: Communication disruptions prevent state synchronization between physical and digital twins

- Adversarial risks: Sophisticated attackers may compromise both physical system and digital twin simultaneously, or manipulate input data to deceive the twin

- Operational complexity: Model maintenance overhead increases as physical systems undergo reconfigurations or aging

2.5.3 Future Research Directions

As digital twin technology matures and computational costs decrease, promising research directions could be:

Federated architectures distributing computation across edge devices to reduce latency

Machine learning-enhanced twins that self-calibrate and improve accuracy over time [72]

Standardized interfaces enabling multi-vendor DER interoperability

Blockchain-based state verification preventing simultaneous compromise

The combination of real-time digital twins with physics-informed machine learning and automated protection coordination represents a natural evolution of the cyber-physical security approaches developed in this thesis.

2.6 Standards, Regulations, and Policy Frameworks

2.6.1 Cybersecurity Standards

NIST Cybersecurity Framework: The NIST Cybersecurity Framework (CSF), published in 2014 and updated in 2018, provides an organizational structure for cybersecurity programs across five functions: Identify, Protect, Detect, Respond, and Recover [73]. While originally developed for critical infrastructure broadly, the framework has been adapted for smart grid applications. The CSF's risk-based approach allows organizations to prioritize cybersecurity investments based on threat likelihood and potential impact, making it particularly relevant for DER operators with constrained resources. The framework's flexibility enables alignment with other standards and regulatory requirements, facilitating compliance with multiple jurisdictions.

NIST Smart Grid Guidelines (NISTIR 7628): The NIST Interagency Report 7628 "Guidelines for Smart Grid Cybersecurity" provides detailed security requirements for smart grid systems [26]. Revised in 2014, this three-volume document catalogs interfaces, vulnerabilities, and security requirements, establishing the baseline for smart grid security assessments. Volume I addresses smart grid cybersecurity strategy, architecture, and high-level requirements. Volume II provides privacy and cybersecurity impact assessment methodologies. Volume III presents specific security requirements for smart grid logical interface categories, defining security controls for encryption, authentication, authorization, auditing, and physical security across different smart grid domains including DER systems.

IEC 62351 Security Standards: The IEC 62351 series provides security extensions for power system communication protocols including IEC 61850, IEC 60870-5, and IEC 61400-25. Fries et al. (2016) documented the development and implementation challenges of IEC 62351, noting that adoption remains limited due to performance overhead

and backward compatibility concerns [25]. The standard defines mechanisms for authentication of data transfer through digital signatures, ensuring only authenticated clients can access servers, encrypting data in transit, ensuring role-based access control, and managing security certificates and keys. However, the computational requirements for cryptographic operations can introduce latency incompatible with time-critical grid services, particularly for GOOSE messaging in substations, creating a fundamental tension between security and operational performance.

IEC 62443 Industrial Automation and Control Systems Security: The IEC 62443 series (formerly ISA-99) provides a comprehensive framework for securing Industrial Automation and Control Systems (IACS), directly applicable to DER infrastructure including VPPs, microgrids, and industrial energy management systems. The standard is structured in four categories: general concepts (IEC 62443-1), policies and procedures (IEC 62443-2), system requirements (IEC 62443-3), and component requirements (IEC 62443-4). IEC 62443-3-3 defines seven foundational requirements: identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability. The standard introduces Security Levels (SL 1-4) that define protection against attackers with increasing capability, from casual or coincidental violations to sophisticated attacks with extended resources. This risk-based approach enables DER operators to implement security proportional to threat levels and asset criticality. IEC 62443-4-2 specifically addresses component security requirements including secure development lifecycle, technical security capabilities, and software update mechanisms, providing concrete guidance for DER device manufacturers and system integrators.

NERC CIP (Critical Infrastructure Protection): In North America, the North American Electric Reliability Corporation (NERC) enforces Critical Infrastructure Protection (CIP) standards mandating cybersecurity measures for bulk electric systems. The CIP standards cover electronic security perimeters, personnel and training, physical security, systems security management, incident reporting, and recovery planning. However, NERC CIP primarily addresses transmission-level systems and large generating facilities, with limited applicability to distribution-level DERs. Recent revisions have begun to address distributed resources through the concept of "dispersed generation," but regulatory gaps remain for smaller-scale DERs including residential solar installations and community energy systems. The applicability threshold (75 MVA for generation resources) excludes most DER aggregations, creating a regulatory blind spot as VPPs increasingly provide bulk system services.

2.6.2 Regulatory Frameworks

European NIS2 Directive: The European Union's Directive on measures for a high common level of cybersecurity (NIS2), adopted in 2022, classifies energy sector entities including power generators and distributors as "essential entities" subject to stringent cybersecurity requirements [74]. Article 21 mandates technical and organizational measures proportional to risks, including risk analysis and information security policies, incident handling procedures, business continuity and crisis management, supply chain security, security in network and information systems acquisition, development and maintenance, policies and procedures to assess the effectiveness of cybersecurity measures, and basic cyber hygiene practices and cybersecurity training. This regulatory framework directly impacts VPPs providing ancillary services, as addressed in Chapter 5 of this thesis. The directive requires member states to ensure essential entities implement appropriate technical, operational and organizational measures to manage cybersecurity risks and prevent or minimize the impact of incidents. Significantly, NIS2 introduces potential liability for management bodies and mandates coordinated vulnerability disclosure, representing a substantial increase in regulatory burden compared to the original NIS Directive.

IEEE 1547 Interconnection Standard: IEEE Standard 1547-2018 specifies requirements for interconnecting DERs with electric power systems, including communication protocols, grid support functions, and security considerations [75]. The 2018 revision significantly expanded cybersecurity requirements compared to earlier versions, mandating authentication and authorization for remote connections, encryption for communications that traverse public networks, provisions for security updates and patches, and cybersecurity capabilities proportional to the DER's potential impact on the grid. The standard requires DER systems to provide grid support functions including voltage and frequency ride-through, active power control, and reactive power capability, many of which depend on secure communication and control systems. IEEE 1547.3, a companion standard under development, provides more detailed cybersecurity guidance specifically for DER interconnection, addressing authentication protocols, encryption methods, and intrusion detection approaches.

Grid Codes and Ancillary Service Requirements: European TSOs coordinated through ENTSO-E have established network codes for DER participation in ancillary services. The "Network Code on Load-Frequency Control and Reserves" specifies technical requirements for frequency containment and restoration reserves [76]. These requirements create timing constraints that introduce cybersecurity vulnerabilities, as analyzed in Chapter 5.

The network codes mandate response times as short as 2 seconds for Frequency Containment Reserves (FCR) and 30 seconds for automatic Frequency Restoration Reserves (aFRR), creating tension between security validation requirements and operational deadlines. The "Network Code on Requirements for Grid Connection of Generators" extends many requirements to larger DER units, creating convergence between transmission-level security expectations and distribution-level operational realities.

2.6.3 Policy and Governance

National and International Initiatives: Multiple governmental initiatives address smart grid cybersecurity. The U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDS) program funds research and development of cybersecurity solutions for energy infrastructure, supporting development of anomaly detection systems, secure communication protocols, and resilience enhancement technologies [77]. The program has funded development of tools including secure SCADA protocols, hardware-based security for substations, and machine learning approaches for intrusion detection. The European Union Agency for Cybersecurity (ENISA) publishes guidelines and recommendations for smart grid security, including specific guidance for smart metering and DER integration [78]. ENISA's "Recommendations for Europe and Member States" addresses governance structures, certification schemes, and incident response coordination. The agency has published sector-specific threat landscapes for smart grids, identifying cyber threats including malware, denial of service, data manipulation, and supply chain compromises, providing operational context for implementation of technical standards.

Information Sharing and Analysis Centers (ISACs): The Electricity ISAC facilitates information sharing about cyber threats and vulnerabilities among electric sector participants, providing real-time threat intelligence, vulnerability alerts, and incident coordination. However, participation is voluntary and information sharing can be limited by competitive concerns and liability considerations. The E-ISAC has expanded to include distribution utilities and DER operators, but participation rates remain lower among smaller entities due to resource constraints and concerns about exposing vulnerabilities. International coordination occurs through partnerships including the European Energy ISAC and cooperation with telecommunications and government ISACs, recognizing that cyber threats transcend sector and geographic boundaries. Despite these initiatives, significant gaps remain in threat intelligence sharing for DER-specific vulnerabilities, as

many attacks target systems below the reporting thresholds of traditional energy sector participants.

2.7 Chapter Summary

This chapter reviewed the evolution from traditional grids to smart, DER-integrated systems and established the theoretical foundation for subsequent research. Key insights include: DER communication protocols (IEC 61850, 60870-5-104, DNP3, Modbus) create multiple attack surfaces; false data injection can bypass traditional state estimation; and machine learning approaches show promise but require physics-informed constraints. Current cybersecurity research focuses predominantly on transmission systems and centralized generation, with limited attention to distributed, multi-stakeholder environments. Critical gaps include a lack of standardized DER-specific datasets, limited quantitative impact analysis of distribution-level attacks, and insufficient integration of physical protection with cybersecurity functions—gaps this thesis addresses in subsequent chapters.

CHAPTER 3

Quantitative Impact Analysis of Cyberattacks on Distribution Grids

3.1 Introduction

This chapter quantifies the electrical consequences of coordinated cyberattacks through power flow simulations of Load Manipulation (LM) attacks against Electric Vehicle Charging Station (EVCS) infrastructure and Renewable Energy Communities (RECs) on IEEE distribution test feeders. Through systematic simulation studies, we establish voltage deviations, current flows, and power system impacts resulting from attacks at various magnitudes and network locations.

We address four questions: the precise electrical consequences when attackers manipulate EVCS and REC infrastructure at realistic penetration levels; how attack impacts differ between low-voltage and medium-voltage systems and what thresholds distinguish localized violations from systemic failures; which attack scenarios—demand increase, generation injection, or reactive power manipulation—pose the greatest threat; and at what magnitude grid code violations trigger protective device operation and potential cascading failures.

The content of this chapter has been published in the following paper:

A. Mokarim, G. B. Gaggero, and M. Marchese, "Evaluation of the Impact of cyberattacks Against Electric Vehicle Charging Stations in a Low Voltage Distribution Grid," in Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm), Glasgow, United Kingdom, Nov. 2023, pp. 1-7, doi: 10.1109/SmartGridComm57358.2023.10333896.

A. Mokarim, G. B. Gaggero, and M. Marchese, "Impact Analysis of Cyber Attacks against Energy Communities in Distribution Grids," Electronics, vol. 13, no. 9, p. 1709, May 2024, doi: 10.3390/electronics13091709.

3.2 Methodology

3.2.1 Attack Model and Threat Assumptions

Load Manipulation Attack Definition: Load manipulation (LM) attacks represent a class of cyber-physical threats where adversaries modify the power consumption or generation profiles of controllable devices to cause grid instability. The attack model assumes that adversaries compromise centralized management platforms (EVCS management systems, REC coordination platforms, VPP energy management systems) and use this access to send malicious setpoint commands to distributed assets.

Attacker Capabilities: The hypothesis of this study is that the attacker can modify loads of all EVCS or REC devices in a defined area within the constraints of the device power ratings. While strong, this hypothesis is plausible: it is common that many devices are controlled by a single platform that uses the public internet to send commands to individual devices. The attacker is assumed to have:

1. Knowledge of the distribution network structure
2. Ability to bypass authentication procedures on the management platform
3. Capability to manipulate active and reactive power setpoints
4. Strategic timing capability to coordinate attacks with load demand patterns

Attack Classification: Following established taxonomy, LM attacks are classified as:

1. **Dynamic or Static:** Dynamic LM aims at load variation over many time intervals, whereas static manipulation varies load only once
2. **Single or Multi-location:** Single-location LM targets a single bus or node, while multi-location LM can target many buses simultaneously
3. **Active or Reactive Power:** Attacks can manipulate active power (demand increase/decrease) or reactive power (inductive/capacitive injection)

3.2.2 Simulation Environment and Tools

All simulations were conducted using MATLAB [79] R2022b with Simulink and the Simscape Electrical toolbox. MATLAB/Simulink provides high-fidelity electromagnetic

modeling capabilities suitable for detailed power system analysis, including representation of power electronics, control systems, and protection devices [14].

MATLAB/Simulink was selected over alternatives (PowerWorld, PSS/E, OpenDSS) for several reasons:

Detailed modeling of power electronics and inverter controls essential for DER representation

Flexibility in implementing custom attack scenarios and control logic

Integration of power system models with communication and control system simulation

Widespread use in academic research enabling reproducibility and comparison

Dynamic simulations used a fixed time step of 50 µs (20 kHz sampling rate) to accurately capture power electronics switching behavior and transient phenomena. For longer-duration studies spanning hours, variable time steps with a maximum of 1 second were employed with phasor-based models.

3.3 Use Case 1: cyberattacks on Electric Vehicle Charging Stations in Low-Voltage Networks

3.3.1 Cybersecurity Issues in EV Charging

Electric Vehicle Charging Station (EVCS) Deployment:

The study assumes widespread EVCS penetration across the distribution network, reflecting anticipated future smart city deployments where most buildings have charging capability. EVCS are classified as follows according their power ratings:

1. Slow AC Chargers: <7.4 kW, charging time up to 6 hours (residential overnight)
2. Standard AC Chargers: 7.4-22 kW, charging time up to 2 hours (workplace/public)
3. Slow DC Chargers: <50 kW, charging time up to 1 hour (commercial fast charging)

All EVCS units communicate with a centralized charging management platform using standardized protocols. As detailed in Section 2.1.3, OCPP 1.6 facilitates charging

station-to-management system communication, while ISO 15118 enables EV-to-station interaction. For this analysis, we assume public internet connectivity without dedicated secure channels—a common real-world deployment reflecting the vulnerabilities documented by Lev et al. [29].

The primary function of EVCS (Electric Vehicle Charging Stations) is to provide electric power for charging EV batteries upon request. When an EV needs to be recharged, the driver communicates through a mobile application to find the nearest available charging station. Information is exchanged between the EV and the charging station via the charging connector. The charging connector is the physical plug that connects the charging station to the EV. It usually has multiple pins or contacts to transmit power and data. Initially, the State of Charge (SOC) along with the voltage and current capacity of the EV battery is shared with the charging station. Accordingly, there are charging protocols that define the communication standards between the EV and the charging station. Commonly used protocols include CHAdeMO, CCS (Combined Charging System), and Tesla Supercharger. These protocols allow the charging station and EV to exchange information and control the charging process [80]. A schematic diagram of the EV charging infrastructure is given in Figure 3.1.

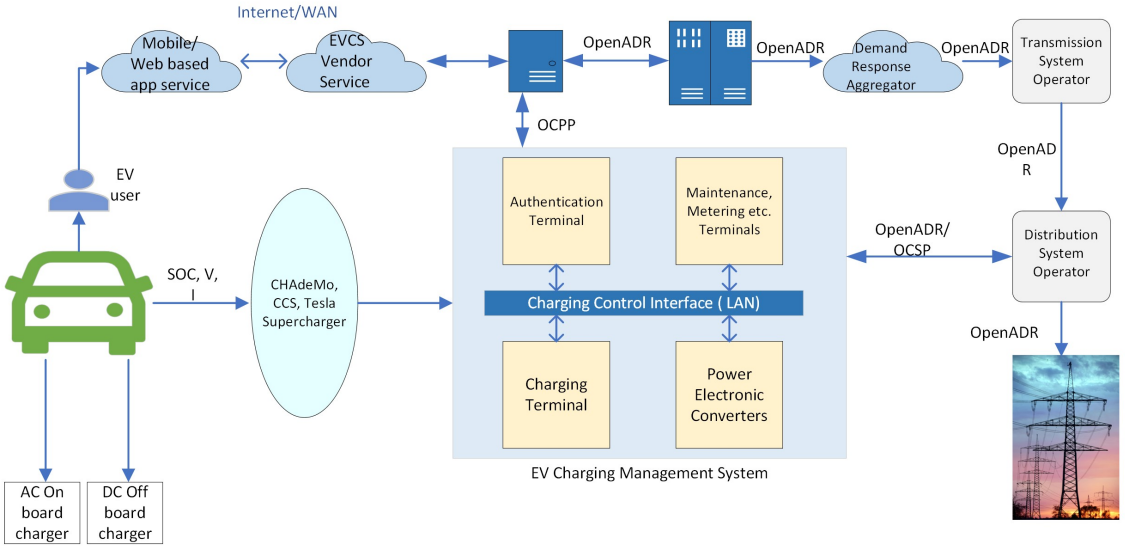

Figure 3.1: Basic EV Charging Infrastructure

This centralized platform architecture creates a single point of failure: compromise of the management platform enables coordinated manipulation of all 200 kW EVCS capacity simultaneously.

3.3.2 Test System: IEEE European Low-Voltage Test Feeder (ELVTF)

The IEEE ELVTF represents a typical European radial distribution network with the following characteristics:

Network Specifications:

Topology: 906 nodes, 905 branches, 55 load buses (radial configuration)

Voltage Level: 416 V phase-to-phase (240 V phase-to-neutral)

Frequency: 50 Hz

Transformer: 11 kV/416 V, 0.8 MVA, delta/grounded wye connection

- Winding resistance: 0.4
- Winding reactance: 4

Load Configuration:

- Phase A: 21 loads
- Phase B: 15 loads
- Phase C: 19 loads

Base Load: 1 kW per bus with 0.95 power factor

Load Modeling: Time-varying residential/commercial profiles over 24-hour period with 1-minute resolution

Geographic Division into Attack Areas: For cybersecurity analysis, the ELVTF was divided into three geographic areas representing different customer densities and EVCS deployment patterns:

Area 1 (Loads 1-18): Primarily residential neighborhood

Area 2 (Loads 19-40): Mixed residential and commercial district

Area 3 (Loads 41-55): Residential area with public charging

This has also been illustrated in Figure 3.2.

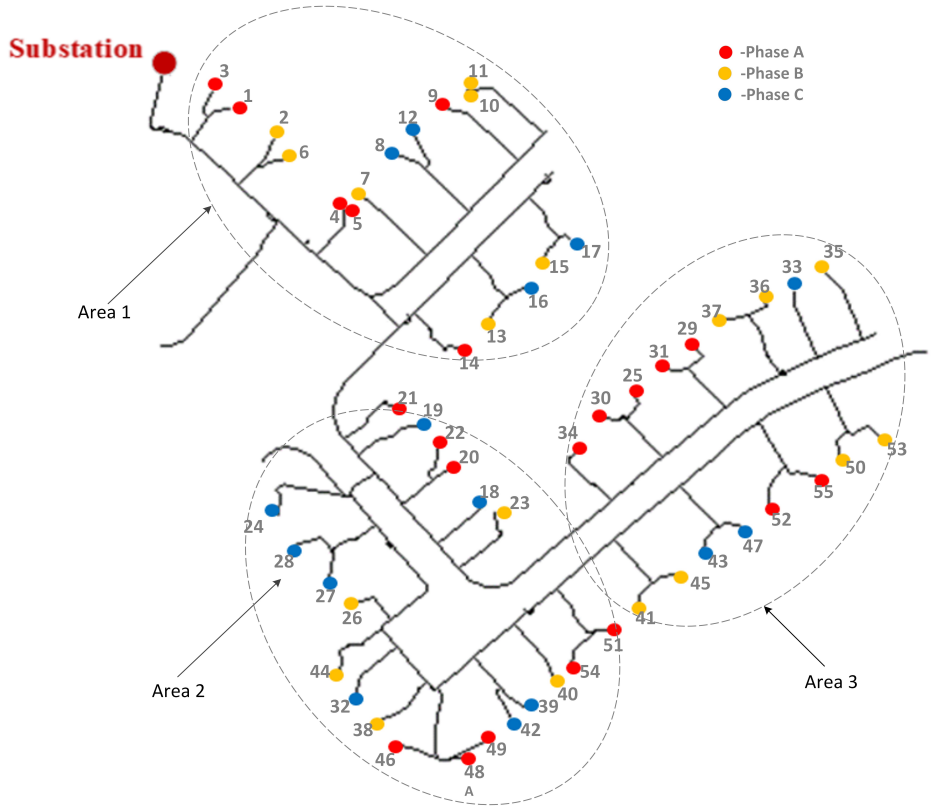

Figure 3.2: Single-line diagram of the European Low-Voltage Test Feeder

3.3.3 Load Demand Patterns and EV Charging Behavior

Base Load Demand Profile: Load patterns were modeled according to Italian grid data from Terna (transmission system operator) depicted in Figure 3.3; reflecting typical Italian residential/commercial daily demand:

Morning Peak (10-11 AM): Peak load hours

Afternoon Decline (12-3 PM): Demand decreases

Evening Peak (6-8 PM): Secondary peak

Night Valley (11 PM-5 AM): Minimum demand

EV Charging Behavioral Patterns: Based on Italian EV charging behavior data (Terna) the EV charging pattern can summarized as follows:

6 AM: End of residential overnight charging, workplace charging begins

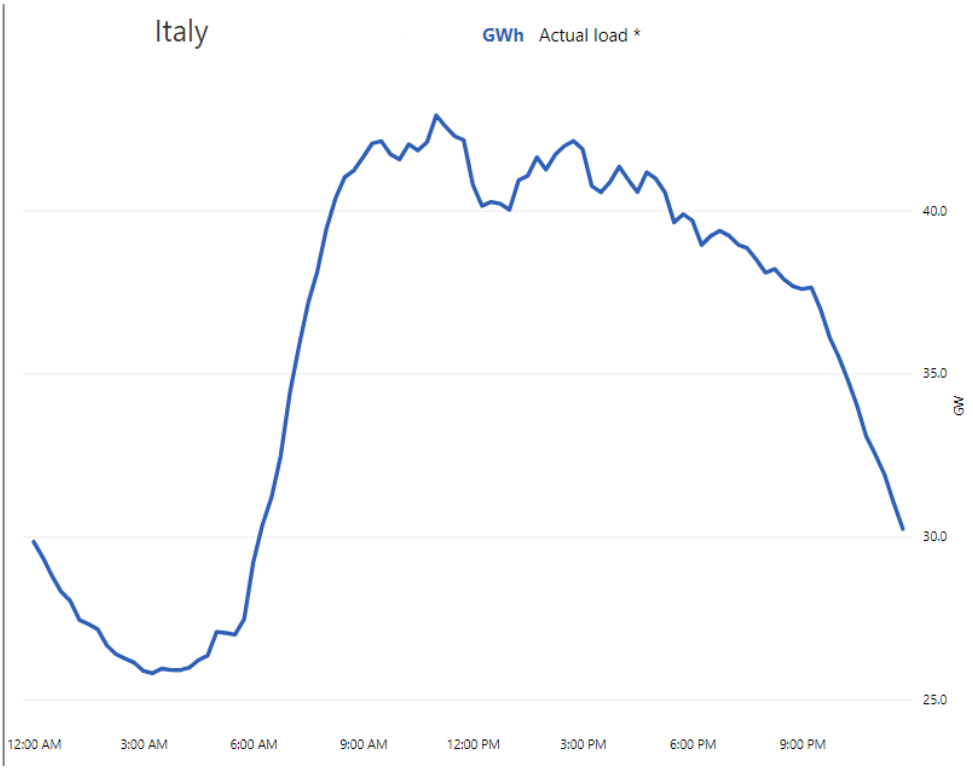

Figure 3.3: Trend of the Italian electricity system's total demand

2 PM: Midday workplace/public charging during business hours

10 PM: Evening return-home residential charging initiation

Normal Charging Coordination: Under non-attack conditions, EVCS management platform implements smart charging algorithms:

Staggered start times to avoid simultaneous high-power demand

Time-of-use pricing response (charge during off-peak hours)

Peak shaving (reduce charging rate during system peaks)

Load balancing across three phases

The given system is simulated under normal conditions and the plots of the three aforementioned loads are sketched as shown in Figure 3.4. As shown by the plot, the voltage for the given system stays between 1 and 1.05 pu which is roughly around 252

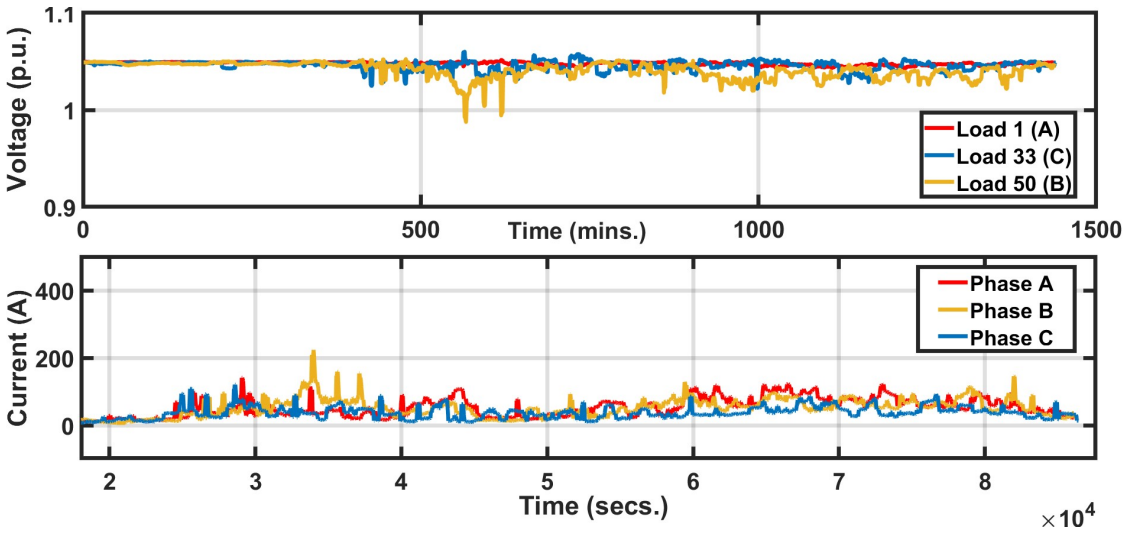

Figure 3.4: Normal Charging Conditions for EVCS

volts. For the sake of simplicity, the three-phase currents of only Load-1 have been plotted. These graphs show the data for a 24-hour duration where the distribution system operates containing residential and commercial loads along with normally functioning EVCSs at most buses.

3.3.4 Attack Scenarios for EVCS

Three attack scenarios were designed to represent different threat vectors against EVCS infrastructure as shown in Table 3.1:

Attack Timing Strategy: The attacker exploits knowledge of the EV charging patterns to maximize grid impact:

1. Injection attacks: Timed during low-load periods (early morning valley).
2. Absorption attacks: Timed during existing peak demand periods.
3. Coordination: All EVCS units manipulated simultaneously, bypassing normal staggering.

Table 3.1: Load Manipulation for every area

	Case 1	Case 2	Case 3
Area 1	50 kW	100 kW	150 kW
Area 2	100 kW	200 kW	300 kW
Area 3	50 kW	100 kW	150 kW
Total attack power	200 kW	400 kW	600 kW

3.3.5 Increase in Demand

3.3.5.1 Case 1: Total Load Manipulation = 200kW

In this attack scenario, the adversary is presumed to have gained control over a substantial fleet of electric vehicles, orchestrating their simultaneous charging initiation to induce voltage degradation within the power grid. According to Figure 3.2 and Table 3.1, the load buses identified within the three designated zones are targeted at approximately 11:00 hours, coinciding with peak demand periods as illustrated in Figure 3.3. This coordinated assault forces electric vehicle charging stations to deliver excessive power to compromised vehicles, thereby depleting system resources and significantly degrading both voltage stability and frequency regulation. Consequently, such synchronized attacks across multiple bus locations possess the capability to destabilize the grid infrastructure and trigger cascading failures.

The graphical representation in Figure 3.5 illustrates the voltage profile for the affected loads and the three-phase current characteristics at load 1. Upon initiation of the attack at 11:00 hours, a voltage depression is observed throughout the system. Load 1 exhibits the minimal voltage reduction, while Load 33 demonstrates a moderately greater decline; however, Load 50 experiences the most substantial voltage drop, decreasing to 0.94 per unit. Nevertheless, the attack produces limited adverse effects, as all voltage magnitudes remain within acceptable operational limits ($\pm 10\%$). The current measurements reveal a sharp escalation in magnitude. Given that the analysis encompasses a 24-hour simulation period, the attack duration has been modeled to persist for 30 minutes to facilitate clear observation of system behavior, despite the fact that such disturbances could potentially cause damage within seconds prior to activation of power system protection mechanisms.

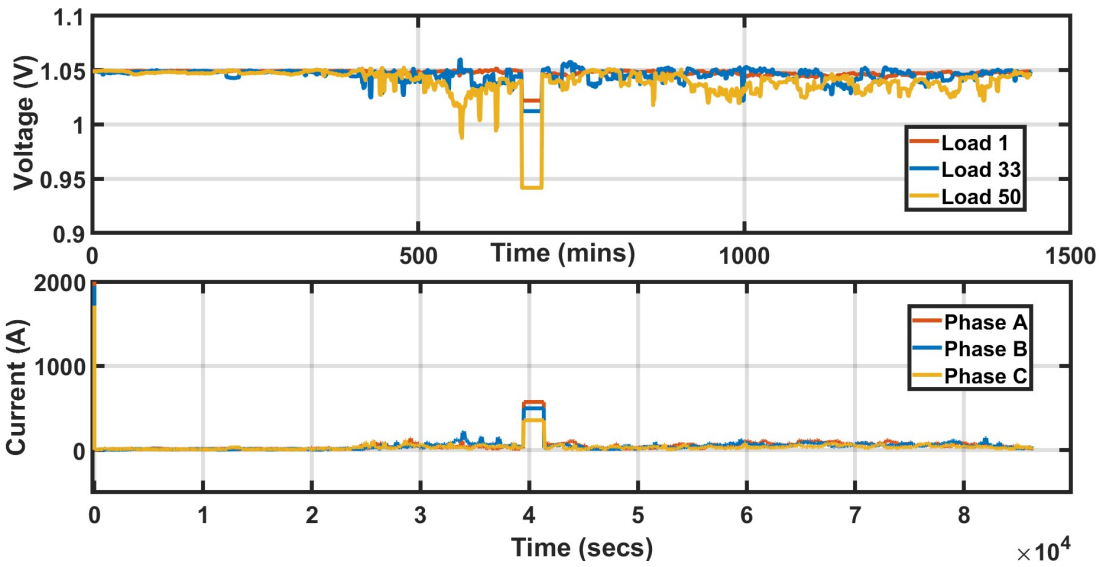

Figure 3.5: Increase in Demand of 200kW, (a) Bus voltages given in per unit, (b) 3-phase currents for Bus 1

3.3.5.2 Case 2: Total Load Manipulation = 400kW

The 400 kW attack scenario is illustrated in Figure 3.6. As observed, Load 50 exhibits a significantly more severe voltage decline, a phenomenon that may also be influenced by its geographical placement within the distribution system. Notably, the coordinated control of 400 kW proves sufficient to cause voltage depression beyond the -10% operational limit at select locations, though the substation itself does not experience such violations.

3.3.5.3 Case 3: Total Load Manipulation = 600kW

Figure 3.7 presents the results for an attack scenario with a magnitude of 600 kW. The analysis reveals that voltage levels reach a minimum of 0.7 per unit at certain grid locations, while the substation experiences comparatively modest reductions. Although the likelihood of an attack of this scale is relatively low, such an event could compromise system operability and performance. Generally, demand-escalation attacks produce relatively controllable consequences unless the electric vehicle charging station penetration level is substantial.

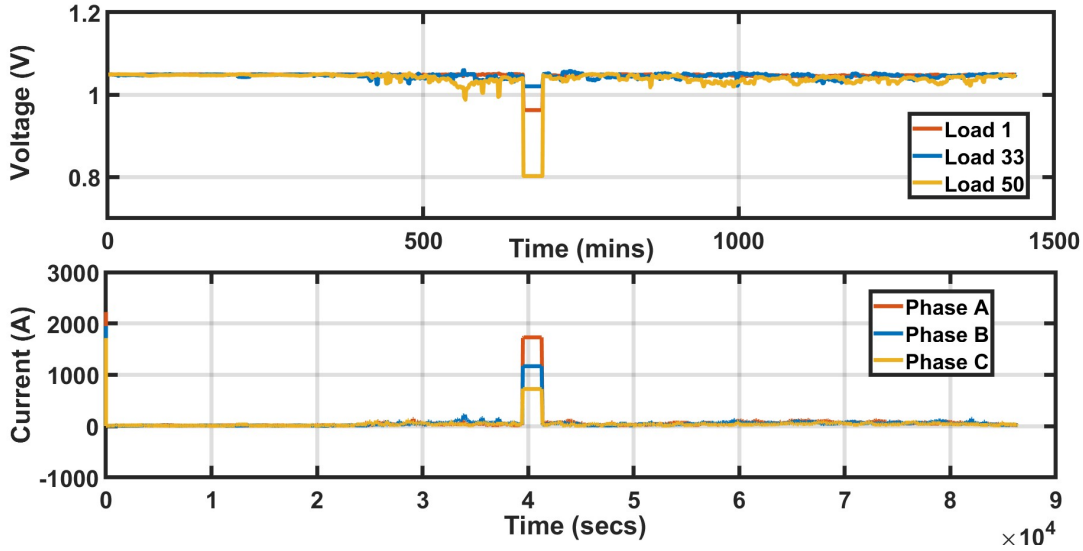

Figure 3.6: Increase in Demand of 400kW, (a) Bus voltages given in per unit, (b) 3-phase currents for Bus 1

3.3.6 Decrease in Demand

3.3.6.1 Case 1: Total Load Manipulation = 200kW

This attack paradigm considers the vehicle-to-grid (V2G) operational mode, enabling electric vehicles to function as prosumers. Under this scenario, the attacker orchestrates synchronized discharging of numerous connected electric vehicles, facilitating power injection back into the distribution network. The load buses are subjected to attack using the previously described approach. This is implemented through simulated load reduction at these buses around 23:00 hours, coinciding with a period of substantially lower demand as shown in Figure 3.3. The attack generates reverse energy flow from the electric vehicle fleet, creating a power surplus within the grid. This results in considerable voltage elevation at the targeted bus locations. The systemic consequences of this attack are presented in Figure 3.8.

Upon attack initiation at 23:00 hours, a substantial voltage elevation is observed throughout the system, with Load 50 experiencing an increase to 1.125 per unit, while Phase A currents rise to approximately 500 amperes.

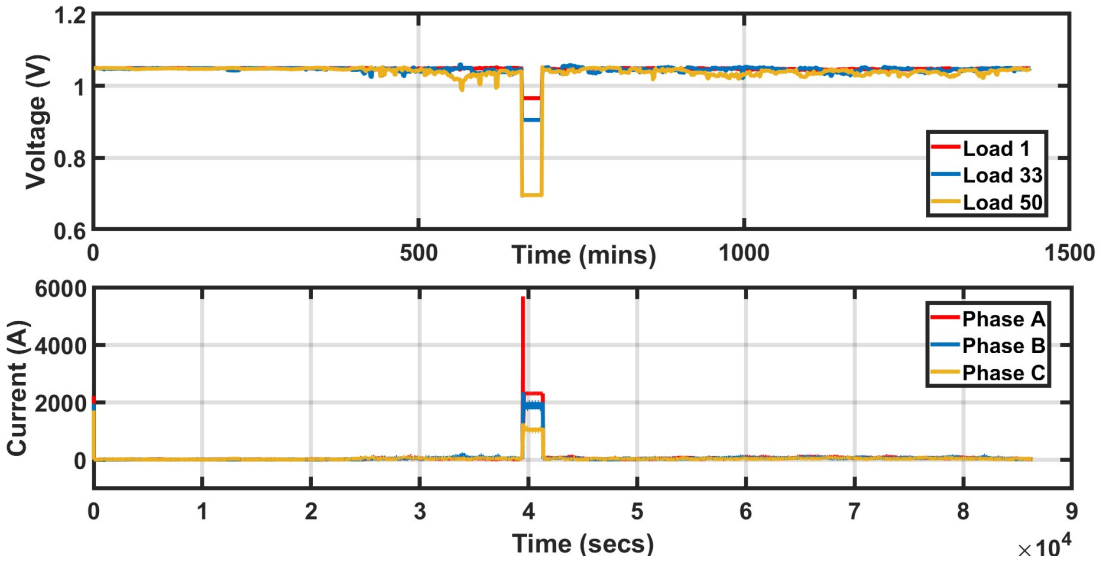

Figure 3.7: Increase in Demand of 600kW, (a) Bus voltages given in per unit, (b) 3-phase currents for Bus 1

3.3.6.2 Case 2: Total Load Manipulation = 400kW

When a power injection of 400 kW is applied, the electric vehicle loads experience elevated loading conditions, with the outcomes presented in Figure 3.9 demonstrating the system-wide effects. Under these conditions, the voltage magnitude approaches approximately 1.2 pu, while the current levels reach 1000 A. Notably, voltage elevations exceeding +10% are observed in proximity to the substation, attributable to its location adjacent to load 1. This magnitude of disturbance poses a significant threat to system integrity, as such scenarios exhibit a relatively high probability of occurrence and generate substantial adverse effects on network operation, specifically violating voltage regulations stipulated in the grid codes of numerous jurisdictions [81].

3.3.6.3 Case 3: Total Load Manipulation = 600kW

As anticipated, the system exhibits the most severe degradation under the third attack scenario, which, despite having the lowest probability of occurrence, presents the greatest risk to system stability when realized. Figure 3.10 illustrates the voltage and current characteristics observed during this attack condition. The voltage magnitude at load 50 surpasses 1.3 pu, while the current in all three phases exceeds 1000 A.

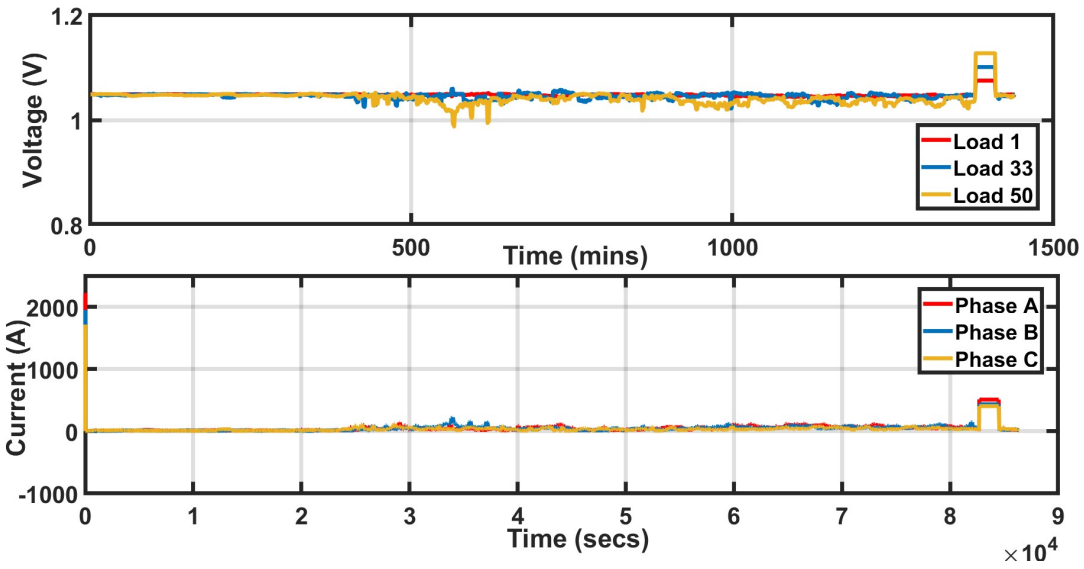

Figure 3.8: Decrease in Demand of 200kW, (a) Bus voltages given in per unit, (b) 3-phase currents for Bus 1

3.4 Use Case 2: cyberattacks against Energy Communities in Distribution Grids

REDII (Directive 2018/2001/EU) constitutes a comprehensive legal instrument for advancing renewable energy sources (RESs) while enabling participatory energy systems through collective self-consumption schemes (CSCs) and renewable energy communities (RECs). These mechanisms operationalize the principles of decentralized RES generation and collaborative energy utilization, with CSCs confined to intra-building arrangements and RECs extending to spatially proximate users relative to generation infrastructure. The integration of REDII provisions into national regulatory frameworks throughout the European Union has precipitated widespread REC establishment, thereby generating substantial market requirements for digital platforms capable of coordinating the multifaceted administrative, financial, and technical operations inherent to community energy management. Platform functionality necessitates continuous access to confidential data streams, particularly high-resolution electricity consumption profiles of community members, alongside command-and-control capabilities for distributed assets such as heat pumps and battery energy storage systems (BESSs). This architectural configuration creates pronounced cybersecurity exposure, with malicious cyber intrusions presenting compound threat scenarios.

