PhD Dissertation

Doctorate School in
Information and Communication Technology and Engineering

Department of Engineering
University of Naples Parthenope

Towards Resilient Energy Systems: Protecting the Energy Supply Chain Against APTs

Alfredo Petruolo

XXXVIII Cycle

Advisor: Prof. Luigi Coppolino

Coordinator: Prof. Agostino Iadicicco

2025

Abstract

The current Electric Power and Energy Systems sector has been profoundly changed by the introduction of smart grid technologies, which have completely reshaped the security measures for protecting energy infrastructure. While conventional power systems were characterized by centralized generation and unidirectional power flows, the emergence of distributed energy resources, renewable energy integration, and prosumer-based architectures has introduced unprecedented complexities in the threat landscape. These evolutionary changes have not only expanded the attack surface of energy systems but have also introduced novel vulnerabilities that stem from the bidirectional nature of modern energy flows, the proliferation of Internet-of-Things devices at the grid edge, and the increasing reliance on information and communication technologies for operational control. The traditional security frameworks that were developed for legacy power systems prove inadequate when confronted with the multifaceted threats inherent in these distributed, interconnected, and digitally-enabled energy ecosystems. Prosumer integration, in particular, has created numerous weak points throughout the infrastructure, as residential and commercial entities equipped with distributed generation, storage systems, and smart devices become integral components of the broader energy network. These edge nodes, often characterized by limited security measures and inconsistent monitoring capabilities, represent critical vulnerabilities that can be exploited to compromise the stability and integrity of the entire energy system. This research addresses these issues by first revealing a profound lack of governance and defined liability for security incidents originating from prosumer assets. It demonstrates that the cumulative threat from aggregated edge devices constitutes an overlooked systemic risk. In response, this thesis presents two key contributions. First, a specialized threat model and a reference APT scenario to guide future research. Second, a novel monitoring framework that use

digital twin technology and data sovereignty principles. Results show that this approach effectively detects prosumer-based malicious activity, thereby securing the continuity of grid operations without compromising citizen privacy, offering a resilient foundation for securing the distributed energy perimeter.

Contents

List of Acronyms

Acronym	Definition
AI	Artificial Intelligence
APT	Advanced Persistent Threat
BPA	Business Process Analyzer
CIM	Common Information Model
DT	Digital Twin
DSCB	Data Space Connector Builder
FL	Federated Learning
SCU	Simulation Control Unit
VAE	Variational Autoencoder
AC	Alternating Current
BESS	Battery Energy Storage System
CHP	Combined Heat and Power
DC	Direct Current
DER	Distributed Energy Resources
DSO	Distribution System Operator
EMS	Energy Management System
EV	Electric Vehicle
HV	High Voltage
LV	Low Voltage
MV	Medium Voltage

Continued on next page

Acronym	Definition
PV	Photovoltaic
TSO	Transmission System Operator
VPP	Virtual Power Plant
AMI	Advanced Metering Infrastructure
API	Application Programming Interface
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IDSA	International Data Spaces Association
IoT	Internet of Things
JSON	JavaScript Object Notation
MQTT	Message Queuing Telemetry Transport
NGSI-LD	Next Generation Service Interfaces - Linked Data
REST	Representational State Transfer
SCADA	Supervisory Control and Data Acquisition
TLS	Transport Layer Security
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DoS	Denial of Service
GDPR	General Data Protection Regulation
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
SIEM	Security Information and Event Management
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, DoS, Elevation of Privilege
CNN	Convolutional Neural Network
DL	Deep Learning
ML	Machine Learning

Continued on next page

Acronym	Definition
NN	Neural Network
RNN	Recurrent Neural Network
BPMN	Business Process Model and Notation
KPI	Key Performance Indicator
MAD	Moving Average Days
SLA	Service Level Agreement

List of Tables

List of Figures

Introduction

The contemporary Electric Power and Energy Systems (EPES) have undergone a profound transformation through the widespread adoption of smart grid technologies and the integration of Distributed Energy Resources (DERs), fundamentally altering the security landscape of energy infrastructure. This evolution represents a paradigmatic shift from the traditional centralized power generation model toward a distributed, interconnected ecosystem where bidirectional energy flows and digital communication systems have become integral to operational functionality [1]. The proliferation of smart grid components has exponentially expanded the attack surface of energy systems, introducing numerous entry points that can be exploited by malicious actors seeking to compromise the integrity, availability, and confidentiality of critical energy infrastructure [2].

The integration of renewable energy sources, while essential for achieving sustainability goals and reducing carbon emissions, has introduced unprecedented challenges from both electrical management and cybersecurity perspectives. The intermittent nature of renewable generation requires sophisticated forecasting, real-time monitoring, and dynamic load balancing capabilities that rely heavily on information and communication technologies. More significantly, the emergence of prosumers—entities that both produce and consume energy—has created a new category of stakeholders whose sheer numerical presence throughout the grid represents a substantial expansion of potential attack vectors. These numerous small-scale prosumer installations, often characterized by limited security measures and inconsistent monitoring capabilities, collectively constitute a distributed vulnerability that can be leveraged to orchestrate large-scale attacks against the broader energy infrastructure [3].

From a regulatory perspective, legislative bodies at both national and international levels have begun to acknowledge the critical importance of securing these evolving energy systems and are actively developing frameworks to govern the integration of distributed energy resources. However, despite these regulatory efforts, the cybersecurity dimension of this integration remains significantly underdeveloped, with current legislative approaches struggling to achieve an adequate balance between operational flexibility and security requirements [4]. The complexity of securing thousands of small-scale prosumer installations, each potentially operating under different technical specifications and security protocols, presents challenges

that existing regulatory frameworks are only beginning to address.

Similarly, while security measures specifically designed for prosumer and consumer environments are gaining recognition within both scientific research and industrial development communities, substantial gaps remain in the implementation and standardization of effective protective measures. The distributed nature of these installations, combined with economic constraints and varying levels of technical expertise among operators, creates a challenging environment for deploying comprehensive security solutions. Current approaches often focus on securing centralized components while leaving edge devices and prosumer installations inadequately protected, creating potential pathways for sophisticated attacks that could propagate throughout the entire energy system.

This thesis addresses critical gaps in the cybersecurity of modern Electric Power and Energy Systems. Its contributions are built upon a comprehensive foundational analysis structured around three key areas of investigation:

- **Cybersecurity Assessment of EPES**: This work examines the current threat landscape impacting electric power and energy systems, systematically identifying vulnerabilities across infrastructure components, with a focus on those introduced by prosumer integration. It covers both traditional centralized systems and the growing distributed architecture, providing a detailed taxonomy of threats and vulnerabilities affecting various levels of the energy system hierarchy.
- **Evaluation of Global Institutional Efforts**: The research investigates regulatory and legislative initiatives by European institutions and key international stakeholders, including the United States, China, Japan, and Canada, to tackle security challenges in distributed energy systems. It characterizes legislative frameworks and guidelines, highlighting their strengths and limitations in governing modern energy system security.
- **Technical Analysis of Prosumer Architecture and Advanced Persistent Threat Scenarios**: The thesis explores prosumer system architectures and their components, analysing a reference Advanced Persistent Threat (APT) scenario to illustrate the envisioned stages of such an attack on the distributed energy infrastructure. It demonstrates the technical feasibility and quantifies their potential impacts on energy system stability and economic operations, offering insights for defensive strategy development.

Collectively, this analysis leads to a significant set of discoveries. This research uncovers a profound gap in the governance and technical monitoring of prosumer systems. It demonstrates that they -prosumers- represent a cumulative, systemic risk to grid stability, largely due to a lack of cohesive governance and defined liability for security incidents originating outside the traditional utility perimeter.

Building upon these findings, the thesis delivers two central contributions that directly address both the theoretical understanding and the practical mitigation of these risks:

- First, it establishes a detailed threat model and a reference Advanced Persistent Threat scenario. This provides a foundational resource for the research community, enabling the development of novel security solutions targeted at emergent and as-yet-undiscovered threat vectors.
- Second, it delivers a novel monitoring framework, designed to advance the state-of-the-art in prosumer security monitoring. The framework's efficacy was then demonstrated and validated in a high-profile industrial context through the European Project CyberSEAS. Founded on digital twin monitoring and principles of data sovereignty, this framework provides a tangible solution for detecting advanced threats. Crucially, it guarantees the continuity of energy services while upholding consumer privacy, thus bridging the critical gap between theoretical research and the operational realities of modern EPES protection.

The research, development, and validation of these contributions are detailed in the subsequent chapters:

Chapter 1 examines smart grid vulnerabilities, providing an overview of industry standards considered throughout the research. It establishes a methodological foundation for understanding the current threat landscape, focusing on attacks originating from prosumer environments that could compromise infrastructure and target the broader energy grid. This study is supported by methodological approaches and empirical evidence demonstrating the feasibility and impact of such attack vectors.

Chapter 2 investigates the governance landscape, evaluating European and international legislative frameworks for energy system security. It offers a global perspective on regulatory gaps, providing actionable recommendations for policymakers. Through a comparative study of regulatory approaches across major stakeholders, this chapter identifies areas needing enhanced governance to address evolving security challenges in distributed energy systems.

Chapter 3 explores the reference architecture of prosumer systems, identifying vulnerabilities and risks within these distributed setups. It introduces a reference Advanced Persistent Threat scenario to illustrate potential attack pathways and methodologies. The chapter quantifies the potential economic and operational impacts of such attacks, including service disruptions and their cascading effects on system stability.

Chapter 4 presents the primary technical contribution of the thesis: a Reference Architecture for a Prosumer-Oriented Cybersecurity Monitoring Framework. This architecture is

specifically designed to address Advanced Persistent Threats that manipulate distributed energy resources and IoT devices. The chapter details the framework's three-layer structure (field, DT, application) and introduces its four core logical software artifacts: the Digital Twin Builder, which creates a high-fidelity, semantically-rich (CIM/NGSI-LD) digital representation for security analysis; the Business Process Analyzer, which uses statistical baselining and coordination tests to detect anomalies in prosumer behavior; the Data Space Connector Builder (DSCB), which enables secure, sovereignty-preserving, cross-border data sharing; and the Simulation Control Unit (SCU), which orchestrates "what-if" scenarios to validate attack impacts and defense responses. This chapter provides the functional specifications, interfaces, and formalisms for each artifact.

Chapter 5 details the practical validation and evaluation of the prosumer-oriented cybersecurity monitoring framework through an in-depth case study of the Berchidda urban distribution network in Sardinia, Italy. This chapter validates the framework's core artifacts by: (i) detailing the construction of the network's security-centric Digital Twin, including the CIM to NGSI-LD pipeline; (ii) evaluating the Business Process Analyzer's performance using real-world data, testing both mathematical and privacy-preserving federated learning models for prosumer behavior baselining; and (iii) demonstrating the feasibility of the Data Space Connector Builder for enabling secure, policy-governed data sharing. The chapter presents quantitative results on the trade-offs in single-prosumer anomaly detection and the effectiveness of grid-level coordination checks, concluding with an economic analysis of the financial impact of undetected prosumer-based attacks.

Conclusion Chapter synthesizes key findings, contributions, and limitations, outlining implications for future research and practical implementation in energy system cybersecurity. It discusses the broader impact of the research on academic knowledge and industry practice, offering recommendations for stakeholders in the energy and cybersecurity domains.

Chapter 1

Electrical and Power Energy Systems: Threats and Gaps

The transformation of traditional Electrical and Power Energy Systems toward highly interconnected and digitally enhanced infrastructures has fundamentally altered their cybersecurity landscape, creating an exponentially broader attack surface [5, 6]. This paradigmatic shift emerges from the convergence of advanced digital communication protocols, the ubiquitous deployment of Internet of Things (IoT) technologies, and the unprecedented emergence of prosumers as bidirectional energy market participants [7]. Although these technological innovations deliver substantial improvements in operational efficiency, grid reliability, and environmental sustainability, they simultaneously introduce complex vulnerability vectors that adversaries may exploit to orchestrate cascading infrastructure failures [8]. This chapter systematically evaluates smart grid critical assets, identifies the threats associated with each infrastructure component, and outlines persistent security deficiencies that are not addressed by modern protection frameworks and standards. Through this assessment, the objective is to establish research priorities and industrial focus areas essential for strengthening the cybersecurity posture of these critical energy systems.

1.1 The Smart Grid System: Vulnerabilities and Entry Points

The smart grid represents a fundamental paradigm shift from conventional electrical distribution networks through the systematic integration of sophisticated communication and information technologies, thereby establishing an intelligent and adaptive energy infrastructure [9]. This technological evolution delivers substantial enhancements in operational efficiency and system reliability; however, it concurrently expands the cybersecurity attack surface across multiple architectural layers, introducing novel vulnerability vectors previously absent in legacy systems [10].

The smart grid architecture encompasses several critical components including the *Advanced Metering Infrastructure (AMI)*, *Supervisory Control and Data Acquisition (SCADA)* systems, *Distributed Energy Resources (DERs)*, communication networks, and end-user devices. Each constituent element presents distinct cybersecurity challenges, collectively forming a highly complex cyber-physical system that poses significant difficulties for overall security implementation. The subsequent analysis examines each component individually, identifying associated risk factors and synthesizing recent Common Vulnerabilities and Exposures (CVEs) with their corresponding Common Vulnerability Scoring System (CVSS) assessments.

1.1.1 Advanced Metering Infrastructure

The Advanced Metering Infrastructure facilitates bidirectional communication channels between utility providers and end consumers, enabling real-time energy consumption monitoring, remote device management capabilities, and implementation of dynamic pricing mechanisms [11]. Although these technological advances substantially improve grid operational efficiency, they simultaneously introduce significant cybersecurity vulnerabilities, particularly manifesting at the smart meter deployment level. Smart meters acquire and transmit energy consumption data, leaving them vulnerable to both unauthorized physical tampering and remote exploitation attempts. Such compromised systems may result in billing data manipulation, energy theft activities, or deliberate service disruption scenarios. Adversaries can exploit inherent weaknesses within communication protocols governing meter-to-utility backend transmission channels, particularly in DLMS/COSEM implementations [12], potentially facilitating unauthorized access to sensitive consumer information or orchestrating distributed denial-of-service attacks against critical infrastructure components.

Table 1.1: Critical Smart Meter Vulnerabilities in Advanced Metering Infrastructure

CVE Identifier	**CVSS**	**Severity**	**Vulnerability Type**	**Affected Component**
CVE-2021-22714	9.8	Critical	Integer Overflow	Schneider ION Smart Meters
CVE-2021-22713	7.5	High	Memory Buffer Overflow	PowerLogic ION Meters
CVE-2016-5809	8.8	High	Access Control Bypass	ION Series Power Meters
CVE-2016-5815	9.8	High	Cross-Site Request Forgery	IONXXXX Smart Meters

The documented vulnerabilities presented in Table 1.1 illustrate the severity of security exposures within smart meter implementations deployed in Advanced Metering Infrastructure, with all identified issues receiving high-to-critical CVSS scores exceeding 7.5. These vulnerabilities demonstrate that attackers can send specially crafted TCP packets to smart meter devices to either cause device reboots or remotely execute code, depending on the architecture

of the targeted device , thereby highlighting the substantial threat confronting modern AMI deployments.

1.1.2 Supervisory Control and Data Acquisition

Supervisory Control and Data Acquisition systems constitute the operational backbone of electrical grid infrastructure, providing comprehensive monitoring and control capabilities for critical assets including substations, transformers, and circuit breakers [13]. The architecture of contemporary SCADA deployments frequently incorporates legacy components that were originally engineered without consideration for modern cybersecurity paradigms. These legacy systems typically operate on obsolete software platforms, lack comprehensive patch management frameworks, and utilize inherently insecure communication protocols that were designed prioritizing functionality over security [14]. Consequently, SCADA infrastructure presents substantial vulnerability surfaces that adversaries may exploit through attacks targeting unpatched software components or leveraging weaknesses in legacy communication protocols. Such exploitation vectors can result in unauthorized access to critical control systems, potentially enabling remote manipulation of grid elements by malicious actors , thereby precipitating operational disruptions, cascading grid failures, or complete compromise of supervisory control functions. The cybersecurity threat landscape affecting SCADA systems demonstrates persistent high-severity vulnerabilities that pose existential risks to grid control integrity and operational continuity.

Table 1.2: Critical SCADA System Vulnerabilities in Smart Grid Infrastructure

CVE Identifier	**CVSS**	**Severity**	**Vulnerability Type**	**Affected System**
CVE-2023-51438	9.8	Critical	Unauthorized Access	Siemens SIMATIC SCADA
CVE-2024-21764	9.8	Critical	Hard-coded Credentials	Rapid SCADA System
CVE-2024-33698	Not Yet Provided	Critical	Buffer Overflow	Siemens UMC Components
CVE-2024-35783	Not Yet Provided	Critical	Privilege Escalation	Siemens SIMATIC PCS 7
CVE-2024-21852	8.8	High	Remote Code Execution	Rapid SCADA Platform

The vulnerability assessment presented in Table 1.2 demonstrates the critical security exposure within SCADA systems deployed across smart grid infrastructure. These vulnerabilities exhibit low attack complexity and remote exploitability characteristics, with two highlited vulnerabilities reaching the score of 9.8 , underscoring the severe threat landscape confronting supervisory control systems. The prevalence of critical-severity exposures across multiple vendor platforms illustrates the systemic cybersecurity challenges inherent in legacy SCADA deployments and emphasizes the urgent need for comprehensive security modernization initiatives

within electrical grid control infrastructure.

1.1.3 Distributed Energy Resources

The integration of Distributed Energy Resources, encompassing photovoltaic systems, wind turbines, and other renewable energy generation technologies, represents a fundamental architectural shift within contemporary smart grid infrastructure [15]. DERs are predominantly managed through prosumer paradigms, wherein end-users function simultaneously as energy producers and consumers, thereby establishing numerous decentralized network entry points that expand the overall attack surface of electrical grid systems.

The critical vulnerability of DER infrastructure to coordinated cyberattacks presents unprecedented risks to grid stability and national security. The U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Energy Response (CESER) emphasized in 2022 that while individual renewable energy resources pose minimal threat, collectively their impact is substantially larger, with sufficiently large DER cyberattacks potentially capable of triggering grid protection mechanisms that could cause localized blackouts [16]. The vulnerability of European grid infrastructure becomes particularly evident when considering that the European Network of Transmission System Operators for Electricity (ENTSO-E) defines 3GW as the "reference incident point"—representing the maximum expected instantaneous power deviation for which the system is designed to respond [17]. Given that European solar capacity reached 336.07 GW by the end of 2023 [18], and considering that the vendors affected by newly discovered vulnerabilities possess cumulative installed generating capacities of approximately 740GW (Sungrow), 300GW (Growatt), and 132GW (SMA) [19], coordinated attacks against these distributed systems could achieve continental grid destabilization.
The operational management of DER assets frequently relies upon Internet of Things devices and cloud-based platforms for real-time monitoring, control, and optimization functions, which often lack comprehensive security implementations commensurate with their critical infrastructure role. These distributed systems present attractive targets for adversaries seeking to manipulate energy production profiles, disrupt power flow dynamics, or establish persistent access to interconnected grid devices. The proliferation of DER deployments correlates directly with an exponential increase in potential attack vectors, particularly when constituent devices implement insufficient authentication mechanisms and inadequate encryption protocols [20, 21].

The vulnerability assessment documented in Table 1.3 illustrates the substantial cybersecurity exposure inherent within DER ecosystem deployments. Following Forescout latest research [19], analysis of over 93 documented vulnerabilities reveals that 32% possess CVSS scores of 9.8 or 10.0, typically indicating that attackers can achieve complete control of affected systems. The most severely affected components include solar monitoring systems (38% of

Table 1.3: Critical Vulnerabilities in Distributed Energy Resource Systems

CVE Identifier	**CVSS**	**Severity**	**Vulnerability Type**	**Affected DER Component**
CVE-2023-28343	9.8	Critical	Command Injection	APsystems Altenergy Platform
CVE-2024-11305	Not Yet Provided	Critical	Remote Code Execution	APsystems Cloud Backend
CVE-2019-19229	6.5	Medium	Path Traversal	Fronius Solar Inverters
CVE-2019-19228	9.8	Critical	Authentication Bypass	Fronius Monitoring Systems
SEDG-2024-1	5.9	Medium	TLS Certificate Bypass	SolarEdge MySolarEdge App

vulnerabilities) and cloud backends (25% of vulnerabilities), with relatively fewer vulnerabilities (15%) directly affecting solar inverters themselves.

1.1.4 End-User Interfaces and Legacy Systems

End-user interfaces, encompassing home energy management systems, smart appliances, and consumer IoT devices, constitute a critical vulnerability domain within smart grid infrastructure, representing the intersection between residential energy systems and broader grid networks. The proliferation of inadequate security practices among consumers, including the persistent use of default authentication credentials and the inability to implement timely software updates, makes these devices attractive and accessible targets for adversarial exploitation [22]. Once compromised, these distributed endpoint devices function as strategic entry points into broader grid infrastructure, enabling sophisticated attack escalation pathways that can propagate to critical operational systems.

The cybersecurity threat landscape has intensified dramatically, with the National Vulnerability Database recording 40,003 CVEs in 2024, representing a 39% increase from 2023's 28,817 CVEs [23] . These increasing number of vulnerabilities demonstrate the systemic exposure of devices, potentially increasing also the exposure of consumer-facing grid technologies. Research indicates that an estimated 80% of IoT devices deployed in smart home environments are vulnerable to wide-ranging cyberattacks , creating extensive attack surfaces that adversaries can exploit to establish persistent access to residential energy management systems and subsequently pivot to utility infrastructure.

The coexistence of contemporary smart grid technologies with legacy operational systems introduces additional architectural complexities that exacerbate cybersecurity vulnerabilities. Legacy systems, predominantly engineered during pre-digital security paradigms, frequently lack support for modern cryptographic protocols and authentication frameworks, creating persistent security gaps that prove both technically challenging and economically prohibitive to address [24]. Critical vulnerabilities in infrastructure management systems, such as CVE-

2024-47575 affecting FortiManager with a CVSS score of 9.8, have demonstrated that missing authentication in critical functions can enable threat actors to execute arbitrary code and steal sensitive configuration data. The substantial financial investment required for comprehensive legacy system modernization often results in organizations maintaining vulnerable infrastructure indefinitely, thereby preserving exploitable attack vectors that sophisticated adversaries can leverage for sustained network persistence.

Table 1.4: Critical Vulnerabilities in End-User Interfaces and Legacy Systems

CVE Identifier	**CVSS**	**Severity**	**Vulnerability Type**	**Affected System**
CVE-2024-47575	9.8	Critical	Missing Authentication	Fortinet FortiManager
CVE-2023-22527	9.8	Critical	Remote Code Execution	Atlassian Confluence
CVE-2024-21887	9.1	Critical	Command Injection	Ivanti Connect Secure
CVE-2023-46805	8.2	High	Authentication Bypass	Ivanti Policy Secure
CVE-2024-21351	7.6	High	Security Feature Bypass	Windows SmartScreen

The vulnerability assessment presented in Table 1.4 demonstrates the severe cybersecurity exposure affecting end-user interfaces and legacy infrastructure systems integrated within smart grid environments. The prevalence of critical-severity exposures across diverse technology platforms underscores the urgent need for comprehensive security frameworks addressing both consumer device management and legacy system modernization within smart grid deployments.

1.2 EPES Standards Analysis

The susceptibility of EPES to sophisticated cyber threats poses a significant risk not only to the operational integrity of these systems but also to the broader infrastructure that depends on a consistent and secure power supply. Various international and national organizations have developed standards for EPES security, including those from ISO, ISA, IEC, and IEEE. Figure 1.1 visually represents the alignment of the Actor identified in NISTIR7628 [25] with the relevant industry standard. It is evident that there is not a specific standard that covers the prosumer integration along with the customer appliances' interaction with the main grid. In this section, we provide a comprehensive assessment of security-related standards associated with smart grid infrastructure. Our analysis delves into analysing the most relevant to smart grid and evaluating their effectiveness in addressing both current and evolving cybersecurity challenges highlighting issues and limitations.

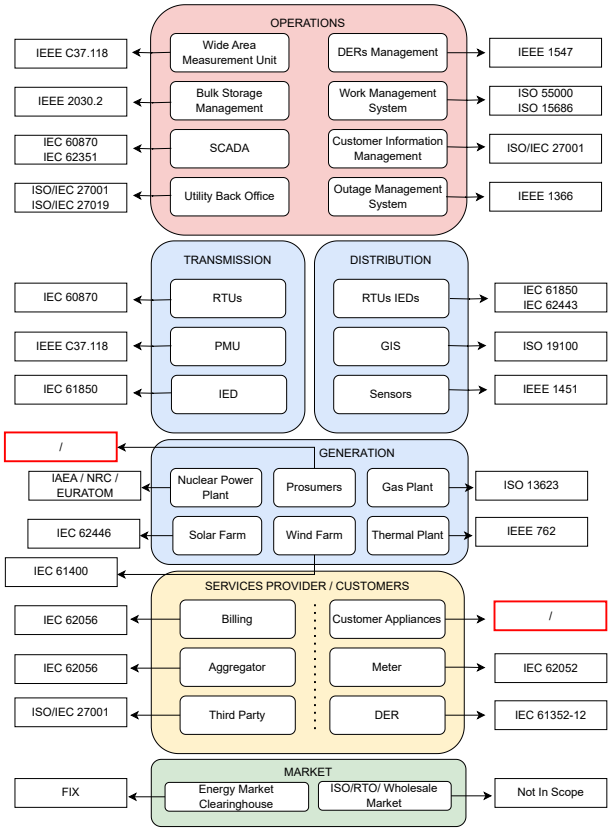


Figure 1.1: The Mapping of The Industry Standard For The Major Actor Presented In The NISTIR 7628

1.2.1 Information Security Management System Standards

The International Organization for Standardization and the International Electrotechnical Commission have developed a comprehensive suite of standards to address information security management across various sectors. The foundational standards ISO/IEC 27001[1] and ISO/IEC 27002[2] establish the fundamental framework for information security management, while sector-specific extensions such as ISO/IEC 27019 provide tailored guidance for specialized industries.

ISO/IEC 27001 constitutes the principal standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). This standard adopts a risk-based approach to information security management, emphasizing the systematic identification, assessment, and treatment of information security risks. The standard is structured around the Plan-Do-Check-Act (PDCA) cycle, ensuring continuous improvement and adaptation to evolving threat landscapes [26]. ISO/IEC 27001 mandates organizations

[1] https://www.iso.org/standard/27001
[2] https://www.iso.org/standard/75652.html

to establish a comprehensive risk management framework that addresses the confidentiality, integrity, and availability of information assets through the implementation of appropriate security controls.
ISO/IEC 27002, conversely, serves as a complementary code of practice that provides detailed implementation guidance for information security controls. While ISO/IEC 27001 establishes the management system framework and requirements, ISO/IEC 27002 offers practical guidance on the selection, implementation, and management of security controls based on the organization's risk assessment outcomes. The standard encompasses 14 security control domains, covering areas such as access control, cryptography, physical and environmental security, and incident management. This complementary relationship ensures that organizations possess both the systematic management framework provided by ISO/IEC 27001 and the practical implementation guidance offered by ISO/IEC 27002.
The fundamental distinction between Information Technology and Operational Technology security paradigms becomes particularly relevant when examining sector-specific implementations. Traditional IT security, as addressed by ISO/IEC 27001 and 27002, prioritizes confidentiality and integrity of information assets. In contrast, OT environments, particularly those found in critical infrastructure sectors, prioritize availability and safety of operational systems, where disruption can result in physical consequences and threats to public safety.

1.2.1.1 ISO/IEC 27019: Energy Sector-Specific Information Security Management

ISO/IEC 27019 represents a sector-specific adaptation of ISO/IEC 27002, developed explicitly to address the unique security requirements and operational characteristics of the energy utility industry. This standard acknowledges that energy sector organizations operate in complex environments where traditional IT systems interface with critical operational technology infrastructure, creating distinct security challenges that require specialized approaches.
The fundamental differentiation of ISO/IEC 27019 from its parent standards lies in its recognition of the energy sector's unique operational context. Energy utilities manage complex interconnected systems that combine legacy control systems with modern digital infrastructure, creating hybrid environments that require specialized security considerations. The standard addresses the critical nature of energy infrastructure, where security incidents can have cascading effects on public safety, economic stability, and national security.

Customer Interface Security Management A critical aspect of ISO/IEC 27019 concerns the management of customer-related security interfaces, as articulated in control 6.1.7 ENR (Energy sector requirement for addressing security when dealing with customers). This control extends beyond the general customer access management principles found in ISO/IEC 27002 by recognizing the complex multi-stakeholder environment characteristic of energy utilities.

The energy sector presents unique challenges in customer relationship management due to the intricate web of relationships between asset owners, system operators, service providers, and end customers. These relationships often involve:

- Internal service providers responsible for transmission or distribution infrastructure operation and maintenance across organizationally separate units
- External service providers managing power generation facilities or distributed energy resources
- Third-party operators of process control infrastructure
- Internal and external customers directly connected to energy supply and process control systems

The standard mandates comprehensive security requirement identification and implementation before granting customer access to organizational information or assets. This approach necessitates careful consideration of the demarcated responsibilities inherent in energy sector business relationships, where operational boundaries may not align with security perimeters. The implementation guidance emphasizes the need for rigorous security assessment when equipment is deployed on customer premises or when process control systems are interconnected across organizational boundaries.

Equipment Security on Customer Premises 11.3.2 ENR – Equipment sited on customer's premises - addresses the critical security challenge of protecting energy utility equipment installed within customer premises. This scenario is ubiquitous in the energy sector, where utilities deploy measurement, control, and service delivery equipment across diverse customer environments. The control mandates comprehensive protection of organizational equipment against environmental threats and unauthorized access while operating in customer-controlled environments.
The implementation of this control requires energy utilities to establish robust security frameworks that account for the reduced physical control over equipment deployed in customer locations. This includes:

- Environmental threat assessment and mitigation strategies for equipment operating in diverse and potentially hostile environments
- Tamper resistance and detection mechanisms to protect against unauthorized physical access
- Secure communication protocols to maintain data integrity and confidentiality across potentially compromised network environments

- Remote monitoring and management capabilities to maintain operational visibility and control

Supply Chain Security Implications The customer-focused controls in ISO/IEC 27019 inherently address critical supply chain security concerns. The complex relationships between energy utilities and their customers, service providers, and equipment suppliers create extended attack surfaces that require comprehensive security management. The standard recognizes that energy sector supply chains are characterized by long-term relationships, critical dependency on specialized equipment, and the integration of multiple vendor technologies within critical infrastructure.
The implementation of customer-related security controls necessitates a comprehensive approach to supply chain risk management, encompassing vendor security assessments, contractual security requirements, ongoing monitoring of third-party security postures, and incident response coordination across organizational boundaries. This approach is essential given the potential for supply chain compromises to propagate across interconnected energy infrastructure, potentially affecting multiple utilities and compromising grid stability.
The differentiation provided by ISO/IEC 27019 in addressing customer interface security and supply chain management reflects the unique position of energy utilities as critical infrastructure providers operating in highly interconnected and interdependent environments. The standard's emphasis on these areas acknowledges that traditional information security approaches, while necessary, are insufficient to address the full spectrum of security challenges faced by energy sector organizations.

1.2.2 Security Industrial Communication Networks Standards

ISA/IEC 62443 The ISA/IEC 62443 standard , developed jointly by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC), is specifically tailored for securing Industrial Automation and Control Systems (IACS). This series of standards and technical reports provides a structured and detailed framework for ensuring the cybersecurity of industrial control systems, which are fundamental in various sectors including manufacturing, energy, and utilities. This standard is structured into several sections as shown in Figure 1.2. Each section addresses different aspects of implementing secure industrial communication networks. This includes defining terminology, establishing security programs, and managing patches. It also specifies system security requirements and technical security needs, while offering an overview of the product development lifecycle requirements. In our discussion, we will describe IEC 61443-3-2, which pertains to system security design, and explore potential ways to enhance the standard. This standard aims to identify the system requiring analysis by offering a standardized approach to describe its architecture, diagrams, and other

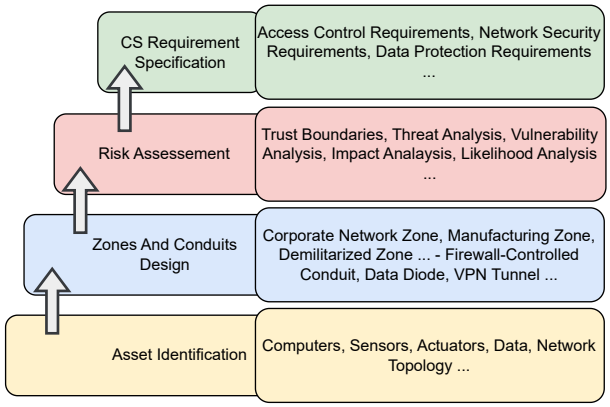


Figure 1.2: IEC 62443-3-2 Standard Process Visualization: From Asset Identification to Cybersecurity Requirements Specification

relevant features. This facilitates conducting a thorough risk assessment and identifying zones and conduits. Additionally, it provides tools for evaluating the threat model. This helps in determining constraints and specifying cybersecurity requirements. The process outlined in the standards includes the initial phase of defining the System Under Control (SUC). This involves integrating the various control systems owned by the facility and identifying the zones and conduits. A security zone is defined as a grouping of systems and components, categorized based on their functional, logical, and physical attributes, which share common security requirements. A conduit is either a logical or physical grouping of communication channels that connect two or more zones, also sharing common security requirements.