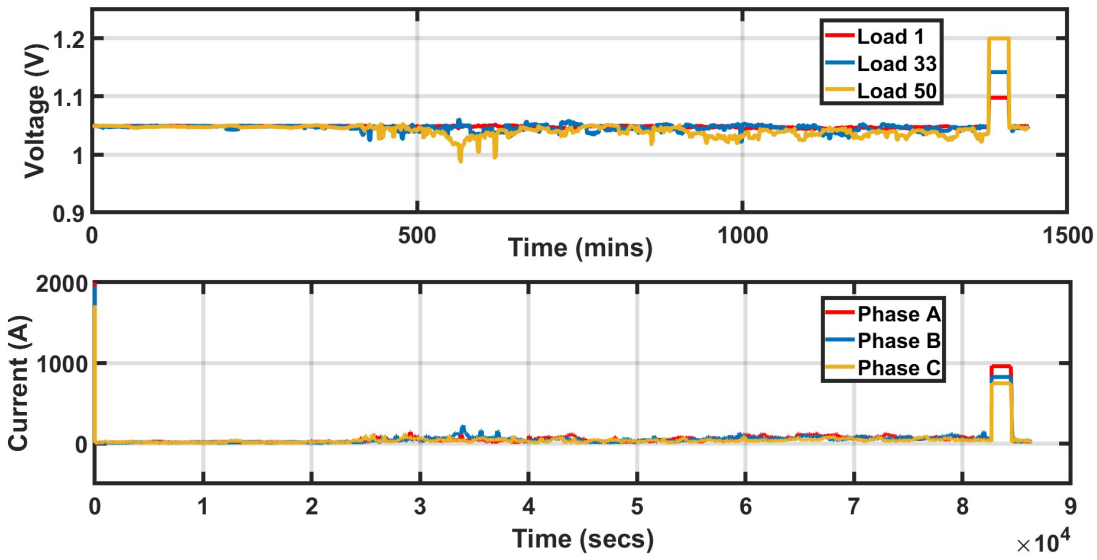

Figure 3.9: Decrease in Demand of 400kW, (a) Bus voltages given in per unit, (b) 3-phase currents for Bus 1

Renewable energy community (REC) participants leverage the existing electrical distribution infrastructure to facilitate energy sharing among members, subject to geographical proximity requirements between generation and consumption sites. The precise definition of "proximity" varies across jurisdictions, as its interpretation is deferred to national regulatory frameworks. For example, French [82] and Spanish [83] legislation restricts energy sharing to members connected downstream of a common secondary substation, whereas Italian regulations [84] permit sharing among participants supplied by the same primary substation. Both the communication architecture and electrical infrastructure supporting these communities are characterized by the absence of dedicated networks, instead relying predominantly on public internet connectivity. A schematic representation of this configuration is presented in Figure 3.11.

3.4.1 Cybersecurity Issues in Renewable Energy Communities

REC Management Platforms: The operational requirements of renewable energy communities necessitate sophisticated software infrastructure capable of streamlining administrative, financial, and technical management functions. To operate effectively, these platforms handle sensitive information including:

Real-time electricity consumption data from all REC members

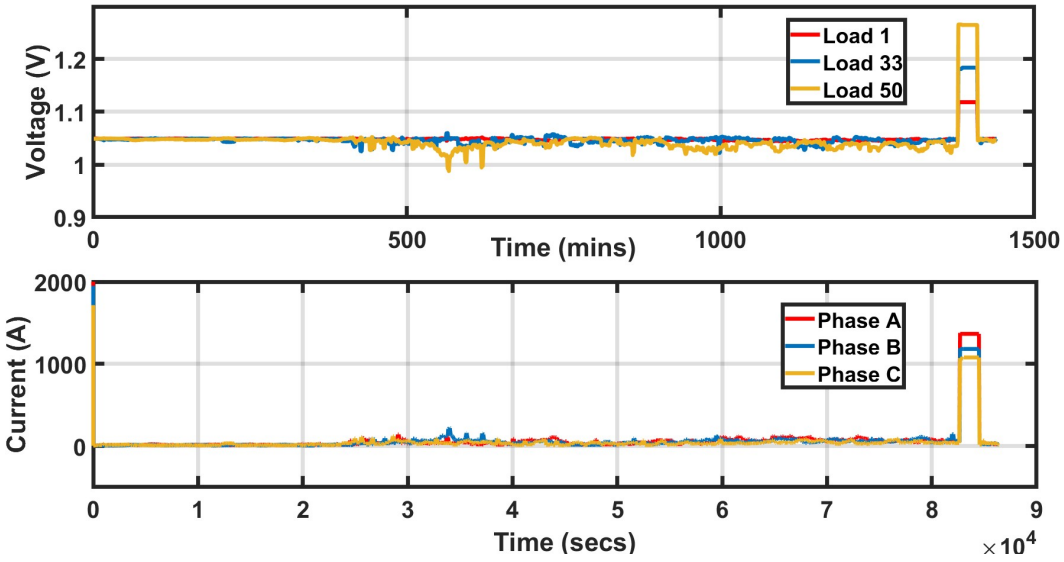

Figure 3.10: Decrease in Demand of 600kW, (a) Bus voltages given in per unit, (b) 3-phase currents for Bus 1

Generation profiles from distributed renewable sources (primarily photovoltaic systems)

Control capabilities for battery energy storage systems (BESSs)

Heat pump and controllable load management

Financial transaction data for energy sharing settlements

Communication Architecture: Within the REC ecosystem, three primary communication channels can be identified:

1. **Local communication:** Protocol exchanges between prosumer equipment (smart inverters, BESSs, smart meters) and the local gateway, typically utilizing Modbus, IEEE 802.11, or Bluetooth standards.

2. **Smart meter—DSO:** Advanced Metering Infrastructure (AMI) for billing, monitoring, and basic control. While technically outside the REC scope, this channel provides baseline measurement data.

3. **Smart gateway—Energy community manager:** The critical vulnerability point utilizing public internet infrastructure and common web protocols (HTTP/HTTPS, MQTT, or proprietary APIs).

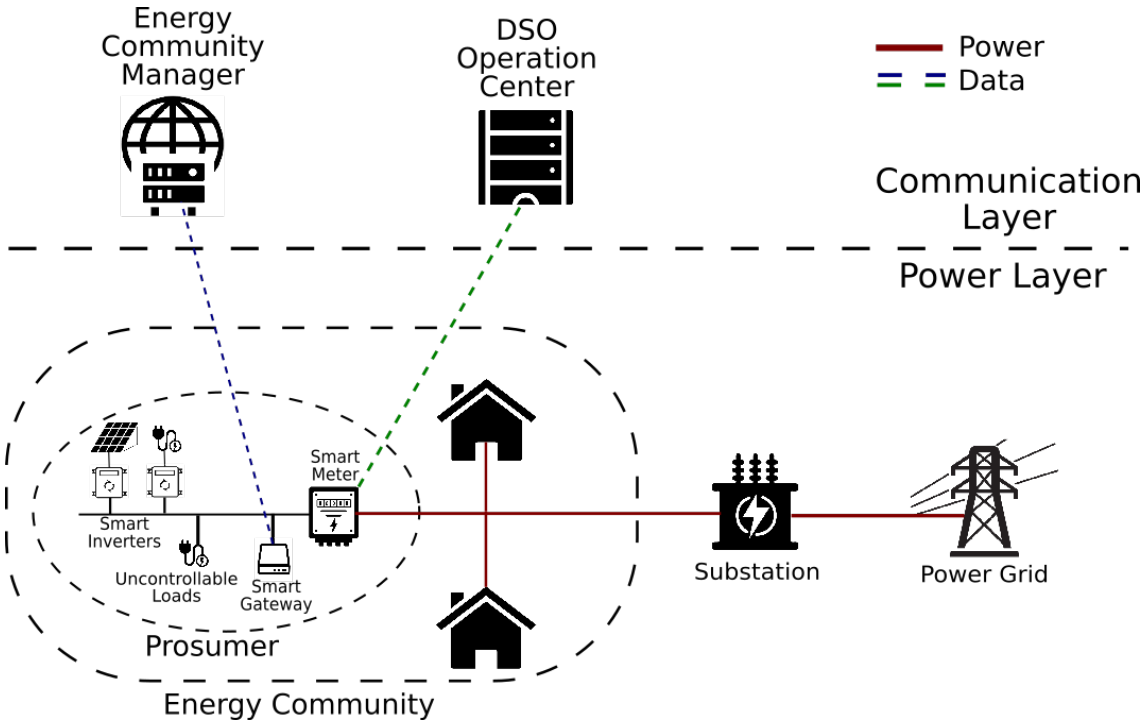

Figure 3.11: Architecture of a Renewable Energy Community

Vulnerability Assessment: The centralized platform architecture creates a single point of failure wherein compromise of the management system enables coordinated manipulation of all controllable assets. Common vulnerabilities include:

1. **Web application vulnerabilities:** SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF)
2. **Authentication weaknesses:** Weak password policies, lack of multi-factor authentication, session hijacking
3. **IoT device vulnerabilities:** Smart gateways often deployed on resource-constrained hardware with limited security capabilities
4. **Protocol vulnerabilities:** Inadequate encryption, lack of message authentication

The attack model depicted in Figure 3.12 illustrates potential compromise vectors.

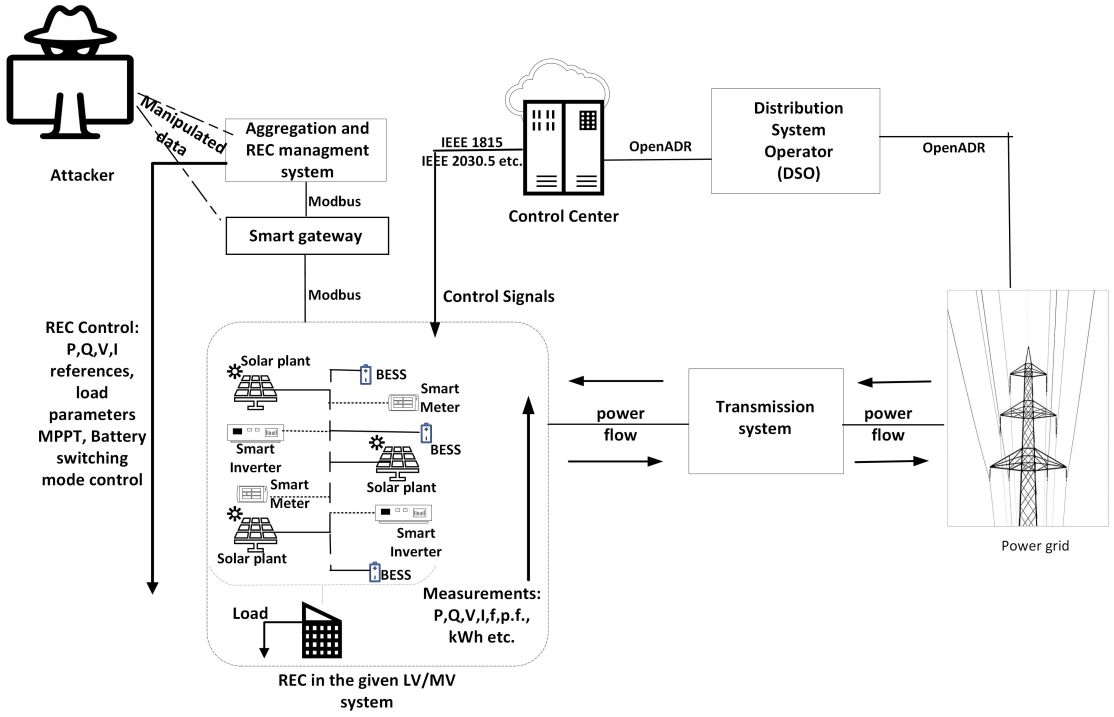

Figure 3.12: Architecture of a Renewable Energy Community

3.4.2 Test Systems for REC Analysis

To comprehensively assess cyberattack impacts on RECs, two distribution network configurations were analyzed corresponding to Italian regulatory frameworks:

Regulatory Context: Italian legislation initially restricted RECs through "Article 42-bis of Law No. 8" [85] to:

1. Low-voltage grid connections only
2. Maximum 200 kW aggregate generation capacity

Subsequently, "Legislative Decree No. 199" [84] relaxed these constraints for medium-voltage systems:

1. Maximum generation capacity increased to 1 MW.
2. The same primary substation must supply all members.

Table 3.2: Attack scenarios for LV REC system

	Case 1 (Injection)	Case 2 (Absorption)	Case 3 (Injection)
Area 1	50 kW	50 kW	100 kW
Area 2	100 kW	100 kW	200 kW
Area 3	50 kW	50 kW	100 kW
Total attack power	200 kW	200 kW	400 kW

3.4.2.1 Low-Voltage System: IEEE European Low-Voltage Test Feeder

The IEEE ELVTF (already described in Section 3.3.2) was utilized with a modified DER deployment to represent a 200 kW REC installation.

Under normal conditions, photovoltaic systems and BESSs operate according to complementary scheduling:

- Daytime (6 AM - 6 PM): PV systems active, BESSs charging from surplus generation.

- Evening/Night (6 PM - 6 AM): PV systems inactive, BESSs discharging to meet local demand.

The energy community scheme is illustrated in Figure 3.13

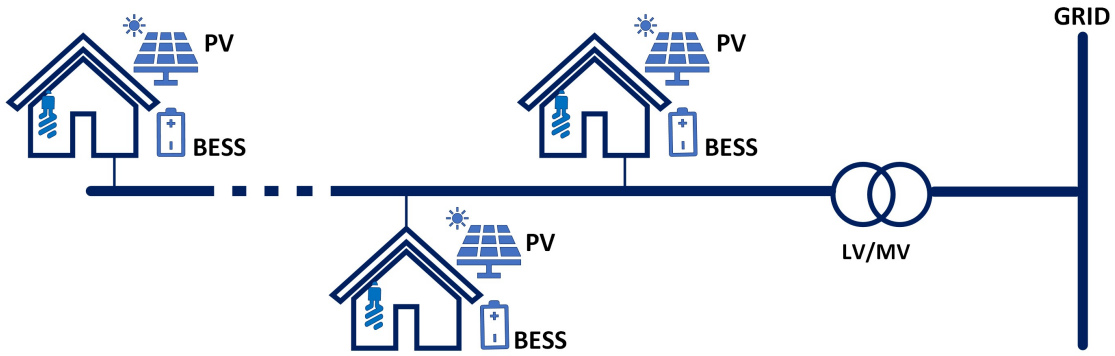

Figure 3.13: Energy community scheme implemented in use case scenarios.

Attack Scenarios for Low-Voltage REC: Table 3.2 presents three attack scenarios of increasing severity for the LV system:

Similar to the attack pattern in the case of 3.3.2, the load manipulations are followed according to the Italian load demand trend (3.3).

Scenario 1 - Power Injection Attack:

Timing: Early morning (5:30-7:00 AM) during load valley

Method: Simultaneous activation of all PV systems and BESS discharge

Objective: Create surplus generation during low-demand period

Table 3.3: Attack scenarios for MV REC system

	Case 1 (Injection)	Case 2 (Absorption)	Case 3 (Injection)	Case 4 (Injection)
Bus 41	800 kW	800 kW	400 kVAr (ind.)	400 kVAr (cap.)
Bus 19	800 kW	800 kW	400 kVAr (ind.)	400 kVAr cap.)
Bus 60	400 kW	400 kW	200 kVAr (ind.)	400 kVAr (cap.)
Total attack power	1MW	1MW	1 MVAr (ind.)	1 MVAr (cap.)

Scenario 2 - Power Absorption Attack:

Timing: Morning peak (8:00-11:00 AM) during high demand

Method: Forced charging of all BESSs while PV offline or curtailed

Objective: Create artificial demand spike

Scenario 3 - Maximum Injection Attack:

Timing: Early morning valley

Method: All assets at maximum output (doubling normal capacity)

Objective: Test worst-case voltage rise scenario

3.4.2.2 Medium-Voltage System: IEEE 69-Bus Test Feeder

For MV analysis, the IEEE 69-bus system was selected with the following characteristics:
Network Specifications:

Voltage Level: 12.67 kV line-to-line

Topology: 69 nodes, 73 branches (radial configuration)

Base Power: 10 MVA

Total Active Load: 3.8 MW

Total Reactive Load: 2.69 MVAr

REC Deployment for MV System: Given the larger geographic area and higher voltage level, the 1 MW REC capacity was distributed across four sub-communities at strategic network locations as shown in Figure 3.14.

Attack Scenarios for Medium-Voltage REC: Table 3.3 outlines the attack scenarios considered for the medium-voltage (MV) system. The analysis examines four forms of power manipulation: the first two involve the injection and withdrawal of active power, while the latter two concern the injection of reactive power—specifically inductive (".ind" in Table 3.3) and capacitive (".cap"). Assessing reactive power at the MV level is significant because large reactive power excursions can materially affect the grid's operating profile.

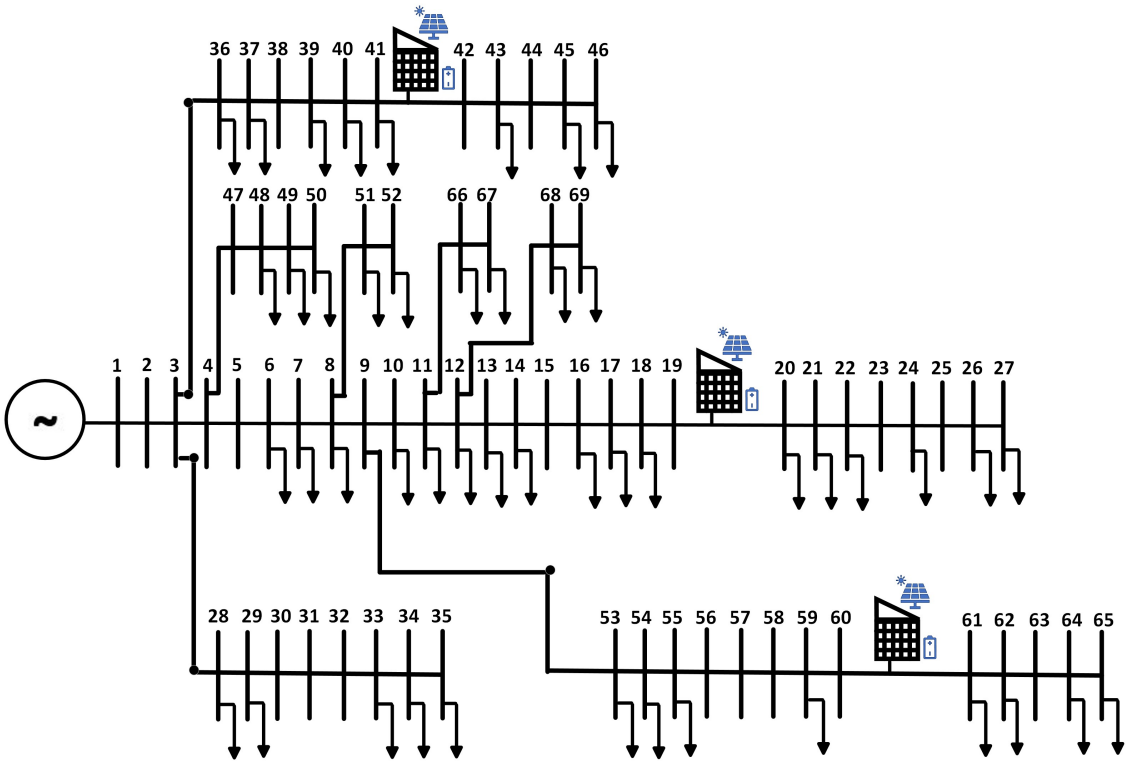

Figure 3.14: Single-line diagram of IEEE 69-bus system integrated with REC.

3.4.3 Results: Low-Voltage REC Attacks

3.4.3.1 Case 1: Active Power Injection (200 kW)

Under normal daytime operation with PV generation active, BESSs should remain in charging or standby mode. However, if an attacker forces simultaneous discharge of all 200 kW BESS capacity during early morning low-demand period (5:30-7:00 AM), significant voltage elevation occurs. Figure 3.15 presents the voltage and current profiles for the 200 kW injection attack.

Observations:

Load 1 (Substation): Voltage rises to approximately 1.06 pu (marginal increase)

Load 34 (Mid-feeder): Voltage rises to 1.12 pu, exceeding +10% limit

Load 50 (Feeder end): Most severe impact at 1.12 pu

Duration: Attack initiated at 500 minutes (8:20 AM) for a 30-minute duration

Current: Reverse power flow evident with negative current direction

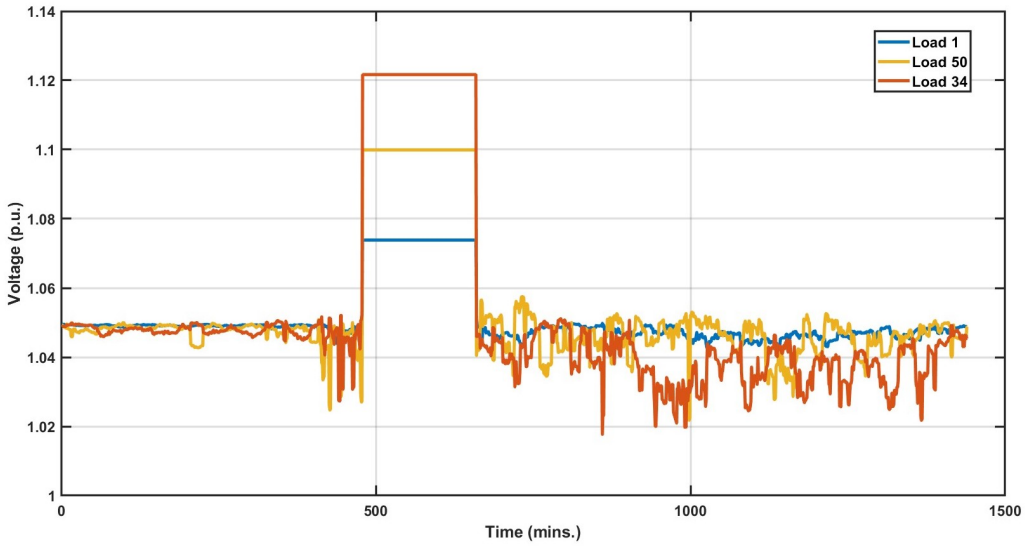

Figure 3.15: Voltage profile for an injection of 200 kW active power.

Analysis: The 200 kW injection creates localized overvoltage violations at mid-feeder and end-feeder locations. Area 2's central position and 100 kW contribution amplify impacts at Load 34. While the substation remains within limits, protection devices at outlying buses may trip, causing service interruption.

3.4.3.2 Case 2: Active Power Absorption (200 kW)

This attack forces all BESSs into charging mode during morning peak demand (8:00-11:00 AM), effectively adding 200 kW load when the system already experiences high consumption. Figure 3.16 shows voltage depression results.

Observations:

Load 1: Voltage drops to 0.98 pu (within limits)

Load 34: Voltage drops to 0.95 pu (approaching -5% threshold)

Load 50: Severe drop to 0.87 pu, violating -10% limit

Current: Sharp increase indicating heavy loading

Attack timing: 500-minute mark (8:20 AM) during demand ramp-up

Analysis: Absorption attacks prove more damaging than injection attacks in LV systems. The combination of existing peak demand plus 200 kW additional load creates voltage violations at feeder extremities. Load 50 experiences 13% undervoltage, likely triggering undervoltage protection.

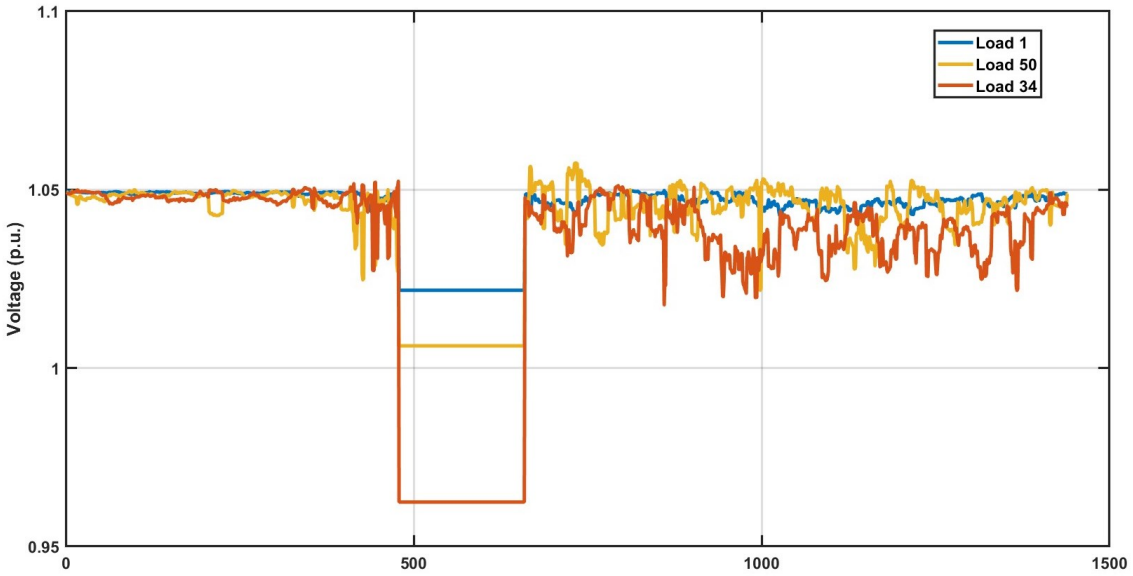

Figure 3.16: Voltage profile for an injection of 200 kW active power.

3.4.3.3 Case 3: Maximum Injection (400 kW)

TThe most severe LV attack scenario assumes the attacker overrides all capacity limits, forcing both PV and BESS to maximum simultaneous output during low-demand period. Figure 3.17 illustrates catastrophic overvoltage conditions:

Observations:

Load 1:Voltage rises to 1.10 pu (substation affected)

Load 34: Voltage reaches 1.15 pu

Load 50: Critical overvoltage at 1.18 pu (+18%)

Current: Extreme reverse power flow

Attack timing: Early morning (approximately 5:30 AM) for maximum impact during demand valley

Analysis:

This worst-case scenario demonstrates that if attackers achieve full control, they can create system-wide overvoltage conditions. Even the substation experiences +10% voltage rise, while feeder ends approach +20%. Such conditions would immediately trip overvoltage protection, disconnecting the entire substation and causing widespread outage.

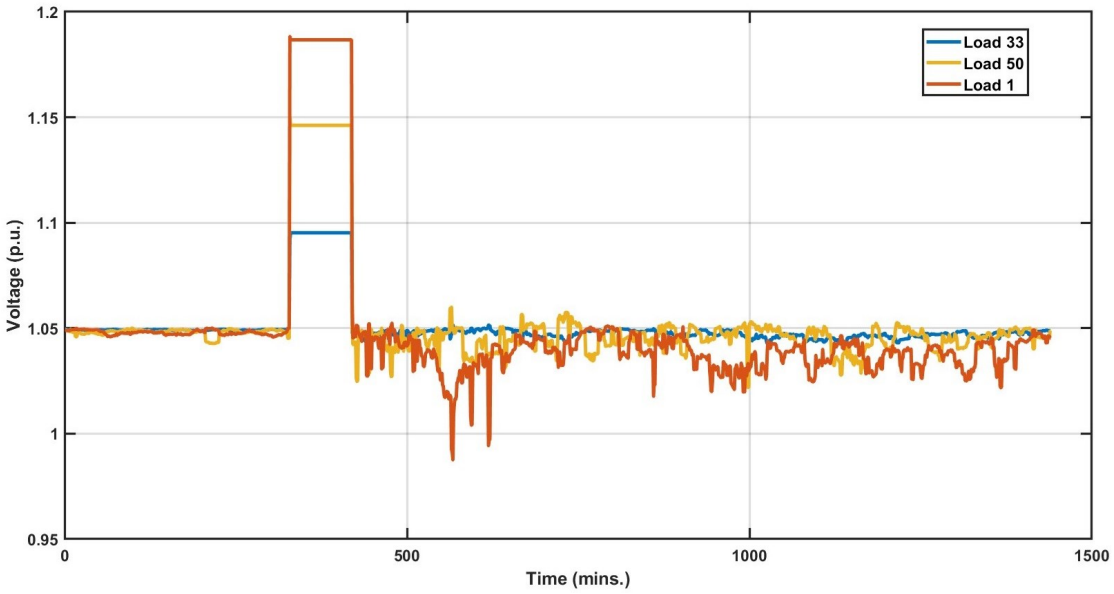

Figure 3.17: Voltage profile for an injection of 200 kW active power.

3.4.4 Results: Medium-Voltage REC Attacks

For MV analysis, voltage (pu), current waveforms, and active/reactive power were measured at Bus 13 (mid-feeder location) and Bus 1 (substation). Results are presented for 10-second windows to capture transient attack dynamics.

3.4.4.1 Case 1: Active Power Injection (2 MW)

Under nominal conditions, the PV plant delivers 1 MW of active power and the battery remains offline. An adversary who seizes control of the battery could force it online at its rated 1 MW, doubling the net active injection to 2 MW and creating a power surplus.

Figure 3.18 presents comprehensive results:

Observations:

Subplot (a) - Bus Voltage Profiles:

Bus 1 (substation): Voltage rises to 1.30 pu during attack

Bus 13 (mid-feeder): Catastrophic rise to 1.80 pu

Attack initiation: Clear voltage step at 4 seconds

Recovery: Immediate return to normal upon attack cessation

Subplot (b) - Instantaneous Voltage and Current:

Voltage and current remain in-phase (unity power factor operation)

Current magnitude increases to 2000 A peak

Clean sinusoidal waveforms indicate inverter control maintained

Subplot (c) - Active and Reactive Power at Bus 13:

Active power: 2 MW injection (positive value)

Reactive power: Near zero ($Q \approx 0$), confirming unity power factor

Step change clearly visible at attack initiation/termination

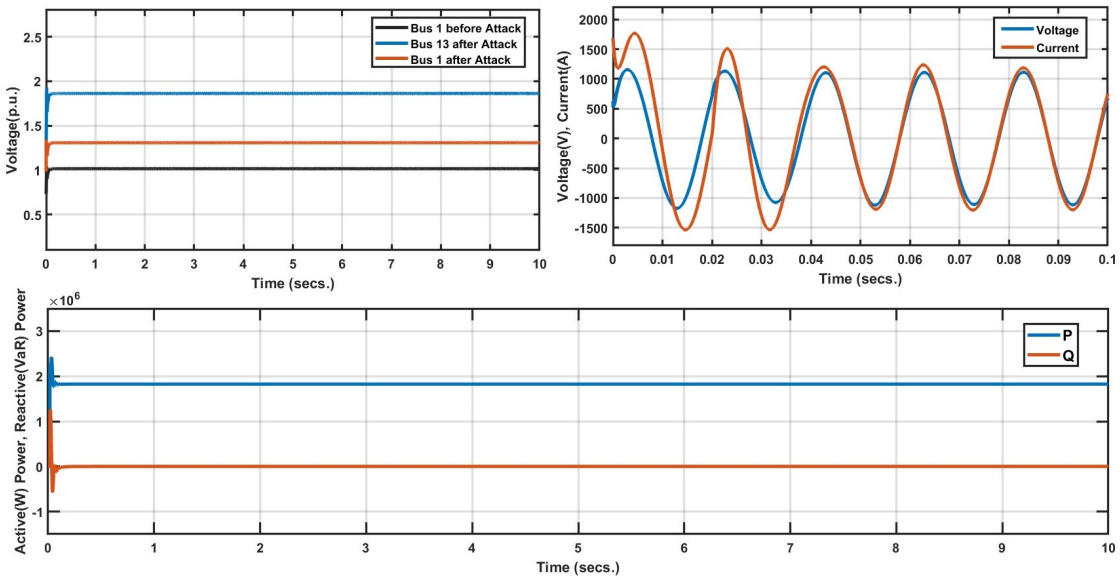

Figure 3.18: Voltage profile for an injection of 200 kW active power.

Analysis: The 2 MW active power injection creates extreme overvoltage, particularly at Bus 13 where voltage reaches 1.80 pu (+80%). This represents a catastrophic grid condition that would trigger instantaneous overvoltage protection, likely causing:

1. Immediate disconnection of the affected feeders
2. Potential transformer damage if sustained
3. Cascading tripping of adjacent feeders
4. Extended service interruption during system restoration

The MV system demonstrates greater vulnerability to injection attacks compared to absorption attacks due to typically light loading conditions.

3.4.4.2 Case 2: Active Power Absorption (2 MW)

This scenario corresponds to periods when the PV plant is offline and the battery provides the required energy. If an attacker forces the battery into charging mode, it effectively becomes an additional load, thereby perturbing the system and inducing distortions in both voltage and current profiles. Figure 3.19 presents absorption attack results:

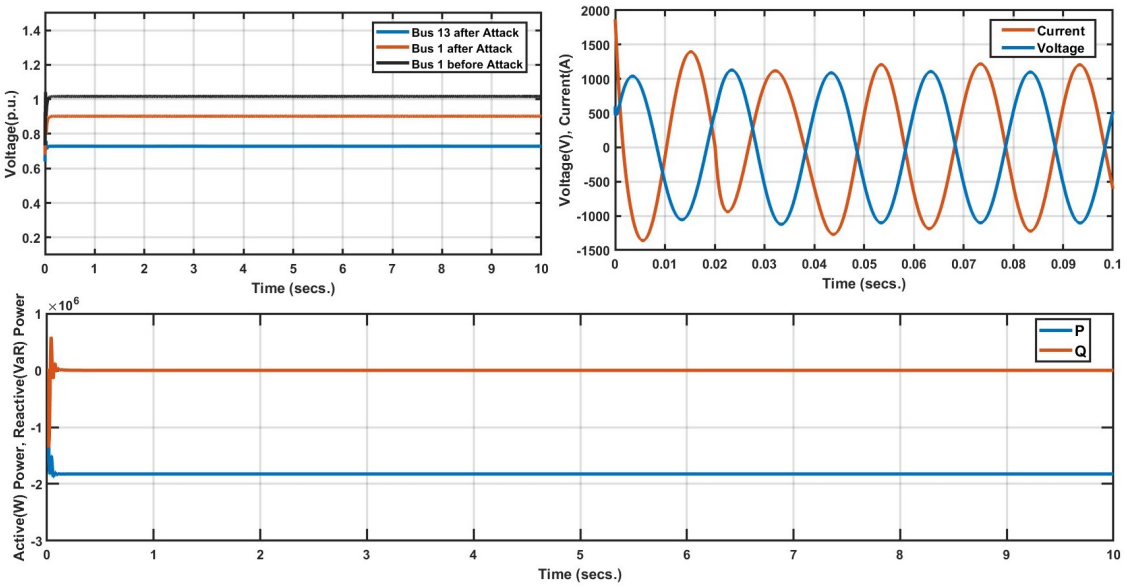

Figure 3.19: Voltage profile for an injection of 200 kW active power.

Observations:

Subplot (a) - Bus Voltage Profiles:

Bus 1: Voltage drops to 0.88 pu (-12%)

Bus 13: Severe drop to 0.75 pu (-25%)

Attack duration: 4-5 second window clearly visible

Subplot (b) - Instantaneous Voltage and Current:

Voltage and current phase shift indicates reactive power demand

Current magnitude reaches about 1500 A

Voltage waveform distortion evident during transient

Subplot (c) - Active and Reactive Power at Bus 13:

Active power: -2 MW (negative indicates absorption)

Reactive power: Minimal variation around zero

Clear step response at attack boundaries

Analysis: While absorption attacks create less severe voltage violations than injection attacks, the 25% undervoltage at Bus 13 remains catastrophic. Such conditions would trigger:

1. Undervoltage load shedding (if implemented)
2. Motor stalling and equipment damage
3. Potential voltage collapse if multiple feeders affected simultaneously
4. Automatic reclosing attempts may fail, requiring manual restoration

The 12% undervoltage at the substation (Bus 1) indicates system-wide impact extending beyond the local feeder.

3.4.4.3 Case 3: Inductive Reactive Power Injection (1 MVAr)

In this scenario, the adversary manipulates the system's reactive power. By commandeering the battery and PV inverters, they can inject substantial inductive or capacitive reactive power into the grid alongside active power. Figure 3.20 presents an inductive reactive power attack:

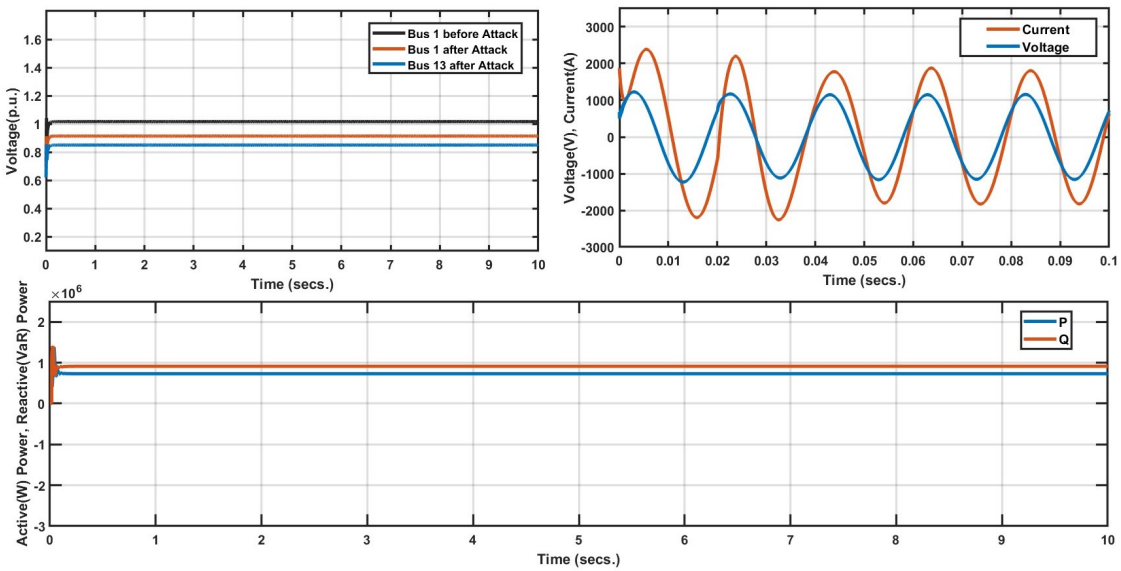

Figure 3.20: Grid parameters for 1 MVAr inductive reactive power injection: (a) p.u. voltage profiles of grid buses, (b) voltage and current waveforms at time of attack, and (c) total active and reactive power measured at bus 13.

Observations:

Subplot (a) - Bus Voltage Profiles:

Bus 1: Voltage drops to 0.90 pu

Bus 13: Drops to 0.80 pu (-20%)

Less severe than active power attacks but still violates limits

Subplot (b) - Instantaneous Voltage and Current:

Current lags voltage (inductive power factor)

Characteristic lagging power factor waveform

Current magnitude 1500 A

Subplot (c) - Active and Reactive Power at Bus 13:

Active power: 800 kW (moderate level)

Reactive power: +1 MVAr (positive indicates inductive/lagging)

Combined P and Q create apparent power stress

Analysis: Inductive reactive power injection creates voltage depression through two mechanisms:

1. Direct reactive power absorption increases voltage drop across line impedances
2. Increased current magnitude (for fixed active power) amplifies resistive losses

The 20% undervoltage at Bus 13 demonstrates that reactive power manipulation alone can create severe grid disturbances, even without maximizing active power attack magnitude. This attack vector may evade detection systems focused solely on active power anomalies.

3.4.4.4 Case 4: Capacitive Reactive Power Injection (1 MVAr)

Conversely, the adversary can now command the inverters to inject capacitive reactive power (leading, injecting vars) while BESSs charge creates voltage elevation. Figure 3.21 presents capacitive reactive power attack:

Observations:

Subplot (a) - Bus Voltage Profiles:

Bus 1: Rises to 1.12 pu (+12%)

Bus 13: Rises to 1.20 pu (+20%)

Substation experiences significant overvoltage

Subplot (b) - Instantaneous Voltage and Current:

Current leads voltage (capacitive power factor)

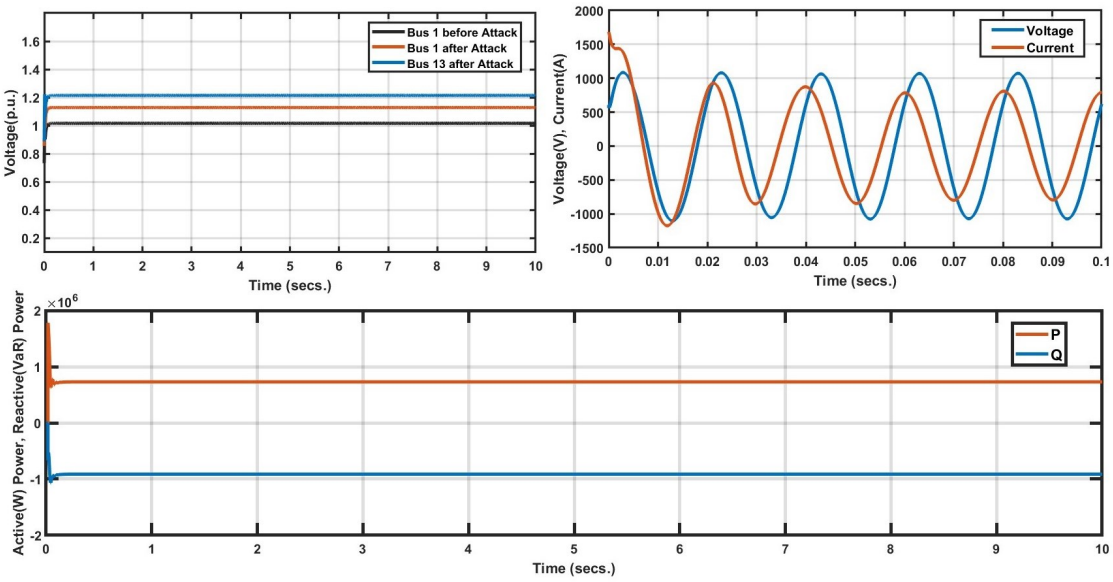

Figure 3.21: Grid parameters for 1 MVAr capacitive reactive power injection: (a) p.u. voltage profiles of grid buses, (b) voltage and current waveforms at the time of attack, and (c) total active and reactive power measured at bus 13.

Leading power factor characteristic evident
Current 1200 A with voltage elevation
Subplot (c) - Active and Reactive Power at Bus 13:
Active power: Negative (BESS charging, -800 kW)
Reactive power: Negative (capacitive injection, -1 MVAr)
Double impact from both P and Q
Analysis: This scenario represents a "double manipulation" attack combining:

1. Capacitive reactive power injection (raises voltage)

2. Active power absorption through BESS charging (reduces loading, raises voltage)

The synergistic effect creates +20% overvoltage at Bus 13 and +12% at the substation—both severe violations. This attack demonstrates that sophisticated adversaries could maximize impact by coordinating active and reactive power manipulation. The substation-level overvoltage indicates potential for system-wide disruption affecting all connected feeders.

3.5 Discussion

This chapter has provided comprehensive quantitative analysis of cyberattack impacts on distribution grids with high penetration of controllable distributed energy resources through two distinct use cases: Electric Vehicle Charging Stations (EVCS) and Renewable Energy Communities (RECs). The systematic simulation studies across both low-voltage and medium-voltage systems reveal several critical insights regarding the vulnerability of modern distribution grids to cyber-physical attacks.

3.5.1 Comparative Analysis: EVCS vs. REC Vulnerabilities

While both EVCS and REC systems demonstrate significant vulnerability to load manipulation attacks, important differences emerge in their threat profiles:

Attack Surface Characteristics:

EVCS systems present a more dynamic attack surface due to the mobile nature of electric vehicles and their variable connection patterns. The charging behavior exhibits predictable temporal patterns (workplace charging during daytime, residential charging overnight), which attackers can exploit for maximum impact. In contrast, RECs combine both generation (PV systems) and storage (BESS) assets, providing attackers with additional degrees of freedom—the ability to manipulate not only demand but also generation and reactive power simultaneously.

Attack Magnitude Comparison: For the low-voltage IEEE ELVTF system with 200 kW installed capacity:

1. EVCS absorption attacks (forced charging) created voltage drops to 0.87 pu at feeder extremities
2. REC absorption attacks (BESS charging with PV curtailed) produced similar voltage drops to 0.87 pu
3. EVCS injection attacks (V2G discharge) caused voltage rise to approximately 1.12-1.13 pu
4. REC injection attacks (simultaneous PV and BESS discharge) produced comparable voltage rise to 1.12 pu

The similarity in voltage deviation magnitudes indicates that at the 200 kW level, the specific DER technology (EVCS vs. REC) matters less than the total controllable capacity and attack timing.

Spatial Impact Patterns:

Both use cases demonstrated that voltage violations concentrate at feeder extremities (Loads 34, 50) rather than near the substation (Load 1) for 200 kW attacks. This spatial pattern reflects the fundamental electrical distance relationship in radial distribution systems—voltage deviations accumulate along feeder impedance. However, when attack magnitude increases to 400-600 kW, substation-level impacts emerge, indicating potential for system-wide disruption.

3.5.2 Attack Timing and Load Correlation

The strategic timing of attacks significantly amplified their impacts across both use cases:

Injection Attacks: Maximum impact occurred during load valley periods (early morning 5:30-7:00 AM, late evening 8:00-11:00 PM) when:

1. System voltage already elevated due to light loading
2. Voltage regulation equipment (tap changers, capacitor banks) positioned for low-load conditions
3. Minimal load diversity to absorb excess generation
4. Reverse power flow potentially overwhelming substation transformer rating

The Italian load profile data (Figure 3.3) showed demand valleys around 25-30 GW nationally, corresponding to minimum loading at distribution level. Injection attacks timed to these valleys created the maximum voltage rise scenarios observed (1.18 pu for 400 kW LV, 1.80 pu for 2 MW MV).

Absorption Attacks:

Maximum impact occurred during peak demand periods (morning 8:00-11:00 AM, evening 6:00-8:00 PM) when:

1. System voltage already depressed due to heavy loading
2. Distribution transformers and feeders operating near capacity
3. Voltage regulation equipment at maximum boost position

4. Additional load creating compound stress on already-loaded infrastructure

The 200 kW LV absorption attack timed to morning peak produced 0.87 pu voltage (13% drop), while the same attack during off-peak would create minimal impact. This 13% differential demonstrates the critical importance of temporal attack coordination.

Implications for Attack Detection:

The timing dependence suggests that effective anomaly detection systems must consider temporal context. A 200 kW EVCS demand spike might be normal during evening hours but highly anomalous at 3:00 AM. Similarly, 1 MW REC generation is expected at solar noon but suspicious before sunrise. Detection algorithms that incorporate time-of-day, seasonal patterns, and correlation with solar/weather conditions will prove more effective than simple threshold-based approaches.

3.5.3 Voltage Level Comparison: LV vs. MV Systems

The analysis reveals fundamentally different vulnerability profiles between low-voltage and medium-voltage distribution systems:

Low-Voltage System Resilience:

The IEEE ELVTF exhibited relative resilience to attacks below 200 kW, with voltage deviations remaining within or marginally exceeding ±10% grid code limits. This resilience stems from:

1. Lower feeder impedances (shorter cable lengths, larger conductor cross-sections)
2. Lower X/R ratios, making voltage less sensitive to reactive power variations
3. Transformer voltage regulation capabilities at the LV substation

However, this resilience disappeared when the attack magnitude reached 400 kW, demonstrating a clear threshold effect. At 400 kW injection, even the substation experienced voltage rise to 1.10 pu, indicating that the LV system's protection mechanisms become overwhelmed beyond this threshold.

Medium-Voltage System Vulnerability:

The IEEE 69-bus MV system demonstrated extreme vulnerability even to attacks within rated capacity limits:

1. 2 MW active power injection created catastrophic 1.80 pu voltage at Bus 13 (+80% overvoltage)

2. 2 MW active power absorption produced 0.75 pu voltage at Bus 13 (-25% undervoltage)
3. 1 MVAr reactive power manipulation alone caused 20% voltage deviations
4. Substation (Bus 1) experienced 12-30% voltage deviations, indicating system-wide impact

This heightened vulnerability reflects the electrical characteristics of MV systems:

1. Higher feeder impedances due to longer line lengths
2. Higher X/R ratios, increasing sensitivity to both active and reactive power flows
3. Radial topology with limited voltage regulation capabilities between the primary substation and load centers

The MV results suggest that current regulatory capacity limits (1 MW for RECs in Italy) may create unacceptable cyber-physical security risks without adequate protective countermeasures.

3.6 Chapter Summary

This chapter established quantitative cybersecurity thresholds for distribution grids through systematic simulation of EVCS and REC cyberattacks. Key findings include: (1) LV systems remain resilient below 200 kW but fail at 400 kW; (2) MV systems show extreme vulnerability with 2 MW attacks creating catastrophic 80% overvoltage; and (3) reactive power manipulation constitutes an underappreciated attack vector, with 1 MVAr producing 20% voltage deviations. The results demonstrate that current Italian regulatory limits (200 kW EVCS, 1 MW RECs) already create exploitable vulnerabilities, with MV systems requiring immediate attention. Attack timing coordination with demand patterns amplifies impact by 30-50%, necessitating temporal-aware detection systems.

Having quantified the system-level impacts of cyberattacks on distribution grids, the following chapter addresses detection at the fundamental DER unit—individual photovoltaic systems.

3.6.1 Research Limitations and Scope Considerations

While this chapter provides quantitative analysis of cyberattack impacts on distribution grids, several methodological limitations require acknowledgment to properly contextualize the findings.

The simulations employed fixed network topologies based on IEEE standard test feeders (European Low-Voltage Test Feeder and IEEE 69-Bus distribution system). Real distribution networks undergo topology changes through switching operations for load balancing, fault isolation, and maintenance. Attack impacts may vary depending on network configuration at the time of compromise.

For instance, the 1.80 pu overvoltage observed at Bus 13 during the 2 MW MV injection attack assumes the specific radial configuration of the IEEE 69-bus test system. Alternative configurations with different switching states or tie-line connections could produce different voltage profiles. The results therefore, represent impacts under the analyzed configurations rather than all possible operational states.

The analysis focused on immediate physical impacts without modeling operator intervention or automated control responses. In practice, distribution system operators would implement responses including:

- Manual voltage regulation via on-load tap changer (OLTC) adjustments

- Re-dispatch of DER generation setpoints

- Network reconfiguration to isolate affected areas

- Intentional load shedding or generation curtailment

These actions would likely reduce attack severity and duration. The presented results therefore represent worst-case scenarios without active mitigation—essentially answering "what happens if an attack occurs and operators cannot respond immediately?" This conservative approach ensures protection mechanisms designed using these results will be robust to operator response delays.

Simulations examined localized impacts within single distribution feeders. Potential cascading effects to neighboring feeders or upstream transmission systems were not modeled. While cascading failures are possible for large-scale coordinated attacks, quantifying these effects requires:

- Multi-feeder co-simulation with transmission system models

- Detailed protection coordination schemes across voltage levels

- Probabilistic failure modeling of protection devices

The catastrophic 1.80 pu overvoltage at Bus 13 would likely trigger protective relays, potentially causing cascading trips if protection coordination is inadequate. However, analyzing the propagation of such events across interconnected distribution networks was beyond this study's scope. The Chapter 6 circuit breaker-based incident response mechanisms aim to prevent cascading failures through early detection and isolation, addressing this limitation in future work.

The threat model assumes attackers achieve perfect control over compromised DERs with instantaneous command execution. Real-world attacks face practical constraints:

- Communication latencies in attack command delivery (50-500ms for ICS protocols)

- Partial system compromise affecting only subsets of DERs

- Physical control limitations preventing certain operations

- Detection during attack execution triggering defensive responses

Results therefore represent upper bounds on attack effectiveness given idealized capabilities. Actual impacts may be reduced by implementation constraints. For example, the coordinated 2 MW injection attack assumes simultaneous activation of both the 1 MW PV plant and 1 MW battery. Communication delays might desynchronize this coordination, reducing peak impact magnitude. This conservative approach ensures protective systems designed based on these results remain adequate even against sophisticated adversaries with significant resources.

Simulations employed deterministic load profiles based on Terna historical data and standard solar irradiance models. Real systems experience stochastic variations from individual consumer behavior, cloud transients causing rapid PV fluctuations, and phase imbalances. These factors could either mask attack signatures (making detection harder) or amplify voltage fluctuations (increasing severity).

Despite these limitations, the analysis provides rigorous quantitative foundations for understanding DER cyber-physical attack impacts. The conservative assumptions ensure security mechanisms designed using these results will be robust to real-world operational variations.

CHAPTER 4

Dataset Development and Benchmarking for PV System Cybersecurity

This chapter presents the development and validation of Photo-Set, a comprehensive dataset specifically designed for cybersecurity monitoring in photovoltaic systems. The work progressed through three distinct phases: initial dataset creation and characterization, establishment of detection algorithm benchmarks, and development of advanced physics-informed detection methods. The dataset addresses a critical gap in PV cybersecurity research by providing physics-based measurements under various attack scenarios, enabling the development and validation of anomaly detection algorithms.

4.1 Dataset Development

4.1.1 Motivation and Background

Modern photovoltaic systems face increasing cybersecurity threats due to their integration with smart grid infrastructure. Research has examined the impact of cyberattacks on numerous DERs, particularly storage systems, showing violated voltage boundaries in

The content of this chapter has been published in the following papers:

A. Mokarim, G. B. Gaggero, G. Ferro, M. Robba, and M. Marchese, "Photo-Set: A Dataset for Physics-Based Cybersecurity Monitoring in Photovoltaic Systems," IFAC-PapersOnLine, vol. 59, no. 9, pp. 37-42, 2025, doi: 10.1016/j.ifacol.2025.08.109.

A. Mokarim, G. B. Gaggero, G. Ferro, M. Robba, P. Girdinio, and M. Marchese, "Photo-Set: A Proposed Dataset and Benchmark for Physics-Based Cybersecurity Monitoring in Photovoltaic Systems," Energies, vol. 18, no. 19, p. 5318, Oct. 2025, doi: 10.3390/en18195318.

D. Fernández Valderrama, G. B. Gaggero, G. Ferro, A. Mokarim, M. Robba, P. Girdinio, and M. Marchese, "An online intrusion detection system for photovoltaic generators through physics-based neural networks," Electric Power Systems Research, vol. 253, p. 112528, 2026, doi: 10.1016/j.epsr.2025.112528.

medium voltage grids [86]. Zografopoulos et al. [87] analyzes attacking DER assets, revealing significant operational impacts from protocol and device-level vulnerabilities, and discusses mitigation strategies in DER cybersecurity. Anomaly detection is crucial in various fields, including cybersecurity, where atypical patterns often indicate critical incidents such as security breaches or device failures. Traditional anomaly detection methods for cybersecurity typically focus on network traffic data and logs generated by applications running on network nodes. In contrast, physics-based anomaly detection introduces a novel paradigm by leveraging domain-specific knowledge from physics to enhance the detection process. By integrating this knowledge, system behavior can be more accurately modeled, improving the identification of deviations and signal anomalies. A comprehensive literature review on physics-based anomaly detection is presented in [61].

Newer approaches increasingly rely on deep learning, which addresses issues such as the growing volume of data and the need for domain-specific knowledge [66]. Shilay et al. [88] discusses an anomaly detection algorithm designed to uncover attacks on PV systems, including PV disconnect, power curtailment, Volt-var attacks, and reverse power flow in distribution grids by using semi-supervised machine learning algorithms. This field is advancing due to developments in neural network techniques, including Physics-Informed Neural Networks (PINNs), which incorporate physics constraints into the optimization functions of neural networks [89]. Gaggero et al. [90] introduces an autoencoder-based anomaly detection algorithm for identifying anomalies in a PV system connected to the grid.

In Gómez et al. [91], the authors propose a methodology for generating reliable anomaly detection datasets in industrial control systems (ICS) and create a dataset for electric traction substations. Conti et al. [92] offers a survey of testbeds and datasets, focusing on datasets that cover ICS traffic and protocols, but not those related to the physical behavior of processes. Faramondi et al. [93] presents a dataset to support researchers in developing Intrusion Detection Systems (IDS) using artificial intelligence and machine learning techniques to detect attacks on water distribution systems. Biswas et al. [94] examines typical distribution-level substations, simulates several cyberattacks, and presents a dataset with multiple traces corresponding to these cases.

However, no work provides a public dataset comprising physics-related information for DERs, and in particular for PV systems. While previous research has identified vulnerabilities, the lack of standardized datasets has hindered the development and evaluation of detection algorithms. Existing cybersecurity datasets focus primarily on network traffic or

generic industrial control systems, failing to capture the unique physics-based relationships inherent in PV operations.

4.1.2 Simulation Environment

A detailed simulation model of an electromagnetic nature was developed using MATLAB/Simulink software, utilizing the Simscape library (Inc., 2022) [79]. The model incorporates various cell arrays, a DC-DC converter, and a power inverter, each with its dedicated controller.

4.1.3 System Components

PV systems are made up of different electrical, electronic, and communication components. The analysis considers a typical scenario involving a storage system linked to a microgrid under the supervision of a SCADA system. From an electrical perspective, the system includes:

PV Cell Modules: Individual PV cells are interconnected in series and/or parallel arrangements to achieve the required DC voltage and desired peak power output. The current-voltage relationship is given by:

$$I = I_{\text{ph}} - I_0 \left[\exp\left(\frac{q(V + I \cdot R_s)}{n \cdot k \cdot T} \right) - 1 \right] - \frac{V + I \cdot R_s}{R_{\text{sh}}} \tag{4.1}$$

where:

I_{ph} is the photocurrent (A)

I_0 is the reverse saturation current (A)

q is the elementary charge (1.602×10^{-19} C)

V is the cell voltage (V)

R_s is the series resistance (Ω)

R_{sh} is the shunt resistance (Ω)

n is the ideality factor (dimensionless)

k is the Boltzmann constant (1.381×10^{-23} J/K)

T is the cell temperature (K)

The photocurrent is temperature and irradiance-dependent:

$$I_{ph} = \left[I_{sc,\text{ref}} + K_i (T - T_{\text{ref}}) \right] \cdot \frac{G}{G_{\text{ref}}} \tag{4.2}$$

where $I_{sc,ref}$ is the short-circuit current at reference conditions, K_i is the temperature coefficient of current, G is the irradiance, and the subscript "ref" denotes reference conditions (25°C, 1000 W/m²).

DC/DC converter: This electronic device regulates the power flow by implementing control strategies that enable maximum power point tracking (MPPT), thereby optimizing the energy harvested from the PV modules. The converter dynamics are governed by:

$$L\frac{di_L}{dt} = V_{pv} - (1 - D) \cdot V_{dc} \tag{4.3}$$

$$C_{\text{dc}}\frac{dV_{\text{dc}}}{dt} = (1 - D) \cdot i_L - i_{\text{out}} \tag{4.4}$$

where D is the duty cycle, L is the inductor value, C_{dc} is the DC-link capacitance, i_L is the inductor current, and i_{out} is the output current.

Power Inverter: Responsible for converting the DC output from the PV system into three-phase alternating current (AC), the inverter facilitates the integration of the generated power into the microgrid or utility network. The inverter converts DC power to three-phase AC using space vector modulation:

$$\begin{bmatrix} v_a \\ v_b \\ v_c \end{bmatrix} = \frac{V_{dc}}{3} \begin{bmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix} \begin{bmatrix} S_a \\ S_b \\ S_c \end{bmatrix} \tag{4.5}$$

where S_a,S_b and S_c are the switching states.

Power calculations:

$$P = \frac{3}{2}(v_d i_d + v_q i_q) \tag{4.6}$$

$$Q = \frac{3}{2}(v_q i_d - v_d i_q) \tag{4.7}$$

where v_d, v_q, i_d, i_q are the d-q axis components of voltage and current.

Control system: The inverter implements dual-loop control with outer voltage control and inner current control:

$$i_d^* = K_{p,v}(V_{dc}^* - V_{dc}) + K_{i,v}\int (V_{dc}^* - V_{dc})\, dt \tag{4.8}$$

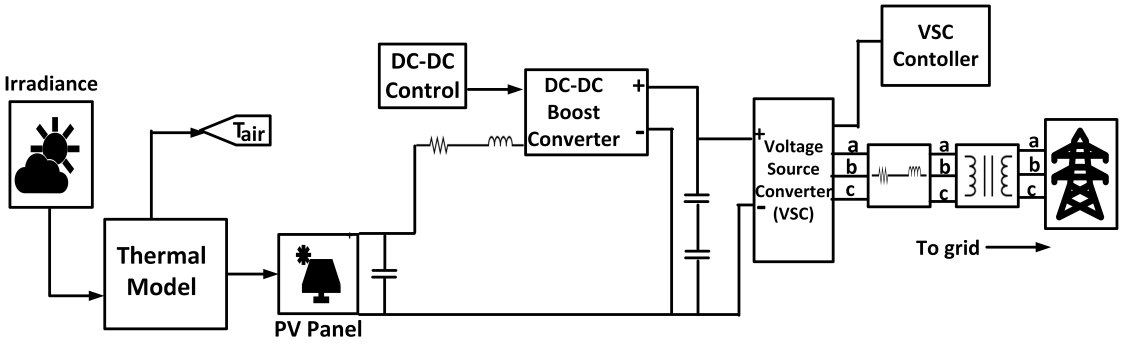

Figure 4.1: Complete Simulink model of the photovoltaic system

$$i_q^* = \frac{Q^*}{1.5 \cdot V_q} \tag{4.9}$$

Panel temperatures range from 25°C during early morning hours to peak values of 65–70°C during high irradiance periods, accounting for ambient temperature effects, solar heating, and thermal inertia. The thermal model incorporates:

$$T_{panel}(t) = T_{ambient}(t) + G(t) \cdot \frac{NOCT - 20}{800} + \tau_{thermal} \frac{dT}{dt} \tag{4.10}$$

where $G(t)$ is the solar irradiance at time t (W/m^2),

NOCT is the Nominal Operating Cell Temperature (°C), typically 45°C for crystalline silicon modules, representing the temperature reached by open-circuited cells in a module under standard conditions (irradiance of 800 W/m^2, ambient temperature of 20°C, wind speed of 1 m/s),

and $\tau_{\text{thermal}} = 300$ s is the thermal time constant, accounting for the slower response of temperature changes compared to irradiance variations.

4.1.4 System Parameters

The PV parameters are as follows: $V_{AC} = 230$ V (single-phase voltage), $S = 100$ kVA (power capacity), $V_{DC} = 500$ V (DC voltage), and $f = 50$ Hz (frequency). The Active Front End (AFE) connects to the main grid via a three-phase connection.

The control strategy includes a Maximum Power Point Tracking (MPPT) algorithm for the DC-DC converter to extract the maximum possible power from the photovoltaic cells depending on the irradiance conditions. The inverter controls the DC voltage, by increasing the injected active power when the DC voltage is increasing and vice versa.

The system response to environmental and operational changes is characterized by different time constants:

Electrical Parameters (voltage, current): 10–100 milliseconds

MPPT Tracking Response: 0.1–1 s

Irradiance Response: 0.1–1 s

Temperature Response: 5–10 min (thermal inertia)

These time constants are crucial for understanding the system's ability to respond to both legitimate operational changes and malicious cyberattacks, as they determine the detection windows available for anomaly detection algorithms.

4.1.5 Monitored Measurements

From the simulation model, a series of measures is extracted that indicate typical inverter exchanges with a SCADA system. These measures are detailed in Table 4.1.

4.2 Attack Taxonomy and Implementation

A simplified version of the taxonomy of attacks on smart inverters was adopted based on the framework presented in [95]. The attacks are categorized into three main types:

1. **Bad Data Injection (Grid-Support):** In this attack, the attacker modifies the commands the controller sends to the inverter. These commands typically pertain to active and reactive power setpoints or power factors. This attack can be executed through a Man-in-the-Middle (MiTM) attack on the communication network. Common protocols like Modbus and IEC 61850 lack authentication, making it easier for attackers to inject malicious packets into the communication network.

2. **False Data Injection (Basic Functions):** Here, the attacker alters the inverter's measurements to the main controller. This can be achieved through a MiTM attack or packet injection. The goal is to deceive the central controller, such as a SCADA system, into making incorrect decisions and sending erroneous commands. This attack is similar in nature to bad data injection, but has been classified differently to distinguish between the attack targets in the two cases. This attack is similar in nature to bad data injection, but we have classified it differently to distinguish between the attack targets in the two cases.

Table 4.1: Features of the dataset

Feature	**Symbol**	**Description**
X_1	Irr	the solar irradiance hitting the panel
X_2	T_{air}	temperature of the air
X_3	T_{PV}	temperature of the solar panel
X_4	V_{cells}	voltage measured at the terminals
X_5	I_{cells}	current emitted by cells array
X_6	V_{dc}	average voltage in the DC link
X_7	V_a	voltage of phase a (AC side)
X_8	V_b	voltage of phase b (AC side)
X_9	V_c	voltage of phase c (AC side)
X_{10}	I_a	current of phase a
X_{11}	I_b	current of phase b
X_{12}	I_c	current of phase c
X_{13}	f_a	frequency of phase a
X_{14}	f_b	frequency of phase b
X_{15}	f_c	frequency of phase c
X_{16}	THD_a	total harmonic distortion of voltage on phase a
X_{17}	THD_b	total harmonic distortion of voltage on phase b
X_{18}	THD_c	total harmonic distortion of voltage on phase c
X_{19}	P	active power emitted by the inverter
X_{20}	$Pset$	last active power setpoint sent by the SCADA controller
X_{21}	Q	reactive power emitted by the inverter
X_{22}	$Qset$	last reactive power setpoint sent by the SCADA controller

3. **Firmware Modification:** Here, the attacker modifies the internal functioning of the inverter, gaining potential control of all its parameters. This can be done by getting physical access to the device or remotely exploiting vulnerabilities in web services exposed by the inverter. The consequences can be severe, as the attacker might alter various parameters of the inverter, and cause disruptions in the local distribution grid.

A summary of this attack taxonomy, along with the specific parameters potentially targeted and their consequences, is provided in Table 4.2. Each of these attack types has been emulated within the previously described simulation environment. The Bad Data Injection scenario was implemented by modifying setpoint values at the inverter's control interface. The False Data Injection scenario was replicated by artificially altering measurement outputs recorded from the simulation. Lastly, the Firmware Modification attack was simulated by altering the underlying control logic within the model of the power converter.

Each attack scenario spans 90–120 seconds and may be initiated at any point during routine operation. This design supports algorithm assessment across diverse operating regimes—peak irradiance, transient cloud cover, and low-light conditions—while affording researchers the flexibility to tailor evaluations to their specific objectives and operational contexts.

The following subsection details each dataset partition, specifying the simulated anomaly type, the impacted control/measurement channels, and the operational context of the abnormal behavior.

4.2.1 Training Dataset

4.2.1.1 Normal Operating Conditions

The normal functioning of the panel was simulated for three days. The days refer to different weather conditions (e.g., sunny or cloudy), so as to vary the irradiance, the temperature of the air, the environmental conditions (so the parameters of the heat exchange with the environment), and the hours of light.

These simulations constitute the training dataset. Each day represents a different seasonal context with characteristic meteorological dynamics to capture a broad spectrum of realistic operating behaviors.

Day 1 (Summer): High irradiance with typical intra-day variability.

Table 4.2: Taxonomy of the attacks on DERs

Attack	**Description**	**Physical Parameters Involved**	**Effects**
BDI	Attacker send malicious commands to the actuators by manipulating the communication channel	Parameters can be listed as: Power on/off Active and/or Reactive Power Islanding Mode	Major effects being: Economic Damages Overload/Excess of Generation Oscillations False Protection Trip
FDI	Attacker sends fake measures to the higher-level controller by manipulating the communication channel	All the measures sent to the controller	Make the controller take bad decisions
Malware/FM	Attacker can modify the Firmware by physical attack or exploiting other web services	Different parameters, including: Voltages Frequencies Waveform ...	Technical damages to the grid, including: Voltage/frequency constraints violations False Protection Trip Hiding real faults to the protections Damages to other devices ...

Day 2 (Spring): Predominantly clear conditions, moderate irradiance, and gradual temperature changes.

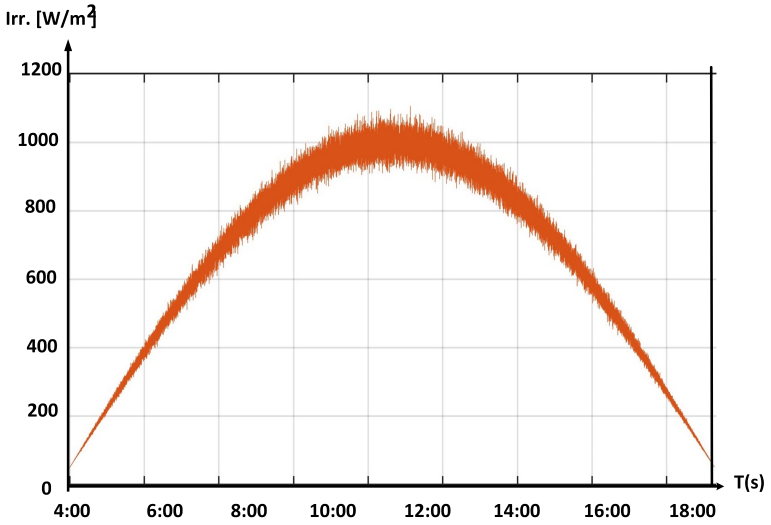

Figure 4.2: Summer day with high peak irradiance

Day 3 (Winter): Reduced irradiance, shorter daylight hours, and lower ambient temperatures.

Figure 4.2, 4.3 and 4.4 depict solar irradiance over four days, capturing seasonal variability and providing a fault-free reference for interpreting system performance. In these plots, t=0 corresponds to midnight.

4.2.1.2 Dataset Structure

The training dataset captures 107,260 operational samples representing this diverse range of normal operating conditions, providing a robust foundation for anomaly detection algorithm training. The temporal sampling rate of 1 Hz ensures adequate resolution for capturing both gradual environmental changes and rapid cloud-induced irradiance variations.

Data are recorded at 1 Hz, so each row represents one second of PV system behavior. The training corpus is unlabeled, facilitating unsupervised or semi-supervised methods. In contrast, all evaluation sets include a label field, where 1 denotes nominal operation and -1 indicates an anomaly.

Building on the established attack taxonomy, we simulated a variety of cyberattacks and operational faults in a photovoltaic (PV) system. The resulting dataset consists of twelve distinct subsets, each corresponding to a specific simulation instance. Table 4.3

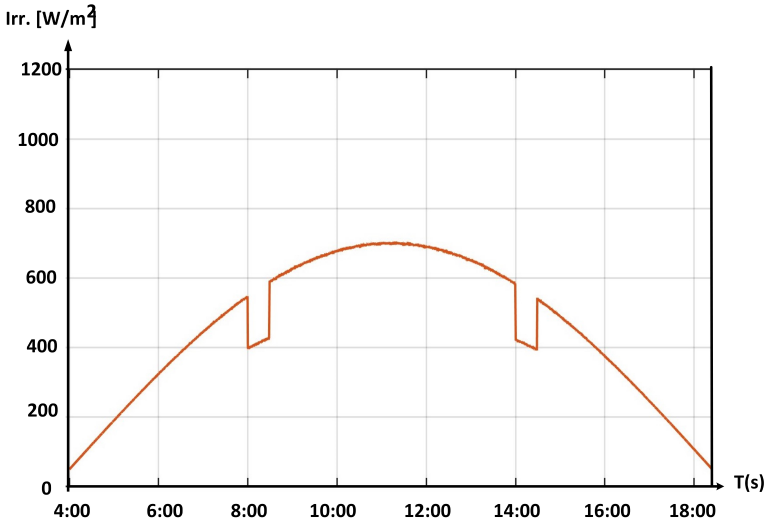

Figure 4.3: Spring day with moderate irradiance and occasional cloud variations

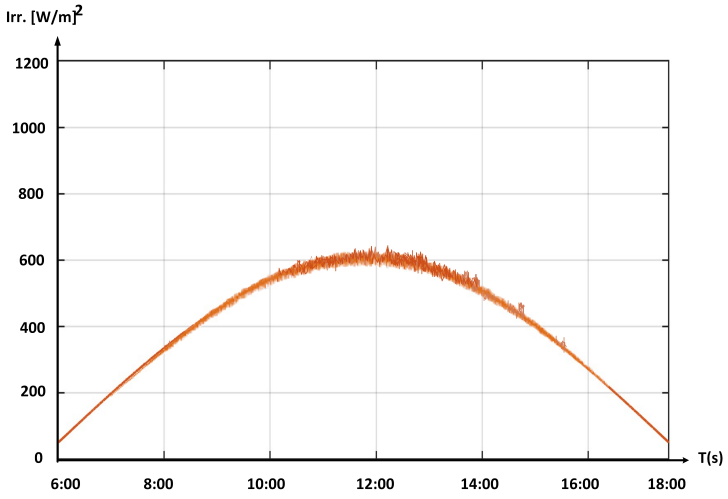

Figure 4.4: Winter day with lower peak irradiance

summarizes the publicly available repository, including file names, dataset dimensions, and brief descriptions for each subset.

Table 4.3: Resume of .csv dataset files

File name	Dimension	Description
training.csv	107260x22	Normal behavior (3 days)
BDI_P_reduction.csv	90x22	Bad Data Injection: P reduced without reason
BDI_Q_increment.csv	90x22	Bad Data Injection: Q becomes negative (inductive power)
BDP_P_oscillation.csv	90x22	Bad Data Injection: P oscillates
BDP_Q_oscillation.csv	90x22	Bad Data Injection: Q oscillates
FDI_P.csv		False Data Injection: P Tampering
FDI_T_panel.csv	120x22	False Data Injection: T_{PV} Tampering
FDI_Irr.csv	120x22	False Data Injection: Irradiance Tampering
Firmware_THD.csv	120x22	Firmware Modifications: Harmonics Tampering
Firmware_MPPT _modification.csv	120x22	Firmware Modifications: MPPT Tampering
Fault_ShortCircuitedCells.csv	120x22	Fault: Short Circuited Cells
Fault_Dust.csv	120x22	Fault: Dust on the panels
Cloudy_Test.csv	43201x22	Normal operation under realistic cloudy conditions

4.2.2 Simulated Attack Scenarios

As mentioned previously, Bad Data Injection attack was simulated by modifying the setpoint parameters at the inverter's terminals.

BDI- P reduction: As the name suggests, the attacker manipulates the active power (P) setpoint sent to the inverter, reducing the power injected without valid reasons. Initially, at a certain irradiance, the system operates normally at the power point of approximately 37 kW. However, at the same irradiance, the attacker suddenly decreases the setpoint to almost 30 kW and gradually to 0.1 kW, representing a 99.7% decrease from the normal activity. This attack is illustrated in Figure 4.5.

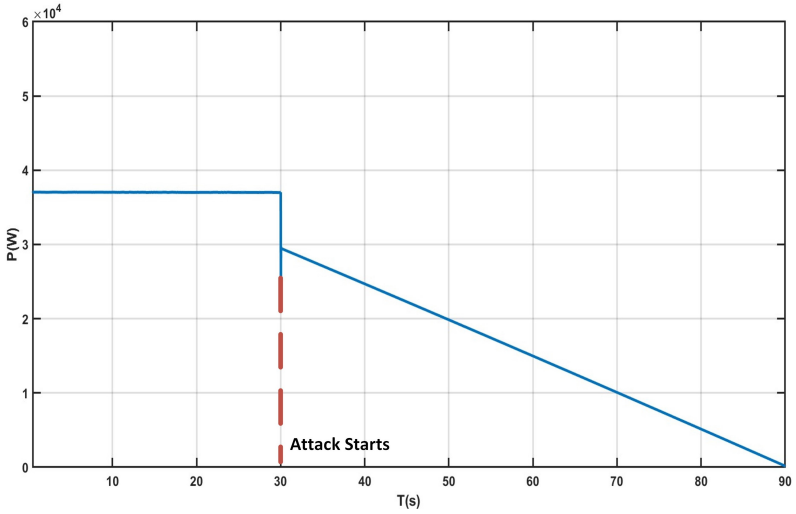

Figure 4.5: P reduction

BDI- Q increment: Here, the attacker manipulates the reactive power (Q) setpoint sent to the inverter, causing it to exceed the model's learned limits. Initially, the system operates normally with a reactive power of 0 kVAR. However, the irradiance being the same, the attacker increases the setpoint initially to 10 kVAR and then gradually to approximately 38 kVAR as shown in Figure 4.6.

BDP- P oscillation and BDP- Q oscillation: Here, two partial Man-in-the-Middle (MitM) scenarios are modeled in which an adversary intermittently perturbs both active (P) and reactive (Q) power setpoints transmitted to the inverter. The injected falsified setpoints induce persistent fluctuations, driving the inverter's output to oscillate between legitimate and malicious commands.

These behaviors expose a common weakness in industrial communications: SCADA systems often dispatch periodic setpoints to field devices without robust authentication or integrity protection. Under packet injection, valid and forged commands coexist, prompting erratic alternation at the inverter.

In the simulation, the adversarial setpoint follows a ramped sinusoid, producing oscillations whose amplitude grows over time. This disturbance undermines system stability and imposes additional stress on inverter control and switching elements.

The resulting trajectories of active and reactive power under this oscillatory attack are shown in Figures 4.7 and 4.8.

The False Data Injection attack was simulated by artificially altering the data saved from the model.

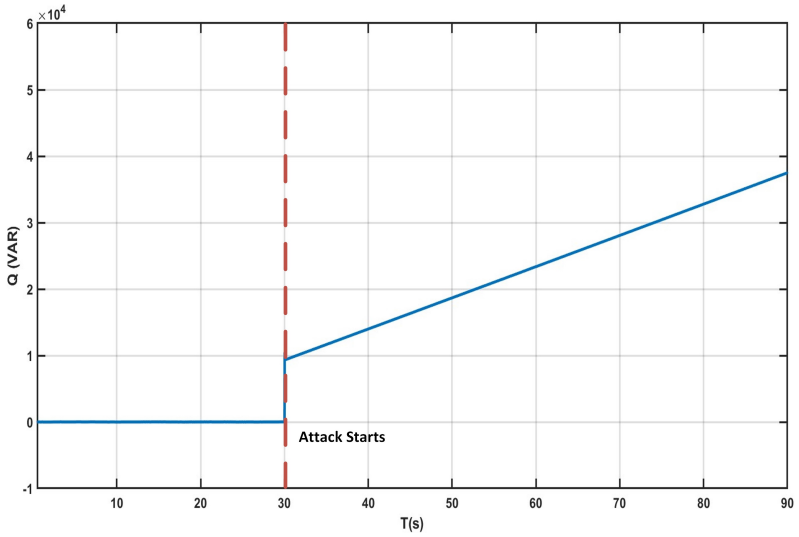

Figure 4.6: Q increment

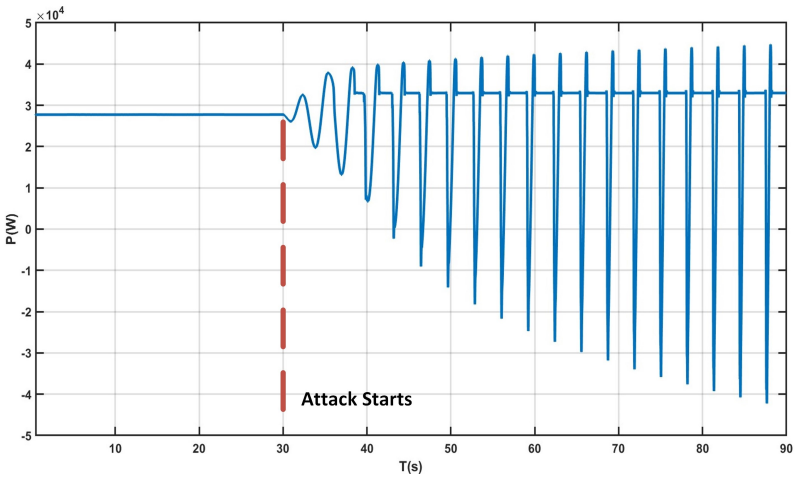

Figure 4.7: P oscillation

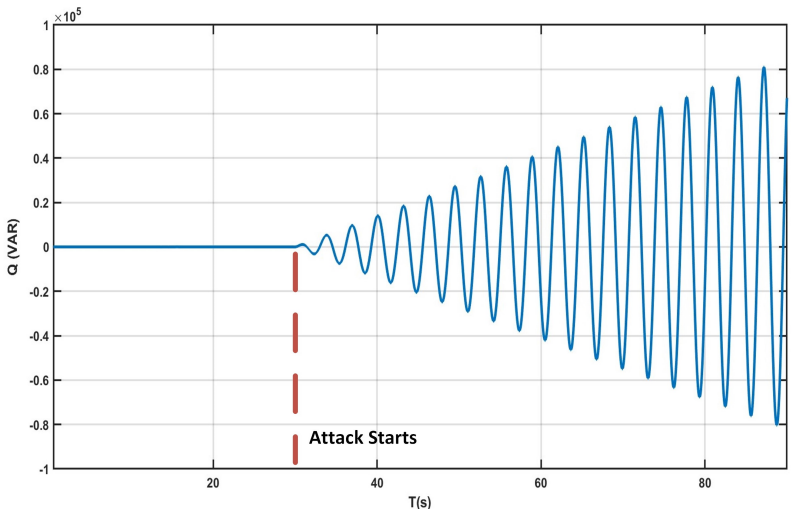

Figure 4.8: Q oscillation

FDI- P: During this attack, the attacker can alter the power injection measurements sent from the inverter to the SCADA system using a Man-in-the-Middle approach. The attacker can only modify a subset of measurements at a time; in this case, the attacker changes only the active power measurement. As a result, the data received by SCADA is inconsistent, as the active power is no longer the correct product of current and voltage measurements. This attack was simulated for 120 seconds on a constant irradiance that produced the correct setpoint of 55 kW. However, at 30 seconds, the attack starts making the measurements inconsistent with the ones generated by the inverter. Figure 4.9 shows the evolution of the falsified active power readings during the attack.