1.2.3 Smart Grid Verticals

The shift from the traditional power grid paradigm to the emerging concept of smart grids has presented diverse opportunities for enhancing energy production efficiency and control through monitoring. Nevertheless, this transition has also exposed the entire energy supply chain to novel threats [18]. Interconnected devices, bidirectional information and energy flow, and the integration of legacy SCADA systems with modern IoT devices have opened new avenues for hackers to exploit vulnerabilities and potentially disrupt the power grid [19]. The IEC 62351 standards, purposefully designed for bolstering cybersecurity in smart grids, not only acknowledge these issues but also acknowledge the emerging challenges in safeguarding the evolving power grid. A primary challenge is the rising threat of cyberattacks on critical power infrastructure from various sources. The standards aim to establish robust security measures to protect power systems from evolving threats. Moreover, Digitalization has introduced vulnerabilities in power systems that require attention, particularly regarding unauthorized access and tampering risks. The standards offer guidance on vulnerability identification and

mitigation. Another crucial aspect pertains to recognizing the inherent complexity of achieving interoperability among a wide array of devices and technologies within power systems. The standards offer guidelines for establishing secure communication and data exchange protocols, with a simultaneous focus on addressing security issues prevalent in widely used message protocols within the EPES domain. Of particular significance to our research is the IEC 62351-12 standard, which specifically targets the domain of Distributed Energy Resources from an industry perspective. By examining the synergies and potential points of contact between this industrial viewpoint and prosumer facilities, we aim to present a comprehensive prosumer threat model in the following sections. This model serves as a foundational basis for developing high-level security guidelines aimed at enhancing the resilience of the entire energy supply chain.

1.2.4 NIST IR 8498: Cybersecurity for Smart Inverters

The NIST Interagency Report 8498 establishes a framework of cybersecurity guidelines tailored for smart inverters within residential and light commercial solar energy systems [27]. The document serves as a crucial resource for various stakeholders, including system owners, installers, maintainers, and manufacturers, by delineating a set of best practices to mitigate cyber risks.

The core of the report is centered on seven key recommendations that collectively aim to secure these devices from unauthorized access and potential compromise. These guidelines include the imperative to change default credentials upon installation to prevent attackers from using known, easily guessable passwords. The implementation of role-based access control (RBAC) is also highlighted, ensuring that different user types (e.g., homeowners vs. installers) are granted only the minimum necessary privileges. To aid in incident response, the report recommends configuring the recording of events in a log for security-relevant activities. Proactive security is addressed through the need to update software regularly via a secure method, patching vulnerabilities as they are discovered. The importance of data integrity and business continuity is underscored by the call to back up system information to allow for quick restoration after a cyber event. Furthermore, the report advises disabling unused features to reduce the attack surface and to protect communications connections to prevent interception or manipulation of data transmitted to and from the inverter.

A particularly unique and critical aspect of the report is its formal acknowledgment of the existing limitations within the industry. The document discloses that during a practical assessment, only two out of five commercially available smart inverters were able to fully implement all seven of the proposed guidelines. This finding underscores a significant gap between the recommended cybersecurity best practices and the current capabilities of many products on the market. In doing so, the report not only provides a security roadmap but also serves as a formal acknowledgment of the practical challenges facing the widespread adoption

of these measures. This is of paramount importance because the supply chain compromise of these devices could have a cascading and destabilizing impact on the electrical grid, a critical infrastructure that increasingly relies on the coordinated operation of distributed energy resources. This systemic risk will be a primary focus of the analysis in the chapters that follow.

1.3 Edge Weaponisation: Leveraging Prosumer Infrastructure as Attack Vectors Against Grid Stability

The proliferation of distributed energy resources and the increasing digitization of energy systems, as examined in Sections 1.1.3 and 1.1.4, have fundamentally transformed the attack surface of modern electrical grids. This transformation has introduced a paradigmatic shift from centralized, physically secured infrastructure to a distributed architecture that extends beyond traditional security perimeters into prosumer environments. The integration of prosumer devices—encompassing residential solar installations, energy storage systems, smart inverters, and demand response technologies—has created numerous entry points that exist outside the rigorous security frameworks typically implemented within utility operational environments.

The security implications of this architectural evolution are profound. Prosumer infrastructure represents the most vulnerable segment of the modern energy ecosystem, characterized by minimal security oversight, heterogeneous device implementations, and limited cybersecurity awareness among end users. Unlike industrial control systems that operate within secured facilities under comprehensive monitoring and access control regimes, prosumer devices are deployed in uncontrolled environments with minimal physical security and often default or weak authentication mechanisms. This disparity in security posture creates an asymmetric threat landscape where adversaries can exploit the least protected elements of the grid to achieve disproportionate impact on overall system stability.

The weaponisation potential of prosumer infrastructure emerges from the aggregated capacity of distributed devices to influence grid operations. Individual prosumer installations, while representing minimal threat in isolation, can collectively constitute significant load or generation resources capable of affecting grid frequency, voltage stability, and power flow patterns when compromised and coordinated. This phenomenon transforms distributed energy resources from passive grid endpoints into potential attack vectors that can be leveraged to destabilize critical infrastructure through coordinated manipulation of their operational parameters.

The theoretical foundation for such attacks has been established through various research contributions that demonstrate the feasibility of large-scale grid disruption through coordinated manipulation of distributed resources. These attack scenarios exploit the inherent trust relationships between prosumer devices and grid operators, the limited real-time visibility into

distributed device behavior, and the potential for cascading effects when multiple devices are simultaneously compromised. The technical feasibility of such attacks is further enhanced by the increasing standardization of communication protocols and device interfaces, which creates common vulnerabilities that can be exploited across large populations of similar devices.

This section provides a comprehensive analysis of theoretically demonstrated attack methodologies that leverage prosumer infrastructure to compromise grid stability and reliability. The examination encompasses various attack vectors that have been proposed in academic literature, ranging from direct device manipulation to sophisticated coordinated campaigns that exploit the distributed nature of modern energy systems. The analysis presented herein underscores the urgent necessity for comprehensive security frameworks that extend traditional utility security models to encompass the distributed prosumer ecosystem, thereby addressing the fundamental security gap that exists at the intersection of critical infrastructure and consumer technology domains.

1.3.1 Manipulation of Demand Attacks

The fundamental attack vector that emerges from the weaponisation of prosumer infrastructure centers on the strategic manipulation of electrical demand patterns to destabilise grid operations. Demand manipulation attacks represent the primary threat category wherein adversaries exploit the inherent requirement for continuous supply-demand balance in electrical systems to achieve various malicious objectives. This attack paradigm leverages the unprecedented access to distributed load and generation resources within prosumer environments to orchestrate systematic disruptions that extend far beyond the capabilities of traditional cyber-physical attacks against centralized infrastructure.

The theoretical foundation of demand manipulation attacks rests on the principle that modern electrical grids operate under increasingly stringent stability margins due to the integration of variable renewable energy sources and the decommissioning of traditional synchronous generation. This operational context creates heightened sensitivity to demand-side disturbances, where relatively small coordinated changes in consumption or prosumer generation can precipitate disproportionate system-wide effects.

The attack methodology framework can be systematically classified into two primary dimensions: *attack execution methodologies* that define the technical approaches for achieving demand manipulation, and *attack objectives* that represent the specific grid stability or economic targets adversaries seek to compromise. This taxonomic distinction is critical for understanding how various technical execution vectors can be employed to achieve multiple strategic objectives, and conversely, how specific objectives may be achieved through diverse methodological approaches.

1.3.1.1 Attack Execution Methodologies

The technical implementation of demand manipulation attacks employs several distinct methodological approaches (CLM and DGM), ash shown in Figure 1.3, each exploiting different aspects of prosumer device functionality and grid interface characteristics.

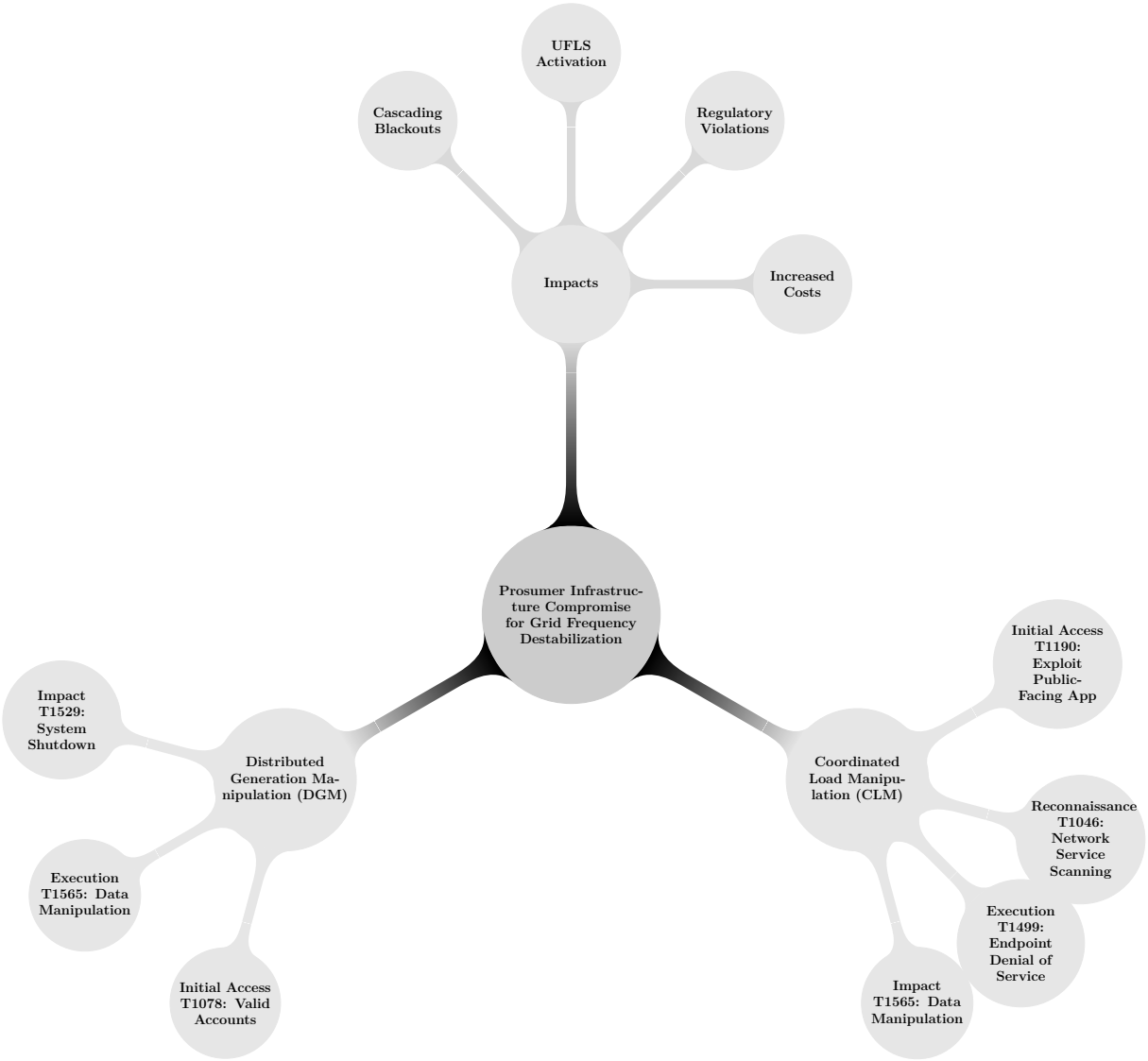


Figure 1.3: Taxonomy of cyberattack vectors targeting prosumer infrastructure for grid frequency destabilization. The hierarchical structure presents two primary attack pathways—Coordinated Load Manipulation (CLM) and Distributed Generation Manipulation (DGM)—with their associated MITRE ATT&CK techniques and resulting impacts on power system stability, including Under-Frequency Load Shedding (UFLS) activation and cascading blackouts.

Coordinated Load Manipulation (CLM) Coordinated Load Manipulation represents the primary execution methodology for achieving demand-side attacks through the orchestrated modification of electrical consumption patterns across multiple prosumer installations. This methodology exploits the aggregated effect of numerous compromised endpoints to achieve system-level impacts that would be impossible through individual device manipulation. The execution framework employs MITRE ATT&CK techniques including *Endpoint Denial of Service* (T1499) through coordinated high-consumption appliance activation, *Data Manipulation* (T1565) for altering power consumption schedules and inverter parameters, and *Service Stop* (T1489) to disable energy efficiency systems during critical operational periods.

The attack methodology follows a systematic multi-stage process that can be classified using the MITRE ATT&CK framework for Industrial Control Systems (ICS). Initial access employs techniques such as *Exploit Public-Facing Application* (T1190) to compromise exposed IoT devices and energy management systems, *Valid Accounts* (T1078) through credential stuffing attacks against prosumer platforms, and *External Remote Services* (T1133) by exploiting remote maintenance interfaces. The reconnaissance phase utilises *Network Service Scanning* (T1046) to identify vulnerable prosumer installations, *Remote System Discovery* (T1018) for mapping residential energy management system topologies, and *Data from Information Repositories* (T1213) through Advanced Metering Infrastructure data exfiltration to analyse consumption patterns.

Persistence and lateral movement implementation leverages *Valid Accounts* (T1078) for maintaining access to compromised systems, *Remote Services* (T1021) for lateral propagation across home automation networks, and *Lateral Tool Transfer* (T1570) to distribute malicious payloads across IoT device ecosystems. Command and control establishment employs *Application Layer Protocol* (T1071) through DNS tunneling and encrypted communications via legitimate cloud services, *Encrypted Channel* (T1573) for secure adversary communications, and *Proxy* (T1090) techniques using compromised prosumer devices as intermediary nodes.

Distributed Generation Manipulation This methodology focuses on the coordinated control of prosumer-owned generation resources, including solar photovoltaic systems, battery energy storage systems, and small-scale wind installations. The approach employs *Data Manipulation* (T1565) to alter Maximum Power Point Tracking (MPPT) algorithms and inverter control parameters, *System Shutdown/Reboot* (T1529) for coordinated generation disconnection, and *Inhibit System Recovery* (T1562.001) to prevent automatic restoration of generation capacity. This methodology enables adversaries to create artificial supply-side constraints that complement demand-side manipulation efforts.

1.3.1.2 Attack Objectives and Impact Scenarios

The strategic objectives of demand manipulation attacks encompass various aspects of grid stability, operational efficiency, and economic functionality. Each objective can be achieved through the application of one or more execution methodologies, creating a flexible attack framework that can be adapted to specific target characteristics and adversary capabilities.

Frequency Stability Disruption This attack objective exploits the fundamental relationship between load-generation imbalance and grid frequency stability through orchestrated rapid switching of large electrical loads to create artificial frequency deviations. The objective leverages the reduced system inertia characteristic of modern power systems with high renewable penetration, making them more susceptible to frequency deviations caused by sudden load changes.

Technical implementation utilises CLM methodologies to execute *Endpoint Denial of Service* (T1499) through rapid load cycling, *Data Manipulation* (T1565) to alter load control algorithms and switching schedules, and *Loss of Control* (T1427) by overwhelming automatic generation control systems.

Impact Assessment: Successful frequency stability attacks can trigger automatic underfrequency load shedding (UFLS) schemes, leading to cascading blackouts across interconnected grid regions. The primary impacts include activation of protective relay systems resulting in widespread service interruptions, forced deployment of expensive emergency generation resources, violation of grid code frequency stability requirements necessitating regulatory intervention, and potential damage to industrial processes sensitive to frequency variations. Long-term consequences encompass reduced grid reliability metrics, increased operational reserve requirements, and elevated system operating costs that ultimately translate to higher consumer energy prices.

Voltage Stability Compromise Voltage stability attacks target the reactive power balance within distribution networks through coordinated manipulation of prosumer-connected equipment, exploiting the voltage-reactive power relationship in electrical networks to create voltage instability that can propagate through interconnected transmission systems. This objective employs both CLM and distributed generation manipulation methodologies to execute *Data Manipulation* (T1565) for altering reactive power control algorithms in inverter-based resources, *Modify Control Logic* (T1562.007) to change power factor correction settings, and *Damage to Property* (T1652) through deliberate voltage instability creation. The attack involves coordinated manipulation of reactive power injection and absorption through inverter-based resources, creating artificial reactive power imbalances that may result in voltage collapse events

in vulnerable network areas.

Impact Assessment: Voltage stability compromise can precipitate localized voltage collapse events that propagate through interconnected transmission networks, potentially leading to regional blackouts. Primary impacts include overvoltage or undervoltage conditions triggering protective equipment disconnection, damage to voltage-sensitive equipment in industrial and commercial facilities, degradation of power quality affecting sensitive electronic loads, and potential physical damage to distribution transformers and other grid infrastructure. Cascading effects encompass reduced transmission system transfer capability, increased reactive power reserve requirements, and potential for dynamic voltage collapse in heavily loaded areas, ultimately compromising grid resilience and requiring extensive infrastructure investment for system recovery.

Duck Curve Amplification This objective specifically targets the characteristic load profile challenges introduced by high penetration of solar photovoltaic systems, exploiting the steep ramping requirements during evening hours when solar generation rapidly declines while residential demand increases. The attack employs distributed generation manipulation methodologies to suppress solar generation during midday hours, followed by sudden restoration or artificial demand injection during critical evening ramping periods. This creates an artificially amplified duck curve effect that can overwhelm grid operators' ability to manage the transition between renewable and conventional generation sources, potentially leading to load shedding events or emergency generation deployment.

Impact Assessment: Duck curve amplification attacks exploit the operational vulnerabilities inherent in high renewable penetration grids, potentially causing ramping capability shortfalls that exceed available flexible generation resources. Primary impacts include forced activation of expensive peaking generation units during evening hours, inability to meet ramping requirements leading to emergency load shedding, increased grid instability during critical transition periods, and accelerated cycling of conventional generation units reducing their operational lifespan. Economic consequences encompass dramatic electricity price spikes during evening peak periods, increased integration costs for renewable energy sources, potential curtailment of renewable generation during off-peak periods, and reduced investor confidence in renewable energy deployment programs. Long-term systemic impacts include delayed renewable energy transition goals and increased reliance on fossil fuel backup generation resources.

Economic Market Disruption Economic manipulation attacks target energy market mechanisms and pricing structures through coordinated prosumer behaviour modification, exploiting

the increasing integration of prosumer resources into energy markets and demand response programs. This objective utilises CLM methodologies to implement *Financial Theft* (T1657) through market manipulation and artificial price volatility creation, *Data Manipulation* (T1565) to alter demand response participation algorithms, and *Fraud* (T1659) by exploiting net metering and feed-in tariff mechanisms. While these attacks may not directly threaten grid stability, they can cause significant economic disruption and undermine market confidence in prosumer integration programs.

Impact Assessment: Economic market disruption attacks primarily target the financial mechanisms underpinning energy market operations, potentially causing widespread market manipulation and fraud. Primary impacts include artificial electricity price volatility undermining market predictability, exploitation of demand response programs resulting in inappropriate compensation payments, manipulation of net metering and feed-in tariff mechanisms causing revenue losses for utilities, and reduced participation in voluntary demand response programs due to compromised system integrity. Secondary effects encompass increased regulatory compliance costs for market operators, reduced investor confidence in demand-side management programs, potential legal liability for utilities managing compromised prosumer resources, and erosion of public trust in smart grid economic incentives. Long-term consequences include delayed deployment of demand response technologies, increased regulatory oversight costs, and potential restructuring of prosumer compensation mechanisms to address security vulnerabilities.

1.3.1.3 Threat Modelling and Attacks: Research Highligths

BlackIoT: Soltan et Al. Soltan et al. [28] have conducted a detailed study on the potential consequences of MadIoT attacks on the operation of the power grid. Their work identifies and analyses several key vulnerabilities and the possible impacts of these attacks. The study utilised publicly available data sets to model the power grid and simulate the effects of MadIoT attacks. They acknowledge that these data sets may not fully represent all existing power grids, suggesting that while the simulations provide valuable insights, they may not capture the full extent of vulnerabilities in every power grid.

The research highlighted the risk posed by high-wattage IoT devices such as air conditioners and water heaters. These devices, if compromised, can cause significant disruptions. Air conditioners with large capacitors, for instance, take several seconds to reach peak load, making them less effective for sudden demand spikes but still a risk for other types of attacks like line failures.

The study did not fully account for existing control mechanisms that mitigate the effects of initial failures, such as preventive load-shedding. Therefore, their analysis primarily reflects worst-case scenarios where these mitigating controls fail or are absent. Unlike DDoS attacks,

MadIoT attacks require that the compromised IoT devices be geographically located within the boundaries of a power system. This constraint makes it challenging to amass a sufficient number of bots within a targeted area to execute a large-scale attack, although it remains a plausible threat given the size of modern botnets like Mirai [29].
Using state-of-the-art simulators, Soltan et al. demonstrated that MadIoT attacks could lead to both local outages and large-scale blackouts, depending on the scale of the attack and the specific operational properties of the power grid. The research also explored the economic ramifications of MadIoT attacks, showing that such attacks could increase the operating costs of the grid, benefiting certain utilities within the electricity market by manipulating demand and supply dynamics.
Soltan et al. emphasised the importance of raising awareness among grid operators, smart appliance manufacturers, and security experts. Their work underscores the need for enhanced security measures and protocols to protect against these emerging threats, especially as the proliferation of internet-connected smart appliances continues to grow.

MaMIoT: Tohid Shekari et al. In their paper, Tohid Shekari et al. [30] introduced MaMIoT, the first energy market manipulation cyberattack in which an adversary can slightly alter the power system real-time demand through a botnet of high-wattage IoT devices. This attack can help market players gain additional profit from the electricity market or cause significant economic damage to a set of market players. The study evaluated the attack models on real datasets from two major electricity markets in the U.S., the California and New York markets. The simulation results revealed that with a botnet of just 200,000 bots, an attacker could cause economic damage worth 2.8 million USD and 3.8 million USD to the demand and generation side players of the California and New York markets, respectively. Additionally, the MaMIoT attack could enable a typical power plant owner to gain an additional 30% profit from the energy market, while maintaining stealth for increased repeatability.
The paper underscores the importance of making electricity markets more secure against such cyberattacks, especially as the number of smart appliances with Internet connectivity continues to grow.

Thermostat Attacks: Yan et al. Yan et al. [31] examined the vulnerabilities and impacts of cyberattacks on power systems, focusing on the manipulation of demand (MAD) attacks through compromised thermostatically controlled loads (TCLs). They highlighted incidents in Ukraine [32] and Venezuela [33] as motivations for their research, which underscores the susceptibility of power systems to cyberattacks due to poor network security measures on large-scale controllable loads.

Their study reveals that compromised TCLs, such as air conditioners equipped with IoT

devices, can be manipulated to cause significant harm to power systems. The research demonstrates how MAD attacks can generate malicious electricity demand, impacting both the physical operation of the grid and the financial stability of electricity market participants. The study emphasises that these attacks can be highly concealable, as they operate within the acceptable temperature range for end-use consumers (EUCs), making them difficult to detect.

Yan et al. proposed an attack model based on the response characteristics of compromised TCLs and assessed the potential economic loss and unfair competition in the electricity market caused by these MAD attacks. Their findings highlight the need for improved network security standards for IoT devices associated with TCLs and raise awareness among power grid operators, IoT device manufacturers, and power retailers (PRs) about the significance of these threats.

AMI Attack: El-Nasser et Al. El-Nasser et al. [34] have focused on the potential impacts of cyberattacks on Advanced Metering Infrastructure within the utility's DMZ or third-party WAN. They assume that attackers can infiltrate the AMI through malware delivered to utility systems or third-party WAN providers, using methods such as insider cooperation or infected email attachments. Once the malware is installed, it provides attackers with backdoor access, enabling reconnaissance to learn how to communicate with Electric Water Heaters (EWHs) in the Demand Load Control (DLC) peak shaving program.

Attackers can then inject malicious activation commands to numerous EWHs during peak shaving periods, causing them to simultaneously turn on and create a demand surge. This surge can lead to various grid issues, including increased operating costs, power quality deterioration, voltage problems, equipment damage, line overloads, cascading failures, and potentially large-scale blackouts.

Their study illustrates the impact of such an attack on the Diversified Load Profile (DLP), showing sharp demand increases resulting from the malicious activation of EWHs. The resistive nature of EWH loads contributes to the instantaneous demand surge, making it challenging to respond quickly, especially in large-scale attacks. The study underscores the importance of having mitigation mechanisms to defend the grid against these types of cyberattacks.

Chapter 2

Legal Efforts and Regulatory Frameworks for Prosumer Security Integration

2.1 European Legislative Framework Analysis

The increasing integration of distributed energy resources and prosumer technologies within critical energy infrastructure necessitates a comprehensive examination of the applicable regulatory framework governing cybersecurity, operational security, and legal accountability. This section provides a systematic analysis of the current European legislative landscape, focusing on three fundamental domains: cybersecurity requirements for critical infrastructure, device certification and organizational compliance mechanisms, and legal responsibility frameworks including data protection considerations. The analysis aims to identify regulatory gaps and compliance challenges specific to distributed energy systems, particularly concerning prosumer infrastructure that operates beyond traditional organizational security perimeters.

2.1.1 Network and Information Systems Security Directive (NIS2)

The Network and Information Systems Security Directive 2022/2555 (NIS2) [35] represents the cornerstone of European cybersecurity legislation for critical infrastructure sectors, establishing harmonized minimum security requirements across member states. As a directive requiring national transposition, NIS2 mandates comprehensive cybersecurity measures for entities whose disruption could have significant societal and economic impacts, particularly within the energy sector.

2.1.1.1 Regulatory Framework and Scope

The directive establishes a two-tier classification system distinguishing between essential entities and important entities based on criticality, scale, and potential impact. Essential entities, as defined in Article 3, encompass organizations that exceed medium-sized enterprise thresholds, provide critical services, or are designated by member states due to their strategic importance. Important entities, while not meeting essential entity criteria, remain significant contributors to sectoral resilience and are enumerated in Annexes I and II.

Within the energy sector context, Annex I identifies "producers" as covered entities, referencing the definition established in Article 2 of the Electricity Directive 2019/944 [36]. This definition encompasses "any natural or legal person who generates electricity," creating potential ambiguity regarding the inclusion of distributed energy resources, prosumer installations, and small-scale generation assets within the directive's scope.

The application of NIS2 to distributed energy systems presents significant interpretative challenges that warrant detailed examination. While individual prosumer installations may not meet the quantitative thresholds for essential or important entity classification, their collective impact on grid stability and security may necessitate regulatory consideration. The cumulative capacity and influence of distributed energy resources can reach levels comparable to traditional centralized generation assets, and when assessed collectively, distributed prosumer installations may represent critical infrastructure whose disruption could significantly impact energy security and grid stability.

Furthermore, prosumer devices are increasingly integrated into smart grid networks, automated demand response systems, and virtual power plant configurations, creating systemic dependencies where individual device compromises can propagate across interconnected infrastructure. While the dispersed nature of prosumer infrastructure reduces single points of failure, it simultaneously expands the attack surface and complicates security monitoring and incident response capabilities.

2.1.1.2 Implementation Challenges and Security Requirements

Article 7 mandates the development of National Cybersecurity Strategies incorporating risk assessment mechanisms and asset identification procedures, specifically requiring "a mechanism to identify relevant assets and an assessment of the risks." This requirement assumes particular significance in distributed energy contexts, where asset identification and risk assessment must account for numerous small-scale installations operating under diverse ownership and management structures. The directive also emphasizes the enhancement of "cybersecurity awareness among citizens," directly addressing the prosumer context where individual citizens become critical infrastructure operators requiring appropriate cybersecurity knowledge and awareness.

Table 2.1: NIS2 Directive: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Systems**
Classification Ambiguity	Essential/important entity framework inadequately addresses collective criticality of distributed assets	Individual prosumer installations fall below thresholds but collectively represent critical infrastructure
Compliance Scalability	Security requirements designed for large organizations are infeasible for small-scale operators	Technical and economic barriers prevent effective implementation of organizational-level security measures
Enforcement Challenges	Traditional compliance monitoring mechanisms lack scalability for distributed environments	Regulatory oversight becomes impractical with numerous small-scale participants
Incident Response Coordination	Frameworks assume organizational structures capable of coordinated response	Distributed operators lack formal incident response capabilities and coordination mechanisms

Article 21 establishes mandatory security measures for network and information system protection, several of which present implementation challenges in distributed energy environments. Supply chain security requirements become particularly complex in distributed energy systems, where prosumer devices may be procured through diverse channels with varying security standards. The heterogeneous nature of prosumer equipment, spanning multiple manufacturers and technology generations, complicates comprehensive supply chain risk assessment and management.

Security requirements throughout system acquisition, development, and maintenance phases must account for the consumer-grade nature of many prosumer devices, which may lack enterprise-level security features and update mechanisms. Vulnerability management becomes challenging when device ownership and maintenance responsibilities are distributed across numerous individual prosumers. Additionally, traditional organizational security controls for human resources, access management, and asset control require adaptation for distributed environments where device operators may lack formal cybersecurity training and organizational oversight.

2.1.1.3 NIS2 Regulatory Gap Analysis and Legislative Recommendations

The analysis reveals a fundamental tension between NIS2's organizational-centric approach and the distributed nature of modern energy infrastructure. While the directive's scope theoretically encompasses electricity producers regardless of scale, its implementation framework presupposes traditional organizational structures with centralized security management capabilities. This discrepancy creates several critical regulatory gaps that require systematic addressing to ensure comprehensive cybersecurity coverage for distributed energy systems.

The primary regulatory gaps encompass classification ambiguities, compliance scalability challenges, enforcement limitations, and coordination deficiencies. Classification ambiguity emerges from the essential/important entity framework's inadequate treatment of collective criticality, where distributed assets that individually fall below regulatory thresholds may collectively represent critical infrastructure requiring regulatory oversight. Compliance scalability presents significant challenges as security requirements designed for large organizational entities may be technically or economically infeasible for individual prosumers or small-scale distributed resource operators, creating implementation barriers that undermine regulatory effectiveness.

Enforcement challenges arise from traditional compliance monitoring and enforcement mechanisms that are ill-suited to distributed environments with numerous small-scale participants, lacking the scalability and granularity necessary for effective oversight. Incident response coordination difficulties stem from existing frameworks that assume organizational structures capable of coordinated response, which may not exist in distributed prosumer environments where individual operators lack formal incident response capabilities or organizational coordination mechanisms.

The identified regulatory gaps, summarised in Table 2.1, necessitate systematic legislative and regulatory adaptations to address the unique characteristics of distributed energy infrastructure. The current regulatory framework, while comprehensive in scope, requires evolution to address the security challenges posed by the energy sector's transition toward distributed, digitalized infrastructure. Without appropriate regulatory adaptation, these gaps may undermine the effectiveness of critical infrastructure protection efforts and create systemic vulnerabilities in modernized energy systems.

Regulatory Development Recommendations for Legislative Bodies - NIS2

To address the identified regulatory gaps and ensure effective cybersecurity governance for distributed energy infrastructure, the following legislative adaptations are recommended for regulatory authorities and policy makers:

Graduated Regulatory Framework Implementation: Legislative bodies should consider developing tiered regulatory structures that apply proportionate security requirements based on aggregated risk assessment rather than individual entity characteristics. This approach should incorporate collective compliance mechanisms for distributed resource aggregators, virtual power plant operators, and prosumer cooperatives, enabling scaled regulatory oversight while maintaining proportionality.

Technology-Neutral Security Standard Establishment: Regulatory frameworks should establish minimum cybersecurity standards applicable across diverse prosumer technologies, focusing on essential security functions rather than prescriptive implementation approaches. These standards should address authentication, encryption, secure communication protocols, and vulnerability management capabilities while remaining technology-agnostic to accommodate innovation and technological evolution.

Shared Responsibility Model Development: Legislative frameworks should explicitly define and allocate cybersecurity responsibilities among prosumers, distribution system operators, device manufacturers, energy service companies, and regulatory authorities. This allocation should consider technical capabilities, economic feasibility, and operational responsibilities while ensuring comprehensive security coverage across the distributed energy ecosystem.

Adaptive Regulatory Mechanism Integration: Regulatory frameworks should incorporate mechanisms for periodic review and adaptation to address emerging threats, technological developments, and evolving system architectures. This should include provisions for regulatory sandboxes, pilot programs, and stakeholder consultation processes that enable responsive regulatory evolution.

2.1.2 Commission Recommendation (EU) 2019/553 - Cybersecurity in the Energy Sector

Commission Recommendation (EU) 2019/553 [37] addresses the cybersecurity challenges accompanying the European energy sector's transformation toward a decarbonized economy while maintaining security of supply and competitiveness. As the Commission states, *"The European energy sector is undergoing an important change towards a decarbonised economy, while ensuring security of supply and competitiveness."* This non-legally binding instrument provides guidance to energy operators for securing critical energy infrastructure through comprehensive cybersecurity measures, establishing foundational principles for cybersecurity governance in modernized energy systems that increasingly incorporate distributed resources and prosumer participation.

2.1.2.1 Regulatory Framework and Technical Requirements

The Commission Recommendation establishes cybersecurity guidance across three critical operational dimensions: real-time requirements, cascading effect mitigation, and legacy technology integration challenges. These dimensions collectively address the technical and operational complexities inherent in modern energy infrastructure, particularly concerning the integration of emerging technologies and distributed resources.

The real-time requirements framework mandates that energy network operators apply the most recent security standards for new installations wherever adequate, while considering complementary physical security measures where legacy installations cannot be sufficiently protected by cybersecurity mechanisms alone. The recommendation emphasizes systematic approach through logical zone segmentation, requiring operators to *"split the overall system into logical zones and within each zone, define time and process constraints in order to enable the application of suitable cybersecurity measures or to consider alternative protection methods."* This segmentation approach enables proportionate security implementation based on criticality and operational characteristics.

Cascading effect mitigation represents a central concern of the recommendation, explicitly requiring energy operators to *"ensure that new devices, including Internet of Things devices, have and will maintain a level of cybersecurity appropriate to a site's criticality"* and to *"establish design criteria and an architecture for a resilient grid."* The framework mandates implementation of defense-in-depth measures per site, tailored to site criticality, while *"identifying critical nodes, both in terms of power production capacity and customer impact, and collaborating with other relevant operators and with technology suppliers to prevent cascading effects by applying appropriate measures and services."*

The legacy and state-of-the-art technology integration dimension addresses the challenges

posed by heterogeneous technology environments. Energy operators must *"analyse the risks of connecting legacy and Internet of Things concepts and be aware of internal and external interfaces and their vulnerabilities"* while taking *"suitable measures against malicious attacks originating from large numbers of maliciously controlled consumer devices or applications."* Additionally, operators must *"update software and hardware of legacy and Internet of Things systems to the most recent version whenever adequate,"* establishing comprehensive lifecycle management requirements.

2.1.2.2 Implementation Challenges and Prosumer Integration

The recommendation explicitly acknowledges the distributed nature of modern energy systems, mandating that *"Member States should encourage energy network operators and technology suppliers to follow the relevant internationally accepted standards on cybersecurity wherever possible. Meanwhile, stakeholders and customers should adopt a cybersecurity-oriented approach when connecting devices to the grid."* This recognition directly addresses the expanding attack surface created by distributed energy resources and prosumer participation in energy markets.

The requirement for energy operators to implement measures against attacks *"originating from large numbers of maliciously controlled consumer devices or applications"* explicitly recognizes prosumer devices as potential attack vectors requiring systematic security management. However, the recommendation's organizational-centric approach assumes direct control or influence over connected devices that may not exist in prosumer environments, where individual device owners operate independently of traditional utility oversight structures.

While the Commission Recommendation provides valuable guidance for traditional energy infrastructure, its application to distributed prosumer environments reveals significant implementation challenges. The recommendation's focus on energy network operators and technology suppliers does not adequately address the distributed ownership and management structures characteristic of prosumer installations. Individual prosumers typically lack the technical expertise, economic resources, and organizational structures necessary to implement comprehensive cybersecurity measures as envisioned for traditional energy operators.

Furthermore, the recommendation's emphasis on collaboration between operators and technology suppliers does not extend to the complex multi-stakeholder environment of distributed energy systems, where prosumers, aggregators, energy service companies, and device manufacturers create intricate interdependencies that require coordinated security approaches beyond traditional operator-supplier relationships.

2.1.2.3 Commission Recommendation Regulatory Gap Analysis and Legislative Recommendations

The analysis reveals that while Commission Recommendation (EU) 2019/553 provides comprehensive guidance for traditional energy infrastructure cybersecurity, its non-binding nature and organizational focus create significant implementation challenges for distributed energy systems. The recommendation's emphasis on energy network operators and technology suppliers inadequately addresses the unique characteristics of prosumer infrastructure, where ownership, operation, and security responsibilities are distributed across numerous individual actors operating outside traditional utility management structures.

The primary regulatory gaps encompass scope limitations, implementation scalability challenges, enforcement mechanisms, and stakeholder coordination deficiencies. Scope limitations arise from the recommendation's focus on energy network operators and technology suppliers, which inadequately addresses the distributed ownership and management structures characteristic of prosumer installations where individual actors operate independently. Implementation scalability challenges emerge from recommendations designed for organizational entities with dedicated cybersecurity resources, technical expertise, and formal security management capabilities that individual prosumers typically lack.

Enforcement mechanism deficiencies stem from the recommendation's non-binding nature, which relies entirely on voluntary compliance without mechanisms for ensuring systematic implementation across distributed prosumer environments. This creates potential security gaps where individual prosumer installations may remain unprotected despite their collective potential impact on grid stability. Stakeholder coordination challenges arise from the complex multi-actor environment of distributed energy systems, where traditional operator-supplier relationships do not adequately represent the diverse stakeholder ecosystem including individual prosumers, aggregators, energy service companies, and device manufacturers.

The identified regulatory gaps, summarised in Table 2.2 demonstrate the need for complementary guidance specifically addressing distributed energy infrastructure characteristics. While the Commission Recommendation provides valuable foundational principles for energy sector cybersecurity, its application to prosumer environments requires adaptive implementation approaches that account for distributed ownership, limited technical resources, and diverse stakeholder coordination requirements. Without appropriate adaptation, these gaps may undermine the effectiveness of cybersecurity implementation across the increasingly distributed energy infrastructure landscape.

Table 2.2: Commission Recommendation 2019/553: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Systems**
Scope Limitations	Focus on energy network operators and suppliers inadequately addresses distributed ownership structures	Prosumer installations and small-scale DER operators fall outside primary guidance scope
Implementation Scalability	Recommendations designed for organizational entities with dedicated cybersecurity resources	Individual prosumers lack technical capabilities and economic resources for comprehensive implementation
Enforcement Mechanisms	Non-binding nature relies on voluntary compliance without systematic oversight mechanisms	Lack of mandatory requirements undermines systematic security implementation across distributed environments
Stakeholder Coordination	Traditional operator-supplier relationships inadequately represent complex multi-actor environments	Diverse stakeholder ecosystem including prosumers, aggregators, and service providers lacks coordination framework

Regulatory Development Recommendations for Legislative Bodies - CR2019/553

To address the identified regulatory gaps and enhance the applicability of cybersecurity guidance to distributed energy infrastructure, the following legislative and regulatory adaptations are recommended for policy makers and regulatory authorities:

Prosumer-Specific Security Guidance Development: Regulatory authorities should develop complementary guidance specifically addressing prosumer environments, including simplified security requirements appropriate for individual operators and small-scale distributed resource installations. This guidance should translate organizational-level security principles into actionable measures for non-technical prosumer operators while maintaining essential security functions.

Binding Regulatory Framework Integration: Legislative bodies should consider incorporating critical elements of the Commission Recommendation into binding regulatory frameworks, particularly concerning device security requirements and grid connection standards. This integration should include mandatory minimum security standards for grid-connected devices and enforcement mechanisms appropriate for distributed environments.

Multi-Stakeholder Coordination Mechanism Establishment: Regulatory frameworks should establish formal coordination mechanisms among energy network operators, prosumers, device manufacturers, aggregators, and service providers to ensure systematic cybersecurity implementation across distributed energy systems. These mechanisms should include information sharing protocols, incident response coordination, and collaborative threat assessment processes.

Graduated Implementation Support Framework: Regulatory authorities should develop support mechanisms that enable effective implementation of security measures across diverse prosumer capabilities, including technical assistance programs, economic incentives for security compliance, and collective compliance mechanisms for prosumer cooperatives and virtual power plant configurations.

2.1.3 EU Network Code on Cybersecurity for the Electricity Sector (Commission Delegated Regulation (EU) 2024/1366)

Commission Delegated Regulation (EU) 2024/1366 [38] establishes the EU Network Code on cybersecurity for the electricity sector, recently adopted under the framework of Regulation (EU) 2019/943 (the "Electricity Regulation"). This network code represents a significant development in sector-specific cybersecurity regulation, addressing cybersecurity aspects of cross-border electricity flows through comprehensive rules on common minimum requirements, planning, monitoring, reporting, and crisis management. While primarily focused on international energy exchanges and transmission system operator (TSO) responsibilities, the regulation introduces systematic risk assessment procedures that have broader implications for distributed energy infrastructure security.

2.1.3.1 Regulatory Framework and Risk Assessment Methodologies

The Network Code establishes comprehensive cybersecurity risk assessment frameworks that mandate systematic evaluation of cyber threats across Union, regional, and Member State levels. Article 18 requires TSOs to jointly develop proposals for cybersecurity risk assessment methodologies, creating harmonized approaches for threat identification, impact evaluation, and risk management across interconnected European electricity systems. These methodologies must incorporate comprehensive threat catalogs and systematic impact assessment criteria that extend beyond traditional transmission-level considerations.

The regulation mandates inclusion of supply chain threats as fundamental components of cybersecurity risk assessment, requiring consideration of *"attacks that cause a severe and unexpected corruption of the supply chain," "cyber-attacks initiated through actors in the supply chain,"* and *"the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain."* This comprehensive approach to supply chain security recognizes the distributed and interconnected nature of modern energy systems, where vulnerabilities can propagate across multiple system components and stakeholder boundaries.

The risk impact assessment framework established by Article 18 provides systematic criteria for measuring consequences of cyber-attacks, including *"loss of load," "reduction of power generation," "loss of capacity in the primary frequency reserve,"* and *"loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called 'black start')."* Additionally, the framework incorporates customer impact assessment through evaluation of *"the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers,"* combined with likelihood measurements based on attack frequency of

occurrence.

The regulation establishes *"criteria to evaluate the impact of cybersecurity risks as high or critical, using defined thresholds for consequences and likelihood,"* creating systematic frameworks for prioritizing cybersecurity investments and response measures. This risk-based approach enables proportionate resource allocation and ensures focus on the most critical vulnerabilities and highest-impact scenarios.

2.1.3.2 Implementation Challenges and Prosumer Integration

While the Network Code primarily addresses transmission-level cybersecurity and cross-border electricity flows, its risk assessment methodologies and supply chain security requirements have significant implications for distributed energy infrastructure. The regulation's emphasis on supply chain threats directly acknowledges the potential for cyber-attacks to originate from distributed components, including prosumer installations that form part of the broader energy supply chain.

The Network Code's focus on TSO responsibilities creates implementation challenges when addressing distributed energy resources that operate beyond traditional transmission system boundaries. Prosumer installations, while not directly regulated under this framework, can significantly impact the consequences measured by the regulation's risk assessment criteria, including load loss, generation reduction, and customer outage impacts. However, the regulation does not establish mechanisms for systematic inclusion of prosumer-related risks in TSO risk assessment processes.

The supply chain security requirements, while comprehensive in scope, assume organizational relationships and control mechanisms that may not exist in distributed prosumer environments. The regulation's emphasis on preventing backdoors and weaknesses in ICT products and services requires coordination across diverse stakeholder groups, including individual prosumers who may lack the technical expertise or economic resources to implement comprehensive supply chain security measures.

Furthermore, the regulation's crisis management and reporting requirements focus on TSO capabilities and responsibilities, potentially creating gaps in situational awareness when incidents originate from or involve distributed prosumer infrastructure. The systematic impact assessment criteria established by the regulation may not adequately capture cascading effects that originate from compromised prosumer installations but manifest as transmission-level impacts.

2.1.3.3 Network Code Regulatory Gap Analysis and Legislative Recommendations

The analysis reveals that while the EU Network Code on cybersecurity establishes comprehensive risk assessment methodologies for transmission-level infrastructure, its TSO-centric

approach creates significant gaps in addressing distributed energy security challenges. The regulation's focus on cross-border electricity flows and transmission system cybersecurity does not adequately account for the distributed nature of modern energy systems, where prosumer installations can significantly influence the risk scenarios and impact criteria established by the Network Code.

The primary regulatory gaps encompass scope limitations, risk assessment integration challenges, coordination mechanism deficiencies, and implementation authority boundaries. Scope limitations arise from the Network Code's primary focus on TSO responsibilities and cross-border flows, which inadequately addresses the distributed energy resources that can influence transmission system security and the risk scenarios defined by the regulation. Risk assessment integration challenges emerge from the lack of systematic mechanisms for incorporating prosumer-related risks into TSO risk assessment methodologies, despite prosumer installations' potential to contribute to the impact criteria established by the regulation.

Coordination mechanism deficiencies stem from the absence of formal frameworks for information sharing and threat intelligence exchange between TSOs and distributed energy stakeholders, including prosumers, aggregators, and distribution system operators. Implementation authority boundaries create challenges where TSOs lack direct authority or visibility over distributed resources that can influence transmission system security, yet remain responsible for comprehensive risk assessment and crisis management under the Network Code requirements.

The identified regulatory gaps, summarised in Table 2.3, demonstrate the need for enhanced coordination mechanisms and expanded risk assessment approaches that systematically incorporate distributed energy infrastructure considerations. While the Network Code establishes robust risk assessment methodologies for transmission-level cybersecurity, its effective implementation requires complementary frameworks that address the distributed nature of modern energy systems and the potential for prosumer infrastructure to influence transmission system security and resilience.

Table 2.3: Network Code 2024/1366: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Systems**
Scope Limitations	TSO-centric focus inadequately addresses distributed energy resources influencing transmission security	Prosumer installations affecting transmission-level risks remain outside systematic assessment scope
Risk Assessment Integration	Lack of systematic mechanisms for incorporating distributed energy risks into TSO methodologies	Prosumer-related vulnerabilities may not be captured in comprehensive transmission system risk assessments
Coordination Mechanisms	Absence of formal information sharing frameworks between TSOs and distributed energy stakeholders	Limited visibility and coordination capabilities for threats originating from or involving prosumer infrastructure
Implementation Authority	TSOs lack direct authority over distributed resources affecting transmission system security	Responsibility-authority misalignment undermines comprehensive risk management and crisis response capabilities

Regulatory Development Recommendations for Legislative Bodies - Commission Delegated Regulation (EU) 2024/1366

To address the identified regulatory gaps and enhance the Network Code's effectiveness in addressing distributed energy security challenges, the following legislative and regulatory adaptations are recommended for policy makers and regulatory authorities:

Distributed Energy Risk Assessment Integration: Regulatory frameworks should establish systematic mechanisms for incorporating distributed energy resources into TSO risk assessment methodologies required by the Network Code. This should include formal procedures for distribution system operators and prosumer aggregators to contribute threat intelligence and vulnerability information to transmission-level risk assessments.

Multi-Level Coordination Framework Development: Legislative bodies should mandate formal coordination mechanisms between TSOs, distribution system operators, and distributed energy stakeholders to ensure comprehensive threat visibility and coordinated response capabilities. These frameworks should establish information sharing protocols, joint threat assessment processes, and coordinated crisis management procedures across transmission and distribution system boundaries.

Supply Chain Security Extension: Regulatory authorities should extend supply chain security requirements established by the Network Code to include distributed energy equipment and prosumer devices that can influence transmission system security. This should include mandatory security standards for grid-connected devices and systematic supply chain risk assessment procedures for distributed energy technologies.

Graduated Authority and Responsibility Alignment: Legislative frameworks should establish clear authority and responsibility allocations that enable TSOs to fulfill Network Code requirements while accounting for distributed energy infrastructure. This should include mechanisms for TSO oversight of critical distributed resources and collaborative governance structures for shared cybersecurity responsibilities across transmission and distribution system levels.

2.1.4 Cybersecurity Act (Regulation (EU) 2019/881)

Regulation (EU) 2019/881, commonly known as the Cybersecurity Act [39], establishes a comprehensive framework for cybersecurity certification of ICT products, services, and processes across the European Union. This regulation addresses the growing need for harmonized cybersecurity standards in an increasingly digital and interconnected economy, with particular relevance to distributed energy systems where numerous ICT-enabled devices require appropriate security assurance. The Act establishes the legal foundation for European cybersecurity certification schemes, defining security levels, conformity assessment procedures, and market surveillance mechanisms that directly impact prosumer devices and distributed energy infrastructure components.

2.1.4.1 Regulatory Framework and Certification Requirements

The Cybersecurity Act establishes a tiered certification framework with three distinct security levels: basic, substantial, and high, each corresponding to different risk profiles and security requirements. Basic level certification addresses products with limited cybersecurity risks, substantial level targets products where cybersecurity incidents could have significant negative impact, while high level certification applies to products where cybersecurity failures could have catastrophic consequences. This graduated approach enables proportionate security requirements based on the criticality and potential impact of different ICT products and services.

The regulation mandates that cybersecurity certification schemes shall specify the categories of ICT products, services, and processes covered, define the cybersecurity requirements and evaluation criteria for each security level, and establish the evaluation methods to be used by conformity assessment bodies. For distributed energy systems, this framework is particularly relevant as prosumer devices including smart inverters, energy management systems, electric vehicle charging stations, and battery storage systems may fall under various certification requirements based on their potential impact on grid operations and customer safety.

Article 46 establishes specific requirements for cybersecurity risk assessments that must consider the state of the art of cybersecurity measures, the economic feasibility of implementing security measures, and the severity and likelihood of cybersecurity risks. The regulation requires systematic evaluation of potential vulnerabilities, threat scenarios, and impact assessments that encompass both individual device security and broader system-level implications. This comprehensive approach recognizes that individual device vulnerabilities can cascade into larger system compromises, particularly relevant in interconnected energy infrastructure.

The certification framework mandates ongoing security maintenance throughout product lifecycles, requiring manufacturers to provide security updates, vulnerability management processes, and incident response capabilities. Article 51 specifically addresses the validity and

monitoring of certificates, establishing requirements for continuous compliance verification and adaptation to evolving threat landscapes. This lifecycle approach is particularly critical for prosumer devices that may remain operational for extended periods while facing evolving cybersecurity threats.

2.1.4.2 Implementation Challenges and Prosumer Integration

The Cybersecurity Act's certification requirements present significant implementation challenges when applied to the diverse ecosystem of prosumer devices and distributed energy resources. Many prosumer technologies, including residential solar inverters, home energy management systems, and electric vehicle charging equipment, are produced by manufacturers operating across global supply chains with varying cybersecurity capabilities and regulatory familiarity. The regulation's requirements for comprehensive security documentation, vulnerability management processes, and conformity assessment procedures may represent substantial compliance burdens for manufacturers serving the prosumer market.

The economic feasibility considerations mandated by Article 46 become particularly complex in prosumer contexts, where cost sensitivity is typically high and security benefits may not be immediately apparent to end users. A critical challenge emerges from the disconnect between individual device risk assessment and collective system impact: a single prosumer inverter or high-wattage appliance may individually warrant only basic level certification due to its limited isolated impact, yet the coordinated compromise of multiple such devices could trigger cascading effects on power infrastructure requiring high level security assurance. This creates a fundamental economic paradox where individual device owners face cost burdens for high-level certification despite their devices appearing individually non-critical, while the collective security risk necessitates comprehensive protection measures.

The regulation's emphasis on proportionate security measures must balance comprehensive protection requirements with market accessibility and adoption rates for distributed energy technologies. This economic dimension is further complicated by the competitive dynamics of prosumer device markets, where security features may not represent primary purchasing decisions for individual consumers, yet the aggregated security implications require systematic high-level protection across distributed installations.

Conformity assessment and market surveillance challenges arise from the distributed nature of prosumer device deployment and operation. Unlike traditional enterprise ICT systems that operate within controlled environments under professional management, prosumer devices are deployed across numerous individual installations with varying technical expertise and maintenance capabilities. The regulation's requirements for ongoing compliance verification and security maintenance must account for this distributed operational reality while ensuring systematic security assurance.

Furthermore, the Cybersecurity Act's focus on individual product certification may not adequately address the system-level security challenges characteristic of distributed energy infrastructure. While individual devices may achieve certification compliance, their integration into broader energy management systems, aggregation platforms, and grid interface technologies creates complex interdependencies that require coordinated security approaches beyond individual product certification scope.

2.1.4.3 Cybersecurity Act Regulatory Gap Analysis and Legislative Recommendations

The analysis reveals that while the Cybersecurity Act establishes comprehensive certification frameworks for ICT products and services, its application to distributed energy infrastructure presents significant challenges related to system integration, economic feasibility, and ongoing compliance management. The regulation's product-centric certification approach may not adequately address the complex interdependencies and system-level security requirements characteristic of modern distributed energy systems.

The primary regulatory gaps encompass system integration limitations, collective criticality misalignment, economic feasibility challenges, lifecycle compliance management difficulties, and market surveillance scalability issues. System integration limitations arise from the Act's focus on individual product certification, which may not adequately address the security implications of integrating multiple certified devices into complex distributed energy systems where emergent vulnerabilities can arise from device interactions and system-level configurations.

Collective criticality misalignment represents a fundamental gap where individual prosumer devices may warrant only basic level certification based on isolated risk assessment, yet their coordinated compromise could trigger cascading effects requiring high level security assurance. This creates an economic and regulatory paradox where the certification level required for individual devices does not align with the collective security impact of multiple compromised devices, particularly for high-wattage prosumer equipment whose aggregated manipulation could significantly affect power infrastructure stability.

Economic feasibility challenges emerge from the substantial compliance costs associated with cybersecurity certification procedures, which may create market barriers for innovative distributed energy technologies or smaller manufacturers serving prosumer markets. The regulation's proportionality requirements must balance comprehensive security assurance with market accessibility, particularly for cost-sensitive prosumer applications where security investments compete with functional capability investments.

Lifecycle compliance management difficulties stem from the regulation's requirements for ongoing security maintenance and certificate validity monitoring across distributed prosumer installations. The practical implementation of vulnerability management, security update deployment, and compliance verification becomes complex when devices are distributed across

numerous individual installations with varying technical capabilities and maintenance practices.

Table 2.4: Cybersecurity Act 2019/881: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Systems**
System Integration Limitations	Product-centric certification approach inadequately addresses complex system-level security requirements	Emergent vulnerabilities from device interactions and system configurations may not be captured by individual product certification
Collective Criticality Misalignment	Individual device certification levels do not reflect aggregated security impact of multiple compromised devices	High-wattage prosumer devices requiring basic certification individually could trigger cascading effects when compromised collectively
Economic Feasibility Challenges	Substantial compliance costs may create market barriers while collective security risks require high-level protection	Individual prosumer device owners face cost burdens for high-level certification despite devices appearing individually non-critical
Lifecycle Compliance Management	Ongoing security maintenance requirements difficult to implement across distributed installations	Vulnerability management and security updates challenging to deploy systematically across numerous individual prosumer installations
Market Surveillance Scalability	Traditional surveillance mechanisms inadequate for distributed prosumer device deployments	Compliance verification and enforcement challenges across numerous small-scale individual installations

The identified regulatory gaps, summarised in Table 2.4, demonstrate the need for adaptive implementation approaches that account for the unique characteristics of distributed energy infrastructure while maintaining the security assurance objectives of the Cybersecurity Act. The regulation's comprehensive certification framework provides valuable foundations for prosumer device security, but its effective application requires complementary mechanisms that address system-level integration, economic accessibility, and distributed compliance management challenges.

Regulatory Development Recommendations for Legislative Bodies - Cybersecurity Act

To address the identified regulatory gaps and enhance the Cybersecurity Act's applicability to distributed energy infrastructure, the following legislative and regulatory adaptations are recommended for policy makers and regulatory authorities:

System-Level Certification Framework Development: Regulatory authorities should develop complementary certification schemes that address system-level security requirements for distributed energy configurations, including integration security assessment procedures for multiple certified devices operating within coordinated energy management systems and virtual power plant configurations.

Graduated Economic Support Mechanisms: Legislative bodies should establish economic support mechanisms that facilitate cybersecurity certification compliance for distributed energy technologies, including reduced certification costs for prosumer-focused devices, collective certification procedures for standardized device categories, and incentive programs that offset certification costs through security compliance benefits.

Distributed Compliance Management Framework: Regulatory frameworks should establish scalable approaches for lifecycle compliance management across distributed prosumer installations, including automated compliance monitoring systems, collective maintenance mechanisms through device manufacturers or service providers, and simplified vulnerability management procedures appropriate for non-technical device operators.

Adaptive Market Surveillance Approach: Regulatory authorities should develop market surveillance mechanisms specifically designed for distributed prosumer device deployments, including risk-based sampling procedures, remote compliance verification capabilities, and collaborative surveillance approaches involving distribution system operators and device aggregators as compliance monitoring partners.

2.1.5 Cyber Resilience Act (Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements)

The Cyber Resilience Act (CRA) represents a paradigm shift in European cybersecurity legislation, moving from a voluntary certification approach to a mandatory market access framework. While NIS2 addresses the security of entities and operators, the CRA targets the hardware and software products that form the technological substrate of critical infrastructure. For distributed energy systems, which rely heavily on a myriad of consumer-grade connected devices—from smart inverters and residential battery controllers to electric vehicle chargers—the CRA establishes the first comprehensive "security by design" legal obligation for manufacturers.

2.1.5.1 Regulatory Framework and Product Scope

The CRA applies to "products with digital elements" (PDEs), covering hardware and software engaged in data connection. The regulation establishes essential cybersecurity requirements that manufacturers must meet to affix the CE marking and place products on the EU market.

Crucially for the energy sector, the CRA introduces a classification system for critical products. Class I and Class II critical products require stricter conformity assessment procedures involving third-party auditing. Components vital to energy system stability, such as industrial smart metering systems and certain classes of microcontrollers and smart home energy interfaces, fall within these critical categories depending on their potential impact on essential services.

The regulation mandates two primary sets of obligations that directly benefit the non-technical prosumer:

- **Security by Design and Default:** Manufacturers must ensure products are secure out of the box (e.g., no default passwords, encrypted communications) without requiring complex configuration by the end-user.

- **Vulnerability Handling and Updates:** Manufacturers are obligated to provide security support and automatic updates for the expected product lifetime (typically 5 years or more), ensuring that prosumer devices do not become obsolete vulnerabilities within the grid.

This framework effectively shifts the burden of cybersecurity from the user (the prosumer) to the manufacturer, acknowledging that the average prosumer lacks the technical expertise to secure their own infrastructure.

2.1.5.2 Implementation Challenges and Prosumer Context

While the CRA significantly elevates the baseline security of distributed energy resources (DERs), it introduces specific challenges for the mass adoption of prosumer technologies.

The Legacy Device Dilemma: The CRA applies to products placed on the market after the regulation's enforcement. It does not retroactively mandate updates for the millions of smart inverters and IoT energy devices already installed in European homes. This creates a "bifurcated grid" scenario where new, secure CRA-compliant devices must coexist with a vast legacy infrastructure of insecure prosumer devices that may remain operational for 15-20 years without security updates.

Cost and Market Accessibility: The compliance costs associated with third-party assessments and continuous vulnerability monitoring may increase the unit cost of prosumer technologies. While essential for security, this "security premium" could impact the economic return on investment (ROI) for small-scale residential installations. For cost-sensitive households, this might slow the adoption of smart grid technologies or encourage the purchase of non-compliant "grey market" devices imported from outside the EU.

Update Management and Service Continuity: For non-technical prosumers, the mandatory update regime introduces operational risks. An automatic security patch applied to a smart inverter or battery system could inadvertently cause compatibility issues with other home energy management components. Unlike standard consumer electronics, where a reboot is a minor inconvenience, a disrupted energy device can impact household power supply or grid balancing services. Ensuring that security updates do not compromise operational reliability is a critical challenge for manufacturers serving the residential market.

2.1.5.3 CRA Regulatory Gap Analysis and Legislative Recommendations

The analysis indicates that while the CRA solves the "unregulated device" problem, it creates new frictions regarding legacy transition and the operational continuity of interconnected systems.

The primary gaps involve the management of the transition period for existing infrastructure, the definition of "expected product lifetime" for energy assets (which significantly exceeds typical IT lifecycles), and the risks of system fragmentation where updates to one device break interoperability with others in the prosumer's home network.

The identified gaps, summarized in Table 2.5, highlight the disconnect between IT regulation cycles and the long-term operational reality of energy infrastructure.

Table 2.5: Cyber Resilience Act: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Systems**
Legacy Infrastructure	Regulation applies only to new market entrants, leaving existing widespread DERs unregulated	Long-lifecycle assets (inverters, batteries) installed pre-CRA remain vulnerable points of entry for decades
Product Lifecycle Definition	Ambiguity in "expected product lifetime" for support periods	Mismatch between consumer electronics support cycles (3-5 years) and energy infrastructure longevity (15-20 years)
Interoperability Risks	Focus on individual product security may overlook system-level integration	Automatic security updates may disrupt communication between devices from different vendors, causing service outages
Market Segmentation	Increased costs for compliant devices may drive "grey market" imports	Prosumers may unknowingly purchase cheaper, non-compliant equipment, undermining grid security

Regulatory Development Recommendations for Legislative Bodies - CRA

To ensure the Cyber Resilience Act effectively secures the distributed energy landscape without hindering adoption, the following legislative adaptations are recommended:

Extended Support Lifecycles for Energy Assets: Regulatory authorities should define specific "expected product lifetimes" for energy-relevant PDEs (e.g., inverters, EV chargers) that align with their operational reality (10+ years), exceeding the standard consumer electronics baseline to prevent premature e-waste and security obsolescence in the grid.

Legacy Transition Frameworks: Legislative bodies should develop incentive mechanisms (e.g., "scrap and replace" schemes) to encourage prosumers to replace pre-CRA legacy equipment with compliant secure devices, accelerating the sanitization of the distributed grid attack surface.

System-Level Interoperability Standards: Regulations should mandate that security updates undergo rigorous interoperability testing to ensure that patching a vulnerability does not disrupt the device's ability to communicate with the wider grid or home energy management systems.

2.1.6 Artificial Intelligence Act (Regulation (EU) 2024/1689)

Regulation (EU) 2024/1689, commonly known as the AI Act [40], establishes the first comprehensive regulatory framework for artificial intelligence systems within the European Union, addressing the governance challenges posed by the increasing deployment of AI technologies across critical sectors. The regulation adopts a risk-based approach to AI regulation, establishing different requirements based on the potential impact of AI systems on fundamental rights, safety, and societal well-being. While the AI Act acknowledges the deployment of AI systems within critical infrastructure sectors, including energy, it does not provide domain-specific regulatory guidance for the unique characteristics and operational requirements of distributed energy systems, creating significant gaps in the governance of AI-enabled prosumer technologies and distributed energy management systems.

2.1.6.1 Regulatory Framework and Risk Classification

The AI Act establishes a comprehensive risk-based regulatory framework that categorizes AI systems into four distinct risk levels: unacceptable risk (prohibited), high-risk, limited risk, and minimal risk. High-risk AI systems, as defined in Article 6 and detailed in Annex III, include those used in critical infrastructure sectors, which explicitly encompasses "digital infrastructure, transport, water, energy, waste, electronic communications networks, and services." This classification acknowledges that AI systems deployed within energy infrastructure require enhanced regulatory oversight due to their potential impact on essential services and societal security.

The regulation defines AI systems broadly in Article 3, encompassing machine learning approaches, logic- and knowledge-based approaches, and statistical approaches that can influence the environment with which they interact. This comprehensive definition captures the diverse range of AI technologies increasingly deployed within distributed energy systems, including demand forecasting algorithms, grid balancing optimization systems, prosumer behavior prediction models, virtual power plant management platforms, and predictive maintenance systems for distributed energy resources.

Article 9 establishes comprehensive requirements for high-risk AI systems, including risk management systems, data governance and management practices, technical documentation requirements, record-keeping obligations, transparency provisions for users, human oversight requirements, and accuracy, robustness, and cybersecurity measures. These requirements create systematic frameworks for ensuring AI system reliability and accountability, particularly relevant for energy systems where AI decisions can significantly impact grid stability, consumer costs, and service reliability.

The regulation mandates conformity assessment procedures under Articles 43-47, requiring

systematic evaluation of AI system compliance with regulatory requirements before market deployment. For energy sector AI systems, this includes assessment of safety measures, risk mitigation strategies, and ongoing monitoring capabilities. However, the Act's generic approach to critical infrastructure does not address the specific technical and operational characteristics that distinguish energy systems from other critical sectors, potentially creating implementation challenges for specialized energy applications.

2.1.6.2 Implementation Challenges and Prosumer Integration

The AI Act's application to distributed energy systems reveals significant challenges stemming from its generic approach to critical infrastructure regulation. While the regulation acknowledges AI deployment in energy systems, it does not provide domain-specific guidance addressing the unique operational characteristics of distributed energy infrastructure, including real-time balancing requirements, bidirectional power flows, market integration complexities, and the distributed ownership structures characteristic of prosumer environments.

Distributed energy systems increasingly rely on sophisticated AI algorithms for demand response optimization, prosumer aggregation management, grid edge resource coordination, and predictive analytics for maintenance and operation. These applications often involve multiple stakeholders, including individual prosumers, aggregators, distribution system operators, and energy service companies, creating complex accountability chains that the AI Act's provider-user framework may not adequately address. The regulation's focus on individual AI system compliance may not capture the systemic implications of interconnected AI applications operating across distributed energy networks.

The economic and technical feasibility challenges become particularly acute for prosumer-focused AI applications. Many distributed energy management systems incorporate AI capabilities for optimizing household energy consumption, electric vehicle charging, battery storage operation, and solar generation forecasting. These systems often operate with limited technical oversight and may be developed by companies lacking extensive regulatory compliance capabilities. The AI Act's comprehensive documentation, testing, and monitoring requirements may create substantial compliance burdens that could limit innovation and market accessibility for prosumer-oriented AI solutions.