FDI- T panel: Here, the attacker alters the temperature measurements sent from the inverter to the SCADA system. Assuming that the attacker can only modify a subset of measurements at a time, the attacker changes only the measurement of the PV panel temperature. This causes inconsistency in the data received by SCADA, as the temperature no longer aligns with all the other measures (for example, the irradiance and active power). This attack was simulated for 120 seconds on a constant irradiance that produced the correct temperature setpoint of 14 degrees Celsius. However, at the 30th second, the attack drives the temperature directly to 36 degrees which then follows an increasing trend of incorrect temperature measurements. The manipulated temperature trend is illustrated in Figure 4.10.

FDI- Irr: Again, the attacker could use the MiTM attack to manipulate irradiance measurement sent from the inverter to the SCADA system. Assuming the modification of only a subset of measurements at a time, the attacker changes just the measurement

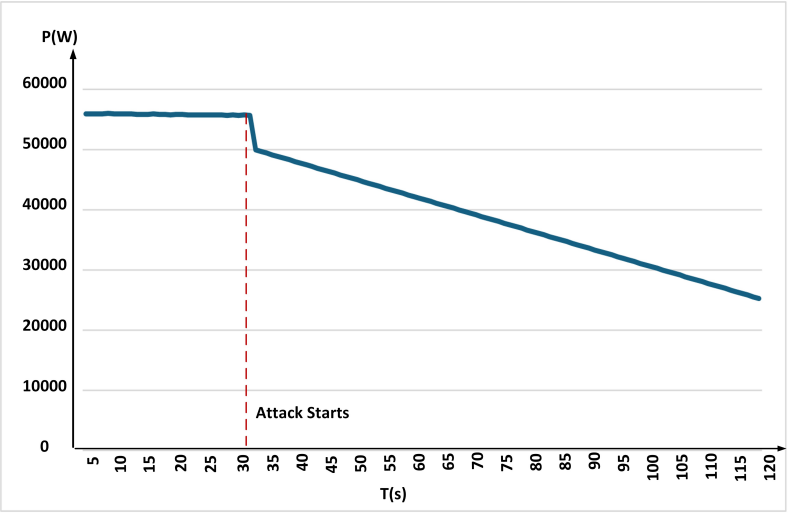

Figure 4.9: P tampering

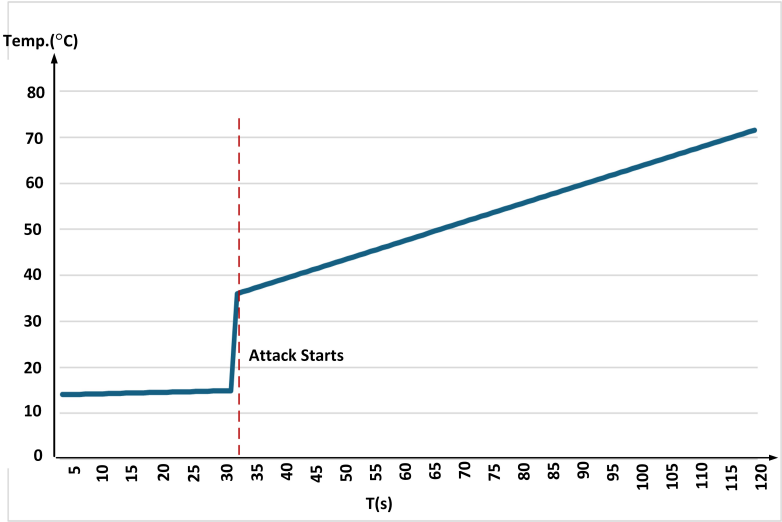

Figure 4.10: Tampering of the Panel Temperature

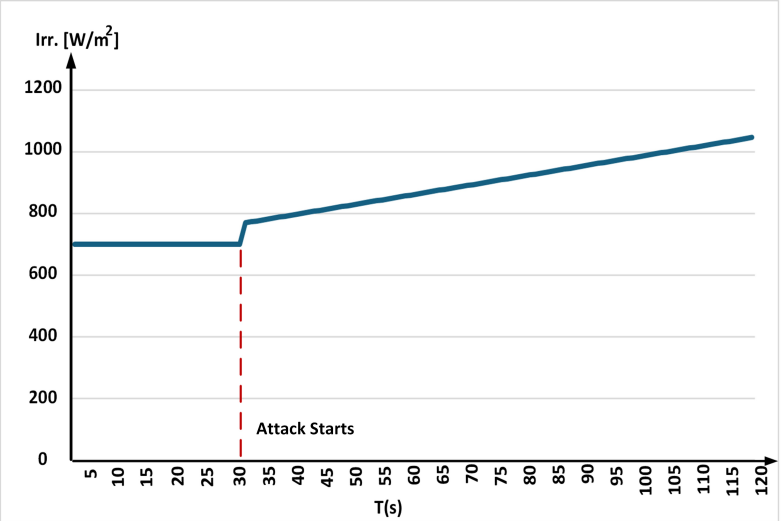

Figure 4.11: Irradiance tampering

of the irradiance. As a result, the data received by SCADA becomes inconsistent, as the irradiance no longer aligns with all the other measures, such as active power. Like the previous cases, this attack is also simulated for 120 seconds with the starting irradiance setpoint of 700 W/m^2. At 30 seconds, the attacker increases the original irradiance by 10% which then follows an increasing trend of incorrect irradiance measurements. The distorted irradiance profile is shown in Figure 4.11.

Anomaly detection algorithms are expected to quickly identify these false data injection attacks because the measurement vector generated by the attacker represents physically implausible data.

The Firmware Modification attack was simulated by changing the code controlling the power converters.

Firmware- THD: In this attack scenario, the intruder can alter the internal operations of the inverter, specifically modifying the waveform it generates. The hypothesis involves injecting an extra harmonic into the sine waveform. The harmonic's magnitude is increased in three stages. In the initial step, the Total Harmonic Distortion (THD) surpasses the power quality thresholds established by the IEEE 519-2022 Standard. This method creates a grid-impacting attack that can be identified by noise. An anomaly detection algorithm is expected to promptly identify the attack, as it causes significant variations in several parameters, particularly the Total Harmonic Distortion (THD) of the voltage across all three phases. The staged escalation of the harmonic component—and the resulting THD variation—is depicted in Figure 4.12.

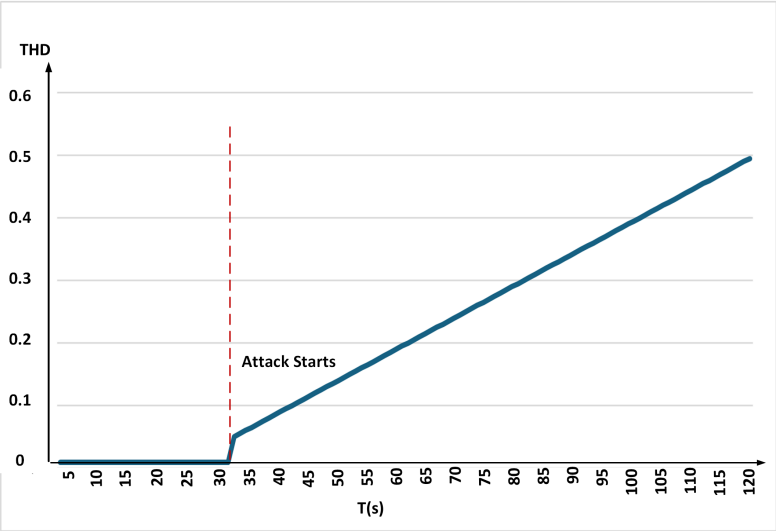

Figure 4.12: Tampering of Harmonics

Firmware- MPPT modification: During this attack, the intruder specifically targets the control of the DC/DC converter. This is especially dangerous, as it may lead to hazardous operating conditions, potentially causing damage. The degree of variation increases in three increments. Due to significant fluctuations in battery and DC-link voltage, an anomaly detection algorithm can quickly identify this attack. The simulated manipulation is introduced in three escalating stages, each causing progressively more severe deviations in system behavior. The evolution of this disturbance is illustrated in Figure 4.13.

In addition to cyberattacks, two common physical fault conditions were included:

Fault- Short Circuited Cells: A fault that can occur in solar panels due to short-circuited cells is a "hot spot" formation. This happens when one or more cells become short-circuited and dissipate energy as heat instead of converting it into electricity. Since the short-circuited cells no longer contribute to the overall voltage, the total output voltage of solar panels and power output decrease proportionally to the number of affected cells. The normal voltage of the PV panel is around 282 V but the short-circuit fault in some PV cells leads to a reduced voltage of 226 V. This fault was simulated across two other different situations at 60 and 90 seconds which led to further reduction of the panel voltage. The full progression of the panel voltage under this simulated fault condition is depicted in Figure 4.14.

Fault- Dust: A common fault in solar panels caused by dust accumulation on the surface is reduced light absorption. Dust particles block and scatter sunlight, decreasing

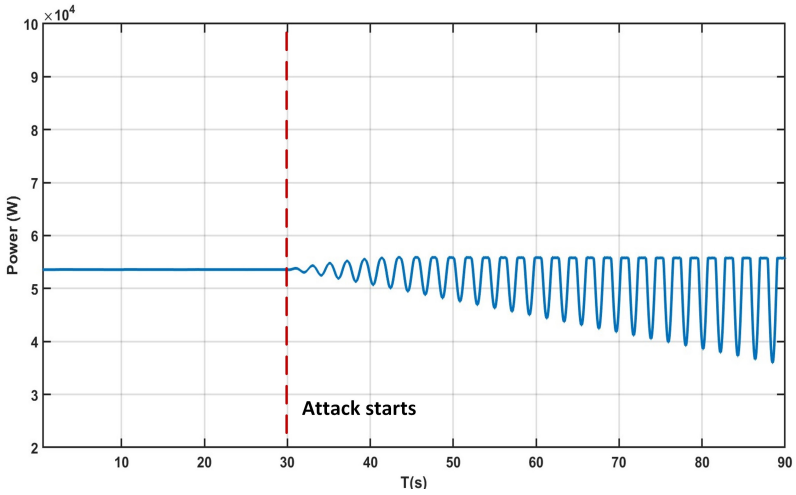

Figure 4.13: Effects of Tampering the MPPT

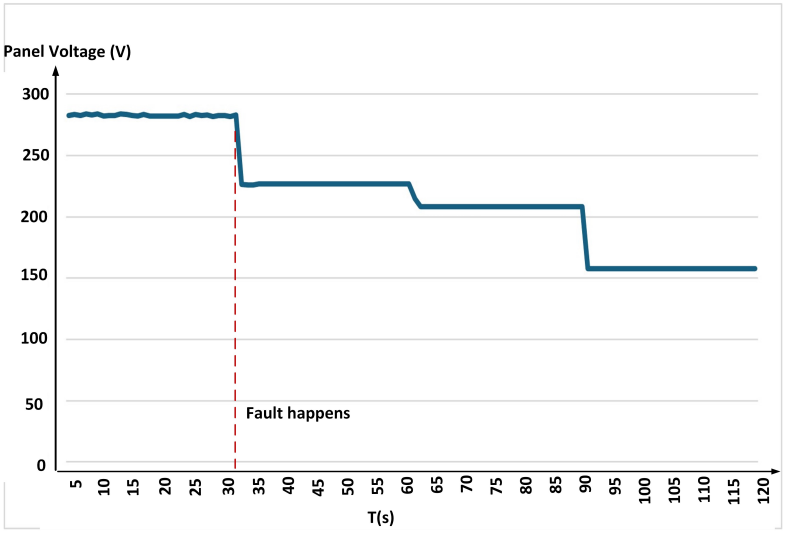

Figure 4.14: Short circuiting of cells in the PV panel

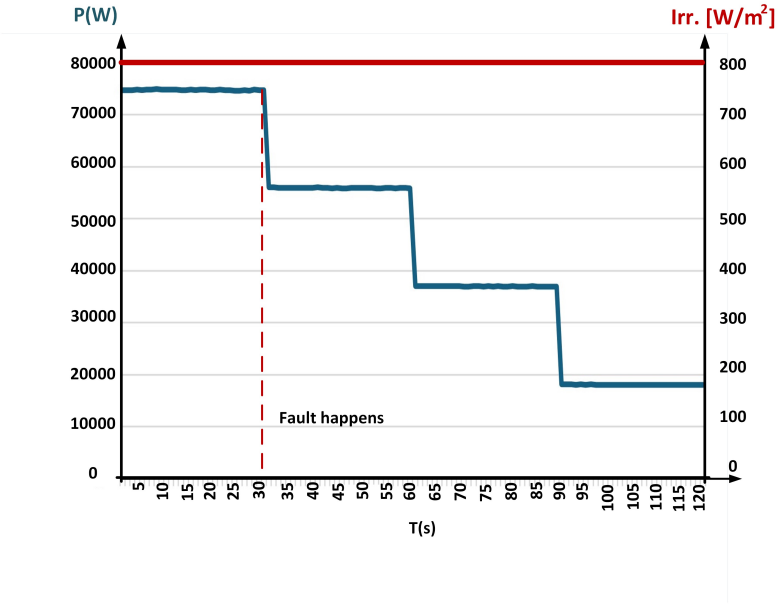

Figure 4.15: Fault- Dust on panels

the panel's efficiency. Subsequently, this has a significant impact on the power emitted. Depending on the extent of the dust coverage, this can lead to a noticeable drop in the overall energy production of the PV system.

While operating normally, the active power produced by the PV plant was around 75 kW but the presence of dust is simulated at the 30th second which generates a reduced active power production of around 56 kW. Simulating the progressive fault again at 60 and 90 seconds led to a further reduction of the power. The progressive impact of dust accumulation on the system's active power output is shown in Figure 4.15.

4.2.2.1 Realistic Environmental Conditions

To evaluate algorithm performance under realistic operational conditions, a comprehensive cloudy day dataset spanning natural weather variations was included. Unlike the controlled attack scenarios, this dataset captures the inherent variability present in actual PV system operations, including gradual irradiance changes, cloud transients, and temperature fluctuations that occur during normal cloudy weather patterns. Theis profile has been illustrated in Figure 4.16.

The dataset contains 43,201 samples of normal PV system operation under variable cloudy conditions, representing the type of environmental challenges that anomaly detec-

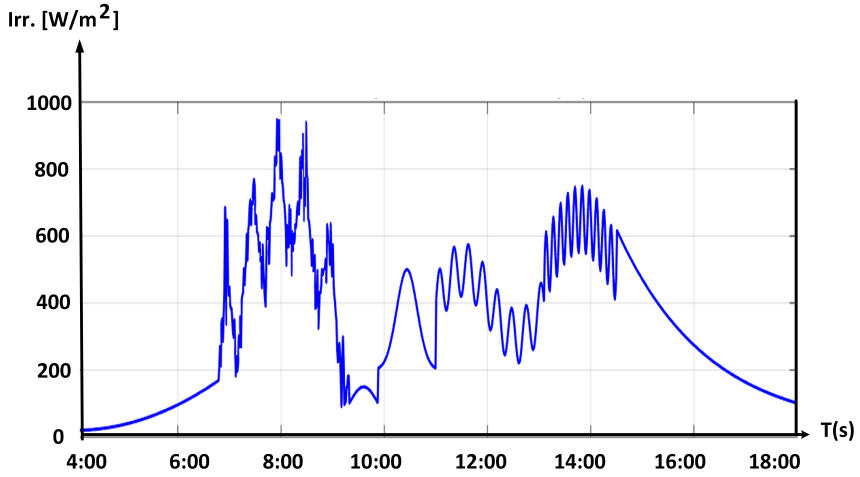

Figure 4.16: Realistic Cloudy Day Profile

tion algorithms must handle in real-world deployments. All samples are labeled as normal operation (label = 1), as no attacks or faults occur during this period.

The inclusion of this dataset addresses a significant gap in cybersecurity research, where algorithms often perform well under controlled conditions but fail when deployed in variable real-world environments.

4.2.3 Usage of the Dataset

The dataset emphasizes on how cyberattacks can influence the electrical behavior of a medium-scale grid-connected photovoltaic (PV) system. As such, it supports a range of valuable applications:

1. **Cyberattack Risk Assessment:** This dataset can play a vital role in evaluating the risks posed by cyber threats in PV environments. While existing research has extensively documented smart inverter vulnerabilities, quantifying the real-world impact of such threats remains complex. The dataset bridges this gap by providing time-series trends for key electrical variables under each attack scenario. Additionally, the included simulation model allows users to tailor and extend experiments based on their own configurations or threat models.

2. **Design of Cyber-Responsive Electrical Protections:** Emerging research focuses on leveraging traditional electrical protection schemes as part of the cyber incident

response toolkit [96]. Engineers can implement or tune relay protections to ensure system stability in the face of malicious interference. The dataset offers quantitative insights into how attacks influence system dynamics, providing a foundation for configuring effective protection mechanisms based on measurable thresholds.

3. **Development of Physics-Aware Anomaly Detection Systems:** A core objective of this dataset is to foster the creation of anomaly detection algorithms that can identify a wide range of attack types in PV systems. Physics-based approaches, which rely on the underlying physical laws governing system behavior, show strong promise as demonstrated in [90]. The dataset offers labeled instances of various anomalies, allowing data scientists and machine learning practitioners—even those without deep power systems expertise—to experiment with detection strategies. In this way, it promotes interdisciplinary research in monitoring and securing industrial control systems.

The variables selected for inclusion, as detailed in Table 4.1, are based on a survey of commercial inverter communication module manuals. They reflect the most widely exchanged operational parameters and control signals. Consequently, Photo-Set provides a flexible testbed for validating algorithms across diverse inverter brands. If a specific product reports a narrower set of metrics, irrelevant variables can simply be excluded—preserving only the applicable features for targeted analysis.

4.3 Benchmark Evaluation

Building upon the previously introduced Photo-Set dataset, a benchmark evaluation of anomaly detection algorithms for PV cybersecurity applications was conducted. The evaluation serves multiple purposes:

1. Establishing baseline performance metrics for future research comparisons
2. Identifying which attack types are most challenging to detect
3. Providing guidance for real-world PV system monitoring implementations
4. Revealing algorithm-specific strengths and limitations

4.3.1 Algorithm Selection and Methodology

Three state-of-the-art unsupervised anomaly detection algorithms were evaluated, representing different detection paradigms commonly used in cybersecurity applications:

4.3.1.1 One-Class Support Vector Machine (OC-SVM)

OC-SVM learns a decision boundary that encapsulates the normal data distribution by solving the optimization problem:

$$\min_{w,\xi,\rho} \frac{1}{2}\|w\|^2 + \frac{1}{\nu n}\sum_{i=1}^{n}\xi_i - \rho \tag{4.11}$$

subject to:

$$w^T\phi(x_i) \geq \rho - \xi_i, \quad \xi_i \geq 0 \tag{4.12}$$

where $\phi(x)$ maps input data to a higher-dimensional space using a kernel function, $\nu \in (0,1]$ controls the fraction of outliers, and ρ determines the decision boundary. The decision function is:

$$f(x) = \text{sign}\left(w^T\phi(x) - \rho\right) \tag{4.13}$$

4.3.1.2 Isolation Forest

Isolation Forest exploits the principle that anomalies are few and different, requiring fewer random splits to isolate them in feature space. The algorithm constructs t isolation trees, each built by recursively selecting random features and split values. The anomaly score for point x is:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \tag{4.14}$$

where $E(h(x))$ is the average path length over all trees, and $c(n) = 2H(n-1) - \frac{2(n-1)}{n}$ with H being the harmonic number. The algorithm's time complexity is $O(t \cdot \psi \cdot \log\psi)$ for training and $O(t \cdot \log\psi)$ for prediction, where ψ is the subsample size.

4.3.1.3 Local outlier factor (LOF)

LOF measures the local density deviation of a data point with respect to its neighbors. The algorithm computes:

k-distance:

$$d_k(A) = \text{distance to the k-th nearest neighbor}$$

Reachability distance:

$$\text{reach-dist}_k(A, B) = \max\{d_k(B),\ d(A, B)\}$$

Local reachability density:

$$\text{lrd}_k(A) = \frac{|N_k(A)|}{\sum_{B \in N_k(A)} \text{reach-dist}_k(A, B)}$$

Local outlier factor:

$$\text{LOF}_k(A) = \frac{\sum_{B \in N_k(A)} \frac{\text{lrd}_k(B)}{\text{lrd}_k(A)}}{|N_k(A)|}$$

where $N_k(A)$ represents the k-distance neighborhood of point A, defined as the set of objects whose distance from A is not greater than the k-distance. The k-distance is the distance between A and its k-th nearest neighbor, establishing a local density measure for anomaly detection.

Normal operation data (training.csv) was used to train all models, while each attack scenario was evaluated separately to assess detection performance for specific threat types.

4.3.1.4 Performance Metrics

Standard binary classification metrics adapted for anomaly detection were employed, where normal operation samples are treated as the positive class and attack samples as the negative class.

Accuracy: Overall correctness of predictions across all samples.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4.15}$$

Sensitivity: Fraction of actual attacks successfully detected.

$$Sensitivity = \frac{TP}{TP + FN} \tag{4.16}$$

Specificity: The model's ability to accurately identify normal cases and avoid false alarms.

$$Specificity = \frac{TN}{TN + FP} \tag{4.17}$$

Where TP: True Positive, TN: True Negative, FP: False Positive, and FN: False Negative.

The performance metrics established in this study serve as reference points for subsequent algorithm development, facilitating objective comparisons among alternative detection approaches. The evaluation protocol offers a standardized and reproducible framework for assessing PV cybersecurity methods. Collectively, this experimental setup defines a proposed benchmark for anomaly detection in photovoltaic systems. The subsequent section reports the performance outcomes across all algorithm–attack combinations, providing data-driven insights to inform practical deployment strategies.

4.3.2 Benchmark Results

4.3.2.1 One-Class SVM Performance

The performance metrics of One-Class SVM are presented in Table 4.4.

OC-SVM achieved perfect sensitivity (100%) across all attack scenarios but zero specificity, resulting in moderate accuracy. This indicates the algorithm classified all samples as anomalous. The Cloudy_Test results are particularly revealing: with only 49.42% of samples correctly classified as normal, the algorithm flagged over half of legitimate cloudy-day operations as anomalous.

4.3.2.2 Isolation Forest Performance

The performance metrics of Isolation Forest are presented in Table 4.5.

Isolation Forest demonstrated effective detection capabilities across multiple attack scenarios, achieving good performance on firmware-level attacks and reactive power manipulation scenarios. However, it completely failed on all FDI attacks (0% sensitivity) and struggled with the short circuit fault. The Cloudy_Test showed 83.14% specificity, demonstrating better handling of realistic conditions compared to OC-SVM and LOF.

4.3.2.3 Local Outlier Factor Performance

The performance metrics of Local Outlier Factor are presented in Table 4.6.

Local Outlier Factor exhibited systematic classification issues similar to OC-SVM. While achieving perfect sensitivity on attack scenarios, it suffered from zero specificity. The Cloudy_Test performance was dramatically worse than other algorithms (3.68% accuracy), flagging 96.32% of normal cloudy operations as anomalous.

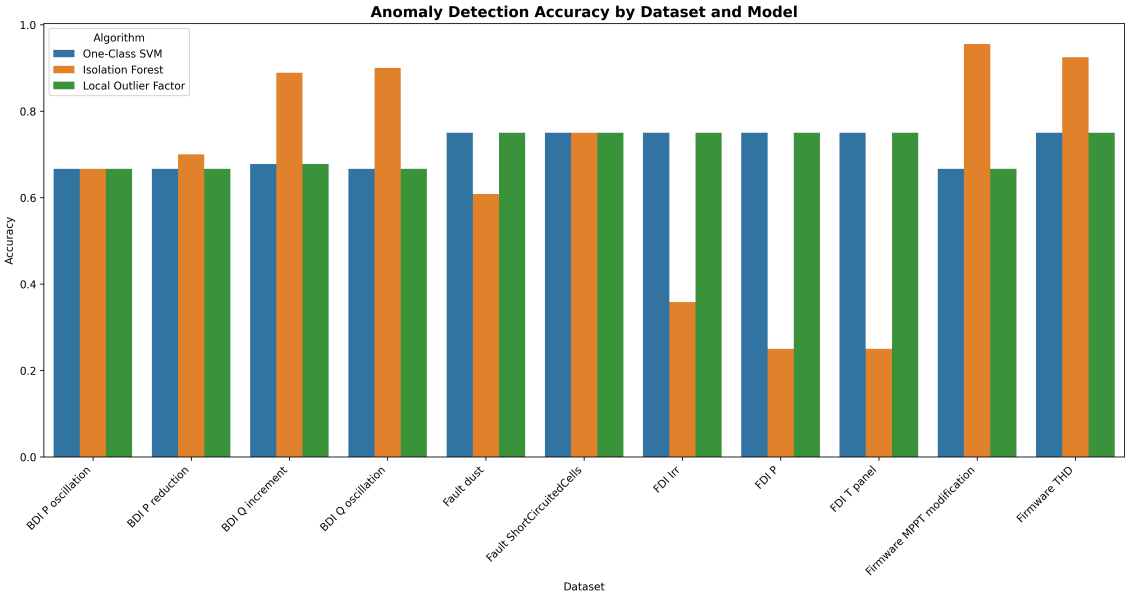

Figure 4.17: Accuracy comparison of anomaly detection algorithms across all attack scenarios

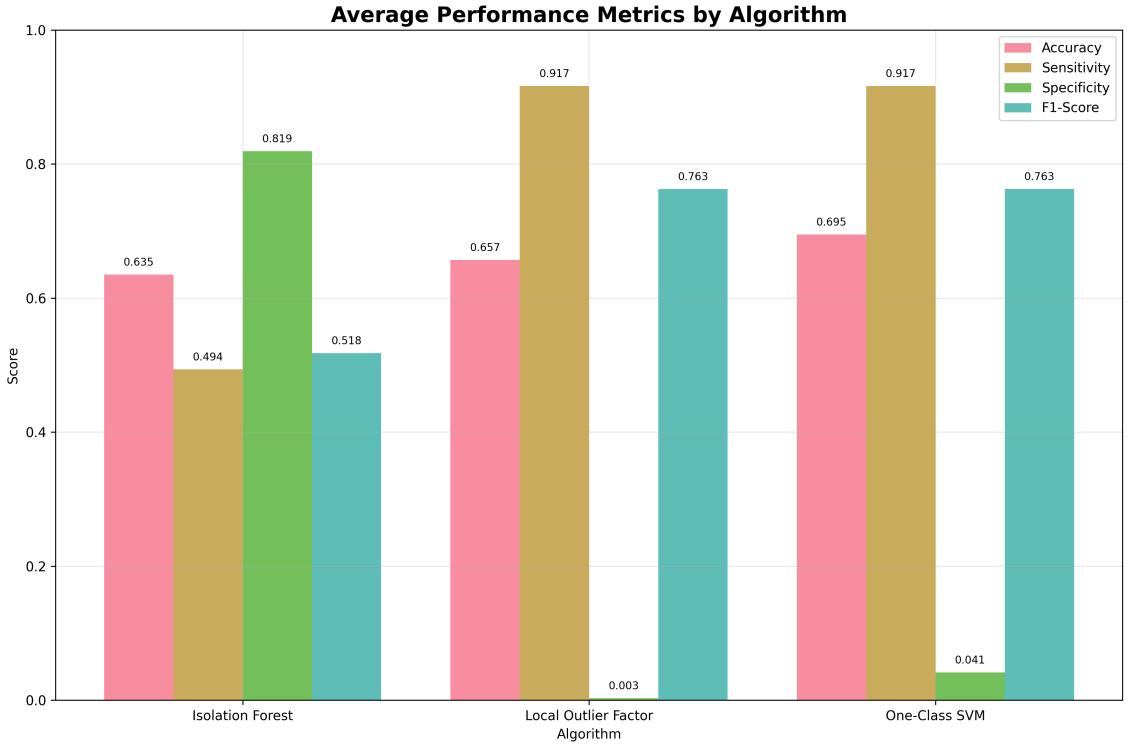

Figure 4.18: Average performance metrics (Accuracy, Sensitivity, Specificity) across all algorithms

Table 4.4: One Class SVM Results

Dataset	Accuracy	Sensitivity	Specificity	Confusion Matrix
BDI_P_reduction	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
BDP_P_oscillation	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
BDI_Q_increment	67.78%	100%	0%	TP=61 FP=29 FN=0 TN=0
BDP_Q_oscillation	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
FDI_P	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
FDI_T_panel	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
FDI_Irr	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
Firmware_THD	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
Firmware_MPPT _modification	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
Fault_ShortCircuitedCells	75%	100%	0%	TP=60 FP=30 FN=0 TN=0
Fault_Dust	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
Cloudy_Test	49.42%	0%	49.42%	TP=0 FP=21851 FN=0 TN=21350

4.3.3 Critical Findings

To provide a comprehensive view of algorithm performance across all attack scenarios, we present comparative visualizations that synthesize the results from Tables 4.4,4.5, and 4.6. Figure 4.17 presents a side-by-side comparison of detection accuracy for all three algorithms across the 12 attack scenarios. Figure 4.18 presents the average performance across all evaluation metrics for each algorithm

The Cloudy_Test results reveal a critical limitation in current anomaly detection approaches for PV systems. Isolation Forest demonstrated the highest specificity (83.14%) among the three algorithms, suggesting better discrimination of normal operational pat-

Table 4.5: Isolation Forest Results

Dataset	**Accuracy**	**Sensitivity**	**Specificity**	**Confusion Matrix**
BDI_P_reduction	57.78%	36.67%	100%	TP=22 FP=0 FN=38 TN=30
BDP_P_oscillation	100%	100%	100%	TP=60 FP=0 FN=0 TN=30
BDI_Q_increment	96.67%	95.08%	100%	TP=58 FP=0 FN=3 TN=29
BDP_Q_oscillation	95.56%	93.33%	100%	TP=56 FP=0 FN=4 TN=30
FDI_P	25%	0%	100%	TP=0 FP=0 FN=90 TN=30
FDI_T_panel	25%	0%	100%	TP=0 FP=0 FN=90 TN=30
FDI_Irr	25%	0%	100%	TP=0 FP=0 FN=90 TN=30
Firmware_THD	100%	100%	100%	TP=90 FP=0 FN=0 TN=30
Firmware_MPPT _modification	70%	55%	100%	TP=33 FP=0 FN=27 TN=30
Fault_ShortCircuitedCells	9.17%	12.22%	0%	TP=11 FP=30 FN=79 TN=0
Cloudy_Test	83.14%	0%	83.14%	TP=0 FP=7284 FN=0 TN=35917

Table 4.6: Local Outlier Factor Results

Dataset	**Accuracy**	**Sensitivity**	**Specificity**	**Confusion Matrix**
BDI_P_reduction	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
BDP_P_oscillation	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
BDI_Q_increment	67.78%	100%	0%	TP=61 FP=29 FN=0 TN=0
BDP_Q_oscillation	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
FDI_P	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
FDI_T_panel	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
FDI_Irr	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
Firmware_THD	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
Firmware_MPPT _modification	66.67%	100%	0%	TP=60 FP=30 FN=0 TN=0
Fault_ShortCircuitedCells	75%	100%	0%	TP=60 FP=30 FN=0 TN=0
Fault_Dust	75%	100%	0%	TP=90 FP=30 FN=0 TN=0
Cloudy_Test	3.68%	0%	3.68%	TP=0 FP=41612 FN=0 TN=1589

terns, while Local Outlier Factor performed worst (3.68% specificity), flagging nearly all cloudy conditions as anomalous.

This finding underscores the critical need for physics-informed approaches that can distinguish between legitimate environmental variations and actual cyberthreats, representing a fundamental limitation that must be addressed for real-world PV cybersecurity monitoring systems. Three attack categories proved consistently undetectable using standard anomaly detection approaches:

1. Physical degradation faults that manifest as gradual efficiency losses indistinguishable from environmental variations.

2. Subtle power oscillations that fall within normal operational fluctuation ranges.

3. Attacks that maintain physical system constraints while manipulating individual parameters.

Sensitivity analysis from the Isolation Forest demonstrates that attack detection coverage varies significantly by attack type, with firmware modifications achieving detection rates of more than 90%, while physical faults remain completely undetected.

4.4 Physics-Informed Detection Approach

Extending on the previous work of dataset generation and benchmark evaluation, this section explores the anomaly detection approach by Physics-Informed Neural Networks (PINNs).

Multiple studies have developed intrusion detection mechanisms for power grid components including advanced metering systems, digital substations, synchrophasor units, and SCADA environments[97].

Network-focused IDS may miss attacks that manipulate system behavior without altering traffic patterns [98]. In distributed energy resource (DER) environments, combining cyber and physical monitoring is essential [99]. Physics-based monitoring augments network analysis by detecting malicious activities through physical outputs like voltage, current, and frequency [58].

Supervised learning faces data imbalance between normal operations and anomalies. Novelty detection (one-class classification) addresses this by identifying deviations from learned normal behavior patterns [100].

Autoencoder-based architectures are popular for anomaly detection [101]. Recurrent Neural Networks (RNN) capture temporal dynamics through internal memory [102]. Recent implementations include:

GRU-based autoencoders for temporal patterns [103] LSTM autoencoders for wind turbine malfunction detection [104] Variational autoencoders [105] Bidirectional RNNs for Cyber-Physical Systems [106].

This work monitors photovoltaic (PV) system cybersecurity by analyzing physical and electrical behavior using real-time measurements to automatically detect anomalies, simulating experienced operator oversight.

4.4.1 System Architecture

A monitoring architecture was developed consisting of: The PV system periodically exchanges a set of measures and control packets with the SCADA. A generic representation is shown in Figure 4.19. The PV periodically exchanges a set of measures and control packets with the SCADA. We define $x^R(t) = \{x_1^R(t), x_2^R(t), ..., x_n^R(t)\}$ the set of real measures, i.e., the set of real physical parameters that are present on the PV. We define $x^{HMI}(t) = \{x_1^{HMI}(t), x_2^{HMI}(t), ..., x_n^{HMI}(t)\}$ the set of measures that are collected on the SCADA/HMI platform and are available to human operators. Finally, we define $x^{IDS}(t) = \{x_1^{IDS}(t), x_2^{IDS}(t), ..., x_n^{IDS}(t)\}$ that can be extracted from network packets collected by the Intrusion Detection Systems. In case of an ongoing attack, $x^R(t)$, $x^{HMI}(t)$ and $x^{IDS}(t)$ may not coincide.

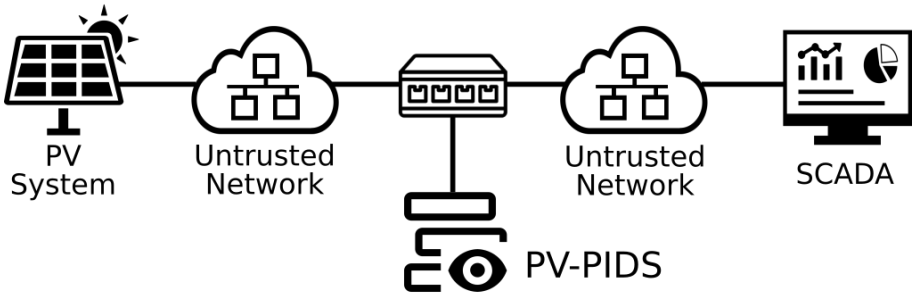

Figure 4.19: Architecture of the proposed PV-PIDS system

The proposed PV-PIDS extracts $x^{IDS}(t)$ through the passive analysis of the network traffic in an intermediate node of the network (for example, a switch), and subsequently analyzes it with the AI approach described below.

4.4.2 Physics-Informed Supervised LSTM Encoder-Decoder

The objective is to learn a function $f_\Theta : \mathcal{X} \rightarrow \mathcal{Y}$, defined by a parameter set Θ, that closely approximates the relationship between inputs and outputs. The accuracy of this approximation is evaluated using a loss function $\ell : \mathcal{Y} \times \mathcal{Y} \rightarrow \mathbb{R}$. The parameters Θ are optimized solely based on a collection of n_d input-output pairs, forming the dataset $\mathcal{D} = \{(x_1, y_1), \ldots, (x_{n_d}, y_{n_d})\}$, where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. Specifically, the encoder maps the input sequence $x \in \mathcal{X}$ to a latent representation $z \in \mathcal{Z}$, and the decoder reconstructs the input from z, producing $y \in \mathcal{Y}$. Specifically, the temporal sequence is encoded using an LSTM layer. We aim to reconstruct the last time step of the inserted time series sequence by combining data-driven sequence modeling with prior physical knowledge.

Typically, the training process involves solving the following optimization problem:

$$\min_{\Theta} F(\Theta) = \sum\nolimits_{(x,y)\in\mathcal{D}} L\left(f_\Theta(x), y\right) \tag{4.18}$$

Where $F(\Theta)$ is the loss function to minimize by tuning the parameter set of the model Θ during the training.

$f_\Theta(x)$ corresponds to the output of the model with respect to the input x and the parameters Θ. Finally, $L(f_\Theta(x), y)$ corresponds to the error function, which quantifies the difference between $f_\Theta(x)$ and y.

To incorporate physics-based knowledge into the training of neural networks, the loss function in (4.18) must be extended to include an additional term, $L_{phys}\left(f_\Theta(x), y, r\right)$, which encodes the physical constraints or relationships between the inputs and outputs. The modified loss function can be expressed as follows:

$$\min_{\Theta} \left[F(\Theta) + \| L_{pys}\left(f_\Theta(x), y, r\right) \|_2^2\right] \tag{4.19}$$

Here, r is a tunable parameter that controls the influence of the physics-based term. By incorporating this second term into (4.19), equality constraints derived from the system's physical principles can be softly enforced during the training process. This can be interpreted as a physics-informed latent mapping, where the model maps the space guided by physical principles related to the last time sequence. A similar benefit can be observed in [107], where we implement directly the physics knowledge, instead of nonlinear manifold statistics. This helps prediction accuracy where known dynamics govern the final state.

The physical relationships included in our model are outlined below, where each parameter is described in Table 4.1.

$$V_a I_a + V_b I_b + V_c I_c = \sqrt{P^2 + Q^2} \tag{4.20}$$

$$V_{cells} I_{cells} = P \tag{4.21}$$

$$P = \alpha Irr \tag{4.22}$$

The model is composed of five layers, where the LSTM layer is located in the input. Input and output consist of 22 neurons, in accordance with the features of the PV system. The hidden layer is constructed of three layers with fifteen, eight and fifteen neurons sequentially. The physics are implemented in the middle layer (eight neurons), which means that not all the neurons are related to physics, half of them are kept free for better reconstruction. Figure 4.20 illustrates the designed model of this work.

4.4.3 Training Methodology and Implementation Details

This subsection provides the methodological details for the physics-informed LSTM encoder-decoder implementation, addressing dataset partitioning, training procedures, and architectural specifications.

The Photo-Set dataset was organized into two primary components:

1. Training Set: Normal operation data (training.csv, 107,260 samples) representing three days of normal PV system operation under various environmental conditions

2. Test Set: Individual attack scenario files, each containing attack-specific data for evaluation (as detailed in Table 4.3)

This partitioning reflects the anomaly detection problem formulation where algorithms learn normal system behavior from benign operational data, then detect deviations during testing. Each attack scenario was evaluated separately to assess algorithm performance for specific threat types.