Furthermore, the regulation's emphasis on human oversight requirements presents practical challenges in distributed energy contexts where AI systems often operate autonomously to manage rapid grid fluctuations and market responses that exceed human reaction capabilities. The requirement for meaningful human control must be balanced with the operational necessities of real-time energy management while ensuring appropriate accountability and intervention capabilities for critical decisions affecting grid stability and consumer impacts.

2.1.6.3 AI Act Regulatory Gap Analysis and Legislative Recommendations

The analysis reveals that while the AI Act establishes comprehensive governance frameworks for AI systems in critical infrastructure, its generic approach to energy sector applications creates significant gaps in addressing the unique technical, operational, and stakeholder characteristics of distributed energy systems. The regulation's acknowledgment of energy as critical infrastructure lacks the domain-specific guidance necessary for effective governance of AI-enabled prosumer technologies and distributed energy management systems.

The primary regulatory gaps encompass domain-specific guidance limitations, stakeholder accountability complexity, real-time operational requirement challenges, and prosumer market accessibility concerns. Domain-specific guidance limitations arise from the Act's generic treatment of critical infrastructure, which fails to address the unique technical requirements of energy systems including real-time balancing constraints, bidirectional power flows, market integration complexities, and distributed ownership structures that distinguish energy applications from other critical sectors.

Stakeholder accountability complexity emerges from the multi-actor environment characteristic of distributed energy systems, where AI applications often involve coordination across prosumers, aggregators, distribution system operators, and energy service companies. The AI Act's provider-user framework may not adequately address the complex responsibility allocations and accountability chains that characterize distributed energy AI deployments, potentially creating gaps in oversight and liability assignment.

Real-time operational requirement challenges stem from the tension between the Act's human oversight requirements and the operational necessities of energy systems that require autonomous AI decision-making for managing rapid grid fluctuations, frequency regulation, and market responses that exceed human intervention capabilities. This creates potential conflicts between regulatory compliance and operational effectiveness in critical energy management functions.

The identified regulatory gaps demonstrate the need for sector-specific guidance that addresses the unique characteristics of AI deployment within distributed energy infrastructure while maintaining the AI Act's fundamental risk-based approach and safety objectives. The regulation's comprehensive framework provides valuable foundations for AI governance, but its effective application to energy systems requires complementary guidance addressing domain-specific technical, operational, and stakeholder management challenges.

Table 2.6: AI Act 2024/1689: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Sys tems**
Domain-Specific Guidance Limitations	Generic critical infrastructure approach lacks energy sector-specific technical and operational guidance	AI systems for energy managemen lack tailored regulatory framework addressing real-time balancing, bidi rectional flows, and distributed own ership
Stakeholder Accountability Complexity	Provider-user framework inadequately addresses multi-actor distributed energy environments	Complex responsibility chains acros prosumers, aggregators, and opera tors create accountability gaps in A system oversight
Real-Time Operational Conflicts	Human oversight requirements conflict with autonomous operation necessities in energy systems	Tension between regulatory compli ance and operational effectiveness fo critical real-time energy managemen functions
Prosumer Market Accessibility	Comprehensive compliance requirements may create barriers for prosumer-oriented AI solutions	Innovation and market accessibil ity challenges for distributed energ AI applications serving cost-sensitiv prosumer markets

Regulatory Development Recommendations for Legislative Bodies - AI Act

To address the identified regulatory gaps and enhance the AI Act's applicability to distributed energy infrastructure, the following legislative and regulatory adaptations are recommended for policy makers and regulatory authorities:

Energy Sector-Specific AI Guidance Development: Regulatory authorities should develop complementary guidance specifically addressing AI systems in distributed energy infrastructure, including technical standards for real-time operation, bidirectional power flow management, market integration requirements, and prosumer coordination protocols that account for the unique operational characteristics of energy systems.

Multi-Stakeholder Accountability Framework Establishment: Legislative bodies should establish clear accountability allocation mechanisms for AI systems operating across complex distributed energy stakeholder networks, including responsibility-sharing agreements between prosumers, aggregators, distribution system operators, and AI system providers, with appropriate liability distribution based on control and benefit allocation.

Adaptive Human Oversight Mechanism Development: Regulatory frameworks should develop sector-appropriate human oversight requirements that balance AI Act compliance with operational necessities of real-time energy management, including graduated oversight levels based on decision criticality and time constraints, with enhanced monitoring and intervention capabilities for high-impact autonomous decisions.

Prosumer-Accessible Compliance Framework: Regulatory authorities should establish simplified compliance pathways for prosumer-oriented AI applications, including standardized assessment procedures for common distributed energy AI use cases, collective compliance mechanisms for similar AI deployments, and economic support mechanisms that facilitate AI Act compliance for innovative distributed energy solutions.

Sectoral Harmonization Mechanism Integration: Legislative frameworks should establish coordination mechanisms between AI Act requirements and existing energy sector regulations (NIS2, Network Code, Cybersecurity Act) to ensure coherent regulatory compliance across overlapping requirements and avoid conflicting obligations for distributed energy AI systems.

2.1.7 Legal Accountability and GDPR Applicability (Regulation (EU) 2016/679)

The General Data Protection Regulation (EU) 2016/679 (GDPR) [41] constitutes the European Union's principal legal instrument governing personal data processing, establishing comprehensive obligations for any activity involving data that identifies or can be linked to natural persons. Within distributed energy infrastructure contexts, GDPR applicability becomes particularly complex due to the dual nature of prosumer installations: while individual prosumer devices operate within household environments traditionally protected by GDPR exemptions, their integration into critical energy infrastructure creates potential data processing activities that extend beyond purely personal use. This regulatory intersection raises fundamental questions about liability allocation, accountability frameworks, and the scope of data protection obligations when individual prosumer activities collectively impact critical infrastructure security and stability.

2.1.7.1 Regulatory Framework and Data Controller Responsibilities

The GDPR establishes comprehensive data protection obligations centered on the concept of data controllers, defined as entities that determine the purposes and means of personal data processing. In distributed energy system contexts, data controller identification becomes complex due to the multi-stakeholder environment where prosumer data may be processed by various entities including platform operators, aggregators, distribution system operators, energy service companies, and potentially the prosumers themselves. Each entity's data controller status depends on their level of control over data processing activities and their decision-making authority regarding data processing purposes and methods.

Article 5 establishes fundamental data processing principles including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. These principles create systematic obligations for ensuring secure data processing throughout distributed energy systems, with particular emphasis on the integrity and confidentiality requirements that mandate appropriate technical and organizational measures to protect personal data against unauthorized processing, accidental loss, destruction, or damage.

Articles 24 and 25 establish specific obligations for data protection by design and by default, requiring controllers to implement appropriate technical and organizational measures to ensure and demonstrate GDPR compliance. In distributed energy contexts, these requirements mandate secure system design, privacy-preserving data processing architectures, and comprehensive security measures that protect prosumer data throughout collection, processing, storage, and transmission activities. The regulation's emphasis on accountability requires controllers to demonstrate compliance through documentation, monitoring, and regular assessment of data

protection measures.

Article 33 and 34 establish comprehensive data breach notification obligations, requiring controllers to notify supervisory authorities within 72 hours of breach awareness and inform affected data subjects when breaches pose high risks to their rights and freedoms. For distributed energy systems, these obligations create complex notification scenarios where breaches affecting prosumer data may have implications extending beyond individual privacy to encompass infrastructure security and grid stability concerns.

The household exception established in Article 2(2)(c) exempts personal data processing "by a natural person in the course of a purely personal or household activity" from GDPR obligations. This exception traditionally protects individual prosumers from data controller obligations when their energy management activities remain within household contexts. However, the exception explicitly applies only to natural persons and excludes activities that extend beyond purely personal or household purposes, creating potential gaps when prosumer activities collectively impact critical infrastructure systems.

2.1.7.2 Implementation Challenges and Prosumer Integration

The application of GDPR to distributed energy systems reveals significant challenges stemming from the evolution of prosumer roles from passive energy consumers to active participants in critical infrastructure operations. Traditional household exception interpretations assumed individual energy consumption activities with minimal external impact, yet modern prosumer installations increasingly contribute to grid balancing, demand response programs, virtual power plant operations, and market participation activities that extend beyond purely personal use.

When cyber-attacks target prosumer equipment and manipulate personal data for infrastructure disruption purposes, multiple data controller relationships may be implicated. The attacker clearly violates GDPR obligations through unauthorized data processing, but liability questions extend to other stakeholders involved in prosumer data processing activities. Platform operators, aggregators, and energy service companies managing prosumer infrastructure may qualify as data controllers if their systems facilitate data processing or if inadequate security measures contribute to successful attacks.

The most complex accountability question concerns prosumer liability under GDPR obligations. While the household exception traditionally protects natural person prosumers, the nature and scale of modern prosumer activities increasingly challenge this classification. Individual prosumer installations that participate in demand response programs, provide grid services, or operate within virtual power plant configurations may process data in ways that affect other citizens and critical infrastructure operations, potentially exceeding the scope of purely household activities.

Corporate prosumers face clearer obligations as they cannot benefit from household exemp-

tions and likely qualify as data controllers for their prosumer-related data processing activities. This creates systematic compliance requirements for secure data processing equipment, appropriate technical and organizational measures, and comprehensive incident response capabilities. Failure to implement adequate security measures could result in GDPR liability toward affected individuals and regulatory sanctions from supervisory authorities.

The distributed nature of prosumer data processing creates additional challenges for determining appropriate technical and organizational measures. Individual prosumers may lack the technical expertise, economic resources, and organizational capabilities necessary to implement comprehensive data protection measures equivalent to those expected from traditional data controllers, yet their collective data processing activities may create risks to other citizens that exceed traditional household activity impacts.

2.1.7.3 GDPR Regulatory Gap Analysis and Legislative Recommendations

The analysis reveals that while GDPR establishes comprehensive data protection frameworks, its application to distributed energy infrastructure creates significant gaps in accountability allocation, household exception interpretation, and technical implementation requirements. The regulation's traditional approach to data controller identification may not adequately address the complex multi-stakeholder environment and collective impact characteristics of distributed energy systems where individual prosumer activities aggregate into critical infrastructure operations.

The primary regulatory gaps encompass household exception boundary ambiguity, collective impact accountability deficiencies, technical implementation scalability challenges, and multi-stakeholder liability coordination difficulties. Household exception boundary ambiguity arises from unclear criteria for determining when prosumer activities exceed purely personal or household purposes, particularly as prosumer participation in grid services, demand response programs, and virtual power plant operations becomes more sophisticated and impactful.

Collective impact accountability deficiencies emerge from GDPR's focus on individual data processing activities, which may not adequately address scenarios where multiple prosumer installations create aggregated privacy and security risks affecting other citizens and critical infrastructure systems. The regulation's individual-centric approach may not capture the collective accountability implications when numerous prosumer data processing activities combine to create systemic risks requiring coordinated protection measures.

Technical implementation scalability challenges stem from GDPR's comprehensive security requirements, which may be difficult for individual prosumers to implement despite their potential data controller status. The regulation's emphasis on appropriate technical and organizational measures assumes organizational capabilities that individual prosumers may lack, creating potential compliance gaps when prosumer activities extend beyond household exemp-

tion scope.

Table 2.7: GDPR 2016/679: Regulatory Gaps in Distributed Energy Infrastructure Context

Gap Category	**Description**	**Impact on Distributed Energy Systems**
Household Exception Boundary Ambiguity	Unclear criteria for determining when prosumer activities exceed purely personal or household purposes	Individual prosumer participation in grid services may exceed household exemption scope without clear regulatory guidance
Collective Impact Accountability	Individual-centric approach inadequately addresses aggregated privacy and security risks from multiple prosumers	Multiple prosumer data processing activities may create systemic risks requiring coordinated protection beyond individual accountability
Technical Implementation Scalability	Comprehensive security requirements difficult for individual prosumers to implement despite potential controller status	Individual prosumers may lack organizational capabilities for appropriate technical and organizational measures
Multi-Stakeholder Liability Coordination	Complex liability allocation among prosumers, platforms, aggregators, and operators creates accountability gaps	Unclear responsibility distribution when prosumer data breaches affect infrastructure security and other citizens

The identified regulatory gaps demonstrate the need for adaptive GDPR interpretation and complementary guidance that addresses the unique characteristics of distributed energy infrastructure while maintaining fundamental data protection principles. The regulation's comprehensive privacy protection framework provides valuable foundations, but its effective application to prosumer environments requires clarified accountability mechanisms, scaled implementation approaches, and coordinated liability frameworks that reflect the collective nature of distributed energy data processing activities.

Regulatory Development Recommendations for Legislative Bodies - GDPR

To address the identified regulatory gaps and enhance GDPR applicability to distributed energy infrastructure, the following legislative and regulatory adaptations are recommended for policy makers and data protection authorities:

Household Exception Clarification Framework: Data protection authorities should develop specific guidance clarifying household exception boundaries for prosumer activities, including criteria for determining when energy-related data processing exceeds purely personal purposes, with clear thresholds based on market participation, grid service provision, and collective impact potential on other citizens and infrastructure systems.

Collective Accountability Mechanism Development: Legislative bodies should establish frameworks for addressing collective data protection risks arising from multiple prosumer installations, including shared responsibility models for aggregated privacy risks, collective compliance mechanisms for coordinated prosumer activities, and liability-sharing agreements among distributed energy stakeholders.

Graduated Technical Implementation Support: Regulatory authorities should develop scaled technical and organizational measures appropriate for different prosumer controller categories, including simplified security requirements for individual natural person prosumers, enhanced obligations for corporate prosumers, and technical assistance programs to support appropriate measure implementation.

Multi-Stakeholder Liability Coordination Framework: Data protection authorities should establish clear liability allocation mechanisms for distributed energy data processing environments, including responsibility-sharing protocols among prosumers, platform operators, aggregators, and distribution system operators, with appropriate liability distribution based on control, benefit, and capability to implement protective measures.

Energy Sector-Specific Data Protection Guidance: Regulatory frameworks should develop sector-specific data protection guidance addressing unique characteristics of energy data processing, including real-time operational requirements, infrastructure security implications, and coordination requirements between data protection and energy security obligations.

2.2 Global Perspectives on Prosumer Legislation

Outside the European Union, major economies are pursuing divergent regulatory strategies that reveal significant variation in how jurisdictions conceptualize prosumer cybersecurity risks, with some treating prosumers as critical infrastructure assets requiring protection and others viewing them primarily as potential attack vectors requiring containment.

This analysis demonstrates a clear evolutionary trajectory from voluntary cybersecurity guidelines toward mandatory compliance frameworks, driven by growing recognition that distributed energy resources create an exponentially expanding attack surface that traditional centralized security models cannot adequately protect. The research reveals that while documented large-scale prosumer cybersecurity incidents remain relatively uncommon, identified vulnerabilities have catalyzed substantial regulatory evolution that fundamentally reconceptualizes energy sector cybersecurity governance.

2.2.1 United States: Comprehensive Federal-State Coordination Framework

The United States has developed the most comprehensive prosumer cybersecurity framework through a sophisticated multi-layered approach combining federal oversight, market-based incentives, and state-level implementation. This regulatory architecture treats prosumers as essential infrastructure participants requiring enabling cybersecurity support rather than viewing them primarily as security threats to be contained.

2.2.1.1 Federal Regulatory Foundation

The Department of Energy (DOE)'s landmark Cybersecurity Baselines for Electric Distribution Systems and Distributed Energy Resources, published in February 2024, represents the first comprehensive global attempt to establish uniform cybersecurity standards specifically for industrial-scale prosumer systems [42]. Developed through an unprecedented public-private collaboration between the National Association of Regulatory Utility Commissioners (NARUC) and federal agencies, these baselines establish minimum cybersecurity requirements for distributed energy resources while providing scalable frameworks to accommodate diverse large-scale system configurations.

The Federal Energy Regulatory Commission's (FERC) regulatory approach demonstrates sophisticated integration of cybersecurity requirements within market participation frameworks. Order No. 2222, implemented in 2021, explicitly enables distributed energy resources to participate in electricity markets while establishing mandatory cybersecurity coordination requirements between regional transmission operators, DER aggregators, and distribution utilities [43]. This framework fundamentally reconceptualizes prosumers as market participants requiring cybersecurity enablement rather than treating them as peripheral security concerns.

FERC's 2023 Cybersecurity Incentives Program provides substantial economic incentives for voluntary cybersecurity investments exceeding mandatory standards, offering 200 basis points rate-of-return adders for qualifying investments [44]. This market-driven approach encourages enhanced security through economic incentives rather than purely regulatory mandates, demonstrating regulatory philosophy that views cybersecurity investment as economically rational behavior requiring appropriate market signals.

2.2.2 China: Centralized Coordination with Market Integration

China's regulatory approach represents centralized coordination with market-based evolution, where prosumers are integrated into comprehensive national energy transformation planning rather than treated as separate cybersecurity concerns. This framework emphasizes comprehensive coordination through national planning mechanisms while enabling rapid market expansion of prosumer systems.

2.2.2.1 National Planning Integration

The 2024 Action Plan for Accelerating the New Type Power System, coordinated by the National Development and Reform Commission and National Energy Administration, targets 200+ GW annual renewable capacity additions through 2027, with cybersecurity requirements embedded within broader grid modernization frameworks rather than treated as separate regulatory concerns [45].

2.2.3 Canada: Mandatory Compliance Framework

Canada's approach through Bill C-8, reintroduced in June 2025, demonstrates mandatory compliance philosophy with the Critical Cyber Systems Protection Act creating comprehensive cybersecurity frameworks for critical infrastructure including interprovincial power systems [46]. The legislation imposes penalties up to $15 million per day for corporations failing to maintain adequate cybersecurity programs, representing one of the most stringent penalty regimes globally for cybersecurity non-compliance.

Natural Resources Canada's Cyber Energy Security Policy coordinates public-private information sharing through forums that explicitly include prosumer system operators, treating them as stakeholders in national energy security rather than peripheral market participants [47]. This approach demonstrates regulatory recognition of prosumers as critical infrastructure components requiring protection and coordination rather than viewing them primarily as security threats requiring containment.

The Canadian regulatory framework emphasizes mandatory compliance with significant penalties, contrasting with United States market-based incentive approaches while maintaining

similar recognition of prosumers as essential infrastructure participants requiring cybersecurity enablement.

2.2.4 Japan: Industry-Led Standards Development

Japan's sophisticated industry-led standards development reveals advanced regulatory thinking about emerging prosumer cybersecurity threats through collaborative governance between the Ministry of Economy, Trade and Industry and industry stakeholders. The May 2025 Cybersecurity Guidelines for Energy Resource Aggregation Business Version 3.0 explicitly addresses gateway-less demand response systems and IoT device vulnerability management, representing regulatory adaptation to technological evolution that outpaces traditional regulatory cycles [48].

Japan's approach uniquely recognizes prosumers as potential cybersecurity weak points requiring specialized protection frameworks, implementing three-pronged cybersecurity methodology addressing cloud-based control systems, IoT device vulnerabilities, and information security risks from device utilization patterns. The March 2025 launch of the IoT Product Security Labeling Scheme demonstrates proactive regulatory intervention in prosumer technology markets, requiring security evaluations before market deployment.

The Japanese regulatory framework demonstrates sophisticated technical understanding of prosumer cybersecurity challenges while maintaining industry leadership in standards development, enabling both innovation and security through collaborative governance mechanisms.

2.2.5 Comparative Analysis and Regulatory Trajectories

The comparative analysis reveals three distinct regulatory philosophies emerging globally: infrastructure enablement approaches (United States, Australia) that treat prosumers as essential participants requiring cybersecurity support; threat containment approaches (Japan, some Canadian frameworks) emphasizing sophisticated monitoring and control requirements; and market integration approaches (China, South Korea) where prosumer cybersecurity requirements are embedded within comprehensive energy transformation planning.

2.2.5.1 Regulatory Convergence Trends

Despite philosophical differences, regulatory convergence trends include movement toward mandatory compliance frameworks with significant penalties for non-compliance, enhanced supply chain security requirements addressing international coordination challenges, expanded regulatory scope covering previously exempt smaller prosumer systems, and international coordination mechanisms addressing cross-border cybersecurity governance.

The period 2020-2025 represents regulatory acceleration driven by growing recognition of

prosumer cybersecurity risks, with all major jurisdictions implementing enhanced regulatory frameworks reflecting sophisticated understanding of distributed energy resource cybersecurity challenges.

Chapter 3

Prosumer Security Analysis

The objective of this chapter is to introduce a reference prosumer system architecture by systematically detailing each operational plane and its constituent technical components, as depicted in Figure 3.1. This multi-layered architecture facilitates rigorous security analysis through systematic examination of attack surfaces, threat vectors, and potential entry points across the hierarchical architectural planes. In this chapter a detailed threat modeling and risk assessment for individual planes is detailed, systematically identifying critical security vulnerabilities, implementation gaps, and emerging threat. Through this approach, this analysis establishes a security baseline for prosumer infrastructures while highlighting open research challenges and mitigation strategies for next-generation distributed energy systems.

3.1 Reference Architecture and Components

The proposed architecture encompasses five distinct planes: generation, storage, control and management, communication and networking, and market interface planes, each being analyzed in the following subsections. The system components of each plane will be systematically deconstructed by providing the reader a comprehensive understanding of the bidirectional interactions, energy flow dynamics, and data exchange patterns that characterize modern prosumer operations.

3.1.1 Generation Plane Components

The generation layer constitutes the foundational stratum of the prosumer architecture, encompassing distributed energy resources that facilitate bidirectional power exchange with the electrical grid through the grid interconnection interface. This plane integrates three primary generation technologies: photovoltaic systems, wind micro-generation units, and combined heat and power (CHP) installations, each employing distinct control mechanisms and opera-

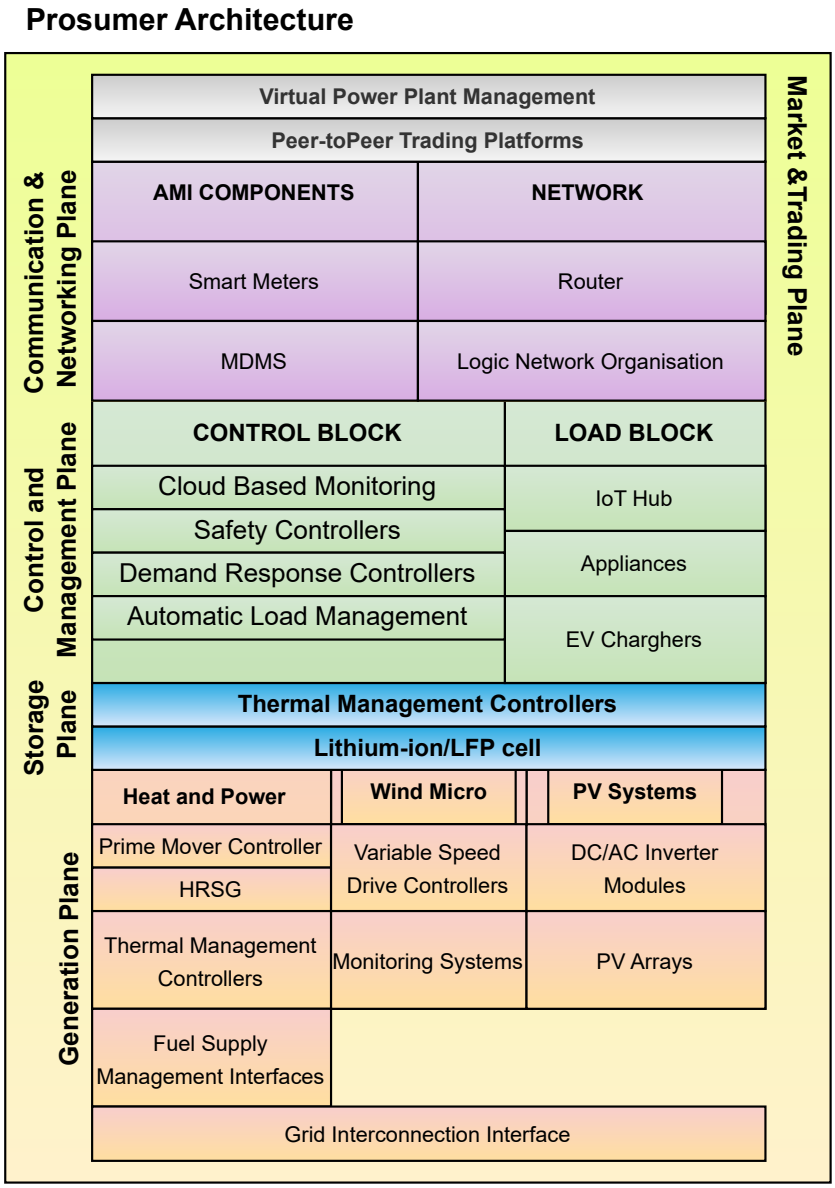


Figure 3.1: Multi-layered prosumer architecture framework illustrating the hierarchical integration of generation, storage, control, communication, and market interface planes with constituent technical components for autonomous energy management and grid interaction.

tional paradigms.

3.1.1.1 Photovoltaic System Architecture

The PV system architecture, displayed in Figure 3.2 ,comprises multi-level power conversion stages including DC/AC inverter modules with integrated maximum power point tracking (MPPT) controllers operating at appropriate switching frequencies for optimal efficiency. The inverter modules generally implement three-phase grid-tie functionality with low total harmonic distortion (THD) specifications and comprehensive power factor correction capabilities spanning leading to lagging operational ranges. Smart inverter functionalities include volt-VAR control, frequency-watt response, and generic functionalities command that can be sent remotely.

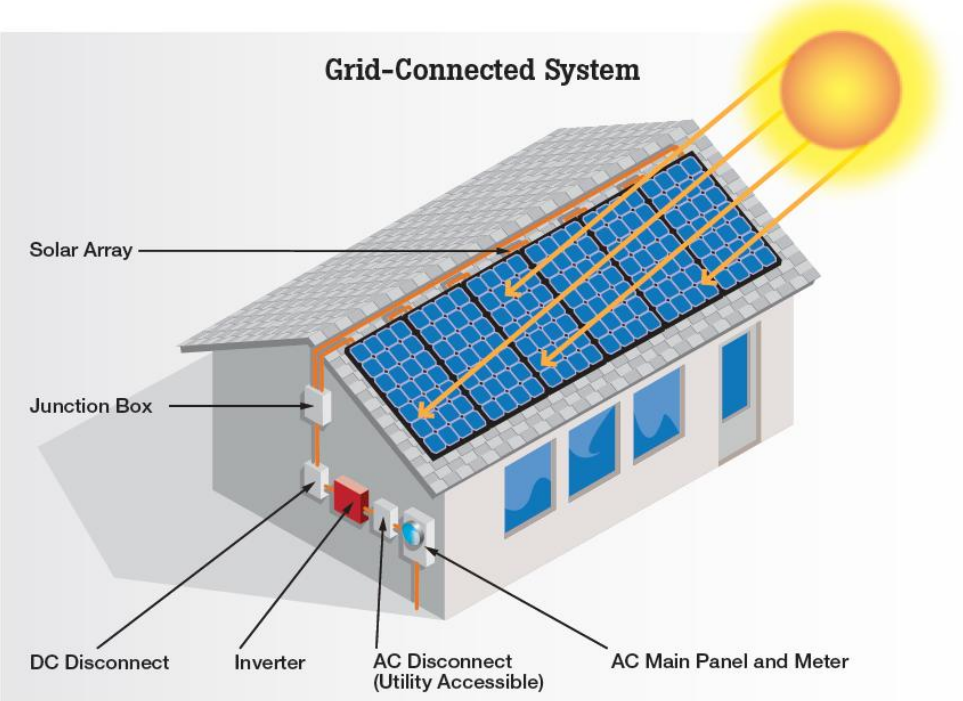


Figure 3.2: Photovoltaic electrical components view [49].

Real-time data acquisition encompasses DC string voltages and currents within operational ranges typical for residential and commercial installations, module temperatures across standard environmental operating conditions, and solar irradiance measurements covering the full spectrum of natural solar conditions. The system generally maintains historical databases containing cumulative energy production, performance ratio calculations, and module degradation tracking throughout operational lifetime. Environmental data such as ambient temperature, wind speed, relative humidity, and barometric pressure can be used for comprehensive perfor-

mance correlation analysis. The MPPT controllers utilize industry-standard algorithms such as perturb-and-observe or incremental conductance methods with high tracking efficiency under standard test conditions, while anti-islanding protection mechanisms provide rapid grid disturbance detection using established active detection methods.

The control system accepts different operational commands including inverter enable/disable functions, variable power curtailment set-points across the full rated capacity range, reactive power control commands within standard power factor operational ranges, and volt-VAR curve parameter adjustments. MPPT algorithm selection commands facilitate switching between various tracking methodologies including perturb-and-observe, incremental conductance, and constant voltage tracking modes. Grid-tie operational commands encompass synchronization control, anti-islanding sensitivity adjustments, and protective relay set-point modifications for voltage and frequency parameters within acceptable grid operational ranges. Communication interfaces implement standard protocols such as Modbus RTU or SunSpec [50] for data exchange, transmitting critical performance parameters including instantaneous power output, cumulative energy production, thermal conditions, and comprehensive fault status indicators.

Table 3.1: Photovoltaic System Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
DC/AC Inverter	Three-phase voltage/current within operational ranges, low THD performance, adjustable power factor, grid frequency monitoring	Enable/disable, variable power curtailment, reactive power control, volt-VAR curve adjustment
MPPT Controller	DC string voltage/current monitoring, high tracking efficiency, comprehensive irradiance measurement	Algorithm selection, tracking parameter optimization, operational mode control
Grid Synchronization	Grid frequency monitoring, phase angle detection, voltage magnitude assessment, synchronization status, islanding detection	Synchronization control, anti-islanding sensitivity adjustment, protective relay configuration
Environmental Monitoring	Module temperature monitoring, ambient condition assessment, meteorological data collection	Calibration commands, measurement interval configuration, sensor management

3.1.1.2 Wind Micro-Generation Infrastructure

Wind micro-generation systems typically employ three-phase permanent magnet synchronous generators (PMSG) coupled with variable speed drive controllers implementing field-oriented control (FOC) algorithms for optimal torque and flux regulation. The power electronic converters utilize back-to-back AC-DC-AC topology with intermediate DC bus voltage regulation at appropriate voltage levels and optimal switching frequencies to minimize electromagnetic interference. Pitch control systems maintain blade angle optimization through servo-controlled actuators with high angular resolution, responding to wind speed variations with rapid response times. Data acquisition systems collect measurements of electrical parameters including three-

Table 3.2: Wind Micro-Generation Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
PMSG and Drive Controller	Three-phase voltage/current within operational ranges, rotational speed monitoring, DC bus voltage regulation	Start/stop sequences, operational mode selection, variable power curtailment, reactive power control
Pitch Control System	Blade pitch angle monitoring, actuator position feedback, rapid response characteristics, tip-speed ratio optimization	Target blade angle commands with high resolution, tracking mode selection, emergency feathering
Yaw Control System	Nacelle orientation monitoring, wind direction tracking, precise alignment control	Yaw position commands, wind tracking enable/disable, manual positioning override
Condition Monitoring	Vibration amplitude across frequency spectrum, bearing temperature monitoring, gearbox health assessment, tower oscillation analysis	Monitoring sensitivity adjustment, alarm threshold configuration, diagnostic test activation

phase voltages, currents, power factor, and frequency. Mechanical parameters encompass generator rotational speed within operational ranges, blade pitch angles across the full adjustment spectrum, nacelle yaw position throughout complete rotational range, and vibration amplitude measurements across comprehensive frequency bands. Meteorological data includes wind speed across operational ranges, wind direction measurements, air density, and turbulence intensity assessments. Advanced control algorithms implement tip-speed ratio optimization, maintaining optimal values for maximum power coefficient extraction, while cut-in wind speeds are established at appropriate thresholds with rated wind speeds determined for optimal energy

capture.

Operational commands include turbine start/stop sequences, emergency shutdown activation, and operational mode selection encompassing power optimization, noise reduction, and grid support functionalities. Pitch control commands specify target blade angles with high angular resolution for wind speed tracking and power regulation, while yaw control commands direct nacelle orientation adjustments for optimal wind tracking. Power curtailment commands enable variable output limitation across the full rated capacity range for grid stability support, and reactive power commands provide voltage support capabilities within generator VA rating limits. Condition monitoring systems employ accelerometers for comprehensive vibration analysis, implementing Fast Fourier Transform (FFT) algorithms for bearing fault detection and gearbox health assessment.

3.1.1.3 Combined Heat and Power Systems

CHP installations integrate reciprocating engines or microturbines with electrical generators and heat recovery systems, achieving high overall system efficiencies through simultaneous electricity and thermal energy production [51]. Prime mover controllers implement closed-loop combustion control maintaining air-fuel ratios within optimal stoichiometric limits for superior emissions performance and fuel efficiency. Heat recovery steam generators (HRSG) capture exhaust heat through finned-tube heat exchangers, generating hot water at appropriate temperatures or low-pressure steam within operational pressure ranges.

Engine management systems monitor critical parameters including coolant temperature, lubricating oil pressure, exhaust gas temperature, and engine speed at high-frequency intervals. Electrical measurements encompass three-phase output power across rated capacity, precise voltage regulation, frequency stability, and comprehensive power factor monitoring. Thermal system data includes heat recovery temperatures, operational flow rates, thermal output across rated capacity, and cumulative thermal energy production. Fuel system monitoring tracks gas supply pressure, flow rates, heating values within standard ranges, and fuel composition analysis for combustion optimization.

Operational commands encompass engine start/stop sequences with appropriate pre-lubrication and warm-up procedures, load set-point adjustments across full rated capacity, and operational mode selection including baseload, load-following, and peak-shaving operations. Power output commands specify electrical generation targets with appropriate ramping rate limitations, while thermal management commands control heat recovery circuit temperatures, circulation pump speeds across operational capacity, and three-way valve positions for optimal heat distribution. Synchronization commands coordinate grid connection sequences, including voltage matching, frequency synchronization, and phase angle alignment prior to breaker closure. Maintenance commands enable comprehensive diagnostic test sequences, emissions monitoring calibration,

and protective system function verification.

Table 3.3: Combined Heat and Power Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Prime Mover Controller	Engine speed monitoring, coolant temperature control, oil pressure monitoring, optimal air-fuel ratio maintenance	Start/stop sequences, variable load set-points, operational mode selection, ramping rate control
Electrical Generator	Three-phase power across rated capacity, precise voltage regulation, frequency stability, comprehensive power factor monitoring	Power output commands, synchronization control, voltage regulation, protective relay configuration
Heat Recovery System	Exhaust temperature monitoring, thermal output measurement, operational flow rate control, heat exchanger efficiency assessment	Thermal management commands, circulation pump control, valve position optimization
Fuel Management	Gas pressure monitoring, flow rate measurement, heating value assessment, comprehensive fuel composition analysis	Fuel supply control, pressure regulation, composition monitoring, safety shutdown systems

3.1.2 Storage Plane Components

The storage plane serves as the critical energy buffering and management layer within the prosumer architecture, enabling temporal decoupling between energy generation and consumption while providing grid stabilization services. This layer encompasses battery energy storage systems (BESS), supercapacitor technologies, and hybrid storage configurations, each contributing distinct operational characteristics for power quality enhancement, peak shaving, and grid support functions.

3.1.2.1 Battery Energy Storage Systems

Battery energy storage systems utilize lithium-ion or lithium iron phosphate (LFP) cell configurations organized in series-parallel arrangements to achieve desired voltage and capacity specifications. The battery management system (BMS) implements cell-level monitoring and control through integrated circuits measuring individual cell voltages, temperatures across operational ranges, and current flow at high-frequency sampling intervals. State-of-charge es-

timation generally employs coulomb counting, open-circuit voltage correlation, and extended Kalman filtering algorithms to maintain high accuracy under dynamic operating conditions.

Power conditioning systems integrate bidirectional DC-DC converters and DC-AC inverters to facilitate grid interconnection with power ratings appropriate for residential prosumer applications. The converters maintain DC bus voltage regulation with minimal ripple content, while implementing soft-switching techniques to minimize electromagnetic interference and switching losses. Battery protection circuits incorporate overcurrent, overvoltage, undervoltage, and thermal protection with rapid response times for critical fault conditions.

Control commands encompass charge/discharge power set-points with high resolution, operational mode selection including grid-following, grid-forming, and islanding capabilities, and protective parameter adjustments for voltage and current thresholds. State-of-health (SOH) monitoring tracks capacity fade, internal resistance increases, and cycle counting for predictive maintenance scheduling. The system accepts frequency regulation commands for primary and secondary grid support services, implementing droop control characteristics with rapid response times for frequency deviations.

Table 3.4: Battery Energy Storage System Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Battery Management System	Cell voltage monitoring, temperature measurement across operational ranges, high-accuracy SOC estimation, SOH tracking, cycle counting	Charge/discharge commands, balancing control, protection threshold adjustment, calibration sequences
Power Conditioning System	DC bus voltage regulation, AC output across rated capacity, high conversion efficiency, low THD performance	Power set-points with high resolution, operational mode selection, grid synchronization commands, protection configuration
Thermal Management	Cell temperature monitoring, coolant flow measurement, thermal gradient assessment, heating/cooling power tracking	Temperature set-point control, fan/pump operation, heating element activation, thermal protection limits
Grid Interface Controller	Grid frequency monitoring, voltage regulation, power factor control, rapid response characteristics	Frequency regulation commands, voltage support control, islanding management, droop characteristic adjustment

3.1.2.2 Supercapacitor Energy Storage

Supercapacitor systems provide high-power, short-duration energy storage with exceptional power densities and extended cycle life ratings. The systems utilize electric double-layer capacitor (EDLC) technology with operational voltages per cell, configured in series strings to achieve appropriate system voltages [52]. Voltage balancing circuits maintain cell voltage equalization through passive resistive or active switching methods, preventing overvoltage conditions and ensuring uniform aging characteristics. Energy management algorithms coordi-

Table 3.5: Supercapacitor System Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Supercapacitor Modules	Cell voltage monitoring, capacitance measurement, ESR assessment, leakage current tracking, temperature monitoring	Voltage balancing control, precharge sequences, module isolation commands, safety disconnect
Power Electronics	DC-DC converter monitoring, optimal switching frequency operation, high efficiency performance, rapid response characteristics	Power reference commands with high update rates, control mode selection, current limiting, protection configuration
Energy Management Controller	SOC estimation, power flow measurement, cycle counting, degradation tracking, grid synchronization	Charge/discharge scheduling, power smoothing optimization, grid support activation, hybrid coordination
Condition Monitoring	Impedance spectroscopy analysis, aging indicator assessment, thermal imaging, vibration analysis, comprehensive diagnostics	Diagnostic test activation, calibration procedures, health assessment triggers, maintenance scheduling

nate supercapacitor discharge for high-frequency power compensation, grid fault ride-through support, and rapid response grid services. The power electronic interface implements buck-boost DC-DC conversion with optimal switching frequencies to minimize filtering requirements and maximize dynamic response. Current control loops achieve rapid response times for step changes in power demand, enabling participation in fast frequency response markets and power quality improvement services.

Control systems accept power reference commands with high update rates, enabling real-time power smoothing and voltage regulation support. Capacitance monitoring tracks aging degradation through impedance spectroscopy measurements, while leakage current monitoring

ensures system integrity during standby operations. The systems implement coordinated control with battery storage for hybrid energy management, providing complementary high-power and high-energy storage capabilities.

3.1.2.3 Thermal Management Systems

Thermal management systems maintain optimal operating temperatures across all storage technologies through active cooling and heating mechanisms. Liquid cooling systems utilize appropriate coolant mixtures circulated through heat exchangers integrated within battery modules, maintaining uniform cell temperatures across the pack. Variable-speed circulation pumps adjust flow rates based on thermal load requirements, while heat exchangers facilitate heat rejection to ambient air or ground-source heat pumps. Temperature monitoring

Table 3.6: Thermal Management System Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Liquid Cooling System	Coolant temperature monitoring, variable flow rate measurement, pressure differential assessment, pump power tracking	Flow rate commands, temperature set-point control, pump speed adjustment, valve position optimization
Temperature Monitoring	High-accuracy cell temperature measurement, thermal gradient assessment, ambient condition monitoring, heat exchanger performance evaluation	Sensor calibration, sampling rate configuration, alarm threshold adjustment, thermal imaging activation
Phase Change Materials	PCM temperature monitoring, latent heat capacity utilization, thermal conductivity assessment, solidification tracking	Thermal buffering activation, PCM regeneration control, thermal capacity optimization
HVAC Integration	Heat recovery measurement, COP assessment, seasonal efficiency tracking, waste heat utilization monitoring	Heat recovery control, HVAC coordination, seasonal optimization, efficiency maximization

employs distributed sensor networks with high-accuracy thermistors at appropriate sampling rates. Thermal modeling algorithms predict temperature evolution based on charge/discharge profiles, ambient conditions, and aging characteristics to optimize cooling system operation. Phase change material (PCM) integration provides passive thermal buffering during high-rate charge/discharge events, reducing active cooling power consumption and improving system

efficiency.

Control algorithms coordinate heating and cooling systems based on predictive thermal management, pre-conditioning storage systems for anticipated operating conditions. Heating elements activate during cold weather conditions to maintain appropriate minimum operating temperatures, while cooling systems prevent thermal runaway through active monitoring of temperature rise rates. Integration with building HVAC systems enables waste heat recovery for space heating applications, improving overall system efficiency.

3.1.3 Control and Management Plane

The control and management plane constitutes the supervisory layer responsible for coordinating distributed energy resources, load management, and grid interaction within the prosumer architecture. This plane encompasses centralized control functions through cloud-based monitoring systems, distributed safety controllers, demand response mechanisms, and automated load management systems. The architecture facilitates bidirectional communication between generation assets, storage systems, and controllable loads while ensuring compliance with grid codes and operational safety requirements.

3.1.3.1 Control Block

The control block implements hierarchical control structures encompassing cloud-based monitoring systems, distributed safety controllers, demand response controllers, and automatic load management systems. These components work in coordination to optimize energy flows, maintain system stability, and respond to both local operational requirements and external grid signals.

Cloud-Based Monitoring Systems Citizen-deployed cloud-based monitoring architectures facilitate comprehensive data aggregation, analytical processing, and visualization capabilities for privately-owned distributed prosumer installations. These systems enable prosumers to maintain autonomous oversight of their energy assets through centralized data management platforms. Real-time telemetry streams capture multidimensional operational parameters from all distributed energy resources within the prosumer's environment, encompassing photovoltaic generation output, battery energy storage system state-of-charge metrics, residential and commercial load consumption profiles, and ambient environmental variables affecting system performance. The analytical framework may employ sophisticated data processing engines that synthesize both historical datasets and real-time information streams to develop predictive computational models. These models enable accurate energy production forecasting, load demand prediction, and predictive maintenance scheduling algorithms. Machine learning methodologies systematically analyze operational behavioral patterns to optimize system efficiency, detect

statistical anomalies, and provide autonomous fault identification capabilities through pattern recognition algorithms.
Web-based visualization interfaces provide comprehensive system monitoring capabilities through intuitive dashboard architectures, facilitating remote system supervision and detailed performance analytics. Automated notification systems generate alerts for operational deviations, predictive maintenance requirements, and grid interaction anomalies through multi-channel communication protocols.

Safety Controllers Safety controllers implement distributed protection and safety functions across all prosumer system components, ensuring personnel safety and equipment protection under normal and fault conditions . These controllers utilize hardwired logic and programmable safety systems with certified safety integrity levels appropriate for energy system applications. Emergency shutdown capabilities provide rapid system isolation in response to hazardous conditions, equipment failures, or grid disturbances.

Arc fault detection systems monitor electrical installations for dangerous arc conditions, implementing rapid circuit interruption to prevent fire hazards. Ground fault protection monitors insulation integrity and provides personnel protection through differential current detection. Thermal protection systems monitor equipment temperatures and implement protective actions to prevent overheating and thermal damage.

Gas detection systems in CHP installations monitor for combustible gas leaks, implementing automatic fuel shutoffs and ventilation activation. Electrical isolation systems provide lockout/tagout capabilities for maintenance operations, ensuring safe working conditions. The safety controllers maintain continuous operation through battery backup systems and implement fail-safe operational modes.

Demand Response Controllers Demand response controllers facilitate participation in utility demand response programs and grid support services through automated load control and generation adjustment capabilities [53]. These systems receive external signals from utility companies, aggregators, or market operators, implementing predetermined response strategies based on economic and operational criteria.

Load curtailment algorithms prioritize essential loads while reducing non-critical consumption during demand response events. Generation dispatch optimization coordinates distributed energy resources to maximize economic benefits while maintaining system stability. Energy storage coordination ensures optimal charge/discharge scheduling to support demand response objectives while preserving battery lifetime.

Price-responsive control systems implement dynamic load management based on real-time electricity pricing signals, automatically shifting energy consumption to periods of lower cost.

The controllers maintain user comfort and operational requirements while optimizing economic performance through intelligent load scheduling and generation dispatch.

Automatic Load Management Automatic load management systems optimize energy consumption patterns through intelligent control of controllable loads, energy storage systems, and distributed generation resources [54]. These systems implement predictive algorithms based on weather forecasts, occupancy patterns, and historical consumption data to optimize energy flows and minimize operating costs.

Load scheduling algorithms coordinate the operation of thermal loads, electric vehicle charging, and energy storage systems to minimize peak demand and maximize renewable energy utilization. Power quality management maintains voltage and frequency stability through coordinated control of distributed resources and reactive power compensation.

Energy optimization algorithms balance multiple objectives including cost minimization, renewable energy maximization, and grid support service provision. The systems implement adaptive control strategies that learn from operational experience and adjust control parameters to improve performance over time.

Table 3.7: Control Block Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Cloud-Based Monitoring	Real-time operational data aggregation, performance analytics, predictive modeling results, system health indicators	Data acquisition configuration, alert threshold settings, analytics parameter adjustment, dashboard customization
Safety Controllers	Equipment status monitoring, fault detection signals, emergency conditions, protection system states	Emergency shutdown activation, protection setting adjustment, safety system testing, isolation control
Demand Response Controllers	Utility signals, price information, load curtailment status, generation dispatch levels	Demand response activation, load curtailment commands, generation adjustment, economic optimization
Automatic Load Management	Load consumption patterns, energy optimization results, scheduling parameters, system efficiency metrics	Load scheduling commands, optimization parameter adjustment, control strategy selection

3.1.3.2 Load Block

The load block encompasses controllable load systems, communication infrastructure, and end-use devices that respond to control signals from the management plane. This block includes IoT communication hubs, smart appliances, and electric vehicle charging systems, all integrated through standardized communication protocols and control interfaces.

IoT Hub Systems IoT hub systems provide centralized communication and control interfaces for distributed loads and smart devices within the prosumer installation [55]. These hubs implement multiple communication protocols including WiFi, Zigbee, Z-Wave, and cellular connectivity to accommodate diverse device requirements and ensure comprehensive system integration.

Device management capabilities include automatic discovery, registration, and configuration of connected devices. Protocol translation services enable interoperability between devices using different communication standards, ensuring seamless integration within the overall system architecture. Security frameworks implement encryption, authentication, and access control mechanisms to protect against cybersecurity threats.

Data aggregation functions collect operational data from connected devices, providing local processing capabilities to reduce communication bandwidth requirements and improve system responsiveness. Edge computing capabilities enable local decision-making for time-critical control functions while maintaining connectivity to cloud-based management systems.

Smart Appliances Smart appliances encompass household and commercial equipment capable of responding to external control signals while maintaining user comfort and operational requirements. These devices include heating, ventilation, and air conditioning (HVAC) systems, water heaters, refrigeration systems, and other energy-intensive loads.

HVAC systems implement smart thermostats with occupancy sensing, weather compensation, and predictive control algorithms. These systems respond to demand response signals by adjusting temperature set-points within acceptable comfort ranges while maintaining indoor air quality requirements. Heat pump systems coordinate operation with renewable energy availability and electricity pricing signals.

Water heating systems implement thermal storage capabilities, utilizing off-peak electricity and renewable energy availability to minimize operating costs while ensuring hot water availability. Smart controls optimize heating schedules based on usage patterns and external price signals. Refrigeration systems implement thermal mass utilization to provide demand response capabilities without compromising food safety requirements.

Electric Vehicle Charging Systems Electric vehicle charging systems provide controllable load capabilities with bidirectional power flow potential for vehicle-to-grid applications. These systems implement smart charging algorithms that coordinate charging schedules with renewable energy availability, electricity pricing, and grid support requirements while meeting vehicle mobility needs.

Charging controllers implement multiple charging rates and scheduling capabilities, allowing optimization based on departure times, energy costs, and grid conditions. Vehicle-to-grid capable systems enable electric vehicles to provide grid support services through controlled discharging during peak demand periods or grid emergencies.

Load balancing systems coordinate multiple charging stations to prevent local transformer overloading and minimize infrastructure upgrade requirements. Communication interfaces provide user interaction capabilities through mobile applications, enabling charging schedule customization and energy cost tracking.

Table 3.8: Load Block Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
IoT Hub Systems	Device connectivity status, communication protocol data, network performance metrics, security event logs	Device configuration commands, protocol selection, security parameter settings, network optimization
Smart Appliances	Energy consumption patterns, operational status, comfort parameters, efficiency metrics	Load control commands, scheduling parameters, set-point adjustments, operational mode selection
EV Charging Systems	Charging status, battery state-of-charge, power flow measurement, vehicle connectivity	Charging schedule commands, power level control, V2G activation, load balancing coordination
Communication Interface	Data transmission rates, signal quality metrics, latency measurements, error rates	Communication parameter configuration, quality-of-service settings, protocol optimization

3.1.4 Communication and Networking Layer

The communication and networking layer provides the essential infrastructure for data exchange, command transmission, and system coordination within the prosumer architecture. This layer encompasses Advanced Metering Infrastructure components and comprehensive networking systems that enable bidirectional communication between distributed energy re-

sources, control systems, and external grid operators. The architecture implements standardized communication protocols, cybersecurity frameworks, and quality-of-service mechanisms to ensure reliable and secure data transmission across all system components.

3.1.4.1 AMI Components

The Advanced Metering Infrastructure components form the foundation of the communication system, providing accurate measurement capabilities and data management functions essential for prosumer operations. These components encompass smart meters for precise energy measurement and Meter Data Management Systems (MDMS) for comprehensive data processing and storage.

Smart Meters Smart meters implement advanced measurement capabilities with bidirectional communication functions, enabling precise monitoring of energy flows in both consumption and generation modes. These devices utilize high-accuracy measurement circuits with appropriate sampling rates to capture power quality parameters, energy consumption patterns, and generation output data. The meters incorporate time-of-use functionality, demand measurement capabilities, and power quality monitoring including voltage, current, frequency, and harmonic analysis.

Communication interfaces implement multiple protocols including cellular, power line communication (PLC), radio frequency mesh networks, and fiber optic connections to ensure reliable data transmission under diverse operational conditions. The meters maintain secure communication channels through encryption algorithms and authentication protocols, protecting against cybersecurity threats and unauthorized access attempts.

Data logging capabilities store measurement data locally with appropriate storage capacity and retention periods, ensuring data availability during communication outages. Event logging functions record power quality disturbances, outage events, tamper detection, and system anomalies for comprehensive system monitoring and forensic analysis. Load profile recording captures detailed consumption and generation patterns at configurable intervals for billing, forecasting, and optimization applications.

Remote configuration capabilities enable utility operators to update measurement parameters, communication settings, and operational modes without physical site visits. Disconnect/reconnect functionality provides remote service control capabilities while maintaining safety compliance and customer notification requirements. The meters implement self-diagnostic functions with automated health monitoring and fault reporting capabilities.

Meter Data Management Systems provide centralized data collection, validation, editing, and estimation functions for smart meter data streams. These systems implement scalable database architectures capable of processing high-volume data streams from multiple pro-

sumer installations while maintaining data integrity and availability. Smart meter data typically reaches the MDMS via an Advanced Metering Infrastructure (AMI) Head-End System. This data can originate either directly from meters communicating with the Head-End System, or indirectly from meters that first transmit their data to local aggregators (which may be strategically located near substations or other points in the distribution network) before being forwarded to the Head-End System. Data validation algorithms detect and correct measurement errors, communication failures, and data inconsistencies through automated processing rules and exception handling procedures.

Data aggregation functions compile individual meter readings into meaningful reports for billing, load forecasting, and system planning applications. Historical data analysis capabilities provide trend identification, pattern recognition, and performance benchmarking functions. The systems implement data warehousing capabilities with appropriate retention policies and archival procedures for regulatory compliance and long-term analysis requirements.

Integration interfaces connect MDMS with utility billing systems, distribution management systems, and customer information systems through standardized data exchange protocols. Real-time data streaming capabilities provide immediate access to critical measurement data for operational decision-making and emergency response procedures. Data export functions support regulatory reporting requirements and third-party system integration needs.

Quality assurance mechanisms implement data validation rules, outlier detection algorithms, and estimation procedures for missing or erroneous data. The systems maintain audit trails for all data modifications and provide comprehensive reporting capabilities for regulatory compliance and operational transparency.

3.1.4.2 Network Infrastructure

The network infrastructure provides the communication backbone for prosumer systems, implementing robust networking solutions that ensure reliable data transmission, and quality-of-service management across diverse communication requirements.

Router Systems Router systems provide packet routing and network management capabilities for prosumer communication networks. These devices implement multiple communication interfaces including Ethernet, cellular, satellite, and wireless connections to accommodate diverse connectivity requirements and ensure communication redundancy. Advanced routing protocols optimize data transmission paths based on network conditions, latency requirements, and quality-of-service parameters.

Network security functions implement firewall capabilities, intrusion detection systems, and virtual private network connections to protect against cybersecurity threats. Traffic management capabilities provide bandwidth allocation, priority queuing, and congestion control

Table 3.9: AMI Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Smart Meters	Bidirectional energy measurement, power quality parameters, demand profiles, event logging, communication status	Configuration updates, measurement interval adjustment, disconnect/reconnect commands, diagnostic procedures
MDMS	Data validation results, aggregated consumption patterns, system performance metrics, quality indicators	Data processing configuration, validation rule updates, report generation commands, integration parameters
Communication Interface	Signal strength indicators, data transmission rates, error statistics, latency measurements	Protocol configuration, security parameter updates, quality-of-service settings, network optimization
Data Storage Systems	Database performance metrics, storage utilization, backup status, data integrity indicators	Retention policy configuration, backup scheduling, archival commands, performance optimization

mechanisms to ensure critical data transmission during peak usage periods. The routers maintain network performance monitoring with real-time analysis of throughput, latency, packet loss, and connection availability.

Edge computing capabilities enable local data processing and decision-making functions, reducing communication bandwidth requirements and improving system responsiveness. Protocol translation services facilitate interoperability between different communication standards and legacy systems. Network redundancy features provide automatic failover capabilities and load balancing across multiple communication paths.

Logic Network Organisation Logic network organisation encompasses the architectural framework for network topology design, protocol selection, and communication flow optimization within the prosumer system. This framework implements hierarchical network structures with appropriate segmentation for operational efficiency, security isolation, and scalability requirements.

Network topology design considers communication requirements, geographic constraints, and reliability objectives to optimize data transmission paths and minimize single points of failure. Protocol standardization ensures interoperability between diverse system components while maintaining flexibility for future technology integration. Communication flow optimiza-

tion balances bandwidth utilization, latency requirements, and energy efficiency considerations.

Network management systems provide centralized monitoring and control capabilities for distributed communication infrastructure. Configuration management ensures consistent network parameters across all system components while enabling localized optimization for specific operational requirements. Performance monitoring capabilities track network utilization, identify bottlenecks, and optimize resource allocation.

Table 3.10: Network Infrastructure Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Router Systems	Network performance metrics, traffic analysis, connection status, security event logs	Routing configuration, security policy updates, QoS parameter adjustment, diagnostic commands
Logic Network Organisation	Network topology data, protocol performance, communication flow analysis, scalability metrics	Network architecture configuration, protocol selection, topology optimization, standards compliance
Network Management	System-wide performance data, configuration status, maintenance schedules, compliance reports	Configuration management commands, performance optimization, maintenance scheduling, reporting parameters

3.1.5 Market and Trading Interface

The market and trading interface provides the economic optimization and transaction mechanisms that enable prosumer participation in electricity markets and peer-to-peer energy trading systems [56], [57]. This interface encompasses Virtual Power Plant management capabilities and distributed trading platforms that facilitate energy monetization, market participation, and collaborative energy sharing among prosumer communities. The architecture implements sophisticated bidding algorithms, settlement mechanisms, and regulatory compliance frameworks to maximize economic benefits while ensuring grid stability and market integrity.

3.1.5.1 Virtual Power Plant Management

Virtual Power Plant management systems aggregate distributed energy resources from multiple prosumer installations to create virtual generation and storage portfolios capable of participating in wholesale electricity markets [58]. These systems coordinate diverse energy assets

including renewable generation, energy storage, and controllable loads to provide grid services, energy arbitrage, and ancillary service provision with market-scale operational capabilities.

Resource Aggregation and Coordination Resource aggregation systems combine individual prosumer assets into portfolios with sufficient capacity and reliability characteristics for wholesale market participation. Advanced forecasting algorithms predict aggregate generation output, storage availability, and load flexibility based on historical patterns, weather forecasts, and operational constraints. The systems implement sophisticated optimization algorithms that balance individual prosumer preferences with overall portfolio performance objectives.

Portfolio management functions coordinate charging and discharging of distributed storage systems to maximize energy arbitrage opportunities while maintaining grid support capabilities. Load aggregation algorithms identify and coordinate flexible loads across multiple installations, creating virtual demand response resources with predictable performance characteristics. Generation dispatching coordinates renewable energy output with storage systems and controllable loads to provide firm capacity commitments to wholesale markets.

Risk management frameworks assess and mitigate operational risks associated with weather variability, equipment failures, and market price volatility. The systems implement diversification strategies across geographic regions, technology types, and customer segments to reduce portfolio risk and improve market performance predictability. Automated rebalancing mechanisms adjust portfolio composition based on performance metrics and market conditions.

Compliance monitoring ensures adherence to market rules, grid codes, and regulatory requirements across all participating prosumer installations. Performance tracking systems monitor individual asset contributions and overall portfolio performance against market commitments. Settlement and reconciliation functions allocate market revenues and costs among participating prosumers based on contribution metrics and contractual agreements.

Market Participation and Bidding Market participation systems implement automated bidding strategies for day-ahead, real-time, and ancillary service markets based on portfolio capabilities and economic optimization objectives. Bidding algorithms consider forecast generation, load patterns, storage state-of-charge, and market price predictions to formulate optimal bid strategies. The systems maintain real-time monitoring of market conditions and portfolio status to enable dynamic bid adjustments and performance optimization.

Price forecasting models utilize machine learning algorithms and market analysis to predict electricity prices across different market timeframes and products. These forecasts inform bidding strategies and operational decisions to maximize revenue while minimizing risks associated with price volatility. Advanced analytics identify market opportunities and optimal timing for energy trading activities.

Grid service provision capabilities enable Virtual Power Plant participation in frequency regulation, voltage support, and ramping services through coordinated control of distributed resources. The systems implement rapid response mechanisms that can adjust portfolio output within market-specified timeframes for ancillary service provision. Performance verification systems ensure compliance with market requirements and maintain qualification for premium ancillary service markets.

Communication interfaces provide real-time data exchange with wholesale market operators, transmission system operators, and regulatory authorities. Automated reporting systems generate required market reports, compliance documentation, and performance metrics for regulatory oversight. The systems maintain secure communication channels with market participants while protecting proprietary operational data and customer privacy.

Table 3.11: Virtual Power Plant Management Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Resource Aggregation	Portfolio capacity data, forecasting results, performance metrics, risk assessments	Asset coordination commands, portfolio rebalancing, optimization parameters, compliance monitoring
Market Bidding Systems	Market price data, bid performance, portfolio availability, settlement results	Bidding strategy configuration, price threshold settings, market participation commands, performance optimization
Grid Service Provision	Ancillary service performance, response time metrics, qualification status, grid support capabilities	Service activation commands, performance parameter adjustment, qualification maintenance, response coordination

3.1.5.2 Peer-to-Peer Trading Platforms

Peer-to-peer trading platforms enable direct energy transactions between prosumers within local communities, bypassing traditional utility intermediaries while maintaining grid stability and regulatory compliance. These platforms implement blockchain-based transaction systems, automated trading algorithms, and community energy sharing mechanisms that optimize local energy utilization and provide economic benefits to participating prosumers.

Distributed Transaction Systems Distributed transaction systems utilize blockchain technology and smart contracts to facilitate secure, transparent, and automated energy transactions

between prosumers. These systems implement consensus mechanisms that validate transactions without requiring centralized authorities while maintaining transaction integrity and preventing double-spending issues. Cryptographic security frameworks protect transaction data and participant privacy while enabling transparent market operations.

Smart contract implementations automate transaction execution based on predefined trading rules, pricing mechanisms, and delivery schedules. These contracts include dispute resolution mechanisms, penalty clauses for non-performance, and automatic settlement procedures that reduce transaction costs and eliminate counterparty risks. The systems maintain immutable transaction records that provide audit trails and regulatory compliance documentation.

Scalability solutions implement layer-2 protocols and off-chain transaction processing to handle high-frequency trading volumes while maintaining reasonable transaction costs. Interoperability frameworks enable integration with external payment systems, utility billing platforms, and regulatory reporting requirements. The systems implement energy tokenization mechanisms that represent energy units as tradeable digital assets with verifiable authenticity and ownership.

Community Energy Markets Community energy markets create localized trading environments where prosumers can buy and sell energy within geographical or virtual communities based on shared preferences, environmental goals, or economic objectives [59]. These markets implement dynamic pricing mechanisms that reflect local supply and demand conditions while considering grid constraints and community objectives.

Matching algorithms pair energy buyers and sellers based on preferences, proximity, timing requirements, and pricing criteria. The systems implement auction mechanisms, bilateral trading, and continuous market operations to accommodate diverse trading preferences and optimize market efficiency. Price discovery mechanisms establish fair market prices based on local supply and demand dynamics while considering external market conditions.

Community governance frameworks enable participant communities to establish trading rules, dispute resolution procedures, and market operation parameters through democratic decision-making processes. The systems implement reputation mechanisms that track participant reliability and performance to build trust within trading communities. Incentive structures encourage grid-friendly behavior and community cooperation through performance-based rewards and penalties.

Grid integration systems ensure that peer-to-peer transactions comply with distribution system constraints and maintain grid stability. Real-time grid monitoring capabilities track local network conditions and implement automatic transaction limiting during congestion or emergency conditions. The systems coordinate with distribution system operators to provide

necessary data and control capabilities for safe and reliable grid operation.

Table 3.12: Peer-to-Peer Trading Platform Components: Data Types and Control Commands

Component	**Data Types and Measurements**	**Control Commands and Parameters**
Distributed Transaction Systems	Blockchain transaction data, smart contract status, security metrics, consensus validation results	Smart contract configuration, security parameter updates, consensus mechanism selection, transaction validation
Community Energy Markets	Local market data, participant matching results, pricing information, community governance metrics	Market rule configuration, matching algorithm parameters, pricing mechanism selection, governance procedure updates
Grid Integration Interface	Distribution system status, constraint monitoring data, safety compliance metrics, coordination signals	Grid constraint enforcement, safety limit configuration, coordination protocol updates, emergency response procedures

Risk management functions assess and mitigate trading risks including price volatility, counterparty default, and technical failures. Automated hedging mechanisms provide price stability for risk-averse participants while enabling price exposure for participants seeking higher returns. The systems implement portfolio diversification strategies that spread trading risks across multiple counterparties and time periods.

Performance analytics track trading outcomes, participant satisfaction, and community benefits to continuously improve trading algorithms and market operations. The systems provide comprehensive reporting capabilities that enable participants to analyze their trading performance and optimize their strategies. Market efficiency metrics monitor transaction costs, price spreads, and market liquidity to ensure optimal market performance.

3.2 Prosumer Vulnerability: Highlights

The distributed nature of prosumer energy systems, spanning the generation plane, storage systems, control and management plane, communication infrastructure, and market interfaces analyzed in the previous section, introduces multiple attack vectors that adversaries may exploit to compromise system integrity, manipulate energy flows, or disrupt grid operations. The attack surface encompasses five primary categories of vulnerability: Supply chain compromise of distributed hardware components across generation and storage layers, network and proto-

col exploitation targeting the communication and networking infrastructure, application and software vulnerabilities within the control and management systems, social engineering attacks that exploit human factors in system operation, and lastly the compromise of the sovereignty of data. A complete analysis of these vulnerability is essential for highlighting what is missing in securing prosumer environments.

3.2.1 Supply Chain Compromise

Supply chain compromise represents a critical vulnerability vector within prosumer energy systems that fundamentally challenges traditional cybersecurity threat models and attack assumptions. Conventional cybersecurity literature often theorizes that achieving significant impact on power grid stability requires adversaries to gain control over substantial numbers of distributed prosumer installations within specific geographic regions, necessitating sophisticated coordination and widespread system infiltration [60]. However, the concentrated nature of prosumer technology manufacturing and integration creates a more accessible attack pathway through supply chain infiltration, where compromising a single manufacturer or integrator can potentially affect thousands of installations simultaneously without requiring individual system breaches or complex coordination mechanisms.

The significance of supply chain attacks in prosumer systems extends beyond traditional malware insertion or hardware tampering, encompassing the potential for systematic vulnerabilities embedded within firmware, control algorithms, communication protocols, and hardware components during the manufacturing process. These vulnerabilities can remain dormant for extended periods, activated remotely or triggered by specific operational conditions, enabling adversaries to achieve widespread system compromise through a single point of entry. The distributed nature of prosumer installations amplifies the impact potential, as compromised systems span residential, commercial, and industrial sectors across diverse geographic regions, creating opportunities for coordinated attacks on grid stability, market manipulation, or critical infrastructure disruption.