The baseline anomaly detection algorithms (OC-SVM, Isolation Forest, LOF) are unsupervised methods that learn exclusively from normal operation data without requiring labeled attack examples during training. These algorithms do not perform traditional hyperparameter optimization on anomaly data, as they establish decision boundaries based

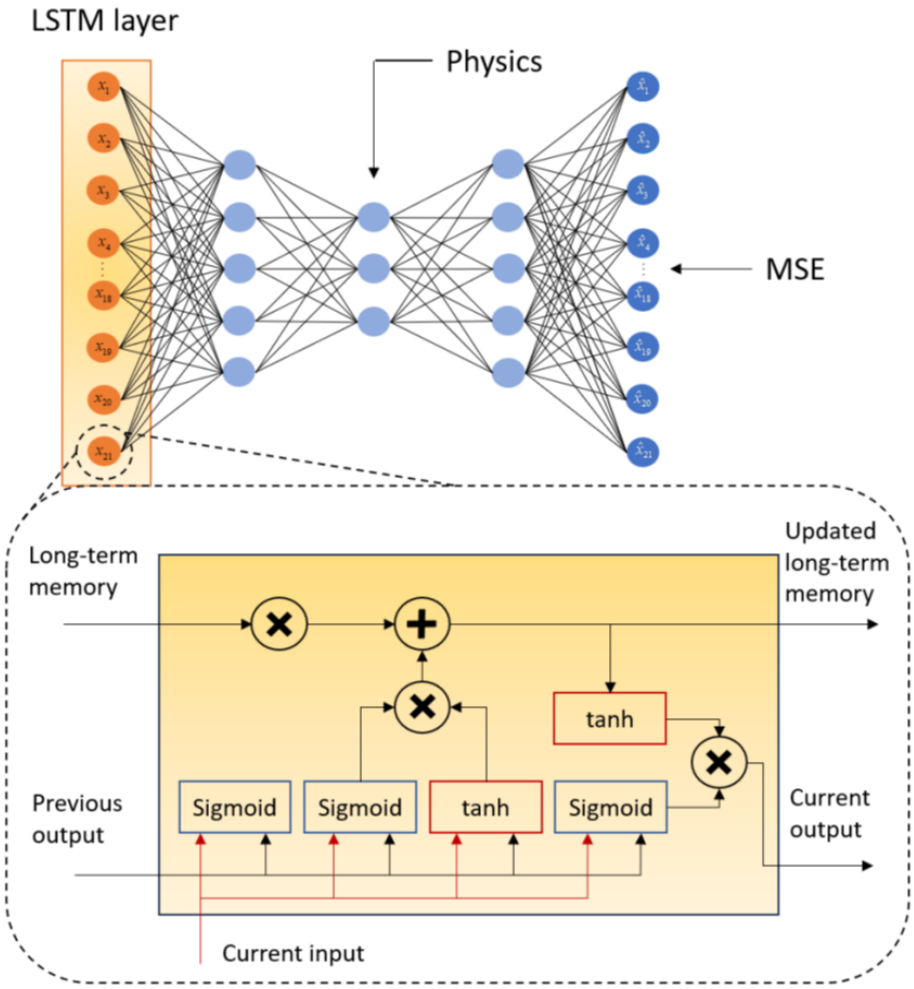

Figure 4.20: Physics-Informed Supervised LSTM Encoder- Decoder model.

solely on normal behavior patterns. Model parameters (e.g., OC-SVM's nu parameter, Isolation Forest's number of trees, LOF's k neighbors) were set to standard values commonly used in the anomaly detection literature.

4.4.3.1 LSTM Encoder-Decoder Architecture Specification

As illustrated in Figure 4.20, the physics-informed supervised LSTM encoder-decoder consists of five layers with the following detailed configuration:

Layer 1 - Input LSTM Layer:

- Input dimension: 22 neurons (corresponding to the 22 features in Table 4.1)
- LSTM units: Configured for temporal sequence processing
- Function: Encodes temporal dependencies in the input measurement sequence

- This layer captures time-series patterns essential for detecting temporal anomalies

Layer 2 - First Hidden Layer:

- Neurons: 15 units

- Activation: ReLU (Rectified Linear Unit)

- Function: Feature extraction and initial dimensionality transformation from the LSTM encoded representation

Layer 3 - Physics-Constrained Layer: - Neurons: 8 units (middle bottleneck layer)

- Physics constraints: Equations (4.20, (4.21), and (4.22) enforced through custom loss function

- Function: Compressed representation incorporating physical relationships

- Design rationale: This bottleneck forces the model to learn a compact representation that respects electrical system physics.

Half of the neurons explicitly encode physics constraints while remaining neurons maintain flexibility for data-driven feature learning.

Layer 4 - Second Hidden Layer:

- Neurons: 15 units

- Activation: ReLU

- Function: Reconstruction pathway expanding from the compressed physics-informed representation back to full feature space

Layer 5 - Output Layer:

- Neurons: 22 units (reconstructing all input features)

- Activation: Linear activation for continuous value reconstruction

- Function: Reconstructs the input measurement vector, enabling anomaly detection through reconstruction error analysis

The symmetric encoder-decoder architecture ($22 \rightarrow 15 \rightarrow 8 \rightarrow 15 \rightarrow 22$) with physics constraints in the bottleneck layer enables the model to learn representations that must satisfy fundamental electrical relationships, improving detection of physics-violating attacks such as false data injection.

4.4.3.2 Training Configuration and Procedure

The physics-informed LSTM encoder-decoder was trained using the following configuration:

- Training data: Normal operation samples from training.csv

- Optimizer: Adam optimizer with learning rate of 0.001

- Batch size: 64 samples

- Maximum epochs: 200 with monitoring of training loss

- Loss function: Combined reconstruction loss and physics-informed penalty (Equation 4.18)

- Physics constraint weight (r in Equation 4.18): Set based on the relative importance of physics constraints versus reconstruction accuracy

The custom loss function (Equation 4.19) combines two components:

1. Reconstruction loss: Standard mean squared error between input and reconstructed measurements

2. Physics penalty: L2 norm of physics constraint violations from Equations (4.20), (4.21), and (4.22)

This dual objective forces the model to both accurately reconstruct normal measurements and respect fundamental electrical laws, making it particularly effective at detecting attacks that violate physical consistency.

Training Process: The model was trained exclusively on normal operation data, learning to reconstruct typical system behavior. During training, the loss function decreased as the model learned both accurate reconstruction and physics-compliant representations. Training continued until the loss stabilized, indicating convergence to a model that captures normal system dynamics while respecting physical constraints.

Anomaly Detection Mechanism: During testing, samples with high reconstruction error (indicating deviation from learned normal patterns) or physics constraint violations are flagged as anomalies. The reconstruction error threshold was determined by analyzing the distribution of reconstruction errors on the training set, setting the threshold to capture 99% of normal operation samples while minimizing false positives.

4.4.3.3 Architecture Design Rationale

The five-layer architecture was designed with specific objectives:

1. LSTM input layer: Essential for capturing temporal dependencies in time-series

2. measurements, enabling detection of attacks that manifest as temporal patterns (e.g., oscillations, gradual drift)

3. Encoder compression (22→15→8): Forces dimensionality reduction, requiring the model to learn essential features that distinguish normal from anomalous behavior

4. Physics-constrained bottleneck (8 neurons): The most critical innovation—by enforcing physics constraints at the compressed representation level, the model cannot "cheat" by memorizing individual patterns but must learn physically consistent representations

5. Symmetric decoder (8→15→22): Enables reconstruction of all input features, allowing detection of anomalies in any measured variable

This architecture differs from standard autoencoders by explicitly incorporating domain knowledge (electrical system physics) into the learning process, as formalized in Equation (4.19).

4.4.3.4 Baseline Algorithm Configuration

For fair comparison, the baseline anomaly detection algorithms evaluated in Section 4.3 were configured as follows:

One-Class SVM (OC-SVM):

- Kernel: Radial Basis Function (RBF)

- Nu parameter: 0.1 (controls the upper bound on the fraction of training errors and lower bound on the fraction of support vectors)

- Training: Fit exclusively on normal operation data (training.csv)

Isolation Forest:

- Number of trees: 100 (ensemble size)

- Contamination: 'auto' (automatically determined based on training data properties)

- Max samples: 256 per tree (subsample size for building each tree)

- Training: Learns normal data distribution from training.csv

Local Outlier Factor (LOF):

- Number of neighbors (k): 20

- Metric: Euclidean distance

- Training: Establishes local density estimates from normal operation data

All baseline algorithms follow the standard anomaly detection paradigm: train on normal data, test on both normal and attack scenarios to evaluate detection capability.

4.4.3.5 Performance Evaluation Protocol

The evaluation methodology was carried out through the following steps:

Training Phase: All algorithms were trained exclusively on normal operation data (training.csv)

For the LSTM, convergence of the training loss was monitored.

For the baseline algorithms, the models were fitted to the distribution of normal data.

Testing Phase:

Each trained model was evaluated separately on every attack scenario.

Confusion matrices were computed for each attack type (as shown in Tables 4.4–4.6).

Performance metrics—Accuracy, sensitivity, and Specificity—were calculated using Equations 4.15–4.17.

Comparative Analysis:

The baseline algorithms (Tables 4.4–4.6) were compared to identify their limitations.

The standard autoencoder (Table 4.7) was evaluated as a deep learning baseline.

The LSTM encoder–decoder without physics (Table 4.8) was assessed.

The superiority of the physics-informed LSTM (Table 4.9) was demonstrated.

The reported metrics in these tables represent test set performance on attack scenarios that the models never encountered during training. This provides unbiased estimates of detection capability on unseen threats.

4.4.4 Implementation

A modular testbed was developed using Python scripts simulating Modbus TCP/IP communication:

Modbus Server: Hosts registers representing measurement variables encoded as IEEE 754 floating-point values split across two 16-bit registers.

Modbus Client: Periodically queries registers to retrieve updated values.

Network Sniffer: Passively monitors traffic, decodes Modbus frames, and extracts measurement vectors for AI analysis. An overall representation is shown in Figure 4.21.

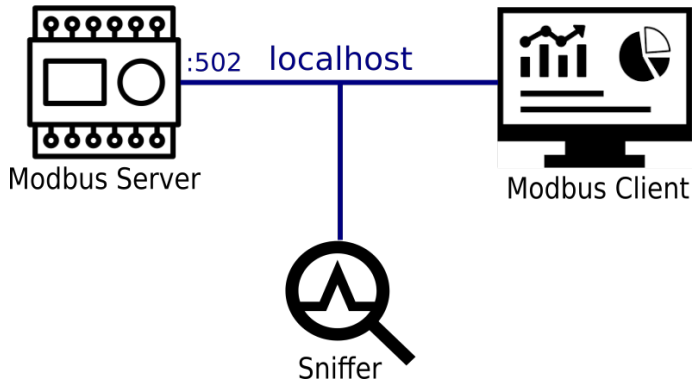

Figure 4.21: Network testbed architecture for online intrusion detection

Cyberattacks were implemented directly on the testbed. For example, the following code is used to implement a Bad Data Injection on the Modbus connection:

```
from scapy.all import *
import os
import socket
import scapy.contrib.modbus as mb

packet=mb.ModbusADURequest(len=6,
unitId=1) /mb.ModbusPDU05WriteSingle
CoilRequest (outputAddr=7,
outputValue=65280)

s = socket.socket(socket.AF_INET,
socket.SOCK_STREAM)
s.connect(("127.0.0.1",502))
s.send(bytes(packet))
```

The code creates and sends a Modbus TCP "Write Single Coil" request to a server running on the local machine at port 502. It uses Scapy's Modbus extension to construct the request packet, where the application data unit specifies that coil number 7 should be written with the value 0xFF00, which corresponds to turning the coil ON. A TCP socket connection is then established with the target, and the crafted packet is transmitted in raw byte form. The overall aim of this code is to remotely control a Modbus coil, demonstrating how to craft and send a Modbus write command for testing or interaction with a Modbus-compatible device or simulator.

4.4.5 Comparative Evaluation

Three architectures were compared: the proposed LSTM encoder-decoder, the enhanced LSTM encoder-decoder with physics constraints, and a simple autoencoder.

Results have been obtained in terms of three metrics commonly used in ML, i.e. Accuracy, Sensitivity, and specificity, which are defined in Equations (4.15), (4.16), and (4.17), respectively.

1. Simple Autoencoder (Baseline): Represents a conventional approach commonly used in anomaly detection literature. The autoencoder is a common solution in the literature for anomaly detection, especially in the field of cyber-physical systems. Table 4.7 reports the results of the classic autoencoder.

Table 4.7: Autoencoder Results

Dataset	**Accuracy**	**Sensitivity**	**Specificity**	**Confusion Matrix**
BDI_P_reduction	33.33%	0%	100%	TP=0 FP=0 FN=60 TN=30
BDI_Q_increment	67.78%	0%	100%	TP=32 FP=0 FN=29 TN=29
BDP_Q_oscillation	67.78%	51.67%	100%	TP=31 FP=0 FN=29 TN=30
FDI_P	25%	0%	100%	TP=0 FP=0 FN=90 TN=30
FDI_T_panel	74.17%	65.56%	100%	TP=59 FP=0 FN=31 TN=30
FDI_Irr	34.17%	12.22%	100%	TP=11 FP=0 FN=79 TN=30
Firmware_THD	81.67%	75.56%	100%	TP=68 FP=0 FN=22 TN=30
Firmware_MPPT _modification	33.33%	0%	100%	TP=0 FP=0 FN=60 TN=30
Fault_Short CircuitedCells	100%	100%	100%	TP=90 FP=0 FN=0 TN=30
Fault_Dust	75%	66.67%	100%	TP=60 FP=0 FN=30 TN=30
Global	60.18%	44.94%	100%	TP=351 FP=0 FN=430 TN=299

2. LSTM Encoder-Decoder: Adds temporal modeling capability through LSTM. Table 4.8 shows the results for the LSTM encoder-decoder architecture. The implemen-

tation of the LSTM layer allows catching time relationships between measures, enhancing the sensitivity. For example, it can be noticed how the performance of that algorithm in datasets that involve malicious oscillations of measures significantly increases.

Table 4.8: LSTM Results (Physics Not Included)

Dataset	**Accuracy**	**Sensitivity**	**Specificity**	**Confusion Matrix**
BDI_P_reduction	96.51%	94.92%	100%	TP=56 FP=0 FN=3 TN=27
BDI_Q_increment	96.51%	95%	100%	TP=57 FP=0 FN=3 TN=27
BDP_Q_oscillation	82.56%	74.58%	100%	TP=44 FP=0 FN=15 TN=27
FDI_P	47.41%	31.46%	100%	TP=28 FP=0 FN=61 TN=27
FDI_T_panel	94.83%	93.26%	100%	TP=83 FP=0 FN=6 TN=27
FDI_Irr	81.03%	75.28%	100%	TP=67 FP=0 FN=22 TN=27
Firmware_THD	87.93%	84.27%	100%	TP=75 FP=0 FN=14 TN=27
Firmware_MPPT _modification	39.53%	11.86%	100%	TP=7 FP=0 FN=52 TN=27
Fault_Short CircuitedCells	100%	100%	100%	TP=89 FP=0 FN=0 TN=27
Fault_Dust	100%	100%	100%	TP=89 FP=0 FN=0 TN=27
Global	83.09%	77.17%	100%	TP=595 FP=0 FN=176 TN=270

3. Physics-Informed LSTM Encoder-Decoder: Adds physics constraints to the learning process. Table 4.9 shows the results after the implementation of physics constraints in the LSTM encoder-decoder architecture. This solution further enhances performance compared to the simple LSTM, particularly in the sensitivity metric.

The enhanced performance can be attributed to the model's improved capability to detect subtle interdependencies within the data through physics-based knowledge integration. This enhancement makes the system particularly effective at identifying specific attack types, such as False Data Injection attacks, where adversaries manipulate individual

Table 4.9: LSTM Results (Physics Included)

Dataset	Accuracy	Sensitivity	Specificity	Confusion Matrix
BDI_P_reduction	100%	100%	100%	TP=59 FP=0 FN=0 TN=27
BDI_Q_increment	97.67%	96.67%	100%	TP=58 FP=0 FN=2 TN=27
BDP_Q_oscillation	93.02%	89.83%	100%	TP=53 FP=0 FN=6 TN=27
FDI_P	75%	67.42%	100%	TP=60 FP=0 FN=29 TN=27
FDI_T_panel	100%	100%	100%	TP=89 FP=0 FN=0 TN=27
FDI_Irr	88.79%	85.39%	100%	TP=76 FP=0 FN=13 TN=27
Firmware_THD	95.69%	94.38%	100%	TP=84 FP=0 FN=5 TN=27
Firmware_MPPT _modification	59.49%	32.20%	100%	TP=19 FP=0 FN=40 TN=27
Fault_Short CircuitedCells	100%	100%	100%	TP=89 FP=0 FN=0 TN=27
Fault_Dust	100%	100%	100%	TP=89 FP=0 FN=0 TN=27
Global	90.87%	87.67%	100%	TP=676 FP=0 FN=95 TN=270

measurements. In these scenarios, the anomaly becomes apparent through cross-validation with related measurements rather than through deviations from historical patterns.

Table 4.10 summarizes the comparative performance across all three architectures. The autoencoder exhibits limited capacity for understanding system dynamics, while the LSTM architecture adds temporal awareness to track sequential patterns. The physics-augmented LSTM encoder-decoder achieves superior reliability when compared to both preceding approaches.

Our experimental findings reveal a consistent improvement trajectory across the three deep learning frameworks investigated. Each progressive architecture exhibits better prediction precision and broader applicability, validating both our methodological approach and its potential for real-world implementation.

The foundational architecture, a standard autoencoder, remains a prevalent choice for anomaly detection and time-series modeling in industrial applications. Its straightfor-

ward design and implementation advantages make it appealing for preliminary system deployment. Nevertheless, our results validate existing concerns about its constraints in modeling intricate temporal relationships and system behavior, especially when dealing with datasets exhibiting long-range dependencies or contextual interconnections. These findings corroborate earlier research demonstrating that autoencoders struggle with multivariate temporal data in dynamic environments.

Table 4.10: Comparison of Models

Metric	**Auto-encoder**	**LSTM (Without Physics)**	**LSTM (With Physics)**
Accuracy	60.18%	83.09%	90.87%
Sensitivity	44.94%	77.17%	87.67%
Specificity	100%	100%	100%

The initial enhancement, incorporating an LSTM encoder-decoder structure, surpasses the basic autoencoder through its temporal memory capabilities, enabling the identification of sequential patterns and more precise trend forecasting. This recurrent design proves especially valuable for temporally-ordered information, consistent with established research highlighting LSTM architectures' effectiveness in condition monitoring and anomaly identification within industrial and cyber-physical environments. Notably, in scenarios where the autoencoder failed to identify any true positives (such as BDI_P reduction, FDI_P, and Firmware_MPPT_modification), the LSTM approach successfully detected at least some instances while excelling in other test cases. The 83.09% accuracy of this architecture, compared to the autoencoder's 60.18%, substantiates the significant advancement achieved.

However, the most substantial progress emerges from incorporating physics-informed neural networks within the LSTM encoder-decoder framework. This integrated methodology incorporates domain-specific knowledge into the training process, enforcing physically plausible constraints on the model. Consequently, the proposed system exhibits enhanced generalization, noise tolerance, and interpretability—essential characteristics for practical industrial deployment. This architecture achieves 90.87% overall accuracy, representing a notable improvement over the 83.09% obtained without physics integration.

These outcomes support the growing consensus in current literature that physics-informed neural networks strengthen model dependability and reduce data requirements, particularly valuable when labeled training data is limited or expensive to acquire.

This finding underscores the critical need for physics-informed approaches that can distinguish between legitimate environmental variations and actual cyberthreats. The persistent detection challenges point to promising research directions:

Physics-informed detection methods that incorporate domain-specific relationships and physical laws.

Hybrid approaches combining anomaly detection with specialized fault diagnosis techniques.

Time-series analysis methods optimized for gradual degradation patterns.

Ensemble approaches that integrate multiple detection paradigms for comprehensive coverage.

The work establishes that the raw application of classical anomaly detection methods is insufficient for high-dimensional cyberphysical systems without domain-specific preprocessing and parameter optimization.

4.5 Discussion

4.5.1 Dataset Contributions

Photo-Set addresses several critical gaps in the field of PV system cybersecurity research. Most importantly, it represents the first PV-specific dataset offering comprehensive physical measurements that span multiple operational aspects of photovoltaic systems. The dataset encompasses diverse attack scenarios covering Bad Data Injection, False Data Injection, and firmware modification attacks, providing researchers with a broad spectrum of threat models to evaluate. Beyond the attack scenarios, the dataset captures realistic operating conditions through multi-day normal operation recordings and variable weather patterns, ensuring that detection algorithms must contend with authentic environmental variations. This combination of features establishes a standardized benchmark that enables reproducible research across different detection methodologies and facilitates meaningful performance comparisons.

4.5.2 Benchmark Insights

The comprehensive evaluation of various detection algorithms revealed important insights about their relative strengths and limitations. Analysis of algorithm-specific performance

showed that Isolation Forest achieved the best overall results, demonstrating robust detection capabilities across most attack scenarios. In contrast, both One-Class SVM and Local Outlier Factor struggled particularly with specificity, generating excessive false positives that would limit their practical utility in production environments. The evaluation also uncovered attack-dependent detectability patterns, with firmware modifications and oscillatory attacks proving considerably easier to identify than subtle manipulations of single parameters. This variance in detection difficulty highlights a fundamental challenge: distinguishing genuine attacks from normal environmental variations remains problematic for conventional machine learning methods, particularly when attackers employ sophisticated strategies that mimic natural system behavior.

4.5.3 Physics-Informed Advantages

The physics-informed LSTM encoder-decoder architecture delivered substantial improvements across multiple dimensions. It achieved 30.69% higher accuracy than the baseline autoencoder and 7.78% improvement over standalone LSTM. The approach detected 95 fewer false negatives globally compared to LSTM alone—critical for cybersecurity where missed attacks have severe consequences. The methodology also provides enhanced interpretability through embedded physical constraints that domain experts can understand and validate, addressing the opacity of purely data-driven approaches. Additionally, integrating prior physical knowledge improves data efficiency, reducing dependence on large volumes of labeled training data—a significant advantage given that annotated attack data is scarce and expensive in operational environments.

4.5.4 Limitations and Future Directions

Despite promising results, three significant challenges remain. First, gradual physical degradation is nearly indistinguishable from natural environmental changes due to slow parameter drifts. Second, sophisticated attacks that maintain physical constraints while manipulating individual parameters evade detection, especially when attackers understand the encoded physical relationships. Third, firmware MPPT modifications achieved only 59.49% detection accuracy, indicating internal control algorithm manipulations require different detection strategies.

These limitations suggest critical research directions. Real-world validation is essential to confirm laboratory findings translate to operational environments. Multi-site

coordinated attack scenarios must be addressed to counter simultaneous compromise of distributed installations. Integration with network-based intrusion detection would provide complementary detection at physical and cyber layers. Real-time embedded implementations would enable deployment in resource-constrained field devices. Finally, hybrid approaches combining physics-based, statistical, and network-based methods may overcome individual limitations and provide robust protection for PV infrastructure.

4.6 Chapter Summary

This chapter presented the development and validation of Photo-Set, a comprehensive dataset for PV system cybersecurity research. The work progressed through three phases: dataset creation with diverse attack and fault scenarios, establishment of performance benchmarks using conventional anomaly detection algorithms, and development of an advanced physics-informed detection approach.

Key contributions include:

1. **Photo-Set dataset:** 12 attack/fault scenarios plus realistic environmental conditions, totaling over 150,000 labeled samples

2. **Benchmark evaluation:** Systematic comparison of three algorithms establishing performance baselines and revealing a clear attack detectability hierarchy

3. **Physics-informed detection:** Novel LSTM-based approach achieving 90.87% accuracy by combining temporal modeling with physical constraints

The results demonstrate that physics-informed approaches offer substantial advantages for PV cybersecurity monitoring, achieving significantly higher detection rates while maintaining interpretability. The publicly available dataset provides a standardized testbed for future algorithm development and comparative evaluation.

While physics-informed detection provides robust anomaly identification for individual DERs, large-scale aggregations like virtual power plants introduce additional attack surfaces requiring systematic vulnerability analysis, as examined in the next chapter.

CHAPTER 5

Virtual Power Plant Ancillary Services and Technical Requirements

5.1 Introduction

While Chapter 4 addressed detection at the individual DER level, larger aggregations like VPPs present distinct challenges requiring systematic vulnerability analysis beyond single-system detection. This chapter presents a comprehensive analysis of cybersecurity in Virtual Power Plants (VPPs), examining the complete spectrum from architectural foundations through threat identification to mitigation implementation. Virtual Power Plants have emerged as critical infrastructure for grid stability, aggregating diverse Distributed Energy Resources (DERs) to provide essential ancillary services including frequency regulation, voltage support, and emergency response capabilities. However, the technical requirements that enable VPPs to deliver these time-critical services simultaneously create unique cybersecurity vulnerabilities that distinguish them from traditional power generation and conventional smart grid systems.

The chapter follows a logical progression that mirrors the relationship between VPP technical requirements and security implications. We begin by examining VPP system architecture and communication infrastructure, establishing the technical foundation upon which all services and vulnerabilities depend. This architectural analysis identifies the critical components, communication protocols, and stakeholder relationships that form the VPP ecosystem. Subsequently, we analyze the ancillary services that VPPs provide, detailing the specific technical requirements—particularly timing constraints—that create operational imperatives influencing security implementations.

The content of this chapter has been published in the following paper:

A. Mokarim, G. B. Gaggero, and M. Marchese, "Securing Virtual Power Plants: Attack Vector Analysis of Cybersecurity Vulnerabilities in Ancillary Grid Services," IEEE Open J. Ind. Electron. Soc., early access, 2025, doi: 10.1109/OJIES.2025.3622528.

Building upon this foundation, the chapter systematically identifies cybersecurity threats through integrated application of NIST and MITRE frameworks. This multi-framework approach ensures both theoretical comprehensiveness and practical applicability for VPP operators, regulators, and technology providers. The NIST Cybersecurity Framework provides organizational structure (Identify, Protect, Detect, Respond, Recover), while MITRE ATT&CK for ICS enables precise threat technique classification. The threat analysis reveals how operational necessities create exploitable vulnerabilities, demonstrating the unique security challenges that emerge when time-critical grid services depend on distributed, multi-stakeholder infrastructure integrated with electricity markets.

The chapter concludes with comprehensive mitigation strategies that address identified vulnerabilities while maintaining operational performance. These strategies recognize that traditional security approaches designed for enterprise IT environments or centralized industrial control systems prove insufficient for VPP environments. Effective VPP security requires specialized frameworks that balance rapid response capabilities with comprehensive threat protection, accommodate diverse stakeholder security maturity levels, and maintain service delivery during security incidents.

Under the NIS2 Directive Article 2, VPPs providing ancillary services qualify as "essential entities" in the energy sector, requiring implementation of technical and organizational measures proportional to their critical grid support functions. This regulatory context emphasizes the importance of systematic cybersecurity approaches that can demonstrate compliance while maintaining operational effectiveness. The integrated NIST-MITRE framework presented in this chapter provides that systematic approach, offering VPP stakeholders actionable guidance grounded in established cybersecurity principles and adapted to energy sector operational realities.

The analysis reveals three fundamental characteristics that create VPP-specific security challenges: (1) stringent timing constraints for ancillary service delivery that limit security validation time, (2) distributed multi-stakeholder architecture that expands attack surfaces across diverse DER technologies and organizational boundaries, and (3) integration with electricity markets that introduces financial attack motivations beyond operational disruption. Each characteristic creates distinct vulnerability categories requiring tailored mitigation approaches, as detailed throughout this chapter.

5.2 VPP System and Communication Architecture

Understanding VPP cybersecurity requires first establishing the technical infrastructure that enables VPP operations. This section examines the system architecture, communication networks, and operational procedures that form the foundation for ancillary service provision. The architectural analysis identifies critical components whose compromise could significantly impact grid stability, maps communication pathways that adversaries might exploit, and establishes the technical context necessary for subsequent threat analysis.

5.2.1 VPP Concept and Functional Architecture

Virtual Power Plants aggregate electricity from numerous small producers and deliver it to the power grid following quantities specified in prior electricity sales agreements. They bridge the gap between conventional power plants and distributed renewable resources through three core functions: (1) aggregation and coordination of diverse DERs, (2) market participation comparable to conventional power plants, and (3) provision of ancillary services for grid stability. Individual generation units on distribution networks cannot independently provide sufficient controllability and reliability to be economically viable in open electricity markets due to unfavorable cost-benefit ratios.

A VPP communicates not only with geographically scattered DERs and responsive loads but also with electricity market retailers, aggregators, Transmission System Operators (TSO), and Distribution System Operators (DSO), providing a versatile communication structure as illustrated in Figure 5.1. This relationship creates complex trust boundaries across organizational domains. The VPP supports demand response programs and facilitates active DER participation in providing ancillary services, with load-frequency control being the most common application. Ancillary services, including frequency regulation, voltage control, and black start capabilities, prove crucial for ensuring grid stability and reliability.

VPPs are functionally divided into two types, each presenting distinct security considerations:

Commercial VPP (CVPP): A CVPP aggregates DERs to enable effective market participation, comparable to conventional power plants. It provides frequency response and reserve services through long-term contracts, making it a target for market manipulation attacks. The financial incentives associated with market participation create attack

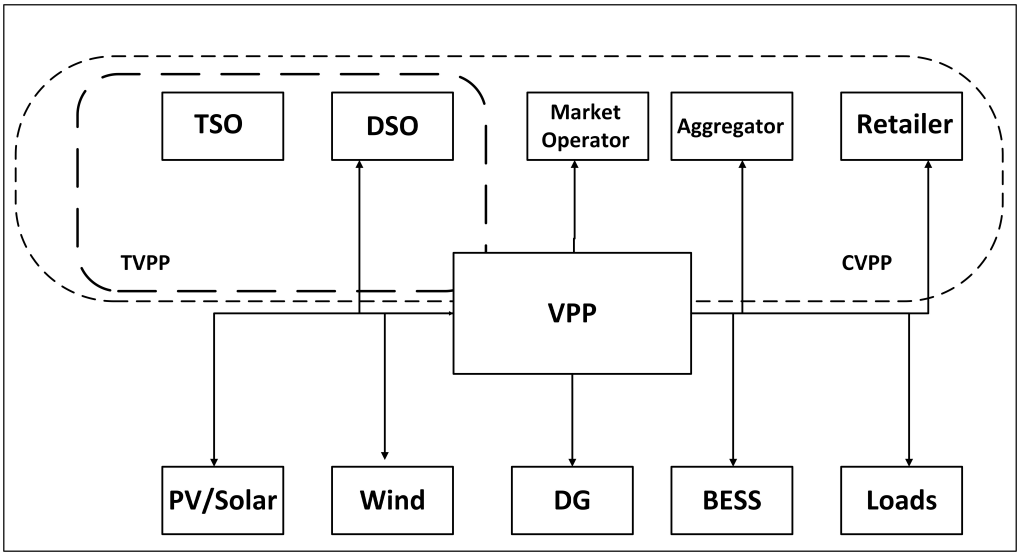

Figure 5.1: VPP Ecosystem Overview: The diagram illustrates the hierarchical relationship between VPP operators and stakeholders.

motivations beyond operational disruption, attracting adversaries seeking economic gain through bid falsification, capacity misrepresentation, or settlement manipulation. From a cybersecurity perspective, CVPPs require particular attention to market interface security, financial transaction validation, and fraud detection capabilities.

Technical VPP (TVPP): TVPP focuses on system management and technical feasibility. It enables DER contribution to system stability while respecting network constraints, making it vulnerable to operational manipulation attacks. TVPPs interact more directly with grid operators (TSOs and DSOs) to provide real-time ancillary services, creating dependencies on time-critical communications and control systems. Security priorities for TVPPs emphasize protecting operational technology, ensuring communication integrity, and maintaining service availability during adverse conditions. From a NIST cybersecurity perspective (NIST ID.AM-1: Asset Management), VPP assets fall into multiple categories requiring different protection strategies based on their criticality to operations and potential impact if compromised:

HIGH Impact Assets:

1. VPP Energy Management System (EMS): Central control platform coordinating all DER activities

2. TSO/DSO communication interfaces: Critical pathways for grid operator commands and status reporting

3. Market bidding and settlement systems: Financial transaction platforms affecting revenue and compliance
4. Frequency regulation control algorithms: Time-critical software governing primary ancillary service

MODERATE Impact Assets:

1. DER aggregation software: Platforms combining individual DER capabilities into portfolio offerings
2. Forecasting and optimization systems: Analytical tools supporting operational and market decisions
3. Customer information systems: Databases containing contractual, billing, and personal information
4. Historical operational data: Archives supporting analytics, compliance, and performance verification

LOW-Impact Assets:

1. Individual DER monitoring interfaces: Single-asset observation tools with limited control capabilities
2. Administrative systems: Back-office platforms supporting business operations
3. Public-facing websites: Information portals for customers and stakeholders
4. Training and documentation systems: Educational resources and procedural guides

The above VPP asset information has been summarised in Table 5.1.

This asset classification informs security control selection, with high-impact assets receiving the most stringent protections and monitoring while lower-impact assets implement baseline security appropriate to their risk profile. However, the interconnected nature of VPP systems means that compromise of low-impact assets can provide adversaries with footholds for lateral movement toward high-impact targets, necessitating comprehensive security across all asset categories.

Table 5.1: VPP Asset Classification for Cybersecurity

NIST Impact Level	**Name of the asset**
HIGH	VPP Energy Management System(EMS) TSO/DSO communication interfaces Market bidding and settlement systems Frequency regulation control algorithms
MODERATE	DER aggregation software Forecasting and optimization systems Customer information systems Historical operational data
LOW	Individual DER monitoring interfaces Administrative systems Public-facing websites Training and documentation systems

5.2.2 Communication Infrastructure and Network Architecture

The VPP infrastructure includes servers, network equipment, and potentially cloud-based installations, along with software-technical solutions needed to manage diverse data and communication requirements arising from heterogeneous DERs and stakeholders. This includes Energy Management Systems (EMS), which serve as central monitoring and control elements. The increasing adoption of internet technology for control efficiency, while beneficial for operational flexibility and cost reduction, unfortunately expands the attack surface significantly.

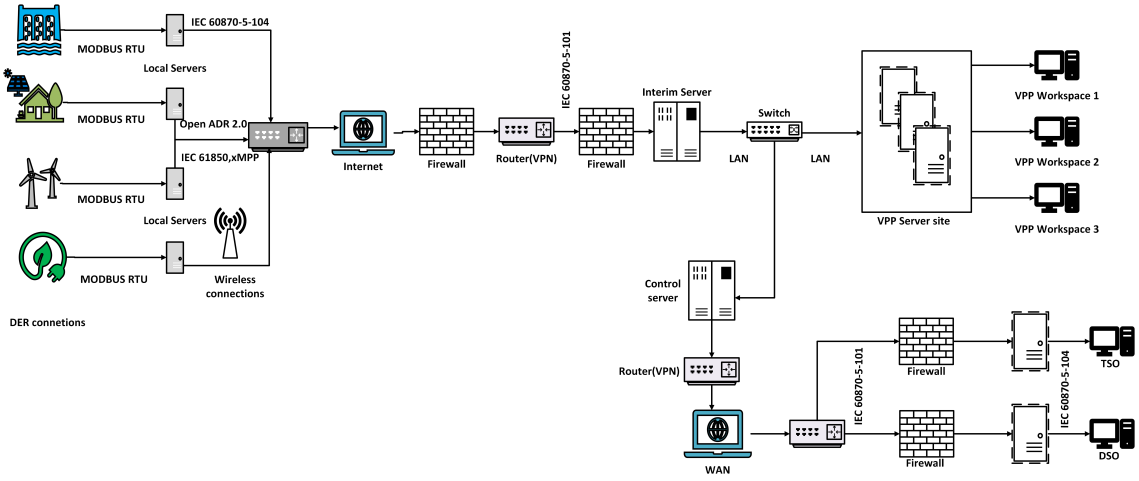

Figure 5.2: VPP Communication Architecture: Multi-layer security architecture showing distributed control points (VPP Workspaces 1-3) connected through secure gateways (Interim Server) with network segmentation (Firewalls) between operational technology (OT) and information technology (IT) domains. Router/VPN connections ensure encrypted communication with geographically distributed DER assets via WAN infrastructure.

Figure 5.2 illustrates the hierarchical VPP communication architecture with multiple security zones. The Interim Server provides secure communication gateway functions, implementing protocol translation, message validation, and security policy enforcement. VPP Workspaces 1-3 represent distributed control points managing different DER portfolios, enabling geographic distribution of control functions while maintaining centralized coordination. Router/VPN connections ensure encrypted communications between remote DER connections and the central VPP infrastructure, protecting command and measurement data traversing public networks. Firewalls provide network segmentation between operational technology (OT) and information technology (IT) domains, with WANs connecting geographically distributed assets.

The infrastructure in a VPP bridges the gap between Information Technology (IT) and Operational Technology (OT) layers. The OT layer encompasses the physical DERs—solar inverters, wind turbines, battery storage systems, controllable loads—while the IT layer includes the EMS and communication systems that monitor and control them. This IT-OT convergence requires security measures aligned with NIST SP 800-53 controls like network segmentation (SC-7: Boundary Protection) and protocol encryption (SC-8: Transmission Confidentiality).

The ICT infrastructure relies on various network technologies to facilitate communication across different geographical scales:

Wide Area Networks (WANs): Connect geographically dispersed DERs and external entities like TSOs, DSOs, and electricity markets. WAN communications typically traverse public internet infrastructure or dedicated carrier networks, creating exposure to internet-based threats. VPN tunnels, MPLS circuits, or dedicated fiber connections provide varying levels of security and performance guarantees. Field Area Networks (FANs): Facilitate communication within a localized area of DERs, such as a solar farm, wind park, or industrial facility. FANs often implement specialized protocols optimized for industrial control applications, including IEC 61850 for substation automation or DNP3 for utility communications.

Neighbor Area Networks (NANs): Connect smart meters and local distribution automation devices within neighborhoods or distribution circuits. NANs support advanced metering infrastructure (AMI) and distribution automation functions, providing granular visibility and control at distribution grid levels.

Home Area Networks (HANs): May be relevant depending on the types of DERs aggregated, particularly when VPPs include residential solar installations, home battery systems, smart thermostats, or electric vehicle chargers. HANs typically implement consumer-oriented protocols like Zigbee, Z-Wave, or Wi-Fi, which may have security characteristics differing from industrial protocols.

5.2.3 Communication Protocols

The communication protocols used by a VPP are integral to its ICT infrastructure, governing how data is formatted, transmitted, and received across the network. The Common Information Model (CIM) standards (IEC 61968/61970) ensure data exchange compatibility between different systems and protocols, providing semantic interoperability that enables diverse systems to share information meaningfully.

IEC 60870-5-104: A widely used telecontrol (SCADA) protocol based on TCP/IP for control and monitoring messages. It provides point-to-point communications between control centers and remote terminal units (RTUs) or intelligent electronic devices (IEDs). The protocol supports various information types including measurements, commands, and event notifications, making it suitable for comprehensive grid monitoring and control.

IEC 61850: A preferred standard for smart grid operations with object-oriented information models, also utilizing IP and Ethernet. It enables interoperability between substation automation devices from different manufacturers through standardized data objects and services. However, it faces cybersecurity and scalability challenges, particu-

larly regarding secure configuration management and protection of time-critical GOOSE (Generic Object Oriented Substation Event) messages.

OpenADR 2.0: Used for demand response and DER integration, enabling exchange of a wider range of data including market information, pricing signals, and control strategies. OpenADR implements web services architecture using XML messaging over HTTP/HTTPS, providing flexibility for complex demand response programs but with potentially higher protocol overhead compared to specialized industrial protocols.

Modbus: Employed for specific data exchange, such as bid-related messages between TSO and VPP in some implementations. Modbus TCP/IP provides simple request-response communications suitable for reading measurements and writing setpoints. Its simplicity contributes to widespread adoption but creates security challenges due to lack of built-in authentication or encryption.

eXtensible Message Presence Protocol (XMPP): Proposed as middleware for enhancing scalability and security over existing protocols like IEC 61850. XMPP provides publish-subscribe messaging patterns, presence information, and extensible data formats that can encapsulate industrial protocol messages while adding authentication and encryption capabilities.

The diversity of protocols reflects the heterogeneous nature of VPP infrastructure, where different DER types, vintages, and manufacturers implement varying communication standards. This protocol heterogeneity creates both interoperability challenges and security complications, as VPP operators must secure multiple protocols simultaneously while maintaining real-time performance requirements.

5.2.4 VPP Operational Procedures

The operation of VPPs relies heavily on timely and accurate exchange of data across various stakeholders, enabling the VPP to manage DERs effectively, participate in electricity markets, and provide ancillary grid services. The core of this interaction involves bidirectional exchange of four key data categories: (1) real-time measurements, (2) capacity and availability, (3) set-points, and (4) market-related information.

According to NIST SP 800-60 (Guide for Mapping Types of Information and Systems to Security Categories), these data can be classified by security impact:

High Impact Data: Real-time control signals, grid frequency measurements, emergency dispatch commands. Unauthorized disclosure could enable adversary planning for

sophisticated attacks; unauthorized modification could cause immediate grid instability; unavailability could prevent essential ancillary service delivery.

Moderate Impact Data: Market bids, capacity forecasts, historical performance data. Compromise affects economic outcomes and regulatory compliance but typically does not create immediate physical consequences.