Furthermore, the complexity of modern prosumer systems, incorporating components from multiple suppliers across the generation layer, storage systems, control and management plane, communication infrastructure, and market interfaces, creates numerous entry points throughout the supply chain. Manufacturing processes involve integration of semiconductors, power electronics, communication modules, and software components from diverse global suppliers, each representing potential compromise points. The extended supply chain geography, often spanning multiple countries with varying cybersecurity standards and regulatory oversight, compounds vulnerability exposure and complicates threat attribution and mitigation efforts. As detailed in the latest report of Wood Mackenzie [61], the current market structure for prosumer technologies demonstrates significant concentration that amplifies supply chain

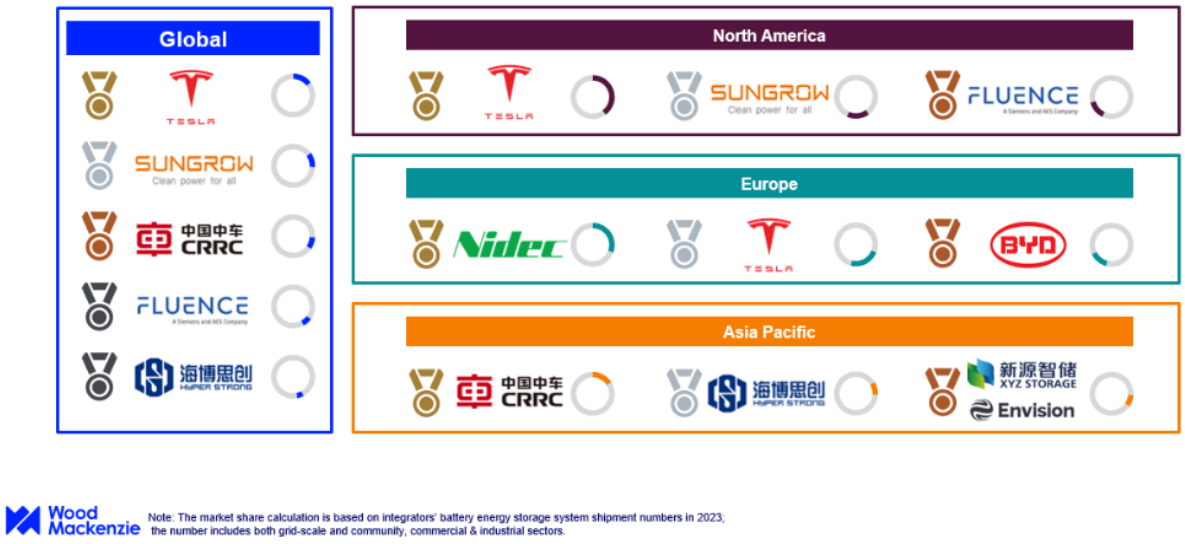


Figure 3.3: Battery energy storage system integrator market share ranking, 2023 [61]

compromise risks to unprecedented levels. According to Figure 3.3, global Battery Energy Storage System Integrator Ranking 2023, Tesla has emerged as the leading producer in the battery energy storage system (BESS) integrator market with a market share of approximately 15% in 2023, overtaking previous market leaders and establishing dominant positions across multiple regional markets. Despite an overall trend toward market fragmentation, with the global top five BESS integrators' combined market share decreasing from 62% in 2022 to 47% in 2023, significant regional concentrations persist that create substantial vulnerability exposure.

Regional market analysis reveals alarming concentration levels that magnify supply chain compromise impacts. In the European market, the top three energy storage system integrators—Nidec, Tesla, and BYD—captured 68% of market share in 2023, representing a 26% year-over-year increase in market concentration. North American markets demonstrate even higher concentration levels, with Tesla, Sungrow, and Fluence commanding 72% of regional market share for BESS shipments in 2023, reflecting a 20% year-over-year growth in market dominance. Tesla's market share in North America specifically surged by 60% year-over-year, driven by vertical integration strategies encompassing manufacturing hardware, software development, and complete energy storage solutions.

The Asia Pacific region presents additional complexity through Chinese market dominance, with six of the global top ten BESS integrators being China-based companies. This concentration reflects both the substantial domestic market demand within China and the competitive advantages achieved through integrated manufacturing ecosystems and government support policies. Chinese companies' strengthened dominance in regional markets, exemplified by

CRRC's emergence as the leading BESS integrator in the Asia Pacific region due to cost competitiveness advantages, demonstrates how supply chain concentration can achieve geographic clustering that amplifies potential attack impacts.

Tesla's vertical integration strategy exemplifies both the efficiency benefits and security vulnerabilities inherent in concentrated supply chains. The company maintains control over the entire value chain from component manufacturing to energy storage solution deployment, operating through centralized production facilities including a 40-GWh Megapack factory in Lathrop, California. While this integration enables rapid feature deployment and improved asset lifecycle management, it simultaneously creates single points of failure where supply chain compromise could affect extensive installations across multiple regions and market segments.

The combination of high-volume production, extensive geographic distribution, and integrated supply chains creates conditions where compromising a single major manufacturer could potentially affect tens of thousands of installations simultaneously.

The implications of supply chain compromise extend beyond individual system security to encompass broader grid stability and market integrity concerns. Compromised prosumer systems operating across multiple geographic regions **could enable coordinated attacks on transmission systems**, **market manipulation through synchronized trading behaviors, or cascading failures through interconnected distribution networks.** The temporal aspects of supply chain attacks, where malicious code or hardware modifications can remain dormant for months or years before activation, complicate detection and mitigation efforts while enabling adversaries to achieve widespread deployment before discovery.

These market dynamics necessitate comprehensive supply chain security frameworks that address vulnerability risks throughout the manufacturing, integration, and deployment processes. The concentrated nature of prosumer technology markets transforms supply chain security from a theoretical concern into a critical infrastructure protection imperative, requiring enhanced oversight, verification procedures, and resilience mechanisms to mitigate the substantial risks associated with manufacturer compromise scenarios.

3.2.2 Cloud Environment Compromise

Cloud infrastructure serves as the core management system for modern prosumer energy installations, providing comprehensive device management, real-time monitoring, and remote control capabilities across the entire distributed energy architecture. A general architecture overview is shown in Figure 3.4.

The cloud-based control architecture extends beyond passive monitoring to encompass active command and control functions that directly influence prosumer system operations. Cloud platforms maintain persistent connections with distributed assets through multiple communication protocols, enabling real-time parameter adjustment, operational mode changes, and emergency

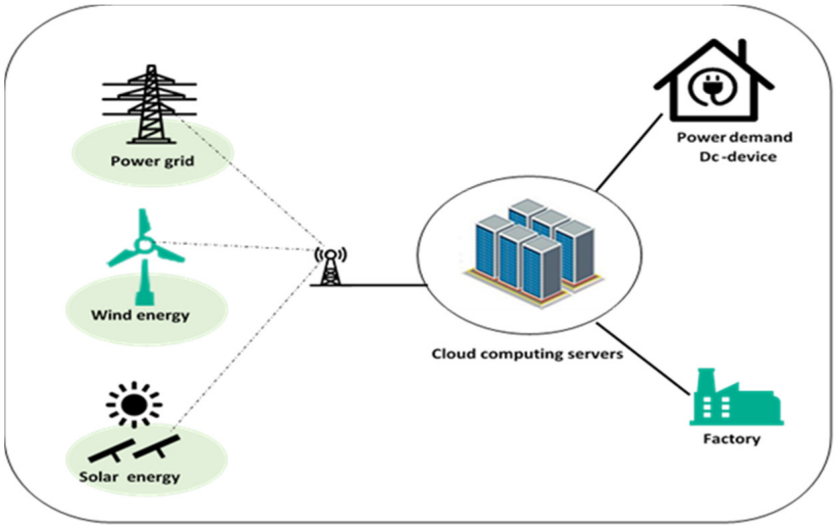


Figure 3.4: Cloud management systems function as centralised platforms for managing vast numbers of devices, including those critical for power systems [62]. A singular compromise of a cloud provider poses a substantial threat to the Electric Power and Energy System.

response coordination. Advanced cloud management systems implement hierarchical control structures where high-level optimization algorithms generate set-points and operational commands that cascade through local controllers to individual device actuators. This architecture enables sophisticated energy management strategies including predictive control, load forecasting, demand response participation, and market optimization that would be impossible to achieve through purely local control systems. The centralized nature of cloud-based prosumer management creates unprecedented vulnerability concentration where compromise of a single cloud platform can provide adversaries with access to extensive fleets of distributed energy assets. Major prosumer technology manufacturers typically operate unified cloud platforms that manage devices across multiple geographic regions, market segments, and technology types, creating attack surfaces that scale with manufacturer market share. Given the concentrated market structure analyzed in the supply chain compromise section, where leading manufacturers control substantial market segments, successful cloud platform infiltration can potentially affect hundreds of thousands or millions of distributed prosumer installations simultaneously.

Cloud-based device management platforms implement comprehensive asset lifecycle management functions including device provisioning, firmware updates, configuration management, and remote diagnostics across diverse prosumer technologies. These platforms maintain detailed device inventories with real-time status monitoring, performance analytics, and predictive maintenance capabilities. Device management functions include remote configuration of operational parameters, security credential updates, and software deployment across distributed installations. The platforms implement device clustering and fleet management capabilities

that enable coordinated control actions across multiple installations, creating opportunities for large-scale synchronized attacks if compromised.

Furthermore, IoT device management through cloud platforms encompasses smart appliances, environmental sensors, energy meters, and home automation systems integrated within the load block of the prosumer architecture. Cloud platforms provide centralized interfaces for managing diverse IoT ecosystems including device discovery, network provisioning, security key distribution, and operational policy enforcement. These systems implement device authentication protocols, encrypted communication channels, and access control mechanisms designed to prevent unauthorized device access. However, compromise of cloud-based IoT management platforms can bypass local security measures and provide direct access to building automation systems, smart appliances, and environmental control systems.

The command injection capabilities inherent in cloud-based prosumer management create substantial attack vectors for malicious system manipulation. Cloud platforms maintain authorized command channels to distributed prosumer assets, enabling remote modification of operational parameters, set-points, and control algorithms without requiring local access or authentication bypass. Compromised cloud credentials or platform vulnerabilities can provide adversaries with legitimate command authority, making detection significantly more challenging than traditional network intrusion scenarios. Command injection attacks can leverage existing operational interfaces and authorized communication channels, potentially evading intrusion detection systems and security monitoring tools focused on unauthorized access attempts.

Load control attacks through compromised cloud platforms can manipulate energy consumption patterns across extensive residential and commercial installations to create artificial demand spikes, grid instability, or targeted infrastructure overloading. Cloud-based IoT device management platforms typically maintain direct control over smart appliances including HVAC systems, water heaters, electric vehicle chargers, and industrial equipment. Adversaries with cloud platform access can coordinate simultaneous activation of high-power loads across geographic regions to create synchronized demand surges that exceed transmission capacity or destabilize frequency regulation systems. Conversely, coordinated load disconnection can create sudden demand drops that trigger generator ramping issues and grid stability problems.

Smart appliance control through compromised cloud platforms extends beyond simple on/off commands to encompass sophisticated load profile manipulation. HVAC systems can be manipulated to create heating or cooling loads that exceed building infrastructure capacity, potentially causing equipment damage or safety hazards. Water heating systems can be coordinated to create thermal loads that stress distribution transformers or create demand patterns that interfere with utility load forecasting algorithms. Refrigeration systems can be manipulated to compromise food safety through temperature excursions while simultaneously creating coordinated electrical loads.

Electric vehicle charging system compromise through cloud platforms represents particularly critical attack vectors due to the high-power nature of EV charging loads and their integration with distribution infrastructure. Cloud-based EV charging management platforms typically control charging schedules, power levels, and grid interaction functions across extensive charging networks. Compromised platforms can manipulate charging current levels to create dangerous conditions including transformer overloading, voltage regulation failures, and protective relay operation. Coordinated high-power charging activation across distribution feeders can trigger automatic meter disconnection through overcurrent protection, creating cascading outages that extend beyond the immediate attack targets.

Advanced EV charging attacks can exploit vehicle-to-grid capabilities to inject power into distribution systems at inappropriate times or voltage levels, potentially damaging distribution equipment or creating safety hazards for utility workers. Manipulated charging algorithms can create harmonic distortion, voltage fluctuations, and power quality issues that propagate through distribution networks. Coordinated EV charging attacks can create artificial peak demand periods that trigger expensive peaking generation or cause utilities to implement emergency demand response procedures.

Smart inverter platform compromise enables direct manipulation of distributed generation and energy storage systems through cloud-based management interfaces. Major inverter manufacturers operate centralized monitoring and control platforms that manage inverter parameters, grid-tie functions, and safety systems across extensive installations. Compromised inverter platforms can manipulate power output levels, reactive power compensation, frequency response characteristics, and anti-islanding protection systems. These capabilities enable attacks on grid stability through coordinated generation manipulation, artificial frequency deviations, and protective system interference.

Grid-tie inverter manipulation through compromised cloud platforms can create dangerous electrical conditions including overvoltage situations, frequency deviations, and loss of anti-islanding protection. Coordinated inverter tripping can create sudden generation loss equivalent to conventional power plant outages, while coordinated reconnection can create voltage and frequency transients that damage distribution equipment. Manipulated reactive power control can create voltage regulation problems, power factor penalties, and equipment overheating across distribution networks.

Battery energy storage system cloud platforms provide comprehensive control over charge/discharge schedules, grid support functions, and safety systems across distributed installations. Compromised BESS platforms can manipulate state-of-charge management, thermal protection systems, and emergency shutdown functions to create safety hazards including thermal runaway, fire risks, and toxic gas emissions. Coordinated BESS manipulation can create artificial energy arbitrage opportunities, manipulate ancillary service markets, and interfere with

grid stabilization functions during emergencies.

Market manipulation through compromised cloud platforms extends to virtual power plant management systems and peer-to-peer trading platforms that coordinate distributed energy resources for market participation. Compromised VPP platforms can manipulate bidding strategies, generation forecasts, and energy delivery commitments to create artificial market conditions, price manipulation, and grid reliability issues. P2P trading platform compromise can enable fraudulent transactions, market manipulation, and disruption of community energy sharing programs.

The scale and impact potential of cloud environment compromise in prosumer systems far exceeds traditional cybersecurity threat models due to the combination of manufacturer concentration, centralized control architectures, and the critical nature of energy infrastructure. Single cloud platform compromises can potentially affect energy systems across multiple countries, market sectors, and technology types simultaneously. The legitimate command authority inherent in cloud-based management systems enables sophisticated attacks that can remain undetected for extended periods while causing substantial damage to grid stability, market integrity, and public safety. These characteristics position cloud environment compromise as one of the most significant cybersecurity risks facing modern distributed energy systems.

3.2.3 Social Engineering and Human Factor Exploitation

Social engineering and human factor exploitation represent critical vulnerability vectors within prosumer energy systems that leverage the inherent trust relationships, limited security awareness, and operational complexity of distributed energy installations. Unlike traditional centralized power generation systems where human interactions are restricted to trained operational personnel with comprehensive cybersecurity training, prosumer systems rely on widespread deployment across residential and commercial sites, operated by individuals with varying levels of technical expertise and security awareness. This distributed human element creates extensive attack surfaces that malicious actors can exploit to gain unauthorized access to critical energy infrastructure components across the generation layer, storage systems, control and management plane, communication infrastructure, and market interfaces.

The prosumer energy sector demonstrates alarmingly low levels of cybersecurity awareness among end users, contrasting sharply with established security education practices in other critical infrastructure sectors. Current prosumer deployment strategies focus primarily on technical installation procedures, economic benefits, and operational efficiency while providing minimal education regarding cybersecurity risks, threat vectors, and protective measures. End users typically receive basic operational training covering system monitoring, performance optimization, and routine maintenance procedures, but lack comprehensive understanding of how their individual installations contribute to broader grid stability and the potential consequences of

security compromises on critical infrastructure resilience.

This security awareness deficit becomes particularly concerning when contrasted with cybersecurity education practices within the financial services sector, where continuous security awareness campaigns, fraud prevention programs, and threat intelligence dissemination have become standard operating procedures. Financial institutions implement comprehensive customer education programs including regular communications about emerging fraud techniques, phishing prevention strategies, identity verification procedures, and secure transaction practices. These programs utilize multiple communication channels including email notifications, mobile application alerts, website security advisories, and direct customer communications to maintain high awareness levels regarding evolving threat landscapes.

In stark contrast, the prosumer energy sector lacks equivalent systematic security awareness initiatives, leaving end users vulnerable to sophisticated social engineering attacks targeting energy system configurations, access credentials, and operational parameters. The absence of coordinated security education programs means that prosumer operators remain largely unaware of the potential grid-scale impacts that can result from individual system compromises, creating conditions where well-intentioned users may inadvertently enable large-scale infrastructure attacks through seemingly minor configuration changes or credential sharing.

The emergence of advanced artificial intelligence technologies, particularly large language models (LLMs) and sophisticated natural language processing capabilities, has fundamentally transformed the social engineering threat landscape by dramatically reducing the technical barriers to conducting convincing impersonation attacks and fraudulent communications [63], [64]. Modern AI systems can generate contextually appropriate communications that closely mimic legitimate utility companies, equipment manufacturers, technical support personnel, and regulatory authorities with unprecedented accuracy and personalization. These capabilities enable malicious actors to conduct highly targeted social engineering campaigns that leverage specific information about prosumer installations, operational patterns, and individual user preferences to maximize attack effectiveness.

Large language models can analyze publicly available information about prosumer installations, including social media posts, utility billing data, property records, and equipment specifications, to generate highly personalized and technically accurate communications that appear to originate from legitimate sources. Advanced AI systems can maintain consistent personas across extended communication campaigns, respond appropriately to user questions and concerns, and adapt their approaches based on user responses and behavioral patterns. This technological capability enables sophisticated impersonation attacks where malicious actors can convincingly represent themselves as technical support personnel, utility representatives, regulatory inspectors, or equipment manufacturers while conducting extended social engineering campaigns.

Furthermore, AI-powered voice synthesis and deepfake technologies enable real-time voice impersonation capabilities that can convincingly replicate the speech patterns, accents, and mannerisms of trusted individuals including family members, colleagues, utility personnel, or equipment vendors [65]. These capabilities enable phone-based social engineering attacks where malicious actors can conduct apparently legitimate conversations while requesting access credentials, system configurations, or authorization for remote system modifications. The sophistication of modern voice synthesis technologies makes detection of artificial speech increasingly difficult for untrained individuals, particularly during high-stress situations or emergency scenarios where users may be more susceptible to social engineering manipulation.

The combination of AI-enhanced social engineering capabilities with the low security awareness levels prevalent in prosumer environments creates conditions conducive to large-scale manipulation campaigns targeting distributed energy infrastructure. Malicious actors can leverage AI technologies to conduct coordinated attacks across thousands of prosumer installations simultaneously, using personalized communications and convincing impersonation techniques to manipulate users into performing actions that compromise system security or enable unauthorized access to critical infrastructure components.

These AI-enhanced social engineering attacks can target multiple aspects of prosumer system security, including credential harvesting campaigns where users are manipulated into providing authentication information for cloud-based management platforms, device management systems, or utility customer portals. Sophisticated phishing campaigns can utilize AI-generated communications that perfectly mimic legitimate correspondence from equipment manufacturers, utility companies, or regulatory authorities while requesting sensitive information or directing users to fraudulent websites designed to capture login credentials or personal information.

Configuration manipulation attacks represent particularly dangerous social engineering vectors where malicious actors convince prosumer operators to modify system parameters, disable security features, or install unauthorized software under the guise of performance optimization, maintenance procedures, or regulatory compliance requirements. These attacks can leverage AI-generated technical documentation, installation guides, and support communications that appear entirely legitimate while directing users to make changes that compromise system security or enable remote access capabilities.

Remote access facilitation attacks utilize social engineering techniques to convince prosumer operators to install remote access software, modify firewall configurations, or provide network access credentials under pretenses such as technical support, system optimization, or regulatory inspections. AI-enhanced communications can provide detailed technical justifications for these requests while addressing user concerns and objections with appropriate technical explanations and reassurances.

The distributed nature of prosumer systems amplifies the impact potential of successful social engineering campaigns, as individual compromises can provide access to broader networks through lateral movement techniques, or enable coordinated attacks on grid stability through simultaneous manipulation of multiple installations. Social engineering attacks targeting prosumer systems can achieve widespread impact without requiring sophisticated technical exploitation capabilities, instead leveraging human psychology, trust relationships, and information asymmetries to gain authorized access to critical infrastructure components.

The effectiveness of social engineering attacks in prosumer environments is further enhanced by the legitimate operational requirements for remote access, configuration management, and technical support that characterize modern distributed energy systems. Users are regularly required to interact with utility representatives, equipment vendors, technical support personnel, and maintenance contractors through remote communication channels, creating numerous opportunities for malicious actors to insert themselves into legitimate operational processes through impersonation and social manipulation techniques.

Moreover, the economic incentives associated with prosumer systems create additional social engineering vectors where malicious actors can leverage financial motivations to encourage user cooperation with fraudulent schemes. Attacks can target market participation functions, energy trading platforms, and financial incentive programs by convincing users to modify market participation settings, provide trading platform credentials, or authorize financial transactions under pretenses of optimizing economic returns or accessing new incentive programs.

The complex regulatory environment surrounding prosumer systems creates additional social engineering opportunities where malicious actors can impersonate regulatory authorities, compliance inspectors, or certification personnel to request system access, configuration changes, or sensitive information under the guise of regulatory compliance requirements. The technical complexity of grid integration requirements, safety standards, and market participation rules creates information asymmetries that social engineering attacks can exploit by providing seemingly authoritative guidance that actually serves malicious objectives.

The temporal aspects of social engineering attacks in prosumer environments can extend over weeks or months as malicious actors build trust relationships with target users through seemingly legitimate technical support interactions, performance optimization consultations, or regulatory compliance assistance. These extended campaigns can gather detailed information about system configurations, operational patterns, and security measures while gradually introducing requests for information or actions that ultimately compromise system security.

The scale potential of social engineering attacks targeting prosumer systems is amplified by the ability to conduct simultaneous campaigns across thousands of installations using AI-enhanced communication capabilities and automated social engineering platforms. Single

malicious actors or small groups can potentially target extensive populations of prosumer operators simultaneously, leveraging manufacturer customer databases, utility customer lists, or publicly available installation records to conduct widespread manipulation campaigns that achieve grid-scale impacts through coordinated individual compromises.

These characteristics position social engineering and human factor exploitation as among the most significant and underestimated cybersecurity risks facing distributed prosumer energy systems, requiring comprehensive security awareness programs, user education initiatives, and technical countermeasures specifically designed to address the unique vulnerabilities created by the intersection of human psychology, advanced AI capabilities, and critical energy infrastructure dependencies.

3.2.4 Cross-Jurisdictional Data Sovereignty Vulnerabilities

The contemporary prosumer energy ecosystem presents significant vulnerabilities through the absence of guaranteed data sovereignty, creating substantial attack surfaces that transcend national boundaries. This jurisdictional ambiguity manifests as a critical security concern wherein energy-related information and control systems operate across multiple legal frameworks without adequate sovereignty protections, fundamentally challenging traditional approaches to critical infrastructure security.

The most significant vulnerability emerges from the cross-jurisdictional nature of command and control infrastructure governing prosumer operations. Cloud-based energy management platforms that control prosumer devices—including smart inverters, battery management systems, and demand response mechanisms—frequently operate from data centres located in different countries from the prosumer's physical location. This architectural decision introduces critical vulnerabilities where energy infrastructure control systems may be subject to foreign jurisdiction and potential state influence. Command signals that regulate energy generation, storage, and consumption patterns may originate from, or be processed through, infrastructure located within potentially adversarial jurisdictions, creating scenarios wherein prosumer energy assets become vulnerable to foreign manipulation through legitimate access to cloud-based control systems.

The fragmented nature of global energy markets, combined with the lack of jurisdictional sovereignty protections, creates opportunities for state-sponsored cyber operations to exploit cross-border energy infrastructure dependencies. The interconnected and non-fragmented characteristics of contemporary energy markets mean that targeted manipulation of prosumer systems in one jurisdiction can potentially cascade effects across broader regional or international energy networks. State actors with jurisdiction over cloud infrastructure hosting prosumer control systems possess the theoretical capability to influence energy operations in foreign territories through legitimate access to these platforms, representing a novel form of

critical infrastructure vulnerability where traditional concepts of energy security become complicated by the distributed and cross-jurisdictional nature of prosumer management systems. Furthermore, the potential for weaponising these jurisdictional vulnerabilities as diplomatic leverage represents an emerging geopolitical risk. The ability to influence or disrupt prosumer energy systems through cloud-based infrastructure located within one's territory provides state actors with asymmetric capabilities that could be employed during periods of international tension or conflict. This sovereignty compromise inherent in current prosumer architectures necessitates a reconceptualisation of energy security that incorporates jurisdictional risk assessment and cross-border vulnerability management as core components of national critical infrastructure protection strategies, particularly given the potential for these vulnerabilities to be exploited as mechanisms of state-level coercion or influence.

3.3 Reference APT Attack Scenario Analysis

Having established the comprehensive attack surface and vulnerability vectors within prosumer energy systems, this section presents a detailed Advanced Persistent Threat scenario that serves as a reference case study for subsequent security analysis and countermeasure development. The scenario analysis encompasses three critical components: comprehensive threat actor profiling to establish adversary capabilities and motivations, systematic examination of attack progression through distinct operational phases, and quantitative impact assessment measuring potential consequences across technical, economic, and societal dimensions. This reference scenario provides a structured framework for understanding how sophisticated adversaries can exploit the identified vulnerabilities to achieve strategic objectives against distributed energy infrastructure.

3.3.1 Threat Actor Profiling

The threat landscape for prosumer energy systems encompasses diverse adversary categories, each possessing distinct motivations, capability levels, and attack methodologies that align with different vulnerability exploitation strategies. Understanding these threat actor profiles enables comprehensive risk assessment and targeted security countermeasure development appropriate for the specific threats facing distributed energy infrastructure.

Nation-State Adversaries and Advanced Persistent Threats:

Nation-state adversaries represent the most sophisticated and well-resourced threat actors targeting critical infrastructure systems, including distributed prosumer energy networks. These adversaries operate with strategic geopolitical objectives, seeking to establish persistent access to critical infrastructure for intelligence gathering, strategic disruption capabilities, and potential future conflict scenarios. Their motivations encompass national security intelligence

collection, economic espionage targeting energy market operations, technological capability assessment of distributed energy systems, and development of strategic disruption capabilities that could be activated during periods of international tension or conflict. Nation-state threat actors typically operate with substantial financial resources, often exceeding tens of millions of dollars annually for sophisticated cyber operations, enabling sustained multi-year campaigns targeting specific infrastructure sectors. Their technical capabilities include access to zero-day vulnerabilities, custom malware development, advanced social engineering resources, and coordination with human intelligence assets. These adversaries maintain specialized teams of highly skilled technical personnel, including reverse engineers, malware developers, social engineers, and operational planners with deep expertise in industrial control systems and energy infrastructure.

Nation-state adversaries demonstrate exceptional capability for exploiting supply chain compromise vectors through their ability to influence manufacturing processes, infiltrate software development pipelines, and establish relationships with technology vendors. Their substantial resources enable direct engagement with component manufacturers, software developers, and system integrators to insert persistent backdoors, modify firmware, or influence design specifications during the development process. Advanced persistent threat groups have demonstrated capability to maintain supply chain access for years while remaining undetected, creating opportunities for widespread infrastructure compromise across multiple geographic regions.

Cloud environment compromise represents a primary attack vector for nation-state adversaries due to the strategic value of cloud platform access for intelligence collection and strategic positioning. These adversaries possess the sophisticated technical capabilities necessary to conduct advanced cloud security exploitation, including zero-day attacks against cloud infrastructure, advanced lateral movement techniques within cloud environments, and sophisticated data exfiltration methods that evade detection systems. Nation-state groups often target cloud service providers directly, seeking to establish persistent access that enables monitoring and control of extensive customer installations without requiring individual system compromises.

Social engineering and human factor exploitation capabilities of nation-state adversaries include sophisticated persona development, long-term relationship building with target individuals, and coordination with human intelligence assets to enhance credibility and access. These adversaries can maintain complex social engineering campaigns spanning months or years, utilizing detailed background research, cultural expertise, and professional relationship development to gain trust and access from target individuals. Their capabilities include sophisticated impersonation techniques, document forgery, and coordination between cyber and human intelligence operations.

Cybercriminal Organizations and Financial Motivations:

Cybercriminal organizations targeting prosumer energy systems operate with primarily financial motivations, seeking to monetize access to energy infrastructure through ransomware attacks, cryptocurrency mining operations, energy theft, market manipulation, and data theft for financial gain. These adversaries demonstrate sophisticated technical capabilities combined with business-like operational structures, including specialized roles, profit-sharing arrangements, and reinvestment in advanced tools and capabilities. Their financial motivations create strong incentives for targeting high-value systems with substantial economic impact potential, making prosumer energy systems attractive targets due to their critical operational importance and potential for causing widespread disruption.

Cybercriminal organizations typically operate with substantial financial resources derived from previous successful operations, enabling investment in advanced tools, zero-day vulnerabilities, and skilled personnel. Their budgets can range from hundreds of thousands to millions of dollars annually, supporting acquisition of sophisticated attack tools, custom malware development, and recruitment of skilled technical personnel. These organizations often operate as professional enterprises with specialized technical teams, business development functions, and customer support services for their illicit offerings.

Supply chain compromise capabilities of cybercriminal organizations focus on identifying cost-effective insertion points that provide access to large numbers of potential victims simultaneously. These adversaries target software vendors, component manufacturers, and system integrators through advanced persistent attacks, seeking to insert malware or backdoors that can be monetized across extensive customer bases. Cybercriminal groups have demonstrated capability to compromise software update mechanisms, infiltrate manufacturing processes, and establish relationships with insider threats within technology companies.

Cloud environment compromise represents a high-value target for cybercriminal organizations due to the potential for accessing thousands of prosumer installations through single platform compromises. These adversaries possess advanced cloud security exploitation capabilities, including sophisticated attack techniques targeting cloud infrastructure vulnerabilities, advanced persistence mechanisms within cloud environments, and data exfiltration methods designed to evade detection while maximizing financial value extraction. Cybercriminal organizations often target cloud platforms to deploy ransomware across extensive device fleets, conduct cryptocurrency mining operations using compromised infrastructure, or steal sensitive data for financial exploitation.

Social engineering capabilities of cybercriminal organizations include professional-grade phishing operations, sophisticated voice fraud techniques, and business email compromise attacks targeting prosumer operators and service providers. These adversaries often operate specialized social engineering teams with expertise in psychological manipulation, cultural adaptation, and technical impersonation techniques. Their social engineering operations fre-

quently target financial information, authentication credentials, and system access that can be directly monetized through various fraud schemes.

Hacktivist Groups and Ideological Attacks:

Hacktivist groups targeting prosumer energy systems operate with ideological motivations related to environmental activism, anti-corporate sentiments, political protest, or social justice objectives. These adversaries seek to disrupt energy infrastructure operations to draw attention to their causes, demonstrate vulnerabilities in critical systems, or cause economic and social disruption that supports their ideological objectives. Hacktivist motivations can include opposition to specific energy policies, corporate practices, government regulations, or broader systemic issues related to energy production and distribution.

Hacktivist organizations typically operate with limited financial resources compared to nation-state or cybercriminal adversaries, often relying on volunteer participation, crowdfunding, and donations to support their operations. Their budgets are generally measured in thousands rather than millions of dollars, constraining their ability to acquire expensive tools or sustain long-term operations. However, their ideological motivations can inspire sustained volunteer participation and creative problem-solving that compensates for financial limitations. Technical capabilities vary significantly among hacktivist groups, ranging from basic script-kiddie level activities to sophisticated operations conducted by skilled technical personnel with professional cybersecurity experience.

Supply chain compromise capabilities of hacktivist groups are generally limited by their financial and technical resource constraints, making sophisticated supply chain infiltration attacks less common. However, these adversaries may target supply chain vulnerabilities through opportunistic exploitation of publicly disclosed vulnerabilities, social engineering attacks against vendor employees who support their ideological objectives, or coordination with insider threats sympathetic to their causes. Hacktivist groups may also target supply chain components through more accessible attack vectors such as open-source software contributions or public development platforms.

Contemporary Threat Intelligence: Real-World APT Activity in Energy Infrastructure

Recent cybersecurity incidents demonstrate the tangible reality of sophisticated threats targeting energy infrastructure and distributed systems. The 2020 SolarWinds supply chain compromise, attributed to the Russian SVR, affected over 18,000 organizations globally and demonstrated nation-state capability to achieve widespread infrastructure access through single vendor compromises. The 2021 Colonial Pipeline ransomware attack by the DarkSide cybercriminal organization disrupted fuel supplies across the Eastern United States, illustrating how financially motivated adversaries can cause critical infrastructure failures with substantial economic and societal impacts.

In 2023, the Volt Typhoon campaign revealed Chinese nation-state adversaries establishing persistent access to U.S. critical infrastructure, including energy systems, through "living off the land" techniques that evade traditional detection methods. The 2022 compromise of multiple European energy companies during the Ukraine conflict demonstrated how geopolitical tensions translate into increased cyber targeting of energy infrastructure.

These incidents collectively demonstrate that the threat actor capabilities and attack vectors analyzed in this threat profiling are not theoretical concerns but active operational realities requiring immediate attention and comprehensive security countermeasures.

Cloud environment compromise attacks by hacktivist groups typically focus on exploiting publicly known vulnerabilities rather than sophisticated zero-day attacks, due to their limited resources for acquiring advanced exploit capabilities. These adversaries may target cloud platforms through credential stuffing attacks, social engineering targeting cloud service personnel, or exploitation of misconfigurations and security gaps in cloud deployments. Hacktivist groups often prioritize visible impact over sophisticated persistence, seeking to cause immediate disruption that generates media attention and public awareness of their causes.

Social engineering represents a primary attack vector for hacktivist groups due to its relatively low cost and potential for high impact. These adversaries often possess strong communication skills and ideological passion that can be effective in social engineering attacks targeting individuals sympathetic to their causes or concerned about energy infrastructure issues. Hacktivist social engineering operations may leverage environmental concerns, economic inequality issues, or political grievances to gain cooperation from prosumer operators, utility personnel, or technology vendors. Their social engineering capabilities are often enhanced by deep knowledge of the issues they champion, enabling credible and passionate communications

that can be persuasive to target audiences.

3.3.2 Reference APT Scenario

The reference Advanced Persistent Threat scenario presented demonstrates a sophisticated two-phase attack campaign targeting distributed prosumer energy infrastructure with dual strategic objectives: sustained financial exploitation followed by coordinated grid-scale disruption. This comprehensive scenario, fully detailed in literature [66], comprises two distinct operational phases characterised by markedly different temporal dimensions and strategic objectives. The initial stealth phase operates across extended timeframes spanning months to years, focusing on establishing comprehensive control whilst generating sustained financial returns through covert market manipulation. The subsequent disruption phase executes immediate, high-impact operations designed to cause widespread blackouts and critical infrastructure damage. This scenario exemplifies how advanced adversaries exploit the concentrated market structure, cloud-based management platforms, and limited security awareness identified in the attack surface analysis to achieve escalating impact levels from sustained economic exploitation to catastrophic physical disruption.

The attack progression, illustrated in Figure 3.5, follows a deliberate two-phase approach where extended stealth operations establish the foundation for immediate, coordinated physical disruption capabilities that threaten grid stability and public safety.

Phase 1: Stealth Operations and Economic Exploitation (Duration: MM/YY)
The stealth phase represents an extended operational period where advanced adversaries systematically establish comprehensive control over distributed prosumer infrastructure whilst maintaining complete operational security and generating sustained financial returns through covert energy market manipulation. This phase encompasses intelligence collection, access establishment, privilege escalation, device control acquisition, and coordinated economic exploitation operations designed to remain undetected across extended timeframes whilst monetising adversary capabilities.

Intelligence gathering operations initiate the stealth phase through comprehensive reconnaissance targeting victim identity information and network infrastructure mapping to identify high-value prosumer installations and supporting infrastructure components. Advanced adversaries conduct systematic open source intelligence (OSINT) collection, social media analysis, utility customer database exploitation, regulatory filing reviews, and technical infrastructure scanning to develop detailed target profiles encompassing prosumer installations, technology vendors, cloud management platforms, utility interconnections, and key personnel. This intelligence foundation identifies manufacturer concentration patterns, cloud platform relationships,

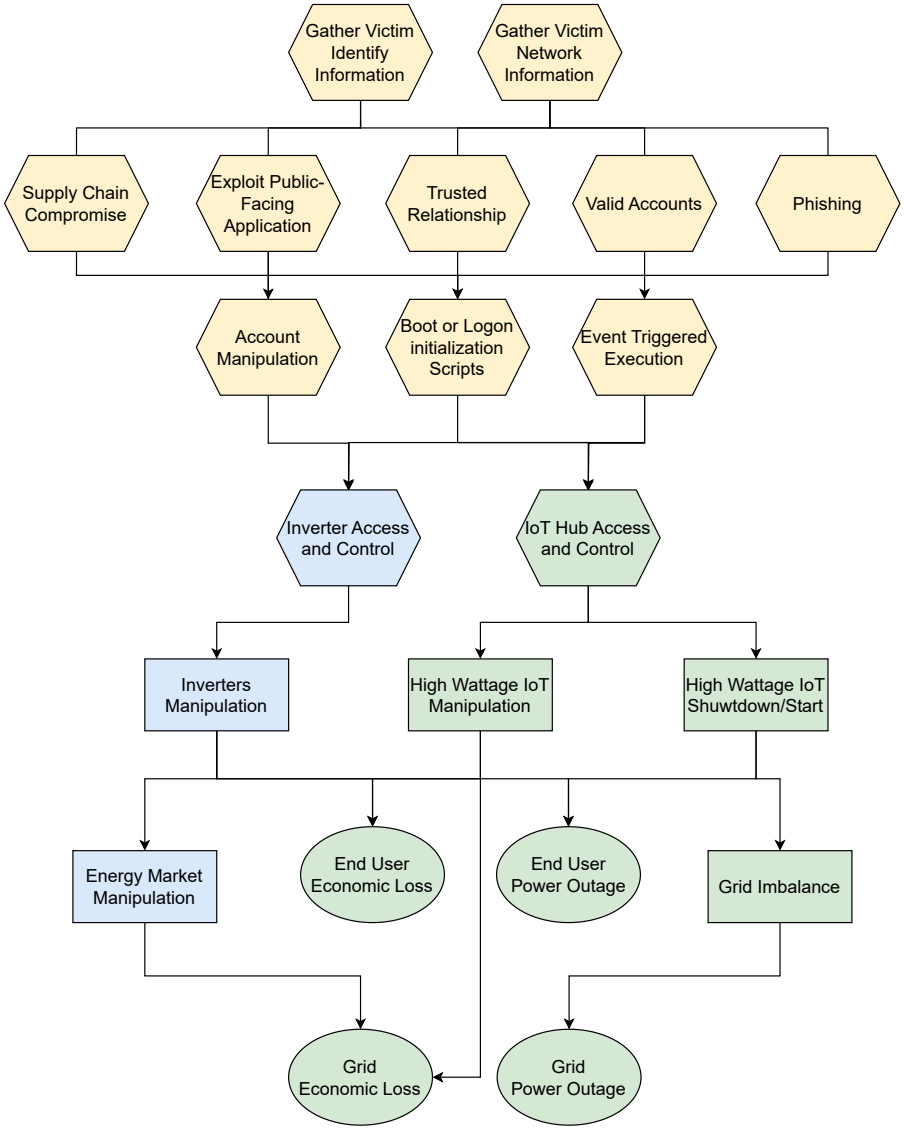


Figure 3.5: APT Attack Tree for Prosumer Energy Infrastructure [66]: Two-phase attack progression from extended stealth operations through immediate disruption capabilities. Yellow nodes indicate MITRE ATT&CK framework technique mapping for initial access vectors, demonstrating systematic advancement from covert economic exploitation to coordinated physical impact objectives.

and communication pathways that enable scalable attack approaches targeting single points of failure providing access to extensive device populations.

Initial access establishment implements multiple attack vectors simultaneously utilising supply chain compromise, exploitation of public-facing applications, trusted relationship abuse, valid account compromise, and sophisticated AI-enhanced phishing campaigns corresponding

to MITRE ATT&CK framework tactics. Supply chain infiltration targets prosumer equipment manufacturers, software vendors, and cloud service providers to insert persistent backdoors and establish widespread access capabilities. Exploitation operations focus on cloud management platforms, utility customer portals, and energy market trading platforms providing access to extensive device populations. Credential harvesting through advanced phishing and social engineering operations captures high-value authentication materials enabling legitimate system access.

Privilege escalation and lateral movement operations systematically expand adversary access scope through account manipulation, persistent malware deployment, and event-triggered execution mechanisms. Advanced adversaries establish administrative access, deploy initialization scripts ensuring continued access through system updates, and implement dormant malware with automated activation capabilities. Lateral movement utilises legitimate administrative tools and encrypted communication channels to expand access across prosumer installations, cloud platforms, and supporting infrastructure whilst maintaining operational security.

Device access and control establishment provides direct command authority over critical prosumer components including smart inverters, IoT hub systems, electric vehicle chargers, HVAC systems, and energy storage devices. Adversaries exploit cloud management platform access, manufacturer support systems, and direct device communication channels to establish persistent control over operational parameters, safety systems, and grid-tie functions. This comprehensive device control enables manipulation of power output levels, reactive power compensation, anti-islanding protection, emergency shutdown capabilities, and coordinated load control across extensive geographic regions.

Economic exploitation operations represent the primary strategic objective of the stealth phase, coordinating distributed prosumer assets to generate sustained financial returns through energy market manipulation whilst maintaining complete operational security. Advanced adversaries utilise extensive device control capabilities to create artificial market conditions, manipulate pricing mechanisms, and exploit market inefficiencies for direct financial gain. Coordinated generation and consumption pattern manipulation influences market prices, disrupts demand forecasting, and creates fraudulent market participation opportunities. Individual prosumer economic targeting generates substantial financial penalties through manipulated consumption patterns, unauthorised system modifications, and equipment damage costs whilst validating attack capabilities and establishing financial motivation for continued operations.

Device population expansion operations systematically acquire control over additional prosumer installations throughout the stealth phase to achieve critical mass necessary for subsequent disruption operations. Advanced adversaries leverage established attack infrastructure, proven exploitation techniques, and operational experience to rapidly expand control across

extensive geographic regions whilst prioritising high-power devices, critical grid interconnection points, and strategic locations maximising disruption potential. Expansion utilises lateral movement, supply chain exploitation, social engineering targeting interconnected systems, and recruitment of unwitting insider threats through trust relationship abuse.

The stealth phase maintains operational security through careful calibration of economic impact operations below detection thresholds whilst generating substantial financial returns and establishing comprehensive infrastructure control. This extended operational period provides adversaries with detailed system knowledge, proven attack capabilities, validated communication pathways, and extensive device populations necessary for subsequent immediate disruption operations.

Phase 2: Immediate Disruption Operations (Duration: Immediate)
The disruption phase transitions from covert economic exploitation to immediate, coordinated physical attacks designed to cause widespread power outages, grid instability, and critical infrastructure failures. This phase represents the culmination of extended stealth operations, utilising comprehensive device control capabilities established during Phase 1 to achieve strategic disruption objectives through synchronized manipulation of thousands of distributed prosumer installations.

Immediate power outage operations coordinate simultaneous manipulation of distributed generation, energy storage, and load control systems to create localized power failures across residential and commercial installations. Advanced adversaries utilise extensive device control capabilities to disable generation systems, rapidly exhaust energy storage reserves, and create artificial load spikes overwhelming local distribution infrastructure. Coordinated inverter shutdown eliminates distributed generation capacity whilst synchronized high-consumption device activation creates demand surges exceeding local supply capabilities.

Grid instability operations leverage comprehensive understanding of grid physics, control system operations, and protective relay coordination to create frequency deviations, voltage instability, and protective system cascading failures propagating throughout interconnected transmission systems. Advanced adversaries coordinate large-scale manipulation of distributed energy resources to create synchronized disturbances overwhelming grid stability mechanisms and triggering automated protective responses causing system-wide instability.

Widespread blackout operations represent the ultimate strategic disruption objective, utilising coordinated manipulation of thousands of distributed prosumer installations to create synchronized disruption overwhelming grid stability mechanisms and emergency response capabilities. These operations demonstrate the potential for distributed cyber attacks to achieve physical impacts equivalent to conventional kinetic attacks against critical infrastructure through

systematic exploitation of prosumer device populations established during extended stealth operations.

The immediate disruption phase can be activated for maximum impact or maintained as persistent threat capability providing strategic deterrence, coercion, or negotiation leverage. Advanced adversaries may utilise demonstrated disruption capability to achieve political objectives, economic concessions, or strategic advantages without necessarily implementing full-scale attacks. The transition from stealth to disruption operations occurs within minutes or hours, leveraging years of preparation to achieve immediate, catastrophic impact.

This two-phase reference scenario demonstrates how the concentrated market structure, cloud-based management architectures, and limited security awareness identified in the prosumer attack surface create conditions where sophisticated adversaries can achieve sustained economic exploitation followed by strategic infrastructure disruption objectives through systematic exploitation of distributed energy systems. The dual-phase approach enables adversaries to monetise their capabilities across extended timeframes whilst maintaining the ability to achieve immediate, catastrophic impacts when strategic objectives require infrastructure disruption.

3.4 Critical Security Gaps and Vulnerabilities

The reference APT scenario analysis reveals fundamental security deficiencies within current prosumer energy infrastructure that enable sophisticated adversaries to achieve grid-scale disruption through systematic exploitation of distributed systems. These critical gaps extend beyond traditional cybersecurity measures to encompass operational monitoring capabilities, cross-jurisdictional coordination mechanisms, and behavioral detection systems specifically designed for distributed energy environments. Addressing these vulnerabilities requires comprehensive security framework development that acknowledges the unique characteristics of prosumer systems while providing robust protection against advanced persistent threats.

Enhanced Infrastructure Monitoring Requirements

Current prosumer monitoring systems lack the granular visibility necessary to detect sophisticated manipulation activities that operate within normal operational parameters while achieving malicious objectives. The reference APT scenario demonstrates how adversaries can conduct prolonged economic manipulation and device control operations that remain undetected by existing monitoring systems designed primarily for performance optimization rather than security threat detection. Traditional monitoring approaches focus on aggregate performance metrics and basic fault detection, failing to identify subtle behavioral anomalies that indicate coordinated malicious activities across distributed installations.

The pressing need for enhanced monitoring capabilities encompasses real-time analysis of

generation patterns, load consumption behaviors, market participation activities, and device operational parameters at sufficient granularity to distinguish between legitimate operational variations and coordinated attack activities. Advanced monitoring systems must implement sophisticated analytics capable of detecting temporal correlations, geographic clustering patterns, and operational anomalies that suggest coordinated manipulation across multiple installations. These capabilities require integration of advanced data analytics, machine learning algorithms, and behavioral modeling techniques specifically designed for distributed energy system monitoring.

Digital Twin Infrastructure Development

The complexity of modern prosumer energy systems necessitates comprehensive digital twin development that enables security testing, vulnerability assessment, and attack scenario validation without impacting critical operational infrastructure. Digital twin platforms provide essential capabilities for modeling potential attack impacts, testing defensive measures, and validating security countermeasures under realistic operational conditions. The reference APT scenario highlights the need for understanding cascading failure mechanisms, grid stability impacts, and economic disruption potential that can only be comprehensively evaluated through sophisticated simulation environments.

Digital twin infrastructure enables proactive security management through continuous modeling of system vulnerabilities, attack pathway analysis, and defensive strategy optimization. These platforms support comprehensive scenario testing including coordinated device manipulation, market disruption modeling, and grid stability impact assessment that inform security investment decisions and defensive capability development. Advanced digital twin implementations incorporate real-time operational data integration, enabling continuous model validation and dynamic threat assessment capabilities that enhance situational awareness and incident response effectiveness.

Cross-Border Information Sharing Frameworks

The geographic distribution potential demonstrated in the reference APT scenario reveals critical gaps in cross-jurisdictional security coordination and information sharing mechanisms among energy stakeholders. Sophisticated adversaries can exploit regulatory boundaries, jurisdictional limitations, and communication gaps between utility operators, equipment manufacturers, and regulatory authorities to conduct coordinated attacks that span multiple geographic regions and regulatory domains. Current information sharing frameworks lack the speed, specificity, and technical depth necessary for effective coordination against advanced persistent threats targeting distributed energy infrastructure.

Enhanced information sharing capabilities must encompass real-time threat intelligence dissemination, coordinated incident response procedures, and collective vulnerability assessment activities that enable proactive security management through collaborative expertise. Cross-border coordination frameworks require standardized communication protocols, compatible threat intelligence formats, and coordinated response procedures that enable rapid information sharing during active attack scenarios. These capabilities necessitate international cooperation agreements, technical standard harmonization, and collaborative security investment strategies that address the transnational nature of cyber threats targeting critical energy infrastructure.

Prosumer-Specific Behavioral Detection Systems

Traditional cybersecurity detection systems designed for enterprise IT environments fail to address the unique behavioral characteristics, operational patterns, and vulnerability profiles that characterize prosumer energy installations. The reference APT scenario demonstrates how adversaries exploit the limited security awareness, diverse technical capabilities, and operational complexity that distinguish prosumer environments from conventional industrial control systems. Prosumer-specific detection systems must account for high behavioral variability, limited security expertise, and diverse operational objectives that characterize distributed energy installations.

Behavioral detection systems specifically tailored for prosumer monitoring must implement adaptive learning algorithms that accommodate legitimate operational diversity while identifying subtle manipulation patterns that indicate malicious activities. These systems require integration of user behavior analytics, device performance modeling, and energy consumption pattern analysis that distinguish between normal operational variations and coordinated attack activities. Advanced detection capabilities must address the challenge of monitoring thousands of installations with varying operational characteristics while maintaining low false positive rates that preserve user confidence and operational efficiency.

Furthermore, prosumer-specific detection systems must address the social engineering vulnerabilities identified in the attack surface analysis by monitoring for indicators of credential compromise, unauthorized access attempts, and configuration changes that suggest human factor exploitation. These capabilities require integration of technical monitoring with user behavior analysis, communication pattern monitoring, and operational change detection that identify complex attack scenarios involving both technical exploitation and social engineering components.

Table 3.13: Critical Security Gaps and Required Capabilities for Prosumer Energy Infrastructure

Security Gap	**Current Limitations**	**Required Capabilities**	**Implementation Priorities**
Enhanced Monitoring	Aggregate performance metrics, basic fault detection, limited security focus	Real-time granular analysis, behavioral anomaly detection, coordinated attack identification	Machine learning integration, advanced analytics platforms, multi-installation correlation
Digital Twin Infrastructure	Limited simulation capabilities, performance-focused modeling, static vulnerability assessment	Comprehensive attack modeling, real-time data integration, cascading failure analysis	High-fidelity simulation platforms, continuous model validation, scenario testing capabilities
Cross-Border Coordination	Jurisdictional limitations, slow information sharing, incompatible systems	Real-time threat intelligence sharing, coordinated response procedures, standardized protocols	International cooperation frameworks, technical harmonization, collaborative investment strategies
Prosumer-Specific Detection	Enterprise IT security models, limited behavioral understanding, high false positives	Adaptive learning algorithms, user behavior analytics, social engineering indicators	Tailored detection systems, prosumer behavior modeling, integrated monitoring platforms

Chapter 4

Reference Architecture for a Prosumer Oriented Cybersecurity Monitoring Framework

4.1 Scope, Basics, and Architectural Overview

This section introduces a reference architecture for a prosumer-oriented cybersecurity monitoring framework for smart grids. It is grounded in the security principles and gaps identified in the previous chapters. The framework targets Advanced Persistent Threats that coordinate distributed energy resources and IoT devices to manipulate demand. Its objective is to provide enhanced monitoring via a security-centred Digital Twin, while enabling data sharing and coordination among stakeholders across national boundaries. The architecture is organised in three layers: *field layer*, *DT layer*, and *application layer*. The field layer includes devices, gateways, and substations producing telemetry and receiving control signals. The DT layer ingests and normalises streams from the field via a publish/subscribe message broker (producer–consumer decoupling), aligns them to a semantic information model (e.g., NGSI-LD), and maintains the evolving state of the infrastructure for security analysis. The application layer hosts security services that consume DT state and events and act on results.

Four logical software Artifacts implement these functions and interact through the DT abstraction (Figure 4.1). The *Digital Twin Builder* realises ingestion, semantic alignment, and state maintenance for security use cases. The *Business Process Analyzer (BPA)* learns baseline prosumer behaviour and detects coordinated deviations consistent with manipulation-of-demand attacks. The *Data Space Connector Builder (DSCB)* enforces identity, access, and usage control for sharing indicators and incidents with cross-border partners. The *Simulation Control Unit (SCU)* orchestrates *what-if* scenarios on the DT to evaluate attacks and responses

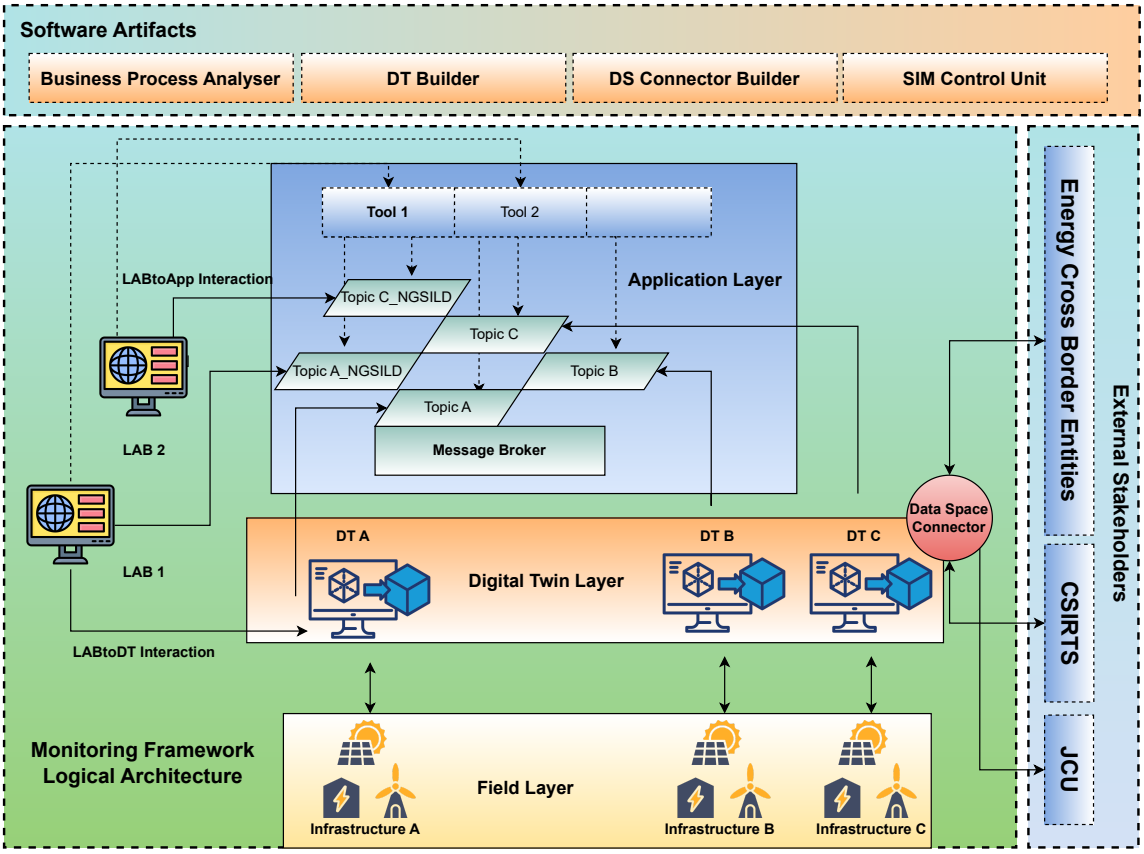


Figure 4.1: Prosumer-oriented cybersecurity monitoring framework reference architecture.

and to feed improvements back into analytics and procedures. These artefacts are specified at the functional level; concrete implementations may vary by technology stack. Figure 4.1 summarises the layers, the message-broker decoupling, and the artefact interactions.

In the next sections, we detail each artefact and its interfaces, providing the technical elements required to understand the coverage of this framework and how it addresses the gaps highlighted in Table 3.13.

4.1.1 Digital Twin Builder

Several definitions of the Digital Twin exist across domains. The Industrial Internet Consortium defines a DT as "a formal digital representation of some asset, process, or system that captures attributes and behaviours suitable for communication, storage, interpretation, or processing within a certain context" [67]. The Digital Twin Consortium describes it as "a virtual representation of real-world entities and processes, synchronised at a specified frequency and fidelity" [68]. In smart grids, these views converge on a bidirectional link between a physical

entity and its digital counterpart to support awareness, prediction, and control.

Formally, a DT can be expressed as the quadruple

$$DT = \{\, M,\ D(t),\ F,\ U \,\} \tag{4.1}$$

where M is the structural and parametric model, $D(t)$ is the time-dependent measurement stream, F is the set of mappings that update the model state, and U are the rules that synchronise and evolve the twin over time or under hypothetical scenarios [69] [70]. The interaction between the physical system $S(t)$ and the DT is

$$S(t) \xrightarrow{\mathcal{A}} D(t) \xrightarrow{F} M(t) \xrightarrow{\mathcal{G}} A(t) \tag{4.2}$$

with $\mathcal{A}$ the acquisition process, $\mathcal{G}$ the analysis/inference process, and $A(t)$ the actionable insights.

A DT maintains static attributes $\mathbf{x}_s \in \mathbb{R}^n$ (e.g., rated capacity, topology) and dynamic states $\mathbf{x}_d(t) \in \mathbb{R}^m$ (e.g., voltage, current, temperature). The state evolution is

$$\frac{d\mathbf{x}_d(t)}{dt} = f\Big(\mathbf{x}_d(t), \mathbf{u}(t), \mathbf{w}(t)\Big) \tag{4.3}$$

where $\mathbf{u}(t)$ are control inputs and $\mathbf{w}(t)$ are disturbances or attack-induced perturbations. Predictive and prospective DT functions rely on simulation models $g_k(\cdot)$, $k = 1, \ldots, K$,

$$\hat{\mathbf{x}}_d(t + \Delta t) = g_k\Big(\mathbf{x}_d(t), \theta_k\Big), \tag{4.4}$$

with θ_k calibrated from historical and real-time data.

DTs can be descriptive (state recording), diagnostic (fault localisation), predictive (state forecasting), prospective (scenario exploration, including cyberattacks), and prescriptive (action recommendation/execution) [71]. They can appear as prototypes during design, instances bound to operational assets, or aggregates that compose multiple instances to represent an infrastructure [72]. For cybersecurity monitoring, DTs integrate operational data with analytics and simulation to assess asset status, detect multi-site anomalies, explore attack paths, anticipate cascading effects, and support operator actions.

The Digital Twin Builder follows a model-driven, standards-compliant process rooted in the Common Information Model (CIM) [73]. Figure 4.2 shows a CIM Unified Modelling Language excerpt with network elements and relations. A CIM dataset from the distribution system operator cab be adopted as the baseline description of the physical grid (substations, lines, switches, measurement points), preserving alignment with the operator's engineering tools and processes. To support dynamic operation, the static CIM representation is transformed

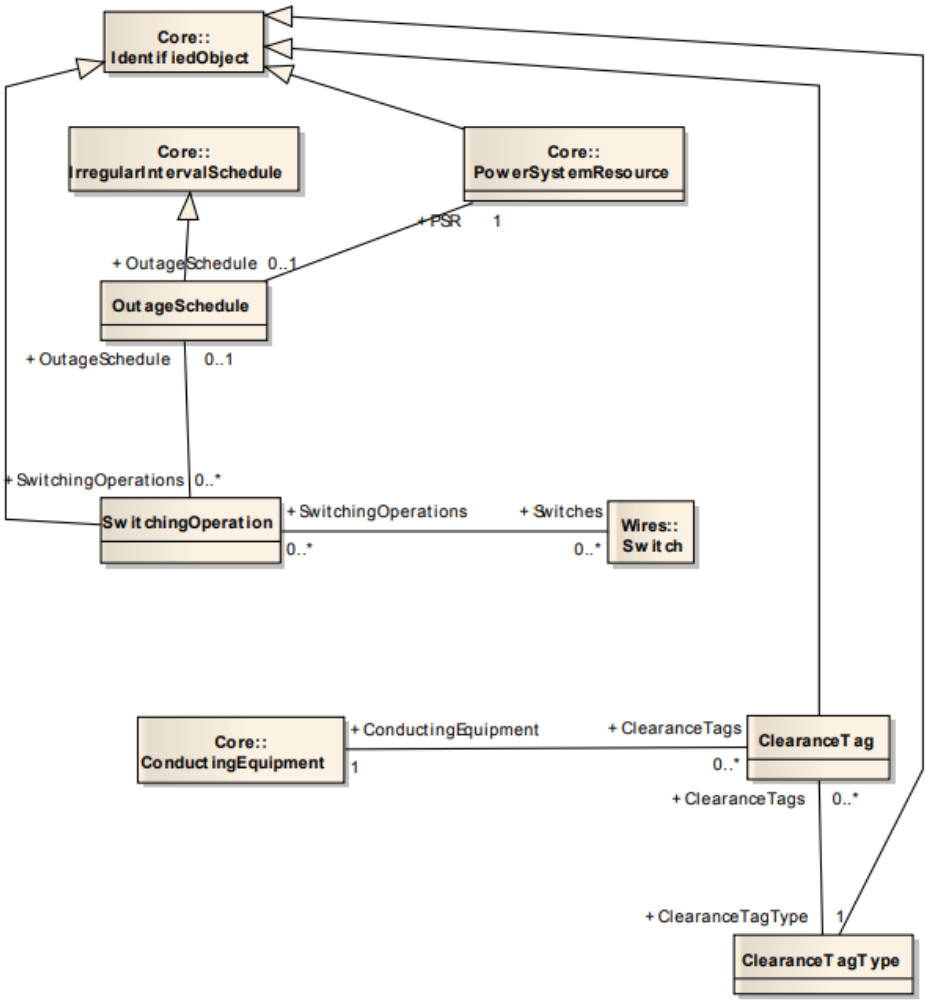


Figure 4.2: Example CIM UML diagram with components, attributes, and relationships [74].

into NGSI-LD. NGSI-LD (ETSI) specifies a linked-data information model and Application Programming Interface for entities, properties, and relationships, with JSON-LD serialisation. Figure 4.3 illustrates the mapping from CIM XML to NGSI-LD, retaining semantic types and topological links. This yields a unified model where static assets and live measurements are handled consistently. Field telemetry is decoupled from consumers through a publish/subscribe message broker (for example, Kafka-class systems). Producers, such as Intelligent Electronic Devices, Remote Terminal Units, and gateways, publish time-stamped records; consumers include the Digital Twin ingestion services, analytics, and archival stores. Decoupling supports buffering, backpressure, late joins, and replay for forensic analysis. Time synchronisation uses Network Time Protocol and Precision Time Protocol according to device class; ingestion enforces monotonicity and reconciles clock drift using sequence numbers and watermarks.

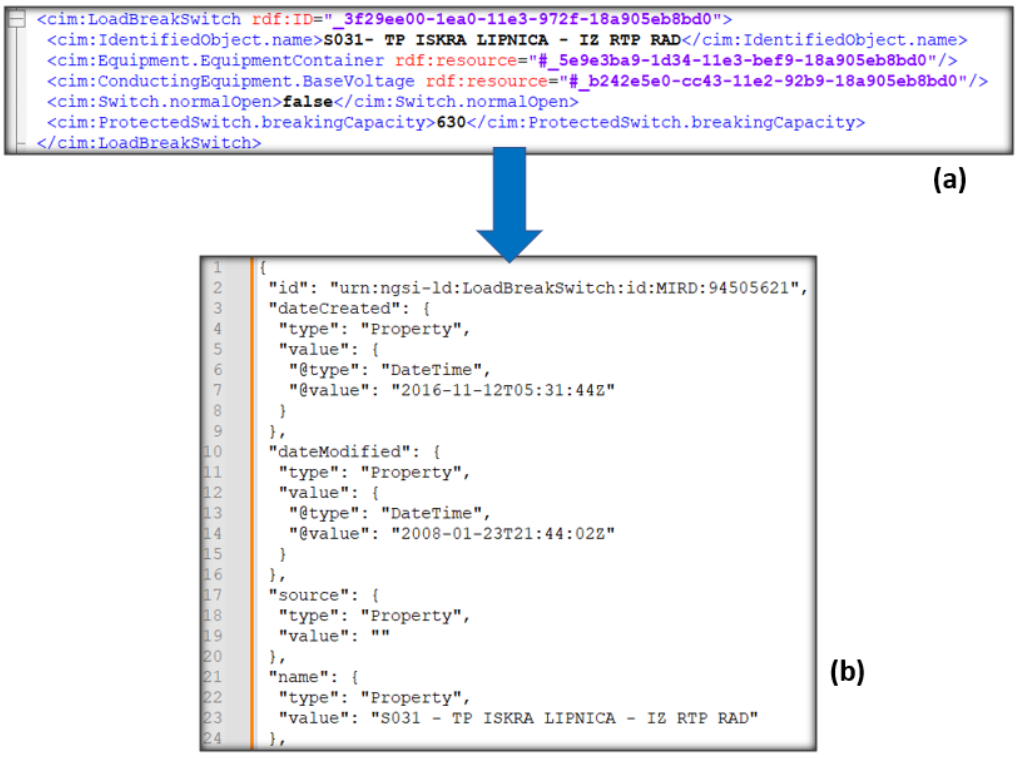


Figure 4.3: Transformation from CIM XML to NGSI-LD [75].

The NGSI-LD graph is managed by a Context Broker that implements the NGSI-LD Application Programming Interface, providing create, update, query, and subscription operations. Heterogeneous device protocols are normalised via Internet of Things Agents that translate field payloads into NGSI-LD entities and properties before insertion. Subscriptions propagate entity changes to downstream services, such as anomaly detectors and simulators, and to time-series storage for historical queries. While multiple stacks can realise these functions, including Eclipse Ditto, Azure Digital Twins with Digital Twins Definition Language adapters, and custom microservices with a graph and time-series database backend, FIWARE represents an optimal choice, offering open-source components that natively support NGSI-LD, easing interoperability and lowering integration effort without constraining deployment choices.

Information modelling concerns The DT Builder addresses: (i) *Topology fidelity*: preservation of CIM connectivity nodes, terminals, and switch states in the NGSI-LD graph; (ii) *Semantic alignment*: mapping of CIM classes to NGSI-LD `type`, with properties/relationships linked to agreed vocabularies; (iii) *Temporal handling*: representation of observations with explicit `observedAt`, sampling period, and quality flags; offloading high-rate series to a TSDB while retaining current state in the graph; (iv) *Control coupling*: optional binding of control

endpoints (setpoints, switching) as NGSI-LD properties guarded by policy and role checks; (v) *Versioning*: model snapshots with immutable identifiers for reproducibility of analyses and simulations.