Low Impact Data: Public market information, general operational statistics. Compromise has limited impact on operations or confidentiality.

These data exchanges are characterized by their time sensitivity, protocol requirements, and implications for operational reliability:

Market and Scheduling Communication: VPPs interact with electricity market platforms via retailers and aggregators by submitting bids for scheduled power delivery. These bids are based on aggregated data from diverse DERs, including solar photovoltaics (PV), wind turbines, combined heat and power (CHP) units, electric vehicles (EVs), and energy storage devices (ESDs). Each DER transmits its available capacity, forecasted generation (weather-dependent for renewables), cost parameters, and operational constraints to the VPP. Using this information, the VPP computes an optimal power-cost portfolio and commits a scheduled power quantity to the DSO. The Energy Management (EM) system within the VPP then receives a dispatch schedule from the DSO, often based on an Optimal Power Flow (OPF) solution. Final setpoints are calculated and assigned to individual DERs to fulfill this committed schedule.

Real-Time Measurements: DERs continuously transmit real-time measurements such as power output, voltage levels, network status, and other operational parameters to the VPP. The frequency of this reporting depends on the type of grid services provided—frequency regulation requires second-scale updates while energy scheduling may accept minute-scale reporting. Protocols like IEC 60870-5-104 are commonly used for this signal-oriented transmission over LAN or WAN. The VPP aggregates measurements received from individual DERs to generate a singular VPP profile representing total capacity. This aggregated data, along with calculated baseline values, is transmitted to the TSO or DSO control center. The timeliness and reliability of measurement data prove crucial for the VPP's monitoring and control functions, as well as for the TSO/DSO to maintain grid stability. Latency and packet loss can impact the accuracy and availability of this information, potentially causing inappropriate control responses.

Capacity and Availability Signaling: DERs provide information about their available capacity (both positive and negative) to the VPP, including operational limits, ramp-up/down capabilities, and current status. Based on the aggregated capacity and availability

of its DER portfolio, the VPP makes bids in electricity markets and offers its capacity for ancillary services to TSOs and DSOs. Commercial VPPs (CVPPs) specifically focus on offering this flexible capacity on the electricity market. The exchange of flexibility information (schedules, baseline data, market prices) requires communication protocols that support these data types, leading to exploration of more advanced protocols beyond legacy SCADA systems.

Set-Points Dispatch and Activation: When the TSO or DSO requires the VPP to provide certain capacity (for example, for frequency restoration), it sends a set-point signal or activation request to the VPP. Upon receiving a set-point from the TSO/DSO, the VPP performs internal optimization and dispatches START activation signals with required set-point values to selected DERs. The VPP also sends signals to terminate the activation process when services are no longer needed. The latency in delivery of set-point signals is critical, especially for ancillary services with strict operational time frames. Delays can compromise the VPP's ability to meet required response times, potentially triggering contractual penalties and reducing grid stability support.

In essence, effective VPP operation depends on seamless and timely exchange of measurements, capacity, availability, and set-point data across its communication infrastructure. The choice of technologies and protocols, along with management of Quality of Service (QoS) parameters like latency and reliability, are critical to ensuring that the VPP can fulfill its roles in grid support and energy markets.

5.3 Ancillary Services and Technical Requirements

Ancillary services guarantee that the power grid runs correctly, maintaining frequency, voltage, and stability within acceptable operating parameters. These services fall under the purview of grid operators (distribution and transmission system operators), who coordinate resources to prevent disturbances and facilitate rapid recovery when incidents occur. Every nation in the European Network of Transmission System Operators for Electricity (ENTSO-E) region has a unique market structure for balancing services. Some countries, like Germany, tender all necessary balancing capacity products in daily auctions. Other nations depend on reserve obligations and secondary markets for certain products. The market for balancing services is becoming increasingly liberalized and accessible to new suppliers, such as aggregators, with ELIA (Belgium TSO) conducting cross-border coordination with many European TSOs. Additionally, Italy has developed a pilot program

enabling aggregation of smaller units and activation of their flexibility by TERNA (TSO in Italy) for balancing purposes.

The four categories of ancillary services are: (1) frequency balance, (2) voltage compensation, (3) supply reconstruction, and (4) operational management. Each category presents distinct technical requirements that influence both operational procedures and cybersecurity considerations.

5.3.1 Frequency Balance Services

Frequency control is critical for maintaining grid stability and involves three hierarchical levels of response. Meeting technical requirements for ancillary services like Frequency Containment Reserve (FCR), Automatic Frequency Restoration Reserve (aFRR), and Manual Frequency Restoration Reserve (mFRR) necessitates specific communication requirements, including stringent data communication cycle times and responsiveness.

Frequency Restoration Reserve (FRR) encompasses both automatic (aFRR) and manual (mFRR) frequency restoration services that follow the initial frequency containment response. FCR provides fast, automatic response to frequency deviations, ensuring short-term grid stability through immediate power adjustments distributed across all generating units. The second response is aFRR, which acts as a follow-up to FCR, offering longer-term response to restore grid frequency and maintain balance. Finally, mFRR is executed manually or semi-automatically, providing the tertiary level of frequency control with the longest response times but sustained duration.

Table 5.2 indicates the activation and cycle times for each of the FRR actions performed.

Table 5.2: FRR services with Activation Times and Cycle Times

FRR service	**Activation Time**	**Cycle Time**
Frequency Containment Reserve (FCR)	15 s–30 s	1–2 s
Automatic Frequency Restoration Reserve (aFRR)	5 min–15 min	1–5 s
Manual Frequency Restoration Reserve (mFRR)	15 min	1 min

Activation Time or T_A, is the time in which a set-point signal is transmitted from the TSO or DSO to the VPP and to the DERs that are activated to participate in the frequency-control service. The cycle time, T_C, is the time needed to gather measurements from the participating DERs and send them back to the TSO/DSO. Key QoS parameters impacting

VPP operation are latency, bandwidth, and packet loss. Latency is particularly critical for time-sensitive services like load-frequency control, where delays of even a few seconds can render responses ineffective.

The stringent timing requirements for FCR (1-2 second cycle times) and aFRR (1-5 second cycle times) create fundamental tensions between comprehensive security validation and operational responsiveness. Traditional authentication and authorization procedures requiring multi-step verification, certificate validation, or human approval cannot be completed within these timeframes without compromising service delivery. This tension between security and performance represents a core challenge for VPP cybersecurity, requiring innovative approaches that pre-validate commands, implement fast cryptographic operations, or accept graduated risk during time-critical operations.

5.3.2 Voltage Compensation Services

Voltage compensation ensures that voltage levels remain within acceptable ranges to protect equipment and maintain power quality. Voltage Support Services involve real-time adjustment of reactive power to maintain voltage levels within operational limits. These services require rapid response capabilities and continuous monitoring of voltage conditions across the distribution network. Network operators address voltage instability through two primary mechanisms:

Power Factor Correction: Minimizing the phase angle between voltage and current in AC systems (ideally approaching 0° for power factor = 1) improves system efficiency and voltage stability. Operators deploy capacitive or inductive elements (such as capacitor banks or reactors) when transformers, grid elements, or consumption processes create reactive power imbalances. Modern smart inverters on distributed generation can provide dynamic power factor correction by adjusting their reactive power output in response to local voltage conditions or central commands. Typical response time for power factor correction is less than 1 minute, enabling real-time voltage support but creating vulnerability windows where attackers might inject false measurements or manipulate control signals.

Loss Energy Management: Compensating for energy dissipation during transmission by forecasting losses and purchasing additional energy addresses the economic and technical aspects of voltage management. These losses, varying with network utilization, represent significant system service costs that TSOs and DSOs work to minimize through optimal dispatch and network reconfiguration. The response time for this service ranges between 5 and 15 minutes, providing more flexibility for security validation compared to

frequency services but still requiring timely decision-making based on accurate forecasts and measurements.

The continuous nature of voltage compensation, with ongoing adjustments responding to changing load and generation patterns, creates persistent attack surfaces. Unlike frequency events that occur episodically, voltage management requires constant monitoring and control, providing adversaries with numerous opportunities to observe system behavior, identify vulnerabilities, and execute attacks during periods of system stress.

5.3.3 Supply Reconstruction Services

Supply reconstruction services ensure rapid restoration of power supply following outages or emergencies. Black start capability—starting without external power sources—is crucial for grid recovery. While thermal plants (nuclear, coal) require external power for startup, hydroelectric, compressed air storage, and gas power plants can start autonomously. Large-scale energy storage systems are increasingly providing black start capability in modern grids, with typical response times of 5 to 15 minutes.

Emergency Response Services provide rapid power injection (within 5 minutes) during system emergencies, helping to arrest frequency decline or voltage collapse before cascading failures occur. Grid Restoration Procedures involve coordinated restart of grid sections following major outages, requiring:

1. **Sequenced restart procedures with precise timing (15-60 minutes):** Each generating station must energize in coordination with transmission system capacity and other generating units to avoid overloading partially restored grid segments or creating voltage/frequency instabilities during restoration.

2. **Coordination between multiple generation sources:** Black start capable units must communicate continuously with system operators and other generating stations to ensure synchronized restoration activities.

3. **Real-time monitoring of system frequency and voltage during restoration:** Restoration procedures operate outside normal grid conditions, requiring enhanced situational awareness and rapid response to unexpected deviations.

The criticality of supply reconstruction services during emergency conditions creates unique vulnerability scenarios. When major outages occur, communication systems may be degraded, operational staff work under extreme pressure, and normal procedures may be

abbreviated to accelerate restoration. These factors create opportunities for adversaries to exploit confusion, inject false information, or execute attacks that extend outage durations. Additionally, the infrequency of actual black start operations means that procedures receive limited real-world validation, potentially allowing security vulnerabilities to persist undetected until actual emergencies occur.

5.3.4 Operational Management Services

Operational management involves grid operators controlling and monitoring the grid while coordinating ancillary services. Redispatch is one key service that controls grid congestion by instructing power plants to adjust production schedules based on load flow calculations, redistributing generation geographically without changing total output. For megawatt-level control, redispatch takes around 1 to 15 minutes, depending on the severity of congestion and the responsiveness of available generation resources.

Feed-in management allows operators to disconnect renewable energy systems during significant power surpluses to prevent grid overloads and maintain stability. Feed-in management requires:

1. **Response time:** 1-15 minutes, depending on urgency: Critical oversupply situations demand rapid curtailment to prevent over-voltage or over-frequency conditions, while less severe situations allow more deliberate response.

2. **Communication requirements: Bidirectional control capability:** Operators must be able to command curtailment and receive confirmation that renewable generation has reduced output as requested.

3. **Curtailment precision: Adjustable in 1-10% increments:** Fine-grained control enables operators to match curtailment precisely to oversupply magnitude, minimizing unnecessary renewable energy waste.

The operational management services present distinct security challenges compared to faster-responding frequency and voltage services. The longer response times (1-15 minutes) provide more opportunity for comprehensive security validation but also create extended windows during which attacks might unfold. The economic implications of redispatch and curtailment—involving payments to generators, market settlement adjustments, and renewable energy certificate impacts—create financial attack motivations beyond purely operational disruption objectives.

5.3.5 Technical Requirements for DER Participation

For the successful implementation of VPP functions and provision of ancillary services, all hardware, software, and communication requirements must be met. Hardware requirements may involve deployment of equipment such as smart meters, home gateways, and smart appliances for energy management. Two-way flow of data and electricity is maintained through advanced metering infrastructure and controllable inverters. Major software requirements include aggregation and generation forecasting software for real-time communication, in addition to distribution system management software. Common interoperable protocols are vital for effective integration of DERs.

The NREL report focusing on frequency support from DERs elaborates on specific technical requirements at the device level, particularly for inverters. DSOs can acquire auxiliary services from DERs that aggregators have previously collected together. These services include both primary and secondary reserves. Primary reserves require rapid response within milliseconds and maintain service provision for brief periods. These frequency regulation services must come from quick-responding resources capable of swift power adjustment, with battery energy storage systems (BESS) being prime examples. Secondary reserves, in contrast, activate within minutes and contribute to system stability by delivering power for extended durations relative to primary reserves. DSOs might implement decentralized management approaches for these resources. There's growing interest in such decentralized control due to issues of distributed generation, including over-voltage, under-voltage, and grid congestion. However, this also poses risks to the security of the entire system.

The response times of various kinds of DERs are presented in Table 5.3. Values in this table represent typical performance under normal operating conditions and may vary based on equipment specifications, network conditions, and environmental factors. Response times are derived from industry standards [108, 109], manufacturer specifications, and peer-reviewed research, including NREL reports on DER frequency support capabilities[110].

Values in this table represent typical performance under normal operating conditions and may vary based on equipment specifications, network conditions, and environmental factors. Response times are derived from industry standards, manufacturer specifications, and peer-reviewed research, including NREL reports on DER frequency support capabilities.

Table 5.3: DER Response times for different services

DER Type	**Service**	**Response time**
Synchronous generators (conventional)	Primary Reserves	Few seconds
Battery Energy Storage Systems (BESS)	Primary Reserves	1–10 seconds, < 30 seconds
Pump Storage	Secondary Reserves	< 15 minutes
Small-scale hydro, wind and gasoline generators	Voltage Control	< 1 minute
Photovoltaics (PV)	Distribution Congestion Management	< 15 minutes
Electric Vehicles (EV) (Aggregated)	Primary Reserves	< 30 seconds
Combined Heat and Power (CHP)	Secondary Reserves	< 15 minutes

Primary reserves requiring rapid response within milliseconds and service provision for brief periods (less than 30 seconds) are particularly susceptible to timing-based attacks. Battery Energy Storage Systems (BESS), while capable of 1-10 second response times, can be compromised through latency injection attacks that delay critical control signals beyond acceptable thresholds. Secondary reserves, activating within minutes for extended duration support, rely on sustained communication channels that present opportunities for man-in-the-middle attacks and signal manipulation over longer timeframes.

It is also important to mention the ramp-up time required by industrial consumers and loads to reach 100% capacity after receiving set-point signals. DER response times and industrial ramp-up times are especially important as they determine the guidelines for frequency-load control action. The different ramp-up times for various industrial loads are given in Table 5.4.

The varying ramp-up times for different industrial loads create operational windows that attackers can exploit. Industrial inverters with potentially sub-second response capabilities are vulnerable to rapid-fire attack sequences. Rapid-fire attacks are defined as coordinated sequences of malicious commands executed within sub-second intervals to exploit the minimal response times of industrial inverters and fast-response systems. These attacks specifically target systems with response times under 30 seconds, such as battery energy storage systems providing primary reserves, by overwhelming validation mechanisms with high-frequency command injection.

Table 5.4: Ramp-up times for different loads

Load Type	**Ramp-up time**	**Category**
Industrial Inverters	Potentially < 1 second	Fast
Power-to-Heat(electrical heating)	< 30 seconds	Fast
Residential loads	< 1 minute	Fast
Chillers	1 minute	Medium
Steel mills, paper mills, cement mills, refineries	2–5 minutes	Medium
Steam or gas turbines (hot start)	5 minutes	Medium
(HVAC)	5–15 minutes	Slow
Steam or gas turbines (cold start)	10–15 minutes	Slow

Slower-responding systems like HVAC (5-15 minutes) and steam turbines (10-15 minutes) present opportunities for sustained manipulation attacks during their startup phases. Steel mills, paper mills, cement mills, and refineries with medium ramp-up times (2-5 minutes) represent critical infrastructure components where cyberattacks could have cascading economic and operational impacts beyond the immediate VPP environment.

Smart meter deployment alongside distributed automation and control systems can support these management strategies, but they are also prone to various cyber risks. The technical requirements and timing constraints described in this section create the operational context within which VPP cybersecurity must function, informing both threat analysis and mitigation strategy development in subsequent sections.

5.4 Threat Landscape and Vulnerability Analysis

VPPs face unique security challenges due to their decentralized nature and reliance on third-party aggregators. Trust and authentication mechanisms are critical in preventing unauthorized access and data manipulation. Cyber threats targeting VPPs include Denial-of-Service (DoS) attacks, ransomware, insider threats, and data integrity attacks. Man-in-The-Middle (MiTM) attacks on communication channels can compromise control signals, leading to unauthorized dispatch of energy resources. VPPs rely on extensive communication networks and control protocols such as IEC 61850, DNP3, Modbus, and

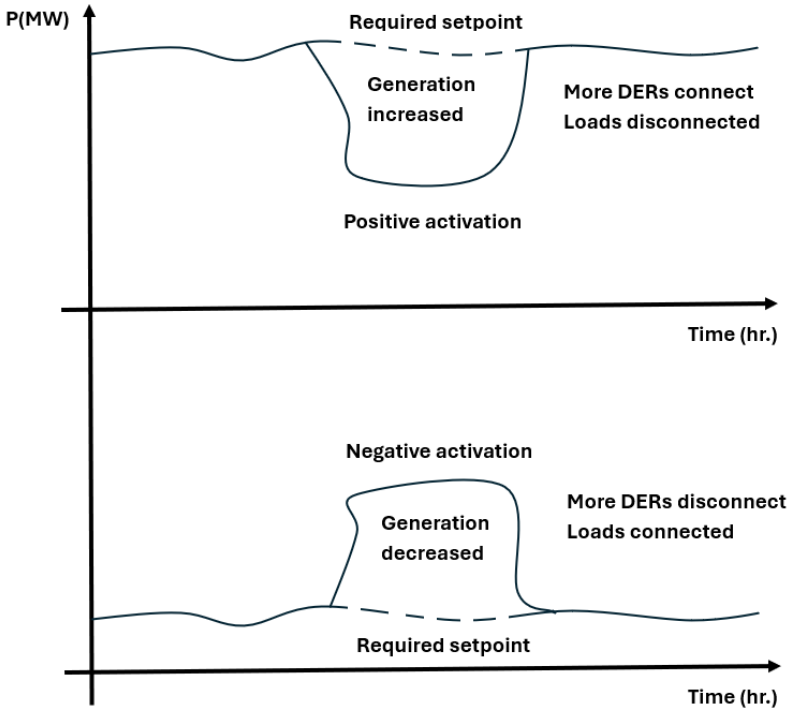

Figure 5.3: Balancing Service Scheme

MQTT, which introduce significant cybersecurity risks. Successful attacks can lead to misinformed decision-making, loss of efficiency, and compromised reliability in market and system operations.

Figure 5.3 illustrates the function carried out by the VPP in case of a power dip or surplus. In both cases, the TSO/DSO gives an activation signal that determines the power setpoint. In case of a dip, generation is increased by connecting more DERs while loads are reduced, and vice versa in case of a surplus. In the case of a cyberattack, the attacker can alter the DER inverter's measurements to deceive the central controller, such as a SCADA system. This can be achieved through a MiTM attack or packet injection, resulting in the controller making incorrect decisions and sending erroneous commands.

5.4.1 Vulnerability Classification Framework

According to the NIST Cybersecurity Framework's "Identify" function (NIST ID.AM-1: Asset Management), understanding asset vulnerabilities requires systematic mapping of technical requirements to potential threat vectors. For VPPs, this mapping reveals three fundamental vulnerability categories that align with NIST risk assessment guidelines:

1. **Time-Critical Operation Vulnerabilities (NIST ID.RA-1):** Tight timing constraints create attack windows
2. **Distributed Architecture Vulnerabilities (NIST ID.AM-3):** Multiple stakeholders expand attack surfaces
3. **Market Integration Vulnerabilities (NIST ID.BE-3):** Financial incentives create additional attack motivations

From a technical point of view, we identify a specific set of vulnerabilities focused on the operation and architecture of VPPs:

5.4.1.1 Timing Vulnerabilities

As mentioned in Section 5.3.5, stringent timing requirements create a sequence of exploitable vulnerabilities where attackers can exploit the tension between security validation time and operational deadlines. The resulting impacts of these timing delays can be broadly classified as:

1. **Level 1 (Service Degradation):** Localized voltage fluctuations and minor frequency deviations that remain within acceptable grid operating parameters but reduce VPP service quality.
2. **Level 2 (Service Interruption):** Regional frequency deviations that trigger protective relay operations and may result in load shedding or generator disconnection.
3. **Level 3 (Cascading Failure):** System-wide emergency response activation leading to widespread instability and potential blackout conditions.

The fundamental challenge lies in the trade-off between comprehensive security validation and rapid response capabilities. Traditional cybersecurity measures such as multi-factor authentication, cryptographic signature verification, and anomaly detection analysis require processing time that may exceed acceptable response thresholds for time-critical services. Attackers can exploit this tension through several mechanisms:

Latency injection attacks introduce deliberate delays in communication channels that push VPP response times beyond acceptable thresholds. For FCR services requiring 1-2 second cycle times, even modest delays of 3-5 seconds can render the VPP unable to fulfill its contractual obligations. These attacks may target network infrastructure

through flooding techniques, manipulate routing protocols to extend packet transit times, or compromise intermediate systems to introduce processing delays.

Timing manipulation attacks exploit the distributed nature of VPP time synchronization mechanisms. By compromising Network Time Protocol (NTP) servers or manipulating timing signals, adversaries can create temporal inconsistencies across VPP components. These inconsistencies can cause control commands to arrive out of sequence, measurements to be correlated incorrectly, or market bids to be submitted outside valid time windows.

Validation bypass attacks leverage the pressure to meet timing deadlines by exploiting reduced security checks during time-critical operations. When VPP operators configure systems to prioritize operational responsiveness over comprehensive security validation, attackers can inject malicious commands that bypass normal authentication and authorization procedures.

5.4.1.2 Communication Architecture Vulnerabilities

The distributed nature of VPPs creates specific challenges for the technical and organizational measures required under NIS2 Directive Article 21:

Supply Chain Complexity: Multiple DER manufacturers with varying security maturity levels create heterogeneous security postures. Solar inverters, wind turbine controllers, battery management systems, and electric vehicle charging stations each implement different communication protocols, authentication mechanisms, and software update procedures. This heterogeneity creates opportunities for adversaries to identify and exploit the weakest security implementations within the VPP portfolio.

Cross-Border Operations: VPPs may span multiple regulatory jurisdictions with varying cybersecurity requirements, incident reporting obligations, and data sovereignty rules. For instance, NIS2 implementation varies across EU member states, while non-EU countries may have different critical infrastructure protection requirements. This regulatory fragmentation requires VPPs to adopt the most stringent applicable controls and maintain compliance documentation for multiple frameworks simultaneously.

Third-Party Dependencies: Reliance on aggregators and cloud service providers introduces trust boundaries across organizational domains. When VPP operators delegate DER aggregation, forecasting, or optimization functions to external service providers, they create pathways that adversaries can exploit. Compromised aggregator credentials

can provide attackers with access to multiple DERs simultaneously, amplifying attack impact.

The multi-stakeholder nature of VPP operations also creates challenges for incident detection and response. Security events may manifest across organizational boundaries, requiring coordinated analysis of logs and alerts from multiple independent entities. Attack attribution becomes complex when malicious activity involves compromised credentials from legitimate stakeholders, making it difficult to distinguish between authorized actions and adversarial behavior.

5.4.1.3 Inherited Smart Grid Vulnerabilities

VPPs inherit baseline smart grid vulnerabilities but with amplified consequences due to their critical grid support functions:

AMI Security: Thousands of smart meters in VPP networks become attack vectors for ancillary services. Smart meter compromise enables adversaries to falsify consumption data, inject fraudulent measurements, or disrupt communications between DERs and VPP control centers.

SCADA Vulnerabilities: VPP EMS systems control grid-critical functions requiring higher security standards than typical SCADA deployments. Legacy SCADA systems may lack authentication, use cleartext protocols, or depend on security-through-obscurity assumptions that prove inadequate against determined adversaries.

Communication Protocol Weaknesses: Protocol attacks affect real-time grid stability rather than just data collection. Vulnerabilities in IEC 61850, DNP3, Modbus, and other industrial protocols enable adversaries to intercept commands, inject false data, or disrupt communications during critical operational periods.

5.4.2 Protocol-Specific Vulnerabilities

The communication protocols used by VPPs represent critical attack surfaces, as they enable the real-time coordination necessary for ancillary service provision. Each protocol implements different security mechanisms, creating a heterogeneous threat landscape that requires protocol-specific protection measures.

Table 5.5 provides representative examples of protocol vulnerabilities and is not exhaustive. Additional attack vectors such as MitM, DoS, and data manipulation apply to IEC 61850 and other protocols, depending on the implementation context.

Table 5.5: Protocol Risks and Requirements

Protocol	**Primary Use**	**MITRE Attack Techniques**	**Required NIST Controls**
IEC 61850	Smart grid operations	T1040 (Network Sniffing)	SC-8 (Transmission Confidentiality)
IEC 60870-5-104	SCADA communications	T1557 (Adversary-in-the-Middle)	SC-23 (Session Authenticity)
DNP3	Utility communications	T1498 (Network DoS)	SC-5 (Denial of Service Protection)
Modbus	Industrial control	T1565 (Data Manipulation)	SI-7 (Software Integrity)
MQTT	IoT communications	T1078 (Valid Accounts)	IA-2 (User Identification)

IEC 61850 serves as the preferred smart grid standard but faces significant cybersecurity challenges. Network sniffing attacks (MITRE T1040) exploit the lack of mandatory encryption, as GOOSE messages transmitting critical control functions are sent in plaintext multicast format. Adversaries can capture these to map VPP topology and prepare subsequent attacks. The required NIST control SC-8 (Transmission Confidentiality) mandates cryptographic protection. IEC 62351-6:2020 recommends HMAC or AES-GMAC over digital signatures for GOOSE protocol to maintain sub-millisecond timing constraints while providing authentication and integrity protection.

IEC 60870-5-104 is a widely deployed SCADA protocol in European transmission networks. Adversary-in-the-middle attacks (MITRE T1557) exploit its lack of built-in authentication, allowing attackers to intercept, modify, or inject control commands. The required NIST control SC-23 (Session Authenticity) prevents session hijacking through mutual TLS authentication, application-layer tokens, or IPsec tunneling.

DNP3 serves North American utility communications with a master-station/outstation architecture. Network denial of service attacks (MITRE T1498) target its polling-based model by flooding outstations with excessive requests, exhausting resources and preventing legitimate commands. NIST control SC-5 (Denial of Service Protection) requires rate limiting, priority queuing, and out-of-band management channels. DNP3 Secure Authentication provides cryptographic protection despite computational overhead concerns.

Modbus, adapted from serial to TCP/IP networking, lacks authentication and integrity protection. Data manipulation attacks (MITRE T1565) allow attackers to inject fraudulent sensor readings or modify commands without detection. NIST control SI-7 (Software,

Firmware, and Information Integrity) requires integrity verification through cryptographic message authentication codes, typically implemented via application-layer gateways for legacy device compatibility.

MQTT has gained adoption for IoT and residential DER integration but faces security challenges. Valid accounts attacks (MITRE T1078) exploit weak authentication in broker deployments relying on simple username/password credentials. NIST control IA-2 (User Identification and Authentication) mandates multi-factor authentication, preferably certificate-based, with topic-based access controls following least-privilege principles.

5.4.3 Service-Specific Attack Vectors

Beyond protocol-layer vulnerabilities affecting all VPP communications, each category of ancillary service presents unique attack vectors related to its specific technical requirements and operational characteristics. This section systematically analyzes these service-specific threats, mapping them to MITRE ATT&CK techniques and demonstrating how operational necessities create exploitable vulnerabilities.

5.4.3.1 Frequency Balance Service Attacks

Frequency balance services directly contribute to power system stability by maintaining grid frequency within acceptable operating bounds. The ability of VPPs to provide Frequency Containment Reserves (FCR), Automatic Frequency Restoration Reserves (aFRR), and Manual Frequency Restoration Reserves (mFRR) makes them critical infrastructure components whose compromise can have immediate grid-wide consequences.

DER-Specific Vulnerabilities:

Compromised Fast-Response Systems (MITRE T1203 - Exploitation for Client Execution): Battery Energy Storage Systems (BESS) providing primary reserves represent high-value targets due to their rapid response capabilities (1-10 seconds) and ability to provide both positive and negative power adjustments. Coordinated malware deployment across 500+ residential battery systems during peak demand periods could remove significant capacity from frequency regulation markets, forcing reliance on slower-responding conventional generation. The attack vector typically involves exploiting vulnerabilities in battery management system firmware or inverter control software. Attackers might leverage unpatched security flaws, default

credentials, or supply chain compromises to deploy malware that lies dormant until triggered by specific grid conditions.

Aggregated Electric Vehicle (EV) Attacks (MITRE T1021.002 - Remote Services: SMB/Windows Admin Shares): Electric vehicle aggregation networks represent an emerging attack surface as Vehicle-to-Grid (V2G) technology enables EVs to provide frequency regulation services. Fleet management system compromise triggering simultaneous charging of 1,000+ vehicles during periods when the grid requires power injection effectively converts frequency regulation capacity into frequency disruption. The attack leverages legitimate remote administration capabilities, making detection challenging when adversaries use compromised credentials.

Industrial Load Manipulation (MITRE T1562.001 - Disable or Modify Tools): Steel mills, paper mills, cement mills, and refineries with medium ramp-up times (2-5 minutes) participate in frequency regulation through load curtailment and restoration. Malware targeting industrial control systems can extend ramp-up times from 2-5 minutes to 15+ minutes during grid frequency events, eliminating the load's contribution to frequency restoration. The attack typically targets Programmable Logic Controllers (PLCs) or Distributed Control Systems (DCS) that manage industrial processes.

Time-Critical FRR Service Vulnerabilities:

Latency Exploitation (MITRE T1499.002 - Service Exhaustion Flood): Network flooding attacks that introduce 5-8 second delays can exceed FCR cycle times (1-2 seconds) and aFRR cycle times (1-5 seconds), rendering VPPs unable to fulfill frequency regulation commitments. The attacks exploit the real-time nature of frequency control, where delayed responses fail to counteract frequency deviations during their most critical initial seconds.

Set-Point Manipulation (MITRE T1565.002 - Transmitted Data Manipulation): Man-in-the-middle attacks reversing frequency restoration commands (+50MW $\rightarrow$ -50MW) represent critical threats to grid stability. When a TSO requests power injection to address declining frequency, manipulated commands that cause power absorption instead exacerbate the frequency deviation, potentially triggering cascading protective disconnections.

Measurement Corruption (MITRE T1565.001 - Stored Data Manipulation): Falsifying frequency measurements to trigger inappropriate responses creates particularly insidious attack vectors. False frequency injection showing 49.8Hz readings during normal 50Hz operations could cause VPPs to inject unnecessary power, potentially driving frequency above acceptable bounds and triggering over-frequency protective actions.

5.4.3.2 Voltage Compensation Service Attacks

Voltage compensation ensures that voltage levels remain within acceptable ranges to protect equipment and maintain power quality. VPPs provide voltage support through reactive power injection/absorption and real power adjustments coordinated across distributed resources.

Power Factor Correction Vulnerabilities:

Phase Relationship Attacks (MITRE T1565.003 - Runtime Data Manipulation): Manipulation of measurements showing phase relationships between active and reactive power enables attackers to trigger unnecessary or harmful power factor correction actions. Smart inverter network infiltration falsifying reactive power measurements across 200+ installations could cause coordinated capacitor bank operations that worsen rather than improve voltage conditions.

Load Addition Exploits (MITRE T1078.004 - Cloud Accounts): Compromised cloud-based control systems can trigger unnecessary capacitor bank operations or reactive power adjustments that degrade voltage stability. Cloud platforms hosting VPP optimization algorithms represent high-value targets, as their compromise affects all DERs managed through the platform.

Stealthy Control Manipulation (MITRE T1557.002 - ARP Cache Poisoning): Address Resolution Protocol (ARP) poisoning attacks position adversaries to gradually degrade voltage stability through cumulative control alterations. Rather than causing immediate, obvious failures, these attacks introduce small perturbations that accumulate over time, slowly degrading power quality while remaining below alarm thresholds.

Loss Energy Management Risks:

Forecast Manipulation (MITRE T1565.001 - Stored Data Manipulation): Compromising loss forecasting systems causes under/over-purchasing of compensatory energy, creating both economic and stability consequences. When VPP forecasting algorithms systematically underestimate distribution losses, insufficient energy procurement leads to voltage sags during high-load periods.

Market Data Corruption (MITRE T1213 - Data from Information Repositories): Altering energy market data influences TSO/DSO purchasing decisions, potentially causing inadequate energy procurement that leads to voltage instability. Attackers who compromise market information repositories can manipulate price signals, availability data, or transmission constraints that inform procurement optimization algorithms.

Measurement Tampering (MITRE T1565.002 - Transmitted Data Manipulation): Smart meter data falsification underreporting distribution losses causes inadequate energy procurement, potentially leading to voltage instability during high-load periods. The attack exploits the reliance on Advanced Metering Infrastructure (AMI) for real-time loss calculation and energy accounting.

5.4.3.3 Supply Reconstruction Service Attacks

Supply reconstruction services ensure rapid restoration of power supply following outages or emergencies. Black start capability—initiating power system restoration without external power sources—represents critical infrastructure functionality whose compromise during emergency conditions could significantly extend outage durations.

Black Start Capability Vulnerabilities:

Startup Sequence Corruption (MITRE T1106 - Native API): Manipulation of startup protocols in hydroelectric plants, compressed air storage, or gas power plants can cause turbine synchronization failures during blackout recovery. Hydroelectric plant protocol manipulation causing turbine synchronization failures during blackouts represents critical vulnerability scenarios where attack timing amplifies impact significantly.

Energy Storage Compromise (MITRE T1485 - Data Destruction): Battery management system data corruption showing false state-of-charge readings can prevent large-scale energy storage systems from providing black start capability. Attacks

targeting the Battery Management Systems (BMS) that monitor cell voltages, temperatures, and charge states to ensure safe, effective operation eliminate storage contribution to restoration.

Critical Communication Disruption (MITRE T1498 - Network Denial of Service): DDoS attacks on restoration communication networks during peak vulnerability periods prevent coordinated black start execution across multiple generation sources. Successful restoration requires precise communication between system operators, generating stations, and transmission operators to manage energization sequences, frequency control, and load restoration.

False Start Signals (MITRE T1090 - Proxy): Proxy attacks triggering premature restart attempts cause equipment damage and delay actual restoration. The attacks exploit the distributed nature of restoration coordination, where multiple stakeholders receive and act upon startup commands without complete system visibility.

5.4.3.4 Operational Management Service Attacks

Operational management involves grid operators controlling and monitoring the grid while coordinating ancillary services. This category encompasses redispatch operations, feed-in management, and real-time congestion management functions.

Redispatch Vulnerabilities:

Load Flow Calculation Attacks (MITRE T1565.001 - Stored Data Manipulation): Falsified data injections manipulate TSO calculations, leading to unnecessary or harmful redispatch actions. Data injection manipulating TSO calculations demonstrates how compromising analytical inputs causes systemic operational impacts.

Control Signal Manipulation (MITRE T1557.001 - LLMNR/NBT-NS Poisoning): Man-in-the-middle attacks tampering with redispatch instructions between TSOs and power plants can cause harmful rather than beneficial grid adjustments. Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) poisoning enables attackers to intercept and modify commands.

Timing Attacks (MITRE T1499.004 - Application or System Exploitation): Deliberate command delays prevent timely congestion management adjustments, potentially

allowing thermal overloads or voltage violations to develop. Application exploitation techniques target computation-intensive operations to introduce processing delays.

Feed-in Management Risks:

Unauthorized Disconnection (MITRE T1529 - System Shutdown/Reboot): Forced renewable system shutdowns during normal operations create artificial instability. System shutdown attacks typically exploit remote control capabilities implemented for legitimate operational purposes.

Sensor Manipulation (MITRE T1598.003 - Spearphishing via Service): Spearphishing attacks on monitoring systems trigger unnecessary feed-in management actions. The attacks target personnel responsible for monitoring renewable generation, compromising their credentials to access control systems.

Denial of Service (MITRE T1498.002 - Reflection Amplification): Reflection amplification attacks blocking curtailment communications during oversupply periods prevent necessary generation reductions, potentially causing over-voltage conditions.

5.4.4 Advanced Persistent Threat Scenarios

Beyond individual attack vectors, sophisticated adversaries may orchestrate Advanced Persistent Threat (APT) campaigns combining multiple techniques across extended time periods. APT scenarios targeting VPP infrastructure pursue strategic objectives related to grid destabilization, intelligence collection, or preparation for future attacks during geopolitical conflicts.

Multi-Stage Attack Campaigns typically unfold across several distinct phases: Initial Access establishes footholds through spearphishing or supply chain compromise; Reconnaissance and Mapping involves extensive data collection to understand VPP topology and procedures; Capability Development sees attackers creating custom tools tailored to identified systems; Pre-Positioning deploys capabilities while maintaining dormancy; and Execution triggers pre-positioned capabilities to achieve strategic objectives.

Strategic Attack Objectives vary by adversary: Grid Destabilization aims to cause widespread outages through coordinated attacks on frequency regulation or voltage control; Intelligence Collection focuses on gathering information about grid operations and

vulnerabilities; Persistent Access establishes long-term footholds enabling rapid attack execution during geopolitical tensions.

Table A.1 in the Appendix provides a structural mapping of identified attack vectors to MITRE ATT&CK techniques, organized by severity level to prioritize threat response efforts.

5.5 Mitigation Strategies and Defensive Frameworks

Building on the threat analysis in Section 5.4, this section presents comprehensive mitigation strategies addressing VPP vulnerabilities through a multi-layered approach aligned with NIST Cybersecurity Framework and MITRE D3FEND countermeasures.

A robust foundation requires meticulous asset and risk governance. Asset Management maintains comprehensive inventories of all VPP components per NIST SP 800-53 CM-8, leveraging automated discovery tools for dynamic DER registration/deregistration. Risk assessment processes must account for both technical vulnerabilities and operational constraints, recognizing that traditional frameworks may underestimate threats to time-critical services or overestimate control feasibility in operational environments.

5.5.1 Addressing Time-Critical Service Vulnerabilities

Pre-authenticated command validation implements NIST SC-8 (Transmission Confidentiality) with modified validation procedures, validating and digitally signing control commands during non-critical periods and storing them in secure command pools for rapid deployment. Commands are validated at pool submission rather than execution time. Digital signatures use elliptic curve cryptography providing equivalent security to RSA with significantly reduced computational overhead.

Commands include validity windows specifying acceptable execution timeframes, preventing replay attacks while maintaining operational flexibility. Secure hardware modules protect signing keys, preventing compromise even if command validation servers are breached. NIST controls IA-2 (User Identification and Authentication) and AC-2 (Account Management) are adapted through: certificate validation during command submission rather than execution, cached revocation status for frequently used certificates, fallback procedures when pre-authenticated pools are exhausted, and audit logging of all command executions for forensic analysis.

Real-time latency monitoring implements NIST SI-4 (System Monitoring) controls with VPP-specific timing metrics, integrating MITRE D3FEND D3-NTA (Network Traffic Analysis) techniques optimized for energy protocols to detect subtle timing manipulation while maintaining sub-second response requirements. Network probes at critical pathways measure end-to-end latency, statistical analysis identifies deviations from baseline timing patterns, and automated alerts trigger when latency exceeds service-specific thresholds with SIEM integration for event correlation.

The system distinguishes benign network congestion from adversarial timing attacks through pattern analysis—legitimate congestion affects all traffic classes proportionally, while targeted attacks selectively delay specific message types or source addresses. Graduated response procedures initially increase monitoring granularity and activate redundant communication paths, then bypass non-critical security checks for high-priority messages while maintaining logging, and finally trigger emergency operating procedures with reduced automation and increased human oversight.

5.5.2 Securing Distributed Multi-Stakeholder Architecture

The distributed nature of VPPs requires tiered trust management recognizing different stakeholder security requirements based on capabilities, risk profiles, and operational roles.

Tiered Trust Framework:

Consumer DERs (Level 1 - NIST IA-2): Device certificates for authentication, TLS 1.3 encrypted communications, automatic security updates with user notification, limited control capabilities restricted to local device functions, and monitoring for anomalous behavior patterns.

Commercial DERs (Level 2 - NIST AC-2): Certificate-based authentication with annual renewal, network segmentation separating DER control from business networks, enhanced 24/7 alert response monitoring, documented security procedures and incident response plans, and annual third-party security assessments.

Critical Infrastructure DERs (Level 3 - NIST SP 800-53 high baseline): Hardware security modules protecting cryptographic keys, defense-in-depth architectures with multiple security layers, continuous monitoring with real-time threat detection, quarterly penetration testing and vulnerability assessments, and dedicated security personnel with formal security governance.

Protocol-Specific Protection:

IEC 61850: Per IEC 62351-6:2020, HMAC or AES-GMAC (recommended over digital signatures for performance) provide message authentication countering T1040 (Network Sniffing) attacks. Implementation: message authentication codes computed using shared symmetric keys, sequence numbers preventing replay attacks, timestamp validation ensuring message freshness within sub-millisecond timing constraints, secure key distribution mechanisms, and regular key rotation procedures.

IEC 60870-5-104: NIST SC-23 (Session Authenticity) protects against T1557 (Adversary-in-the-Middle) through mutual TLS authentication with certificate-based endpoint authentication, strong cipher suites (AES-256 or equivalent), perfect forward secrecy protecting historical communications, certificate revocation checking, and secure session resumption mechanisms.

DNP3: NIST SC-5 (Denial of Service Protection) defends against T1498 (Network DoS) through per-source rate limiting preventing flooding attacks, QoS mechanisms prioritizing critical messages, redundant communication channels with automatic failover, out-of-band management for emergency access, and DNP3 Secure Authentication for message integrity despite computational overhead in resource-constrained environments.

Modbus: NIST SI-7 (Software, Firmware, and Information Integrity) addresses T1565 (Data Manipulation) through application-layer gateways adding authentication to legacy protocols without device modifications, message authentication codes validated before processing, anomaly detection identifying unusual command patterns, transaction logging for forensic analysis, and gradual migration toward inherently secure protocols.

MQTT: NIST IA-2 (Multi-factor Authentication) secures against T1078 (Valid Accounts) through X.509 certificate-based device authentication (beyond simple username/-password), separate authentication for publish and subscribe operations, topic-based access control lists following least-privilege principles, TLS-encrypted communications, and broker hardening with security patching.

Supply chain security addresses vulnerabilities through vendor security requirements in procurement contracts, supply chain risk assessments for critical components, secure boot and firmware verification procedures, code signing for software updates, and third-party security testing of critical equipment.

5.5.3 Protecting Market Integration Operations

Market activity monitoring implements NIST SI-7 (Software and Information Integrity) through cross-validation of capacity bids against actual DER availability and historical

pattern analysis detecting unusual bidding behavior indicative of manipulation attacks. Market interfaces implement application-layer firewalls validating market message formats, separate network segments isolating market communications, transaction signing preventing bid repudiation, automated reconciliation detecting discrepancies, and comprehensive audit logging. Automated bid validation prevents capacity overcommitment through real-time capacity aggregation from DER portfolio, comparison of submitted bids against available capacity, historical pattern analysis identifying anomalous bids, manual override procedures with enhanced authorization, and automated bid rejection for impossible commitments.

Cross-domain attack prevention implements NIST SC-7 (Boundary Protection) with MITRE D3FEND D3-NI (Network Isolation) techniques isolating financial and operational networks: physically separate networks for market and operational functions, data diodes enforcing unidirectional information flow where appropriate, cross-domain guards mediating necessary bidirectional communications, separate credential stores preventing credential reuse across domains, and independent monitoring of each security domain.

5.5.4 Advanced Persistent Threat Protection

Sophisticated APT campaigns require comprehensive detection capabilities identifying multi-stage attacks. Machine learning models trained on VPP operational patterns detect subtle APT indicators through baseline establishment for normal operational patterns, unsupervised learning detecting previously unknown attack patterns, supervised learning identifying known APT techniques, graph-based analysis revealing lateral movement, and integration with threat intelligence feeds.

VPP-mimicking honeypots provide early reconnaissance warnings through realistic VPP environments attracting adversary attention, instrumentation detecting and recording attack techniques, deception credentials planted in production environments, automated alerting when honeypots are accessed, and threat intelligence sharing with sector partners. Graph-based lateral movement detection identifies propagation attempts through network topology mapping identifying sensitive pathways, authentication logging tracking credential usage patterns, anomaly detection identifying unusual lateral movements, automated response limiting adversary progression, and integration with endpoint detection and response systems.

5.5.5 Continuous Security Monitoring and Improvement

Security operations centers implement 24/7 monitoring with expertise in both cybersecurity and energy system operations, addressing detection challenges where operational noise and multi-stakeholder complexity can mask malicious activity. Components include real-time SIEM platforms with VPP-specific analytics rules, ICS-CERT threat feeds for energy sector intelligence, automated correlation engines distinguishing operational anomalies from security incidents, playbooks for common incident scenarios, and coordination procedures with grid operators and law enforcement. Endpoint detection and response across VPP control workstations provides continuous endpoint monitoring, behavioral analysis detecting malicious activities, automated response capabilities, forensic data collection, and SOC integration.

Network traffic analysis monitors diverse communication protocols through deep packet inspection for industrial protocols, protocol anomaly detection, baseline establishment for normal traffic patterns, automated alerting for suspicious activities, and integration with network access control. Continuous improvement requires regular penetration testing simulating realistic adversary capabilities, tabletop exercises practicing incident response procedures, lessons learned analysis following incidents or exercises, metrics-based assessment of security program effectiveness, and stakeholder feedback informing security improvements.

5.5.6 Regulatory Compliance and Governance

Under NIS2 Directive Article 21, VPPs must implement technical and organizational measures proportional to their critical grid support functions. Compliance framework includes comprehensive risk assessments covering all vulnerability categories with board-level oversight, incident detection and reporting procedures with coordination with national cybersecurity authorities and notification of significant incidents within regulatory timeframes, supply chain risk management with vendor security requirements and third-party assessments, and security governance with defined roles and responsibilities, security policies and procedures, training and awareness programs, and regular management reviews.

5.6 Chapter Summary

This chapter presented a comprehensive VPP cybersecurity analysis, progressing from architectural foundations through threat identification to mitigation implementation. VPPs aggregate diverse DERs through complex communication infrastructures spanning multiple protocols (IEC 61850, IEC 60870-5-104, DNP3, Modbus, MQTT) while bridging IT and OT domains. Critical timing constraints—FCR requiring 1-2 second and aFRR requiring 1-5 second cycle times—create fundamental tensions between security validation and operational responsiveness.

Through integrated NIST-MITRE framework application, three fundamental vulnerability categories emerged: time-critical operation vulnerabilities from stringent timing constraints, distributed architecture vulnerabilities from multi-stakeholder complexity and supply chain dependencies, and market integration vulnerabilities introducing financial attack motivations beyond operational disruption.

The mitigation framework employs layered defenses balancing performance with threat protection. Key strategies include pre-authenticated command validation maintaining cryptographic integrity while meeting operational deadlines, real-time latency monitoring for timing-based attack detection, and tiered trust management accommodating diverse stakeholder security maturity. Protocol-specific protections (message authentication for IEC 61850, mutual TLS for IEC 60870-5-104, rate limiting for DNP3, application-layer gateways for Modbus, certificate-based authentication for MQTT) coordinate through centralized security gateways. Market interface security implements bid validation, cross-domain isolation, and transaction monitoring. Advanced threat defense employs behavioral analysis, VPP-mimicking honeypots, and lateral movement detection, supported by integrated security operations centers with dual expertise in cybersecurity and energy systems.

Three critical insights emerged: timing constraints necessitate innovative approaches like pre-authenticated command validation; distributed architecture requires tiered trust management for expanded attack surfaces; and market integration demands strategies addressing both operational disruption and economic manipulation. The integrated NIST-MITRE framework enables systematic vulnerability identification, stakeholder communication, regulatory compliance (particularly NIS2), and continuous security improvement. Future research should examine blockchain, artificial intelligence, and quantum-resistant cryptography for enhanced VPP security.

The vulnerability landscape identified in VPP ancillary services necessitates automated response mechanisms beyond detection alone. Chapter 6 addresses this need through integration of cyberdefense capabilities within electrical protection systems.

5.6.1 Implementation Cost Considerations

While this chapter emphasizes technical VPP security mechanisms, practical deployment requires understanding implementation costs and economic feasibility. VPP cybersecurity investments span three primary categories: communication security infrastructure including secure channels, industrial firewalls, and network segmentation; monitoring and detection systems such as SOC integration, intrusion detection, and SIEM platforms; and protection system enhancements including cyber-aware devices and specialized protection engineering. These investments secure the multi-protocol communication stack discussed in Section 5.2 and implement the continuous monitoring described in Section 5.5.5.

Beyond initial infrastructure, ongoing operational costs include personnel for OT cybersecurity expertise and operator training, maintenance for software licenses, and security patches, and third-party penetration testing. Personnel requirements represent the largest recurring expense, reflecting the specialized knowledge needed to secure industrial control systems in energy environments.

VPP cybersecurity costs must be justified against protected revenue and avoided risks. The ancillary services in Section 5.4 generate substantial revenue vulnerable to cyber disruption, including FCR and aFRR capacity payments proportional to VPP capacity. Avoided costs include lost revenue during service interruptions, market penalties for failed delivery commitments, equipment replacement expenses from cyber-physical attacks, and reputation damage affecting customer retention. Regulatory compliance under the NIS2 Directive (Section 5.5.6) makes security mandatory for critical entities, transforming the economic calculation from discretionary investment to regulatory requirement.

Security costs scale differently than VPP capacity, creating distinct economic profiles. Large VPPs exceeding 50 MW distribute fixed infrastructure costs across substantial revenue bases, creating favorable cost-benefit ratios where initial investment represents manageable percentages of revenue declining over time. Medium VPPs between 20 and 50 MW face proportionally higher costs requiring optimization strategies. Small VPPs in the 5 to 20 MW range experience challenging economics where fixed costs may equal or exceed first-year ancillary revenue, necessitating shared services models or aggregator-provided infrastructure.

Cost optimization strategies include shared services where multiple VPPs pool SOC and incident response capabilities, reducing per-installation costs substantially; phased deployment protecting critical assets first before expanding coverage; and strategic technology choices leveraging open-source tools, cloud-based services, and standardized equipment procurement. These approaches enable smaller installations to achieve economic viability while maintaining security effectiveness.

Practical implications emerge from this analysis. Larger VPPs demonstrate strong economics justifying comprehensive security implementation, while smaller VPPs require creative approaches. Security represents operational necessity for NIS2-regulated entities rather than discretionary investment. Timing constraints for FCR and aFRR services discussed in Section 5.4 necessitate specialized high-performance security solutions beyond standard IT approaches.

Cost considerations directly inform the NIST-MITRE framework implementation in Section 5.5. Tiered trust management enables cost-appropriate security levels for different stakeholder categories, protocol-specific protections prioritize investments on highest-risk channels, and pre-authenticated command validation balances security costs against timing requirements.

In conclusion, VPP cybersecurity requires substantial multi-year investment but provides clear economic justification through protected revenue streams, avoided disruption costs, and regulatory compliance. The technical security framework enables cost-effective implementation through risk-prioritized, scalable approaches appropriate for diverse VPP sizes and business models.

CHAPTER 6

Integrating Cyberdefense into Distribution System Protections

6.1 Introduction

The integration of distributed energy resources (DERs) into modern power distribution systems has introduced significant cybersecurity challenges that traditional operational frameworks are not equipped to address. Unlike conventional power systems where cyberattacks typically trigger manual intervention by operators who disconnect affected devices and initiate restoration procedures, the rapid dynamics of power systems and the distributed nature of modern DERs necessitate faster, automated response mechanisms. The 2015 cyberattack on Ukraine's power system, which impacted 225,000 customers and required distribution system operators to move to manual operations, exemplifies the limitations of purely manual response approaches [111]. This chapter presents a novel approach that integrates cybersecurity functions directly into electrical protection systems, enabling circuit breakers to trip automatically upon detection of cyberattacks. The primary objective of this approach is to maintain power system continuity under cyberattack conditions by treating electrical protections as tools for incident response rather than solely as safety devices against physical faults.

The increasing prevalence of DERs controlled via cloud platforms using public Internet infrastructure has substantially expanded the attack surface of distribution grids. Technologies such as electric vehicle charging systems, energy communities, and virtual power plants (VPPs) often concentrate control of significant generation capacity under single platforms, creating potential single points of failure. Tuyen et al. [112] present a

The content of this chapter has been published in the following paper:

G. B. Gaggero, A. Mokarim, P. Girdinio, and M. Marchese, "Should We Include Cyberdefense Functionalities in Electrical Power System Protections?: A Proposed Approach," IEEE Ind. Electron. Mag., vol. 19, no. 1, pp. 10-16, Mar. 2025, doi: 10.1109/MIE.2024.3416907.

comprehensive review of the system structure and vulnerabilities of typical inverter-based power systems integrated with DERs. If compromised through cyberattacks, these systems could be manipulated to cause severe grid malfunctions, widespread power outages, and damage to critical infrastructure.

This chapter details the proposed approach of incorporating cyberdefense functionalities into electrical protection systems, presents a use case scenario demonstrating its application, and evaluates its performance through simulation studies on a standard IEEE test feeder. The integration of cybersecurity awareness into protection relays represents a paradigm shift in how power systems respond to modern threats, bridging the traditional separation between safety and security functions.

6.2 Background and Context

6.2.1 ANSI Device Numbers and Protection Functions

Electrical protection functions constitute essential components of modern power systems, ensuring safety, reliability, and operational efficiency. The American National Standards Institute (ANSI) has established a standardized system of device numbers that uniquely identify different protection functions. Traditional ANSI device numbers primarily address physical phenomena within power systems, including overcurrent protection (Device 50/51), undervoltage protection (Device 27), and differential protection (Device 87).

Currently, no specific ANSI device number exists for protection against cyberattacks. Protection against cyberthreats in modern power systems is typically implemented through cybersecurity measures and protocols such as firewalls, intrusion detection systems (IDSs), encryption techniques, and secure communication protocols designed to prevent unauthorized access, data manipulation, and other cyberthreats. However, when these cybersecurity devices detect attacks that could potentially compromise safe grid operation, they typically cannot directly influence the physical power system. This creates a fundamental disconnect: safety and security are treated as separate issues addressed by different tools.

Traditional electrical protection functions are designed to address dangerous operating conditions caused by faults and accidents, such as short circuits, but cannot prevent hazardous conditions arising from deliberate malicious actions. Nevertheless, cyberattacks can create dangerous working conditions in power systems that do not trigger conventional protection functions yet require prompt remediation. The proposed approach seeks to bridge this gap by enabling protection systems to respond to cyber-induced threats.

6.2.2 Cyberattack Impact on Distribution Grids

Power distribution systems increasingly rely on public communication networks for monitoring and control purposes. Examples include electric vehicle charging systems, energy communities, and VPPs. In many implementations, a single energy management system (EMS) platform can oversee substantial numbers of generators and controllable loads within the distribution grid. Furthermore, certain technologies, particularly those deployed in energy communities, often concentrate multiple devices under single substations.

If a cyberattack proves successful, attackers could potentially gain malicious control of substantial numbers of devices. The consequences of such attacks are twofold. First, there are potential economic damages resulting from disruption of energy services and infrastructure. More critically, successful cyberattacks have the potential to cause serious power grid malfunctions, leading to widespread outages that impact not only businesses and residential customers but also critical services and essential infrastructure, thereby posing significant risks to public safety and well-being.

Researchers have explored various cyberattack scenarios targeting DERs. Bhattarai et al. [113] present a scenario where the power output of DERs is manipulated to induce sustained oscillations or system instability, though the authors do not deeply evaluate specific locations where DERs can be manipulated to cause higher impact. Tuttle et al. [114] provide similar analysis but focus on assessing the impact of controlling large numbers of storage systems. Linnartz et al. [86] demonstrate how cyberattacks on DERs in the CIGRE medium voltage benchmark grid can violate voltage boundaries. Few studies have conducted simulations considering the features and constraints of single technologies controlling numerous DERs. Nasr et al. [115] explore the impact of cyberattacks on electric vehicle charging infrastructure.

The cybersecurity issues associated with DERs have been broadly investigated in the literature. Qi et al. [116] analyze the challenges introduced by high penetration of DERs in power systems and propose a framework to protect DERs from cyberattacks without compromising grid reliability and stability.

The IEEE 1547 Standard [9] defines the interconnection and interoperability requirements for DERs and provides conformance test procedures and pass/fail criteria. Nevertheless, the document generically refers to "response plans" that grid operators must implement. The proposed solution can act as a technical implementation of such response plans recommended by the standard.

Some research has examined the risk associated with malicious manipulation of circuit breakers. McDermott et al. [117] analyze the risk associated with distance relay protection, providing a taxonomy of communication and proposing mitigation techniques. Jafari et al. [118] assess the feasibility of executing false data injection attacks aimed at generating false relay operations within power systems incorporating high percentages of renewable energy sources. Rajkumar et al. [119] present a cyberattack leveraging the Generic Object-Oriented Substation Event (GOOSE) protocol from the IEC 61850 Standard by introducing falsified GOOSE data frames into bay-level substation communication networks, resulting in unintended activation of multiple protective relays across the power grid, which could lead to widespread blackouts. The report of the IEEE C1 working group of the Power System Relaying Committee [120] analyzes the security of electronic communication paths to protective relays, providing advice for implementing secure-by-design solutions.

Nevertheless, protection relays are often viewed as assets to be defended rather than as potential solutions for incident response. To the best of our knowledge, the approach presented in this chapter represents a novel contribution by positioning electrical protection as an active component of cyber incident response strategies. The topic has been investigated only in industrial articles, such as ABB's work on protection relays playing roles in cyber resilience solutions [121].

6.3 Use Case Scenario

6.3.1 Scenario Description

The use case considers a scenario where multiple electrical generators distributed throughout a distribution grid are controlled by a single energy management platform using the public Internet, as shown in 6.1.

This configuration represents a generic scheme applicable to various technologies for controlling DERs:

Electric Vehicle Charging Systems: Centralized EMS platforms govern electric vehicle charging infrastructure, optimizing power distribution to ensure efficient energy utilization and minimize grid impact. These platforms enable real-time monitoring, demand response, and load balancing, enhancing overall reliability and sustainability of charging networks.

Energy Communities: These decentralized systems enable participants to collectively manage, share, and optimize local energy resources. Advanced technologies and smart

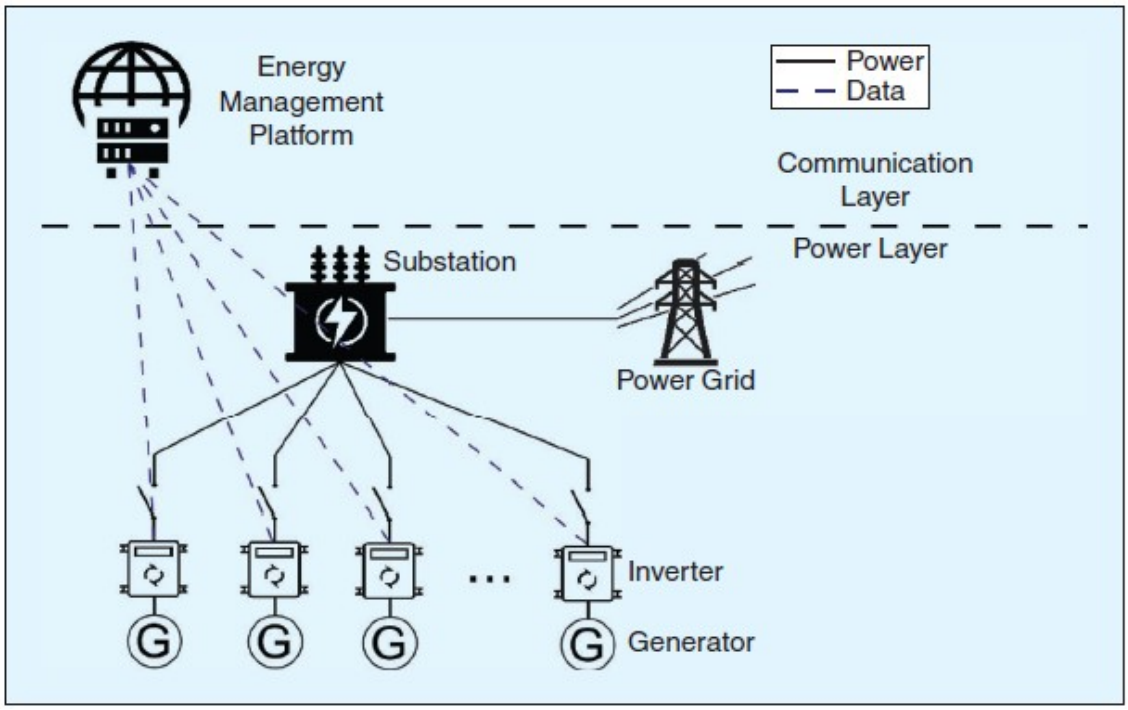

Figure 6.1: A typical network scheme of distributed generation controlled by cloud platforms.

grids empower community members to engage in efficient energy production, consumption, and trading, fostering sustainability and resilience in the broader energy landscape.

Virtual Power Plants: VPPs integrate diverse DERs into unified, optimized networks, enabling aggregated control for enhanced grid stability. Through advanced algorithms and real-time monitoring, VPPs efficiently manage renewable energy sources, storage, and demand response, offering flexible and scalable solutions for modern energy systems.

In all three cases, generators and controllable loads receive power setpoints from Internet servers, either directly (where inverters possess public IP addresses) or through local controllers such as remote terminal units or smart gateways. This architecture means that attackers can attempt to compromise the system through connections to the public Internet.

6.3.2 Attack Methodology and Objectives

The attack objective is to manipulate the power setpoints of electrical generators. This can be achieved by exploiting protocol vulnerabilities in systems utilizing legacy protocols or

by exploiting various vulnerabilities in local controllers, including weak authentication mechanisms, web application security issues, and unused open ports. Due to the potentially high number of local controllers, the simplicity of hardware implementations, and limited computational power, these devices are particularly vulnerable to security issues.

When attackers gain control of large numbers of generators in a distribution grid, severe issues may arise for the main grid. However, these systems often lack the continuous human supervision typical of traditional supervisory control and data acquisition (SCADA) systems. Energy utilities may employ dedicated teams and tools for managing cyberattacks, typically utilizing security operations centers (SOCs) that collect data through security information and event management (SIEM) systems and other sources such as IDSs. Upon detecting attacks, SOCs can activate field technicians directly.

This response model clearly cannot function effectively for geographically distributed generators located on private properties, as is common with the technologies discussed. Therefore, there exists a critical need for automatic response mechanisms whose primary aim is guaranteeing grid continuity over economic interests.

6.4 Proposed Approach

6.4.1 Core Concept

The fundamental concept involves incorporating capabilities for electrical relays to trip upon detection of ongoing cyberattacks, thereby maintaining safe operating conditions. The rationale is that in certain scenarios under cyberattack, disconnecting electrical apparatus from the grid represents the only means of preserving overall system availability and ensuring safety of apparatus and personnel. In this framework, electrical relays and circuit breakers are treated as components of incident response assets in power systems.

6.4.2 Implementation Architecture

The proposed solution implements a lightweight IDS as a hardware component external to the inverter that analyzes traffic directed to smart inverters. Under specified conditions, the IDS can trigger generator circuit breakers directly. This lightweight IDS solution is illustrated in 6.2.

The IDS should implement basic rules appropriate for Internet of Things (IoT) devices. Chaabouni et al. [122] review the techniques used for intrusion detection in the IoT

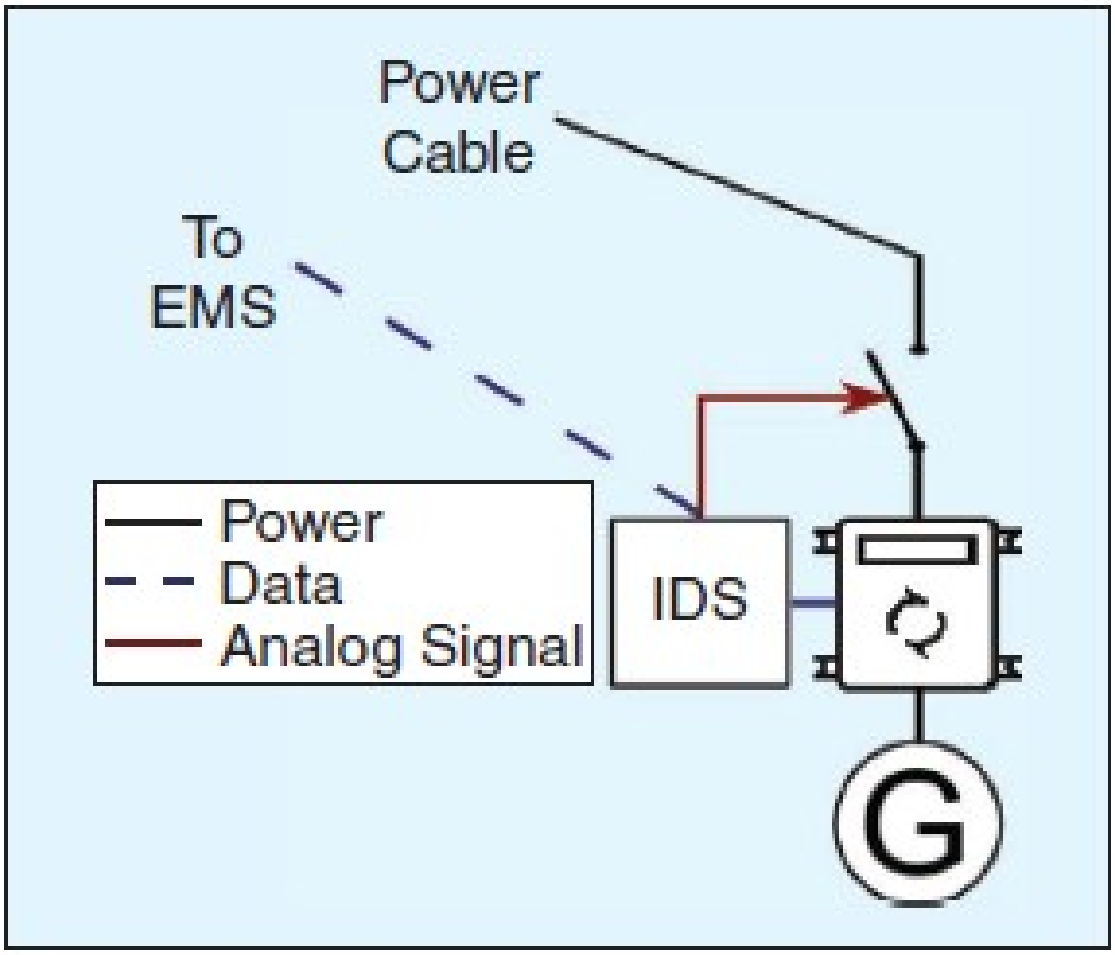

Figure 6.2: The details of the proposed approach.

environment, providing insights into appropriate detection methodologies for resource-constrained devices.

The triggering of circuit breakers is automatically activated upon critical alarms from the IDS. For simple electromechanical circuit breakers common in low-voltage grids, this can be accomplished using appropriate devices enabling triggering from external signals. Where digital relays are present, the IDS can transmit alarms to the relay, which subsequently activates a protection function.

6.4.3 Local Control Philosophy

The proposed approach operates at the local level, meaning attack detection is performed by individual IDSs connected to (or integrated into) smart inverters, with each IDS capable of triggering only its associated circuit breaker. While centralized IDSs located remotely at EMS facilities could potentially enhance detection capabilities, such architectures would simultaneously enlarge the attack surface by making generator circuit breakers remotely controllable. For this reason, the proposal advocates for local control loops that detect attacks locally and trigger nearby circuit breakers.

This distributed approach offers several advantages. First, it minimizes communication dependencies that could themselves become attack vectors. Second, it ensures that protection actions can be taken even if communication with central facilities is compromised. Third, it maintains the principle of defense in depth by creating multiple independent protection layers throughout the distribution system.

6.5 Performance Evaluation

6.5.1 Simulation Setup

To demonstrate the effectiveness of the proposed approach, simulations were conducted using the IEEE European Low-Voltage Test Feeder (ELVTF) [123]. The IEEE ELVTF is a radial distribution network comprising 906 nodes and 55 load buses with a phase-to-phase voltage level of 416 V and a frequency of 50 Hz. The single-line diagram of this system is shown in 6.3

The simulation assumes that attackers may gain control of 400 kW of energy generation through a cyberattack. This power includes photovoltaic systems, battery energy storage systems, and electric vehicles connected with bidirectional converters enabling vehicle-to-grid services. At the moment of attack, devices could be either injecting or absorbing power, depending on EMS schedules. The 400 kW represents 50% of the nominal power of the medium-low-voltage transformer installed at the substation. While this percentage is high, devices are typically installed with high utilization factors since they are not expected to operate simultaneously or in conflicting modes (for example, photovoltaic systems generating while electric vehicles charge).

This hypothesis is reasonable and supported by various studies on cyberattack impacts on electrical distribution systems. The simulation also assumes that attacks are carried

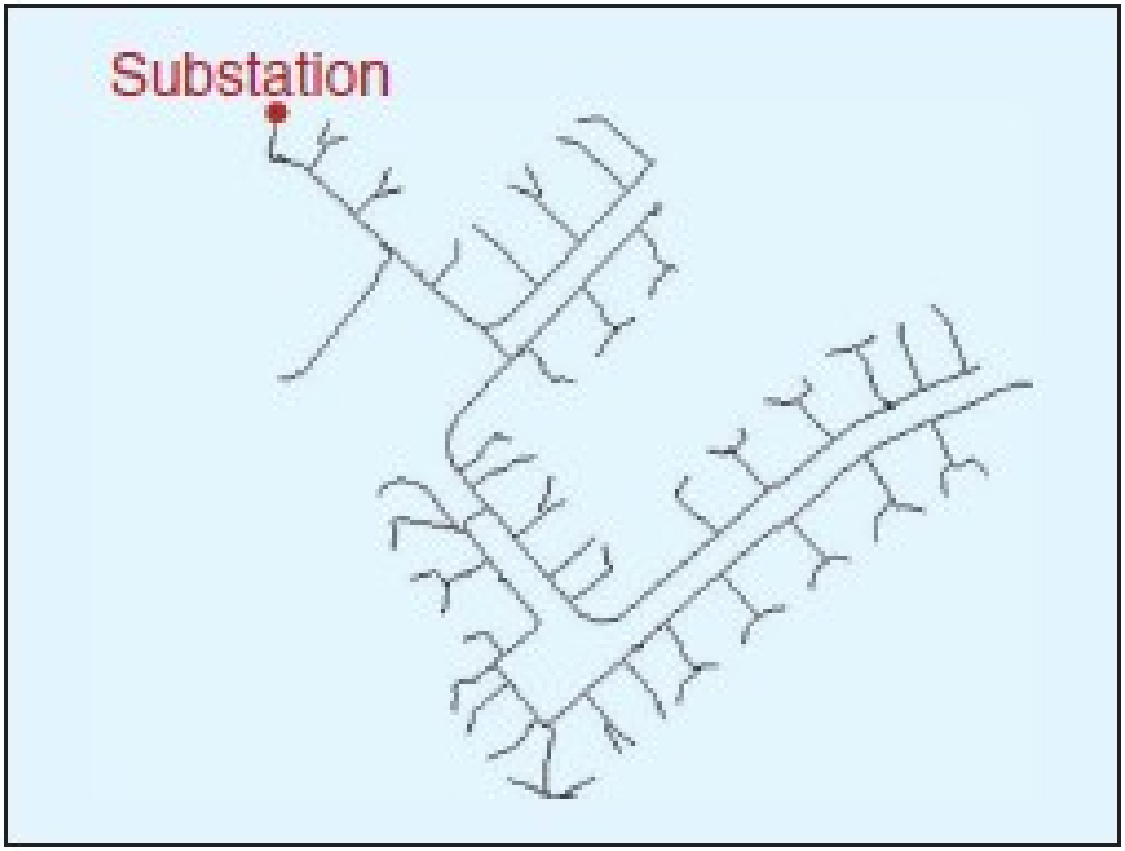

Figure 6.3: The IEEE LV European Feeder electrical scheme.

out against every individual device with the aim of gaining control of generators, such as through brute-force attacks on device passwords. Upon successful compromise, attackers can modify power setpoints of all generators. In this specific scenario, attackers choose to command all generators (storage systems, electric vehicles, etc.) to inject maximum power simultaneously.

6.5.2 Attack Detection Assumptions

The simulations assume that attacks are detected by the IDSs. While detailed IDS implementation will be addressed in future work, it is important to note that generators should trip only upon detection of successful attacks, not during reconnaissance phases or unsuccessful attack attempts. In the low-voltage scenarios under consideration, false positives are acceptable because tripping leads to secure operating conditions for the overall power

system. The priority is maintaining grid stability and preventing damage to infrastructure, even at the cost of temporarily disconnecting some generation resources.

6.5.3 Simulation Results

The simulation results demonstrate the impact of the cyberattack on distribution grid voltage under two conditions: without implementation of the proposed approach, and with the proposed cyberdefense functionality enabled.

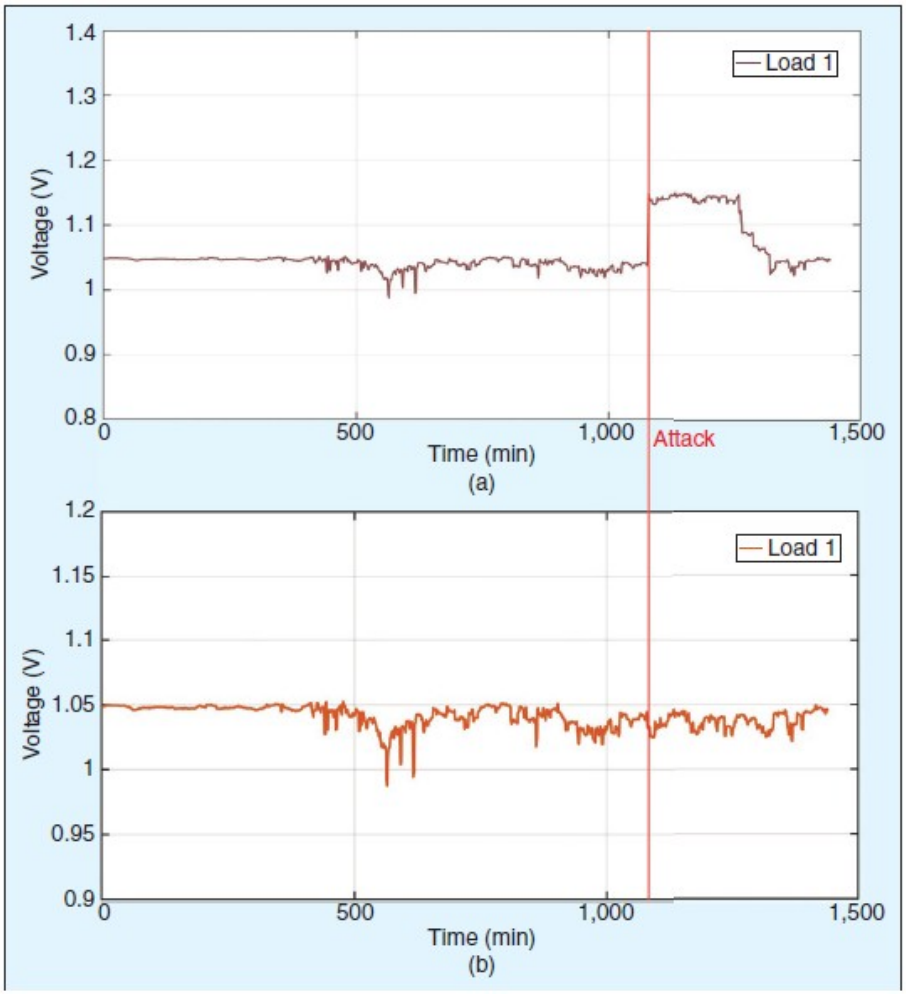

Figure 6.4: The results of the simulation of the attack (a) without and (b) with the implementation of the proposed approach.

Figure 6.4(a) illustrates the voltage at the distribution grid substation (load 1 in the model) when no electrical protections trip in response to the cyberattack. Under attack

conditions, the voltage rises above the +10% limit at the substation, which represents a constraint for most electrical distribution systems. This overvoltage condition may cause disconnection of the entire substation, resulting in severe unavailability and potentially damaging apparatus.

Figure 6.4(b) shows the voltage trend at the substation when the proposed approach has been implemented and generators are disconnected as a result of detecting the cyberattack. When protections trip and generators are disconnected, thereby eliminating generation from the distribution grid, the voltage exhibits small variations but remains within acceptable limits. While this may cause economic damage to users through loss of generation revenue and unavailability of charging services, the system can continue to operate safely.

The simulation results clearly demonstrate that the proposed approach successfully maintains voltage within operational limits during a coordinated cyberattack that would otherwise cause severe overvoltage conditions. This validates the concept of using electrical protection as an incident response tool for cybersecurity threats in distribution systems with high penetrations of DERs.

6.6 Discussion

6.6.1 Broader Implications

While this chapter has focused on one specific scenario as a use case, several important considerations emerge regarding the broader applicability of the approach. The proliferation of electrical generators in distribution grids that are remotely controlled introduces new cybersecurity challenges fundamentally different from those in traditional power systems. One of the most critical characteristics of these systems is the impossibility of maintaining dedicated cybersecurity teams to implement proper incident response for every distributed installation. Therefore, automatic mechanisms capable of maintaining grid continuity even under attack become necessary.

In distribution grids, the absence of distributed generation represents a safe operating condition. Consequently, the proposed approach advocates electrically disconnecting generators under attack, preventing malicious control. The approach prioritizes physical grid stability and safety over economic optimization and short-term revenue generation. This represents a significant philosophical shift in how power systems balance economic and reliability objectives under adversarial conditions.

6.6.2 Limitations and Challenges

Several limitations of the current approach warrant discussion. First, local IDS implementations cannot reliably detect attacks originating from compromised central controllers. When the central EMS platform is compromised, commands to DERs appear legitimate to local protection systems, bypassing detection mechanisms. Current IDS algorithms lack the behavioral modeling capability required to identify anomalous patterns independent of command origin, fundamentally limiting this approach's effectiveness against top-level compromises.

Second, frequent false positives create economic losses that may discourage DER adoption. While acceptable from a safety perspective, unnecessary disconnections undermine user confidence and require careful calibration of detection sensitivity against normal operational variations.

Third, the integration of cybersecurity functions into protection relays raises questions about standardization and interoperability. The IEC 62351 Standard [20] provides security measures for securing electrical control networks, but without standardized protocols and interfaces specifically for cyber-physical protection coordination, implementations may vary widely across manufacturers and jurisdictions, potentially creating gaps in protection coverage or incompatibilities that attackers could exploit.

6.6.3 Integration with Existing Standards

The IEEE 1547 Standard defines interconnection and interoperability requirements for DERs and provides conformance test procedures and pass/fail criteria. However, the standard refers only generically to "response plans" that grid operators must implement. The proposed solution can function as a technical implementation of such response plans recommended by the standard, providing concrete mechanisms for automated incident response that complement manual procedures.

The approach also aligns with broader frameworks for critical infrastructure protection by recognizing that cyber and physical security cannot be treated as entirely separate domains in modern power systems. As systems become increasingly digitalized and interconnected, the boundary between cyber and physical threats becomes increasingly blurred, necessitating integrated protection strategies.

6.6.4 Future Research Directions

Several areas require further investigation to fully realize the potential of cyberdefense functionalities in electrical protection systems. First, comprehensive IDS implementations specifically designed for DER applications must be developed and validated. These systems must balance computational efficiency with detection accuracy, operating within the resource constraints of embedded systems while providing reliable threat identification. The work by Chaabouni et al. [16] on network intrusion detection for IoT security provides a foundation for such developments.

Second, coordination strategies for multiple protection devices must be developed to prevent cascading effects or unnecessary widespread disconnections. When should multiple devices trip independently versus coordinating their responses? How can protection systems distinguish between localized attacks requiring limited disconnections and systemic threats requiring more extensive protective actions?

Third, restoration procedures following cyber-triggered protection operations require careful design. How can systems safely reconnect after attacks without creating opportunities for recurring compromises? What verification procedures should precede reconnection? These questions demand thoughtful answers that balance restoration speed with security assurance.

Fourth, the economic and regulatory frameworks surrounding cyber-triggered protection actions need development. Who bears responsibility for economic losses resulting from protection operations? How should utilities and regulators evaluate the cost-benefit tradeoffs of implementing such systems? What liability frameworks appropriately allocate risks among stakeholders?

6.7 Chapter Summary

This chapter presents a novel approach for ensuring distribution power system availability under cyberattacks by using electrical protections as incident response tools. The approach implements functionality in protection systems enabling circuit breakers near DERs to trip upon cyberattack detection.

Simulation of a coordinated attack on the IEEE European Low-Voltage Test Feeder demonstrated the countermeasure's effectiveness. Without the protection mechanism, an attack commanding 400 kW of distributed generation to inject maximum power simultaneously caused substation voltage to exceed acceptable limits by more than 10%, risking

widespread outages or equipment damage. With the proposed approach, automatic disconnection of compromised generators maintained voltage within operational boundaries, allowing continued service despite the ongoing attack.

This work establishes a foundation for integrating cybersecurity functions into electrical protection systems. The approach recognizes that in modern distribution grids with high DER penetrations, traditional separation of safety and security functions creates vulnerabilities that automated, integrated protection mechanisms can address. By treating circuit breakers and protection relays as active cybersecurity incident response components rather than merely physical fault protection devices, power systems achieve greater resilience.

Future work must address IDS effectiveness verification for sophisticated attacks against network-connected DERs, coordination strategies among distributed protection devices, and appropriate regulatory and economic frameworks for cyber-triggered protection actions. Nevertheless, the fundamental concept—that electrical protection can and should respond to cyber threats—represents an important evolution in power system protection philosophy for increasingly digitalized and distributed grid architectures.

CHAPTER 7

General conclusion

7.1 Research Summary

This thesis addressed five critical DER cybersecurity gaps through interconnected studies:

Quantitative Impact Analysis (Chapter 3) established attack thresholds: 200 kW creates localized LV violations while 400 kW causes system-wide impacts; MV systems proved extremely vulnerable with 1 MVAr reactive manipulation producing 20% deviations and 2 MW attacks creating catastrophic 80% overvoltage conditions.

Photo-Set Dataset (Chapter 4) provided the first comprehensive PV cybersecurity dataset with 22 electrical/environmental features across 12 attack scenarios, enabling reproducible detection research. Benchmark evaluation revealed attack-dependent detectability with firmware modifications proving most challenging.

Physics-Informed Detection (Chapter 4) integrated Kirchhoff's laws and power balance equations into LSTM architectures, achieving 30.69% accuracy improvement over baselines while providing explainable detection through physical law violations.

VPP Security Framework (Chapter 5) addressed time-critical ancillary service vulnerabilities through pre-authenticated validation, real-time latency monitoring, and protocol-specific protections reconciling millisecond response requirements with comprehensive security.

Automated Cyber-Response (Chapter 6) demonstrated electrical protection systems can serve as incident response tools, with simulation showing automatic generator disconnection maintaining voltage within safe limits during coordinated attacks that would otherwise cause widespread outages.

7.2 Key Contributions and Implications

7.2.1 Cyber-Physical Security Integration

This research contributes to a fundamental reconceptualization of power system security appropriate for increasingly digitalized and distributed grid architectures. Traditional frameworks treated cyber threats and physical faults as distinct phenomena requiring separate protection mechanisms. Cybersecurity teams focused on network defenses while protection engineers designed relay schemes for equipment faults. This separation is obsolete and dangerous in modern DER systems.

Cyberattacks manifest as physical system disturbances—voltage violations, frequency deviations, equipment damage. Physical monitoring provides essential signals for cyber threat detection through physics-based anomaly identification. Effective security therefore demands integrated protection strategies leveraging both domains. Cyber monitoring enables early threat detection before physical consequences materialize. Physical safeguards provide defense-in-depth when cyber protections are bypassed.

7.2.2 Physics-Informed Machine Learning

The superior performance of physics-informed detection validates a core proposition: in cyber-physical systems governed by well-understood physical laws, incorporating domain knowledge into machine learning architectures fundamentally improves threat identification. An adversary who carefully maintains learned patterns while violating Kirchhoff's laws reveals themselves through physical inconsistency even when statistical signatures appear normal.

Physical relationships reduce false positives by distinguishing legitimate environmental variations from anomalous behavior. Irradiance fluctuations cause correlated power changes—this is normal. Power changes uncorrelated with environmental conditions indicate anomalies. Interpretability improves dramatically when detections trace to violated physical laws rather than opaque neural network activations. This advantage extends beyond photovoltaic systems to any cyber-physical infrastructure where physical relationships constrain legitimate behavior.

7.2.3 Time-Critical Operations and Security Trade-offs

The VPP analysis illuminates fundamental trade-offs between security validation thoroughness and operational responsiveness. When Frequency Containment Reserve requires 1-2 second cycle times, comprehensive cryptographic validation, anomaly detection analysis, and multi-factor authentication may consume unacceptable portions of the operational timeline.

Pre-authenticated command validation offers a resolution strategy. Computing and storing authentication tokens during idle periods enables rapid validation during operational windows without compromising cryptographic integrity. This pattern generalizes: rather than choosing between security and performance, intelligent temporal separation of computationally expensive operations from time-sensitive execution enables both objectives.

7.2.4 Distributed Architecture Security Challenges

The shift from centralized generation to distributed energy resources creates security challenges qualitatively different from traditional power systems. Centralized plants operate in physically secured facilities with dedicated security personnel, air-gapped control systems, and homogeneous technology stacks. DER systems span thousands of geographically dispersed installations with varying physical security, heterogeneous networks traversing public internet infrastructure, diverse equipment from multiple vendors, and multi-stakeholder ownership.

This distributed architecture expands the attack surface exponentially while complicating defensive monitoring. No single organization maintains visibility across the entire system. Coordination among diverse stakeholders with conflicting incentives proves challenging. Effective DER security requires new architectural patterns: tiered trust management, federated monitoring, automated response mechanisms, and standardized security interfaces.

7.2.5 Risk-Graduated Security Requirements

The quantitative impact analysis demonstrates that current regulatory capacity limits already enable exploitable vulnerabilities. Policymakers face a critical choice: impose more restrictive limits that constrain renewable deployment, or mandate comprehensive security that may increase costs.

A third path exists: risk-based approaches calibrating security requirements to system impact potential. Low-voltage residential installations creating only localized consequences might warrant minimal protections. Medium-voltage community-scale systems with system-wide impact potential require rigorous security controls including intrusion detection, automated protection coordination, and continuous monitoring. This risk-graduated approach enables renewable energy deployment while managing cyber-physical risks proportionate to potential consequences.

7.3 Limitations and Critical Reflections

While this research advances DER cybersecurity, several important limitations warrant acknowledgment. The quantitative impact analysis employed standard IEEE test feeders that enable reproducibility but may not fully capture real distribution network complexity. Non-standard topologies, aging infrastructure, protection coordination challenges, and operational uncertainties in actual networks could affect vulnerability thresholds. Real-world validation across diverse network configurations and loading conditions would strengthen confidence in generalizability.

The physics-based anomaly detection research developed algorithms using laboratory data from controlled PV system testbeds. Operational environments introduce additional complexities—electromagnetic interference, communication network instability, sensor degradation, maintenance activities, and grid disturbances—that may affect detection performance. The transition from laboratory validation to field deployment requires careful consideration of these real-world phenomena and their impact on false positive/negative rates.

The automated cyber-incident response mechanism assumes reliable IDS operation. In practice, IDS implementations face challenging trade-offs between detection sensitivity and false positive rates. While false positives are acceptable from a safety perspective, frequent unnecessary disconnections could undermine user confidence and create economic losses that discourage DER adoption. Sophisticated adversaries aware of IDS implementation details might craft attacks that evade detection or trigger excessive false positives to degrade system availability.

A critical gap remains: local IDS systems may not recognize attacks when the central EMS platform has been compromised, since commands appear to originate from legitimate sources. This scenario significantly reduces effectiveness and highlights the importance of

developing sophisticated attack detection algorithms that can identify anomalous behavior patterns even when commands come from authenticated sources.

The VPP security framework provides comprehensive technical guidance but implementation faces significant practical barriers. Multi-stakeholder VPPs coordinate assets owned by utilities, aggregators, commercial entities, and individual prosumers with divergent economic incentives, technical capabilities, and risk tolerances. Achieving coordinated security implementation requires not only technical solutions but also governance frameworks, liability allocation mechanisms, cost-sharing arrangements, and regulatory mandates beyond this research's scope.

Finally, the research focused primarily on intentional cyberattacks by malicious adversaries, giving less attention to non-malicious threats including software bugs, configuration errors, equipment failures, and human mistakes. While defensive mechanisms would provide protection against both categories, the relative prevalence of malicious versus non-malicious incidents in operational DER systems remains unclear, complicating cost-benefit analysis and resource allocation decisions.

7.4 Future Research Directions

The research presented opens numerous avenues for future investigation spanning fundamental research questions, technological developments, and practical implementations.

7.4.1 Field Validation and Real-World Deployment

The most critical next step involves validation of proposed detection algorithms and protection mechanisms in operational power distribution systems. Laboratory experiments and simulations provide valuable insights but cannot fully replicate real-world complexity and variability.

Field validation should proceed through multiple stages: pilot deployments in controlled environments enable algorithm tuning without systemic risk; expanded testing across diverse geographic regions and network topologies assesses generalization; long-duration monitoring captures seasonal variations and rare conditions; and coordinated red team exercises evaluate defensive effectiveness against adaptive, intelligent threats. This validation requires collaboration between researchers, utilities, manufacturers, and cybersecurity professionals, facilitated by regulatory frameworks enabling responsible testing without compromising grid reliability.

7.4.2 Embedded Systems and Technology Extension

Current algorithms run on general-purpose computing platforms, but practical deployment requires implementation on embedded systems with severe constraints—limited processing power, restricted memory, minimal storage, and power limitations. Research must address model compression through pruning, quantization, and knowledge distillation; algorithm optimization for embedded architectures using fixed-point arithmetic; hardware acceleration via AI accelerators or FPGA implementations; and edge-cloud hybrid architectures partitioning computation between constrained devices and capable infrastructure.

Beyond photovoltaic systems and EV charging stations, the DER ecosystem includes battery storage, demand response, combined heat and power, wind turbines, fuel cells, vehicle-to-grid, and hydrogen electrolyzers. Each exhibits unique physical characteristics, protocols, and vulnerabilities requiring technology-specific physics-informed models, datasets, and threat analyses. Emerging threats warrant investigation: adversarial machine learning targeting AI controls, supply chain compromises introducing malicious hardware, side-channel attacks extracting information through power consumption, and quantum computing threatening cryptographic protections.

7.4.3 Coordinated Attack Detection and Advanced IDS

The most sophisticated threats involve coordinated attacks across multiple DER installations designed to achieve cumulative grid instability while each individual installation exhibits only modest deviations. Detecting such campaigns requires analytics identifying collective patterns across distributed assets rather than anomalies at individual sites. Challenges include developing correlation algorithms respecting privacy constraints, attribution techniques determining malicious versus coincidental coordination, and real-time scalability enabling sub-second analysis across millions of assets.

A critical gap remains: local IDS systems may not detect attacks when central EMS platforms are compromised, since commands appear legitimate. Future research must address distributed IDS architectures with cross-validation, behavioral analysis detecting anomalous patterns from authenticated sources, reputation systems tracking historical command behavior, and hierarchical detection operating at DER, aggregator, and EMS levels. Coordination strategies among multiple protection devices must prevent cascading disconnections while distinguishing localized attacks from systemic threats.

7.4.4 Economic, Regulatory, and Privacy Frameworks

Technical cybersecurity mechanisms exist within broader economic and regulatory contexts significantly influencing adoption. Future work should examine cost-benefit methodologies for security investments, quantifying avoided losses while accounting for low-probability high-consequence events; liability allocation frameworks determining responsibility for attack-caused damage; insurance mechanisms for power system cyber risk; and business models enabling security-as-a-service for small-scale operators lacking expertise.

Regulatory research should address mandatory security standards for DER equipment, certification programs ensuring baseline capabilities, incident reporting requirements balancing transparency with operational security, and international coordination given global supply chains and threat actors. Policy analysis should examine how cybersecurity requirements interact with renewable deployment targets, consumer protection, and reliability standards.

Comprehensive threat detection requires analyzing operational data from millions of installations, potentially revealing sensitive consumption patterns and privacy-relevant details. Promising approaches include federated learning training models on distributed data without centralization, differential privacy adding calibrated noise, homomorphic encryption enabling computation on encrypted data, and secure multi-party protocols allowing collaborative analysis without revealing contributions. Legal research should examine how privacy regulations impact security monitoring and develop governance frameworks balancing security and privacy objectives.

7.4.5 Resilience, Recovery, and Human Factors

While this research focused on threat detection and prevention, equally important questions concern system resilience and recovery following successful attacks. Research directions include graceful degradation strategies maintaining partial functionality under attack; automated restoration sequencing prioritizing critical loads and verifying stability; black start capabilities enabling grid reconstruction after outages; and recovery verification ensuring compromised systems are remediated before reconnection. Post-incident forensics and lessons-learned processes should feed continuous improvement, adapting defenses based on observed attack techniques.

Despite emphasis on automation, human operators remain central through supervisory oversight, complex decision-making under uncertainty, and incident management. Future research should investigate operator interfaces presenting cyber-physical security

information in actionable formats; decision support systems recommending responses while explaining rationale and uncertainty; training programs developing cybersecurity expertise among power system operators and vice versa; and organizational structures integrating security operations centers with utility control rooms. Cognitive load analysis should examine how operators manage simultaneous physical and cyber threats, identifying potential for confusion or incorrect actions. Usability research should evaluate whether detection algorithms produce alerts operators can understand, trust, and act upon appropriately.

7.5 Final Remarks

The energy transition creates electricity systems more complex and interconnected than ever before. This thesis demonstrates that cyber threats to distributed energy resources pose concrete, quantifiable risks—400 kW attacks cause system-wide LV failures while 2 MW attacks create catastrophic MV conditions. Yet practical solutions exist: physics-informed detection achieves 30.69% accuracy improvements, comprehensive VPP frameworks address time-critical challenges, and automated protection mechanisms maintain grid stability during attacks.

Significant challenges remain in transitioning from laboratory validation to operational deployment, but the fundamental proposition is compelling: through sustained research, thoughtful implementation, and multi-stakeholder collaboration, societies can realize DER benefits while managing cyber-physical risks to acceptable levels. The alternative—foregoing distributed generation or proceeding with inadequate protections—presents unacceptable consequences for climate mitigation and energy security. As power systems evolve toward greater decentralization and digitalization, treating cybersecurity as integral to system design becomes not merely advisable but essential.

Appendix

APPENDIX A

Summary of Virtual Power Plant Attack Vectors mapped to MITRE ATT&CK Framework

This table denotes:

1. Severity Levels: Critical (immediate grid impact), High (significant operational impact), Medium (localized disruption).
2. MITRE Techniques: Standardized attack classifications from MITRE ATT&CK framework.
3. Countermeasures: Primary technical controls; additional measures may be required based on implementation context.
4. Cross-Service Attacks: Techniques affecting multiple VPP service categories simultaneously.

Table A.1: VPP Attack Vector to MITRE ATT&CK Mapping

Service Category	**Attack Vector**	**MITRE Technique**	**Severity**	**Recommended Countermeasure**
Frequency Control				
	Fast-Response System Compromise	T1203 (Exploitation for Client Execution)	High	Pre-authenticated command validation
	Aggregated EV Network Attack	T1021.002 (SMB/Windows Admin Shares)	Medium	Network segmentation, Endpoint protection

Continued on next page

Table A.1 – *Continued from previous page*

Service Category	Attack Vector	MITRE Technique	Severity	Recommended Countermeasure
	Latency Injection	T1499.002 (Service Exhaustion Flood)	High	Real-time latency monitoring
	Set-Point Manipulation	T1565.002 (Transmitted Data Manipulation)	Critical	Cryptographic integrity checks
	Measurement Corruption	T1565.001 (Stored Data Manipulation)	High	Data integrity verification
Voltage Compensation				
	Phase Relationship Attack	T1565.003 (Runtime Data Manipulation)	High	Real-time latency monitoring
	Power Factor Manipulation	T1078.004 (Cloud Accounts)	Medium	Multi-factor authentication
	Reactive Power Disruption	T1557.002 (ARP Cache Poisoning)	High	Network traffic analysis
	Loss Energy Forecast Manipulation	T1213 (Data from Information Repositories)	Medium	Data integrity verification
Operational Management				
	Load Flow Calculation Attack	T1565.001 (Stored Data Manipulation)	High	Data integrity verification
	Redispatch Command Interception	T1557.001 (LLMNR/NBT-NS Poisoning)	Critical	Secure communication protocols

Continued on next page

Table A.1 – *Continued from previous page*

Service Category	**Attack Vector**	**MITRE Technique**	**Severity**	**Recommended Countermeasure**
	Feed-in Management Disruption	T1529 (System Shutdown/Reboot)	Medium	Access control and monitoring
	Timing Attack on Grid Operations	T1499.004 (Application or System Exploitation)	High	Real-time latency monitoring
Supply Reconstruction				
	Black Start Sequence Corruption	T1106 (Native API)	Critical	Pre-authenticated command validation
	Energy Storage Compromise	T1485 (Data Destruction)	High	Access control and monitoring
	Emergency Response Delay	T1498 (Network Denial of Service)	High	Network segmentation
	Grid Restoration Manipulation	T1090 (Proxy)	Critical	Secure communication protocols
	False Start Signals	T1557 (Adversary-in-the-Middle)	High	Cryptographic integrity checks
Cross-Service Attacks				
	Communication Protocol Exploitation	T1040 (Network Sniffing)	Medium	Protocol encryption
	Market Data Manipulation	T1565.002 (Transmitted Data Manipulation)	High	Data integrity verification

Continued on next page

Table A.1 – *Continued from previous page*

Service Category	**Attack Vector**	**MITRE Technique**	**Severity**	**Recommended Countermeasure**
	Industrial Load Manipulation	T1562.001 (Disable or Modify Tools)	Medium	Access control and monitoring
	Sensor Data Injection	T1598.003 (Spearphishing via Service)	Medium	Network traffic analysis
	Credential Compromise	T1078 (Valid Accounts)	High	Multi-factor authentication
	Insider Threat Exploitation	T1078.002 (Domain Accounts)	High	Access control and monitoring

Publication record

1. International Journal Papers

[1] A. Mokarim, G. B. Gaggero, and M. Marchese, "Impact Analysis of Cyber Attacks against Energy Communities in Distribution Grids," Electronics, vol. 13, no. 9, p. 1709, May 2024, doi: 10.3390/electronics13091709.

[2] A. Mokarim, G. B. Gaggero, G. Ferro, M. Robba, P. Girdinio, and M. Marchese, "Photo-Set: A Proposed Dataset and Benchmark for Physics-Based Cybersecurity Monitoring in Photovoltaic Systems," Energies, vol. 18, no. 19, p. 5318, Oct. 2025, doi: 10.3390/en18195318.

[3] A. Mokarim, G. B. Gaggero, and M. Marchese, "Securing Virtual Power Plants: Attack Vector Analysis of Cybersecurity Vulnerabilities in Ancillary Grid Services," IEEE Open J. Ind. Electron. Soc., early access, 2025, doi: 10.1109/OJIES.2025.3622528.

[4] G. B. Gaggero, A. Mokarim, P. Girdinio, and M. Marchese, "Should We Include Cyberdefense Functionalities in Electrical Power System Protections?: A Proposed Approach," IEEE Ind. Electron. Mag., vol. 19, no. 1, pp. 10-16, Mar. 2025, doi: 10.1109/MIE.2024.3416907.

[5] D. F. Valderrama, G. B. Gaggero, G. Ferro, A. Mokarim, M. Robba, P. Girdinio, and M. Marchese, "An online intrusion detection system for photovoltaic generators through physics-based neural networks," Electric Power Systems Research, vol. 241, p. 111150, 2025, doi: 10.1016/j.epsr.2025.011150.

2. International Conference Papers

[6] A. Mokarim, G. B. Gaggero, and M. Marchese, "Evaluation of the Impact of Cyber-Attacks Against Electric Vehicle Charging Stations in a Low Voltage Distribution Grid," in Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm), Glasgow, United Kingdom, Nov. 2023, pp. 1-7, doi: 10.1109/SmartGridComm57358.2023.10333896.

[7] A. Mokarim, G. B. Gaggero, G. Ferro, M. Robba, and M. Marchese, "Photo-Set: A Dataset for Physics-Based Cybersecurity Monitoring in Photovoltaic Systems," IFAC-PapersOnLine, vol. 59, no. 9, pp. 37-42, 2025, doi: 10.1016/j.ifacol.2025.08.109.

Participation in Research Projects

Research project 1, SERICS- SEcurity and RIghts in CyberSpace.

Funded by MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU, this research project is focused on cybersecurity of critical infrastructures.

Activity: Development of cybersecurity frameworks for virtual power plants, creation of physics-based attack detection datasets, and analysis of cyber attacks in LV and MV DERs.

Attendance to workshops

Participated in a workshop on Cyber-Physical Systems (CPS): Cyber Security in Smart Grid, Electric Vehicles, and Autonomous Vehicles at Cardiff University, United Kingdom (11th June, 2024- online).

Participated in Maker Faire Rome 2025 – The European Edition project promoted by the Rome Chamber of Commerce and organized by Innova Camera, a special agency that deals with innovation and development of the entrepreneurial system, as part of the PID – Punto Impresa Digitale project, in synergy with other national and international institutions.

Bibliography

[1] U.S. Department of Energy, "Grid 2030: A national vision for electricity's second 100 years," U.S. Department of Energy, Office of Electric Transmission and Distribution, Tech. Rep., 2003, office of Electric Transmission and Distribution.

[2] E. Commission, "European technology platform smartgrids: Vision and strategy for europe's electricity networks of the future," Luxembourg, Tech. Rep., 2006.

[3] S. M. Amin and B. F. Wollenberg, "Toward a smart grid: Power delivery for the 21st century," *IEEE Power & Energy Magazine*, vol. 3, no. 5, pp. 34–41, 2005.

[4] International Energy Agency, *Distributed Generation in Liberalised Electricity Markets*. Paris: OECD Publishing, 2002. [Online]. Available: https://www.iea.org/reports/distributed-generation-in-liberalised-electricity-markets

[5] International Renewable Energy Agency (IRENA), "Renewable power generation costs in 2022," International Renewable Energy Agency, Abu Dhabi, Tech. Rep., August 2023. [Online]. Available: https://www.irena.org/publications/2023/Aug/Renewable-power-generation-costs-in-2022

[6] BloombergNEF, "Battery pack prices fall to an average of $132/kwh, but rising commodity prices start to bite," Press Release, November 2021. [Online]. Available: https://about.bnef.com/blog/battery-pack-prices-fall-to-an-average-of-132-kwh-but-rising-commodity-prices-start-to-bite/

[7] International Energy Agency, "Net zero by 2050: A roadmap for the global energy sector," International Energy Agency, Paris, Tech. Rep., May 2021. [Online]. Available: https://www.iea.org/reports/net-zero-by-2050

[8] B. Kroposki, B. Johnson, Y. Zhang, V. Gevorgian, P. Denholm, B.-M. Hodge, and B. Hannegan, "Achieving a 100% renewable grid: Operating electric power systems with extremely high levels of variable renewable energy," *IEEE Power and Energy Magazine*, vol. 15, no. 2, pp. 61–73, March-April 2017.

[9] IEEE, "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," Institute of Electrical and Electronics Engineers, IEEE Standard 1547-2018, 2018.

[10] R. Teodorescu, M. Liserre, and P. Rodriguez, *Grid Converters for Photovoltaic and Wind Power Systems*. John Wiley & Sons, 2011.

[11] Y. Yang, P. Enjeti, F. Blaabjerg, and H. Wang, "Wide-scale adoption of photovoltaic energy: Grid code modifications are explored in the distribution grid," *IEEE Industry Applications Magazine*, vol. 21, no. 5, pp. 21–31, 2015.

[12] W. Kempton and J. Tomić, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of Power Sources*, vol. 144, no. 1, pp. 268–279, 2005.

[13] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of vehicle-to-grid on the distribution grid," *Electric Power Systems Research*, vol. 81, no. 1, pp. 185–192, 2011.

[14] *Road Vehicles – Vehicle to Grid Communication Interface – Part 1: General Information and Use-Case Definition*, ISO Std. 15 118-1, 2019.

[15] P. Denholm, E. Ela, B. Kirby, and M. Milligan, "The role of energy storage with renewable electricity generation," National Renewable Energy Laboratory, Golden, CO, Technical Report NREL/TP-6A2-47187, 2010.

[16] Australian Energy Market Operator (AEMO), "Initial operation of the hornsdale power reserve battery energy storage system," Australian Energy Market Operator, Tech. Rep., Apr. 2018, published April 2018; focuses on participation in FCAS markets after commissioning in late 2017.

[17] European Union, "Directive (eu) 2018/2001 of the european parliament and of the council on the promotion of the use of energy from renewable sources," Official Journal of the European Union, Dec. 2018, oJ L 328, 21.12.2018, pp. 82–209. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L2001

[18] A. Paudel, K. Chaudhari, C. Long, and H. B. Gooi, "Peer-to-peer energy trading in a prosumer-based community microgrid: A game-theoretic model," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 8, pp. 6087–6097, 2019.

[19] D. Pudjianto, C. Ramsay, and G. Strbac, "Virtual power plant and system integration of distributed energy resources," *IET Renewable Power Generation*, vol. 1, no. 1, pp. 10–16, 2007.

[20] A. G. Zamani, A. Zakariazadeh, and S. Jadid, "Day-ahead resource scheduling of a renewable energy based virtual power plant," *Applied Energy*, vol. 169, pp. 324–340, 2016.

[21] E. G. Kardakos, C. K. Simoglou, and A. G. Bakirtzis, "Optimal offering strategy of a virtual power plant: A stochastic bi-level approach," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 794–806, 2016.

[22] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[23] F. M. Cleveland, "Iec 61850-7-420 communications standard for distributed energy resources (der)," in *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, 2008, pp. 1–4.

[24] N. Naik, "Choice of effective messaging protocols for iot systems: Mqtt, coap, amqp and http," in *2017 IEEE International Systems Engineering Symposium (ISSE)*, 2017, pp. 1–7.

[25] S. Fries, H. J. Hof, and M. Seewald, "Enhancing iec 62351 to improve security for energy automation in smart grid environments," in *2010 Fifth International Conference on Internet and Web Applications and Services (ICIW)*, 2010, pp. 135–142.

[26] National Institute of Standards and Technology (NIST), "Guidelines for smart grid cybersecurity," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Interagency Report NISTIR 7628 Revision 1, 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf

[27] National Electric Sector Cybersecurity Organization Resource (NESCOR), "Electric sector failure scenarios and impact analyses," National Electric Sector Cybersecurity Organization Resource (NESCOR), United States, Technical Report, 2015. [Online]. Available:

https://smartgrid.epri.com/doc/NESCOR%20Electric%20Sector%20Failure%20Scenarios%20and%20Impact%20Analyses%20-%20Version%203.0.pdf

[28] R. Baker and I. Martinovic, "Losing the car keys: Wireless physical layer insecurity in ev charging," in *Proceedings of the 28th USENIX Security Symposium (USENIX Security 2019)*. Santa Clara, CA, USA: USENIX Association, 2019, pp. 407–424. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/baker

[29] A. Lev, S. Hareuveni, and A. Rubin, "Security analysis of the open charge point protocol," in *2019 IEEE Vehicle Power and Propulsion Conference (VPPC)*, 2019, pp. 1–6.

[30] J. Johnson *et al.*, "Cybersecurity for electric vehicle charging infrastructure," Sandia National Laboratories, Albuquerque, NM, USA, Technical Report SAND2020-3930, 2020. [Online]. Available: https://www.osti.gov/biblio/1615165

[31] M. A. Mustafa *et al.*, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2588–2603, 2020.

[32] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[33] C. Liu, Y. Wu, C. Lin, and P. Cheng, "On the security of cyber-physical systems against stealthy deception attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 6, pp. 2346–2356, 2019.

[34] K. T. Järvinen *et al.*, "Securing the gateway for smart grid," in *2014 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2014, pp. 1–6.

[35] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Communications*, vol. 24, no. 4, pp. 88–98, 2017.

[36] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proc. of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, 2010, pp. 61–66.

[37] I. Al-Anbagi, M. Erol-Kantarci, and H. T. Mouftah, "A reliable ieee 802.15.4 model for cyber physical power grid monitoring systems," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 481–494, 2017.

[38] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[39] Cybersecurity and I. S. Agency, "Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations," Alert AA20-352A, December 2020.

[40] R. Falk, M. Fries, and S. Grinberg, "Iec 61850 security mechanisms," in *2016 IEEE International Conference on Industrial Technology (ICIT)*, 2016, pp. 1643–1648.

[41] S. McLaughlin *et al.*, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.

[42] S. Andy, B. Rahardjo, and B. Hanindhito, "Attack scenarios and security analysis of mqtt communication protocol in iot system," in *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2017, pp. 1–6.

[43] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[44] 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.

[45] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 214–219.

[46] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, 2011.

[47] M. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference (GLOBECOM)*, 2012, pp. 3153–3158.

[48] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, 2014.

[49] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, 2017.

[50] S. Soltan, P. Mittal, and H. V. Poor, "Blackiot: Iot botnet of high wattage devices can disrupt the power grid," in *27th USENIX Security Symposium*, 2018, pp. 15–32.

[51] M. A. Rahman, E. Al-Shaer, and P. Bera, "A noninvasive threat analyzer for advanced metering infrastructure in smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 273–287, 2013.

[52] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection designs," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2862–2872, 2018.

[53] S. Sridhar and A. Hahn, "Cyber-physical system security for the electric power grid," in *Proceedings of the IEEE*, 2012, pp. 210–224.

[54] A. Teymouri, A. Mehrizi-Sani, and C.-C. Liu, "Cyber security risk assessment of solar pv units with reactive power capability," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018, pp. 1–6.

[55] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar pv and ess control systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1330–1339, 2017.

[56] M. A. Rahman *et al.*, "False data injection attacks against nonlinear state estimation in smart power grids," in *2013 IEEE Power & Energy Society General Meeting*, 2013, pp. 1–5.

[57] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1643–1653, 2014.

[58] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[59] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on scada systems," in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*, 2011, pp. 380–388.

[60] C.-Y. Lin and S. Nadjm-Tehrani, "Timing patterns and correlations in spontaneous scada traffic for anomaly detection," in *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*, 2019, pp. 73–88.

[61] J. Giraldo, D. Urbina, A. Cárdenas, J. Valente, M. Faisal, J. Ruths, N. O. Tippenhauer, H. Sandberg, and R. Candell, "A survey of physics-based attack detection in cyber-physical systems," *ACM Computing Surveys (CSUR)*, vol. 51, no. 4, pp. 1–36, 2018.

[62] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[63] H. He, G. Yan, and J. Yan, "Cyber-physical attack and defense in smart grid," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, 2020, pp. 1846–1851.

[64] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis*, 2014, pp. 4–11.

[65] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long short term memory networks for anomaly detection in time series," in *23rd European Symposium on Artificial Neural Networks (ESANN) 2015*, 2015, pp. 89–94.

[66] Y. Luo, Y. Xiao, L. Cheng, G. Peng, and D. D. Yao, "Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1–36, 2021.

[67] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7992–8004, 2019.

[68] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 840–852, 2018.

[69] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," *IEEE Systems Journal*, vol. 9, no. 1, pp. 31–44, 2015.

[70] E. Glaessgen and D. Stargel, "The digital twin paradigm for future nasa and u.s. air force vehicles," 04 2012.

[71] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," *IEEE Access*, vol. 8, pp. 21 980–22 012, 2020.

[72] S. Tsegaye, K. G. Heyi, M. T. Endaylalu, Z. A. Melaku, and K. T. Turufi, "Deep neural networks in smart grid digital twins: Evolution, challenges, and future outlooks," *IEEE Access*, vol. 13, pp. 114 845–114 864, 2025.

[73] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity, version 1.1," National Institute of Standards and Technology, Tech. Rep., 2018.

[74] European Parliament and Council, "Directive (eu) 2022/2555 on measures for a high common level of cybersecurity across the union (nis2 directive)," Official Journal of the European Union, 2022.

[75] IEEE, "Ieee standard 1547-2018: Standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," Institute of Electrical and Electronics Engineers, IEEE Standard, 2018.

[76] ENTSO-E, "Network code on load-frequency control and reserves," European Network of Transmission System Operators for Electricity, Tech. Rep., 2013.

[77] U.S. Department of Energy, "Cybersecurity for energy delivery systems (ceds) program," Office of Electricity, accessed 2024.

[78] ENISA, "Smart grid security: Recommendations for europe and member states," European Union Agency for Cybersecurity, Tech. Rep., 2012.

[79] T. M. Inc., "Matlab version: 9.13.0 (r2022b)," Natick, Massachusetts, United States, 2022. [Online]. Available: https://www.mathworks.com

[80] E. M. Szumska, "Electric vehicle charging infrastructure along highways in the eu," *Energies*, vol. 16, no. 2, 2023. [Online]. Available: https://www.mdpi.com/1996-1073/16/2/895

[81] C. Sourkounis and P. Tourou, "Grid code requirements for wind power integration in europe," *Conference Papers in Medicine*, vol. 2013, pp. 1–9, 01 2013.

[82] F. Government, "Ordinance no. 2016-1019 of july 27, 2016 related to self- consumption of electricity (in french, original title: "ordonnance no 2016-1019 du 27 juillet 2016 relative à l'autoconsommation d'electricité")," *J Off Répub Française*, Texte 5 sur 180 2016.

[83] BOE, "Real decreto 244/2019, de 5 de abril, por el que se regulan las condiciones administrativas, técnicas y económicas del autoconsumo de energía eléctrica," Spanish Official Gazette: Madrid, Spain, 2019.

[84] I. Goverment, "Decreto legislativo 8 novembre 2021, n. 199, attuazione della direttiva (ue) 2018/2001 del parlamento europeo e del consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili," Italin Official Gazette: Rome, Italy 2021.

[85] Repubblica Italiana, "Decreto legislativo 8 novembre 2021, n. 199, attuazione della direttiva (ue) 2018/2001 del parlamento europeo e del consiglio, dell'11 dicembre 2018, sulla promozione dell'uso dell'energia da fonti rinnovabili," 2021, gazzetta Ufficiale della Repubblica Italiana, Rome, Italy.

[86] P. Linnartz, A. Winkens, and S. Simon, "A method for assessing the impact of cyber attacks manipulating distributed energy resources on stable power system operation," in *2021 IEEE PES Innovative Smart Grid Technologies Europe (ISGT Europe)*. IEEE, 2021, pp. 01–05.

[87] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, 2023.

[88] D. M. Shilay, K. G. Lorey, T. Weiz, T. Lovetty, and Y. Cheng, "Catching anomalous distributed photovoltaics: An edge-based multi-modal anomaly detection," *arXiv preprint arXiv:1709.08830*, 2017.

[89] M. J. Zideh, P. Chatterjee, and A. K. Srivastava, "Physics-informed machine learning for data anomaly detection, classification, localization, and mitigation: A review, challenges, and path forward," *IEEE Access*, 2023.

[90] G. B. Gaggero, M. Rossi, P. Girdinio, and M. Marchese, "Detecting system fault/-cyberattack within a photovoltaic system connected to the grid: A neural network-based solution," *Journal of Sensor and Actuator Networks*, vol. 9, no. 2, p. 20, 2020.

[91] Á. L. P. Gómez, L. F. Maimó, A. H. Celdrán, F. J. G. Clemente, C. C. Sarmiento, C. J. D. C. Masa, and R. M. Nistal, "On the generation of anomaly detection datasets in industrial control systems," *IEEE Access*, vol. 7, pp. 177 460–177 473, 2019.

[92] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2248–2294, 2021.

[93] L. Faramondi, F. Flammini, S. Guarino, and R. Setola, "A hardware-in-the-loop water distribution testbed dataset for cyber-physical security testing," *IEEE Access*, vol. 9, pp. 122 385–122 396, 2021.

[94] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of iec 61850 based substation," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–7.

[95] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, 2022.

[96] G. B. Gaggero, A. Mokarim, P. Girdinio, and M. Marchese, "Should we include cyberdefense functionalities in electrical power system protections?: A proposed approach," *IEEE Industrial Electronics Magazine*, 2024.

[97] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[98] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes, "Using model-based intrusion detection for scada networks," in *Proceedings of the SCADA security scientific symposium*, vol. 46. Citeseer, 2007, pp. 1–12.

[99] A. Chavez, C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Jones, J. Johnson, and A. Summers, "Hybrid intrusion detection system design for distributed energy resource systems," in *2019 IEEE CyberPELS (CyberPELS)*. IEEE, 2019, pp. 1–6.

[100] M. A. Pimentel, D. A. Clifton, L. Clifton, and L. Tarassenko, "A review of novelty detection," *Signal Processing*, vol. 99, pp. 215–249, 2014.

[101] I. D. Mienye and T. G. Swart, "Deep autoencoder neural networks: A comprehensive review and new perspectives," *Archives of Computational Methods in Engineering*, Mar. 2025.

[102] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[103] F. Harrou, B. Bouyeddou, A. Dairi, and Y. Sun, "Exploiting autoencoder-based anomaly detection to enhance cybersecurity in power grids," *Future Internet*, vol. 16, no. 6, p. 184, May 2024.

[104] Y. Lee, C. Park, N. Kim, J. Ahn, and J. Jeong, "Lstm-autoencoder based anomaly detection using vibration data of wind turbines," *Sensors*, vol. 24, no. 9, p. 2833, Apr. 2024.

[105] C. Sun, Z. He, H. Lin, L. Cai, H. Cai, and M. Gao, "Anomaly detection of power battery pack using gated recurrent units based variational autoencoder," *Applied Soft Computing*, vol. 132, p. 109903, Jan. 2023.

[106] S. Kwon, H. Yoo, and T. Shon, "Ieee 1815.1-based power system security with bidirectional rnn-based network anomalous attack detection for cyber-physical system," *IEEE Access*, vol. 8, pp. 77 572–77 586, 2020.

[107] L. Kuhnel, T. Fletcher, S. Joshi, and S. Sommer, "Latent space non-linear statistics," 2018.

[108] "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," Institute of Electrical and Electronics Engineers, New York, NY, USA, 2018, https://standards.ieee.org/ieee/1547/63180/.

[109] "Communication Protocols for Smart Grids – Distributed Energy Resources and Distribution Automation Logical Nodes," International Electrotechnical Commission, Geneva, Switzerland, 2021, https://webstore.iec.ch/publication/69064.

[110] P. Denholm, T. Mai, R. W. Kenyon, B. Kroposki, and M. O'Malley, "Inertia and the power grid: A guide without the spin," National Renewable Energy Laboratory, Golden, CO, Tech. Rep. NREL/TP-6120-73856, 2020. [Online]. Available: https://www.nrel.gov/docs/fy20osti/73856.pdf

[111] E-ISAC, "Analysis of the cyber attack on the ukrainian power grid," Electricity Information Sharing and Analysis Center, Defense Use Case, March 2016.

[112] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access*, vol. 10, pp. 35 846–35 875, 2022.

[113] R. Bhattarai, S. J. Hossain, J. Qi, J. Wang, and S. Kamalasadan, "Sustained system oscillation by malicious cyber attacks on distributed energy resources," in *Proc. IEEE Power & Energy Soc. General Meeting (PESGM)*. Portland, OR, USA: IEEE Press, 2018, pp. 1–5.

[114] M. Tuttle, M. Poshtan, T. Taufik, and J. Callenes, "Impact of cyber-attacks on power grids with distributed energy storage systems," in *Proc. IEEE Int. Conf. Commun., Control, Comput. Technol. Smart Grids (SmartGridComm)*. Beijing, China: IEEE Press, 2019, pp. 1–6.

[115] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Power jacking your station: In-depth security analysis of electric vehicle charging station management systems," *Computers & Security*, vol. 112, p. 102511, 2022.

[116] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 1, no. 1, pp. 28–39, 2016.

[117] T. E. McDermott, J. D. Doty, J. G. O'Brien, C. R. Eppinger, and T. Becejac, "Cybersecurity for distance relay protection," Pacific Northwest National Lab. (PNNL), Richland, WA, USA, Tech. Rep., 2020.

[118] M. Jafari, M. H. Shahriar, M. A. Rahman, and S. Paudyal, "False relay operation attacks in power systems with high renewables," in *Proc. IEEE Power & Energy Soc. General Meet. (PESGM)*. IEEE Press, 2021, pp. 1–5.

[119] V. S. Rajkumar, M. Tealane, A. Štefanov, and P. Palensky, "Cyber attacks on protective relays in digital substations and impact analysis," in *Proc. 8th Workshop Modeling Simulation Cyber-Phys. Energy Syst.* IEEE Press, 2020, pp. 1–6.

[120] S. Ward *et al.*, "Cyber security issues for protective relays; c1 working group members of power system relaying committee," in *Proc. IEEE Power Eng. Soc. General Meet.* IEEE Press, 2007, pp. 1–8.

[121] ABB, "Protection relay plays a role in cyber resilience solution in power distribution," Available: https://new.abb.com/news/detail/106714/protection-relay-plays-a-role-in-cyber-resilience-solution-in-power-distribution, January 2024, accessed: Jan. 31, 2024.

[122] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 3, pp. 2671–2701, 2019.

[123] IEEE, "Distribution test feeders," IEEE PES Distribution Systems Analysis Subcommittee Radial Test Feeders, May 2015, available: https://cmte.ieee.org/pes-testfeeders/.

Cybersecurity for Distributed Energy Resources: Analysis from Individual Systems to Grid-Scale Communities

Afroz Mokarim