Interfaces and outputs The DT exposes: (a) NGSI-LD queries over the current state and topology; (b) subscription endpoints for event-driven processing; (c) replay interfaces via the broker for time-bounded reprocessing; (d) exports of topology/state slices for the Simulation Control Unit; and (e) feature streams for the Business Process Analyzer. All interfaces are designed to be stack-agnostic and to operate under authenticated, authorisation-controlled channels.

4.1.2 Business Process Analyzer (BPA)

The BPA is the security analytics component that applies business rules over the Digital Twin to monitor the behaviour of entities (e.g., prosumers, devices, substations, applications) at fine granularity. It subscribes to DT state changes and telemetry, derives features, evaluates rule- and model-based conditions, and emits alerts and context for triage. The objective is twofold: (i) single-entity anomaly detection against expected operational behaviour; (ii) grid-level supervision to detect coordinated patterns consistent with advanced attacks (e.g., manipulation of demand). The BPA consumes DT updates via a publish/subscribe interface, queries the DT graph for topology and semantics (asset types, relations), and writes outcomes to the application layer (alerts, metrics, recommended actions). It integrates with incident tooling (e.g., SIEM/SOAR) and with the Simulation Control Unit for replay and what-if validation. The BPA starts from an explicit business-process view of grid operations. Processes are elicited from the DT model and operator procedures, identifying: (i) actors and assets (devices, gateways, services); (ii) events and data flows (telemetry, setpoints, alarms); (iii) constraints and service objectives (safety, availability, energy balance). Each process step is mapped to assets in the DT and to a threat model. Techniques and tactics from established knowledge bases (e.g., discovery, lateral movement, manipulation of control) are associated with process steps and assets. For each step, the BPA defines:

- measurable variables and features (e.g., power output, setpoint adherence, timing, topology-dependent aggregates);
- business rules and invariants (e.g., interlocks, rate limits, time-of-day envelopes, N-out-of-M quorum);
- risk thresholds and tolerances (entity-level and aggregate-level);
- detection windows and sampling plans (fixed, event-driven, or adaptive).

Single-entity baselining and detection For each entity i, the BPA builds an expected-behaviour model $\hat{y}_{i,t} = h_i(\mathbf{x}_{i,t}, \mathbf{z}_t; \theta_i)$, where $\mathbf{x}_{i,t}$ are internal signals (e.g., device counters, setpoints), $\mathbf{z}_t$ are exogenous drivers (e.g., weather, calendar, tariff), and θ_i are parameters. Models can be physics-based, statistical, or ML, such as *Physics-/process-informed* (simplified device/network equations or surrogate models), *Statistical* (seasonal ARIMA/ETS, generalised additive models, quantile regression), or *ML* (gradient boosting, random forests, shallow nets; for strict latency, linear or additive models are preferred). Residuals $r_{i,t} = y_{i,t} - \hat{y}_{i,t}$ are monitored with smoothing and control logic. Common smoothers include a moving average (window J)

$$\mathrm{MA}_{i,t} = \frac{1}{J} \sum_{j=0}^{J-1} y_{i,t-j},$$

and the exponentially weighted moving average (EWMA)

$$\mathrm{EWMA}_{i,t} = \lambda y_{i,t} + (1-\lambda)\mathrm{EWMA}_{i,t-1}, \quad 0 < \lambda \leq 1.$$

Decision rules combine magnitude and persistence:

$$\text{Alarm if } |r_{i,t}| > \tau_i(t) \text{ for } \nu \text{ of the last } M \text{ samples,}$$

with $\tau_i(t)$ possibly time-varying (e.g., quantile bands). Alternative sequential tests include CUSUM:

$$C_t^+ = \max\{0, C_{t-1}^+ + r_{i,t} - k\}, \;\; C_t^- = \max\{0, C_{t-1}^- - r_{i,t} - k\},$$

raising an alarm when $C_t^+ > H$ or $C_t^- > H$.

Feature families typically include: device setpoint tracking, ramp rates, start/stop cadence, topology-aware aggregates (e.g., feeder-level balances), seasonal effects, and cross-signals (e.g., consumption vs. exogenous drivers). Outputs at this stage are per-entity anomaly scores, rule violations, and short explanations (rule ID, residuals, window, contributing features).

Grid-level supervision and coordination tests To infer coordination, the BPA aggregates entity-level alarms within clusters (e.g., by feeder, tariff class, geography, technology). Let n be the number of entities in a cluster, p_0 the expected per-entity alarm rate under normal conditions, and K_t the observed number of alarms in a time bucket. A binomial tail test flags likely coordination when

$$\mathsf{P}(X \geq K_t;\, n, p_0) = \sum_{k=K_t}^{n} \binom{n}{k} p_0^k (1-p_0)^{n-k} < \alpha,$$

with α the chosen significance level. Where over-dispersion exists, a beta-binomial or scan-statistic is used. Spatial or topology-aware correlation (e.g., using the DT graph) refines evidence by favouring clusters that align with electrical connectivity. The BPA can also enforce *k-of-n* quorum rules conditioned on shared attributes (e.g., controller firmware version), raising severity when alarms co-occur across independent control domains.

Rules, policies, and execution Business rules are expressed as deterministic predicates and temporal patterns over DT entities and time windows, e.g.,

$$\texttt{IF } \Delta\texttt{setpoint} > \rho \wedge \texttt{ramp-rate} > \sigma \texttt{ THEN raise\_violation(rule\_ID).}$$

Execution combines: (i) a rules engine for invariants and policies; (ii) a stream processor for stateful windows and joins; (iii) a model runner for expected-behaviour inference. Severity, suppression, and cooldown policies limit alert storms. All decisions carry provenance: rule/model version, DT snapshot ID, feature hashes, and confidence.

Implementation Details The BPA exposes: (a) subscriptions for rule/model outputs; (b) pull APIs for scores and features; (c) cluster-level indicators for the DSCB and external sharing; (d) feedback hooks for the SCU to update thresholds and model parameters after simulations. Window length J, EWMA λ, control limits, and quorum (ν, M) govern the balance between sensitivity and false positives. Tuning uses historical replays (broker-backed) and cross-validation on held-out periods, with constraints from operations (e.g., maximum alert rate, detection delay limits). The BPA can be realised with different stacks. A typical setup uses: (i) a rules/policy engine (e.g., Drools-class or Open Policy Agent/Rego) for invariants and access policies; (ii) a stream processor (e.g., Kafka Streams/Flink-class) for windowed aggregations and joins with DT updates; (iii) a model-serving layer (microservice or embedded library) for prediction and scoring; (iv) a time-series store for residuals and metrics. When NGSI-LD is available, rules reference DT entity `type`, relationships, and `observedAt` to stay consistent with semantics. Other stacks (custom microservices, CEP engines) are viable if they provide the same contracts: stateful windows, deterministic rule evaluation, and auditable outputs. Two approaches are common for representing business processes monitored by the BPA: *FSMs*, suitable for device-centric, deterministic workflows (e.g., start-up, synchronisation, dispatch) with advantages like a small runtime footprint, being amenable to formal verification and code generation, and clear state invariants, but limited in expressiveness for human tasks, compensations, and complex timers; and *BPMN 2.0*, suitable for end-to-end operational procedures with human/system tasks, gateways, timers, and escalation, offering advantages like rich control-flow, wide tool support, and strong audit trails, but limited by heavier execution semantics and overhead, requiring a process engine if enacted at runtime. Selection depends

on scope: FSMs fit embedded or protection-grade logic; BPMN suits cross-team operational workflows. Hybrid use is common: FSMs for equipment sequences; BPMN for orchestration and incident handling.

4.1.3 Data Space Connector Builder (DSCB)

The DSCB enables cross-border data sharing among independent stakeholders while preserving data sovereignty. It mediates all exchanges between the Digital Twin environment and external parties under explicit contracts, policies, and security controls. Its goals are interoperable publication/discovery of data and services, verified participant identity and trust, usage control on every transfer, and full auditability. A data space is a federated setup that avoids centralised storage and keeps data owners in control. It requires semantic and syntactic interoperability so systems can interpret exchanged information; enforceable data-usage policies that constrain access, retention, and processing; authenticated and authorised participation with verifiable credentials; and traceable data flows for compliance. The *connector* is the participant's controlled gateway to the data space [76]. It terminates secure transport, authenticates peers, negotiates and enforces data-use agreements, performs format adaptation, and records provenance. Deployments may add privacy-preserving computation (e.g., trusted execution, encrypted processing). These concepts align with European work such as the IDSA Reference Architecture Model. The DSCB realises the data-space communication paradigm with secure participant connectors that sit at each organisation's boundary. Around them, a Certification Authority issues and validates credentials; a Broker/Catalogue exposes offerings for discovery without relaying payloads; and a Clearing House records transactions for audit and settlement. Usage control engines apply obligations such as time-limited access, geo-scoping, and purpose limitation. Figure 4.4 relates these elements to the IDSA RAM layers (business, functional, information, process, and system).

Interoperability is achieved by adopting NGSI-LD for context data with JSON-LD serialisation, maintaining explicit entity `type`, properties, and relationships. Sector vocabularies (e.g., Smart Data Models) are aligned with the Common Information Model (CIM) so that topology, assets, and measurements retain meaning across parties. When partners use different encodings, the connector performs schema and unit transformations while preserving semantics. Schemas are versioned; quality, sampling, and provenance metadata (source identifiers, signatures, timestamps) accompany each exchange. Identity and trust rely on federated PKI or equivalent identity providers, with attribute-based authorisation where needed. Each transfer is bound to a signed data-use contract that the connector enforces at run time through policy decision and enforcement points. Continuous monitoring supports an adaptive loop: interaction telemetry and threat signals update risk posture, leading to stronger authentication, tighter rate limits, or contract revocation. Threat modelling (e.g., STRIDE) guides the

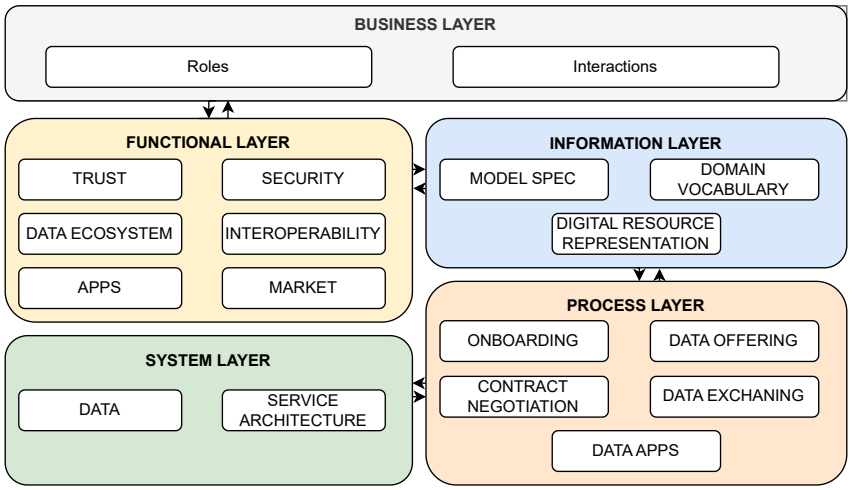


Figure 4.4: IDSA Reference Architecture Model layers and components [77].

placement of controls on channels, endpoints, and processes.

DSCB Operations, placement and implementation Typical interactions follow an offer/contract sequence in which a participant publishes capability metadata to the broker, negotiates usage terms, and signs an agreement. Data movement then uses secure pull APIs, push callbacks, or subscription streams with backpressure and quotas. Eventing delivers indicators, incident notices, and topology deltas with DT-consistent entity references. All operations are metered, rate-limited, and written to immutable logs at the clearing house, with correlation identifiers linking catalogue entries, contracts, and transfers. Data in transit and at rest are encrypted; integrity is protected with signatures or message authentication codes. Within the three-layer architecture, the DSCB sits at the application boundary. It exposes selected DT views and BPA indicators to authorised partners and ingests external context (for example, regional indicators or incident bulletins) into the DT under policy constraints. Only contractually agreed projections and rates are published. Connectors can be implemented with different stacks, including IDSA-aligned Trusted Connector variants, Eclipse Dataspace Connector-class solutions, or bespoke gateways. When NGSI-LD is the internal contract, FIWARE-based connectors are a practical choice due to native NGSI-LD support and existing context-management components; other stacks remain valid if they provide contract negotiation, usage-control enforcement, semantic alignment, strong identity, transport security, and audited logging.

Design notes The DSCB should publish least-privilege projections of DT entities rather than raw device streams unless required by contract; keep control and data planes separate, isolating credential stores and policy engines; support reproducible replay with watermarks without breaching retention obligations; and address cross-jurisdiction constraints through geo-fenced

policies or in-place computation when necessary.

4.1.4 Simulation Control Unit (SCU)

The SCU provides scenario design, orchestration, and execution for grid simulations driven by the Digital Twin's context. It enables both continuous risk screening and offline assessment by coordinating configuration, data preparation, simulator runs, and result publication to NGSI-LD–compliant stores. Its capabilities include scenario parametrisation, perturbation injection, preset management, run scheduling, and reproducible replays over historical or synthetic data. The core coordinates the end-to-end workflow: it resolves presets and modes, compiles a run plan, provisions inputs from the DPU, selects simulator modules, dispatches executions, and tracks completion. It enforces ordering constraints (e.g., topology load $\rightarrow$ parameter binding $\rightarrow$ contingency sweep), manages concurrency and backpressure, and records provenance. It maintains two data stores: a time-series store for simulation traces and KPIs, and a configuration store (e.g., MongoDB) for presets, scenarios, seeds, solver options, and audit metadata. Results are normalised and written back via NGSI-LD APIs for downstream use. The DPU acquires, prepares, and enriches inputs. It accepts NGSI-LD context as well as static datasets. Tasks include collection from declared sources; filtering and de-duplication; unit harmonisation and schema alignment; temporal alignment and interpolation; semantic enrichment with topology and asset metadata; and integration of exogenous drivers (e.g., weather, tariffs) when required by a scenario. Outputs are validated artefacts: network models, boundary conditions, profiles, and parameter vectors ready for simulation. The run-time executes workloads on an execution cluster that hosts simulator modules. Modules encapsulate specific tools and analyses; in our prototype, a `pandapower` module performs load-flow and related studies. The design is modular so that additional solvers (e.g., optimal power flow, short-circuit, stability) can be added under a common contract. Required inputs include the electrical scheme of the infrastructure and, where applicable, time-series profiles and perturbation schedules. The run-time streams intermediate metrics to the time-series store and returns final states, violations, and KPIs to the SCU core.

Operation modes *Monitoring mode* uses live or near-real-time context. The SCU pulls current topology and measurements through the DPU, generates simulator-ready snapshots, executes targeted analyses (e.g., steady-state screening, contingency checks), and publishes results for visualisation, alerting, and operator action. This supports continuous supervision with controlled latency and fixed computational budgets.
Evaluation mode runs offline studies over historical or synthetic datasets. It supports parameter sweeps, what-if scenarios, and safety-critical cases that cannot be exercised in production. Typical uses include strategy evaluation, setpoint policy testing, firmware or control changes,

and training material generation. Runs are reproducible: inputs, presets, solver versions, and random seeds are captured to the configuration store and referenced by immutable run IDs.

Inputs and outputs Inputs comprise: NGSI-LD–derived network models; device and prosumer profiles; exogenous drivers; scenario definitions (faults, outages, perturbations); and solver settings. Outputs include: time-aligned state vectors; KPI series (voltage margins, loading, losses); event logs of limit violations; and topology deltas. All outputs carry provenance (scenario ID, preset, seed, simulator module, commit/version) and are exposed through NGSI-LD entities with `observedAt` timestamps.

Chapter 5

Prosumer Framework Validation: A Real-World Case Study

In this chapter, we present the validation and evaluation of the proposed prosumer-oriented cybersecurity monitoring framework through a case study focused on an urban distribution network in Berchidda, Sardinia, Italy. This evaluation has three primary objectives: first, the construction and validation of the digital twin for this network; second, the performance evaluation of the prosumer behaviour analytics module using real-world data from the network's residential prosumers; and third, demonstrating the feasibility of enabling a data-sharing ecosystem within a data space to guarantee data sovereignty.

5.1 Case Study Overview

Berchidda is a municipality in north-eastern Sardinia with a population of roughly 5,000. The local distribution network is owned and operated by the municipal utility *Azienda Elettrica Comunale* (A.E.C.), which holds the concession for delivery and retail within the municipal boundary. This governance model is uncommon in Italy but offers a clear perimeter of responsibility, direct access to network models and operational data, and a single point of accountability. These conditions are suitable for constructing a security-centred Digital Twin and for validating monitoring and simulation workflows.

5.1.1 Grid topology and assets

The urban distribution network comprises medium-voltage (MV) and low-voltage (LV, shown in figure 5.1) sections with a single MV point of common coupling to the upstream DSO. The asset base includes 18 MV/LV substations with transformer ratings between 100 kVA and 500 kVA (about 5 MVA installed), approximately 4 km of MV underground cables (3.2 km

meshed, 0.8 km radial), 15.4 km of LV overhead lines, and 21.6 km of LV underground cables. The municipality has also acquired a rural network that adds further MV/LV substations and increases distributed generation potential. The single upstream connection simplifies energy exchange metering and provides an unambiguous system boundary for modelling and validation.

Table 5.1: Key characteristics of the Berchidda urban distribution network [78].

MV/LV substations (urban)	18
Transformer rating	100–500 kVA (total $\approx$ 5 MVA)
MV underground cables	4.0 km (3.2 km meshed, 0.8 km radial)
LV overhead lines	15.4 km
LV underground cables	21.6 km
Upstream connection points	1 (at MV)
Installed PV (existing)	67 plants, 608 kWp
Daily gross electric load (mean)	$\approx$ 19 MWh/d
Energy purchased (current)	$\approx$ 16.4 MWh/d ($\approx$ 6.9 GWh/y)

5.1.2 Renewables, storage, and operations

The urban network currently hosts 67 rooftop photovoltaic installations totalling 608 kWp. Their daytime output reduces the net load, producing local injections in limited intervals, while the point of common coupling at MV level remains predominantly in import. The measured mean daily gross load is about 19 MWh/d and the energy purchased from the upstream grid is about 16.4 MWh/d (approximately 6.9 GWh/y).

No community-scale electrical storage is in operation at present and there is no dispatchable on-site generation such as CHP. As a result, flexibility is mainly driven by passive PV variability and the inherent diversity of consumer demand rather than by controllable assets. Operational data are anchored by the single MV interconnection measurement and by standard metering in the LV network, providing a clear system boundary for energy balancing and model validation. This present configuration yields a stable baseline against which the monitoring framework can quantify PV-driven net-load reductions, detect deviations in feeder and prosumer behaviour, and cross-check DT-derived balances with measured imports.

5.1.3 Why Berchidda is a suitable testbed for the framework

Berchidda offers a controlled yet realistic scope:
(i) a clear electrical boundary with a single MV interconnection, which simplifies energy balance validation and model reconciliation;
(ii) access to CIM-aligned network descriptions and the possibility to map them to NGSI-LD

for a semantically consistent DT;
(iii) heterogeneous prosumer portfolios with measurable exogenous drivers, enabling behaviour baselining and anomaly detection;
(iv) planned cross-organisation interactions (municipal utility, upstream DSO/TSO, technology providers) that motivate data-space connectors and usage control;
(v) a roadmap of upgrades that permits structured what-if studies in the SCU, including demand shifting, PV/ESS siting, voltage margin checks, and contingency analyses.
These properties allow end-to-end validation of the four artefacts: DT construction and synchronisation, business-rule analytics for prosumer behaviour, policy-governed data exchange, and simulation-driven planning and monitoring.

5.2 Building The Digital Twin

The digital twin for Berchidda was built with a model-driven, standards-based pipeline. The operator's Common Information Model export was used as the authoritative description of the network. CIM classes (e.g., Substation, PowerTransformer, ACLineSegment, Switch, Terminal, ConnectivityNode, Meter) were mapped to NGSI-LD `types`. CIM attributes became NGSI-LD `Property` values with units and provenance; CIM relations were translated into NGSI-LD `Relationships`. Prosumer devices were attached to the appropriate LV nodes and to their meters; substation equipment was grouped under substation entities with geo references and operational status. The result is a single NGSI-LD graph where static assets and live observations share the same semantics.

Southbound interface (field → DT) Telemetry from selected MV/LV substations and prosumer devices is normalised at the edge and published to Apache Kafka. Gateways adapt vendor/legacy protocols to framed messages (JSON) with explicit schema, units, timestamps, and stable equipment identifiers aligned with the CIM identifiers. Topics follow a hierarchical convention (e.g., `berchidda.substation.S#.measurements`). Transport uses TLS/mTLS; a schema registry governs payload versions.

A stateless Kafka → NGSI-LD bridge validates messages, reconciles device IDs against the DT catalogue, and upserts NGSI-LD entities in the FIWARE Orion-LD broker. Measurements are written as `Property` updates with `observedAt` and quality flags; each update links to the source asset via a `Relationship`. The bridge enforces idempotent writes, handles late/out-of-order data with watermarks, and deduplicates by key+timestamp. Where devices can speak NGSI-LD via lightweight adapters, FIWARE IoT Agents are used; otherwise, the Kafka bridge is the sole ingress path. Long-run series are forwarded from Kafka to a time-series sink; Orion-LD retains the current state and recent history needed for operations.

Figure 5.1: Berchidda Low-voltage distribution panel inside an electrical substation, an example of an asset being monitored for Digital Twin implementation.

Northbound interface (DT → analytics and sharing) Orion-LD exposes the DT through NGSI-LD queries for topology and current state. Change notifications are configured via NGSI-LD subscriptions; each entity delta is posted to Kafka so consumers can process a uniform stream without stressing the broker. The Business Process Analyzer consumes these deltas and joins them with cluster/topology context from the DT graph. The Simulation Control Unit queries snapshot slices (topology, setpoints, profiles) and replays time windows by consuming bounded Kafka offsets. The Data Space Connector exports selected projections and indicators under contract, using the same NGSI-LD views and audited transfers. All flows carry provenance (DT snapshot ID, schema versions, correlation IDs) to support reproducibility and audit.

Topology anchoring and identifiers DT entity identifiers are derived deterministically from CIM keys (e.g., `mRID`) to keep joins stable across ingestion, streaming, and analytics. Switch state changes, topology edits, and equipment updates are represented as NGSI-LD patches on the concerned entities and propagate immediately through subscriptions. Topology-aware

queries (upstream/downstream, feeder membership, cut-set analysis) operate directly on the NGSI-LD relationships, enabling aggregation and impact checks that respect electrical boundaries.

Technology stack and controls The stack consists of FIWARE Orion-LD (NGSI-LD broker), Apache Kafka (streaming), a CIM importer/mapping service, the Kafka ↔ NGSI-LD bridge, optional FIWARE IoT Agents, a schema registry, a time-series sink, and minimal operational services for health and metrics. Components are containerised and use mTLS between services. Identity and access control rely on service accounts and signed client certificates; messages can be signed at the producer for end-to-end integrity. Every update recorded in Orion-LD includes `observedAt`, unit metadata, and source provenance to maintain traceability from field device to DT and onward to analytics.

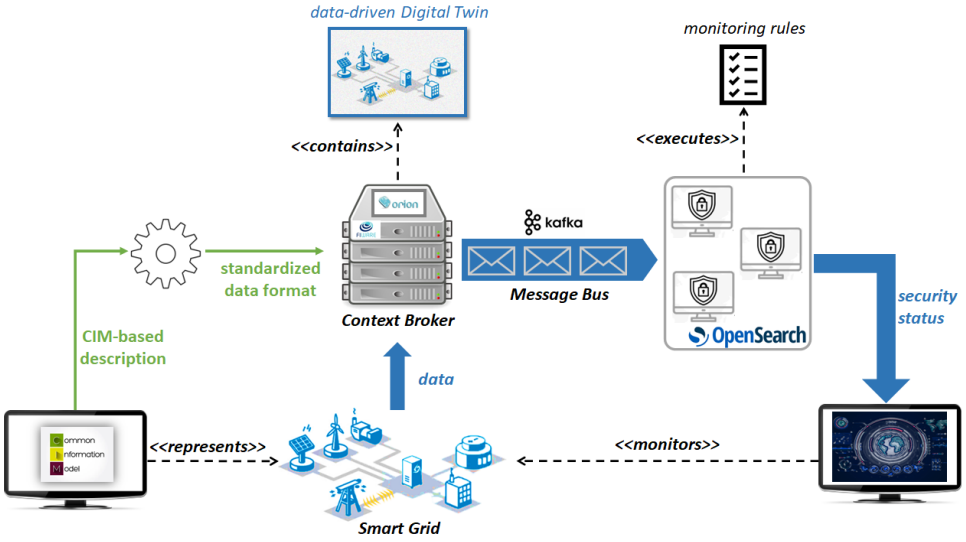


Figure 5.2: General architecture of the proposed Digital Twin system for cybersecurity monitoring. The displayed framework, sourced from [75], is structurally equivalent to our implementation, provided the analytic service is replaced.

5.3 Analysing Prosumer Behaviour via Business Process Analytics

To analyse prosumer behaviour, the business process specification governing the Distribution System Operator operations of dispatching and monitoring within the Berchidda case study has been taken into consideration. Figure 5.3 presents a simplified version of this specification that fully captures the operational activities examined in this analysis. The business process is represented using the Business Process Model and Notation 2.0 formalism, which provides a standardised graphical notation for specifying business processes in a workflow. This for-

malisation enables the systematic creation of the monitoring solution described in subsequent sections. The business process, shown in Figure 5.3 encompasses the critical activities executed for energy management and distribution, including the comprehensive monitoring and failure-handling procedures necessary to safeguard municipal operations. The process incorporates continuous assessment of grid status based on real-time data conforming to the Common Information Model (CIM - IEC 61970) schema, thereby determining grid functionality during component maintenance operations and ensuring operational reliability throughout the distribution network.

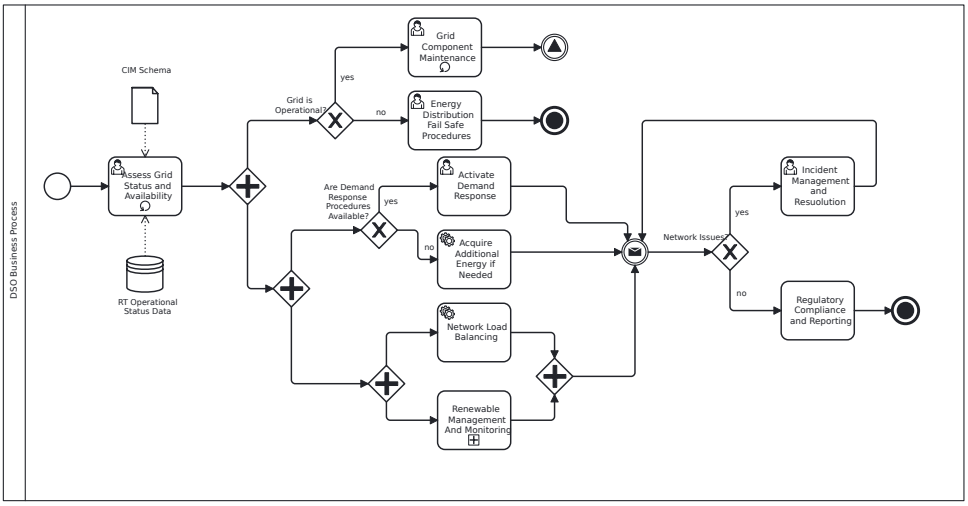


Figure 5.3: Simplified business process specification for renewable energy management and monitoring task integration within the Berchidda DSO operational framework [66].

Business Process Logic Extraction

This section reports how prosumer behaviour was analysed on the Berchidda network using the Business Process Analyzer (BPA). A set of representative prosumers was selected across feeders and user types. For each subject, we collected active power, energy, inverter status and meter readings from the Digital Twin, and paired these with exogenous drivers (e.g., irradiance proxies and ambient temperature from nearby meteorological sources) to support model-based checks. The BPA consumed DT updates via subscriptions, aligned signals in time, and produced two classes of outputs: single-prosumer anomaly flags and grid-level indicators of coordination [66].

5.3.1 Prosumers Behaviour Modelling

The objective of prosumer behaviour modelling is to establish a baseline of expected operation for each prosumer, against which deviations can be detected and analysed. Two distinct approaches were employed to achieve this objective. The first approach is rooted in a de-

terministic mathematical model that comprehensively describes the equipment characteristics associated with individual user profiles, thereby enabling the simulation and prediction of prosumer behaviour based on the technical specifications of installed devices and consumption patterns. The second approach leverages artificial intelligence-based modelling through federated learning techniques, which enable the creation of user profiles characterising production and consumption curves while guaranteeing privacy preservation. This federated learning paradigm allows the model to learn from distributed data across multiple prosumers without requiring the centralisation of sensitive individual consumption data, thus maintaining data sovereignty and ensuring compliance with privacy regulations.

5.3.1.1 Mathematical Based Modelling

For PV-equipped prosumers, the expected generation profile was computed from a process-informed model driven by plant metadata (rated DC power, orientation, tilt, temperature coefficient) and weather inputs. Using a PV performance library (`pvlib`), the DC output was obtained with a PVWatts-style relation

$$P_{\mathrm{DC}}(t) = G_{\mathrm{POA}}(t) \left(\frac{P_{\mathrm{DC0}}}{G_{\mathrm{STC}}} \right) \Big[1 + \gamma \left(T_{\mathrm{cell}}(t) - T_{\mathrm{ref}} \right) \Big],$$

with the cell temperature estimated as

$$T_{\mathrm{cell}}(t) = T_{\mathrm{air}}(t) + \left(\frac{G_{\mathrm{POA}}(t)}{G_{\mathrm{ref}}} \right) \left(\frac{\mathrm{NOCT} - 20}{800} \right).$$

Here G_{POA} is plane-of-array irradiance, P_{DC0} the DC rating at STC, $G_{\mathrm{STC}} \approx 1000\ \mathrm{W/m^2}$, γ the power temperature coefficient, and $T_{\mathrm{ref}} \approx 25^{\circ}\mathrm{C}$. AC output was derived by applying inverter and system losses:

$$P_{\mathrm{AC}}(t) = P_{\mathrm{DC}}(t)\, \eta_{\mathrm{inv}}\, \eta_{\mathrm{loss}}.$$

The residual $r(t) = P_{\mathrm{meas}}(t) - P_{\mathrm{AC}}(t)$ was monitored under smoothing to control day-to-day variability. A moving-average baseline over a window of J samples was used:

$$\mathrm{MA}_J(t) = \frac{1}{J} \sum_{i=0}^{J-1} x(t-i).$$

Decision rules combined magnitude and persistence: an alarm was raised when $|r(t)|$ exceeded a time-varying threshold for a minimum number of points within a sliding window. Thresholds were set from quantile bands of historical residuals and adjusted for seasonality. The same scheme was applied to consumption-only prosumers using demand models driven by calendar features and temperature.

Grid-level supervision and coordination tests To check for coordination, the BPA aggregated alarms within time buckets and clusters (e.g., by feeder or technology) and evaluated the tail probability of observing at least k alarms out of n entities under a background per-entity alarm rate p_0. The binomial tail was used:

$$\mathrm{P}(X \geq k; n, p_0) = \sum_{i=k}^{n} \binom{n}{i} p_0^i \, (1 - p_0)^{n-i}.$$

If P fell below a chosen significance level, the system flagged a likely coordinated event. Topology information from the DT was used to prioritise clusters that aligned with electrical connectivity, reducing false correlations across independent sections of the network.

5.3.1.2 AI-Based Modelling

The second approach to prosumer behaviour modeling employs a federated learning paradigm that integrates user profiling techniques with distributed machine learning to establish baseline consumption patterns while ensuring privacy preservation. This methodology addresses the critical challenge of analysing sensitive energy consumption data without requiring centralisation of individual measurements, thereby maintaining compliance with privacy regulations such as the General Data Protection Regulation and the Electricity Directive. The federated learning architecture is structured according to the hierarchical topology of the smart grid infrastructure, as illustrated in Figure 5.4. Gateway devices function as federated learning clients, receiving processed energy consumption data from smart meters within their respective regions and maintaining computational capabilities sufficient for local model training. The control centre operates as the federated learning server, orchestrating the distributed training process by broadcasting initial model parameters to all gateways and subsequently aggregating the locally computed training parameters to construct an improved global model. This architectural arrangement ensures that raw consumption data remains localised at the gateway level, with only model parameters being transmitted to the central server. The anomaly detection framework combines two complementary techniques to achieve robust user profiling and deviation detection. Initially, the K-means clustering algorithm performs user profiling by categorising prosumers based on their energy consumption patterns, with the optimal number of clusters determined through the silhouette score method. This clustering enables the identification of distinct consumption behaviours across different user groups. Subsequently, a Variational Autoencoder (VAE) is trained on normalised consumption data to learn compact latent representations of typical consumption patterns. The VAE reconstructs input data and calculates reconstruction errors, which quantify deviations from expected behaviour. Anomalies are identified through a multi-criteria approach that considers both cluster membership and

reconstruction error thresholds, thereby reducing false positives by accounting for legitimate variations in consumption patterns across different user profiles.

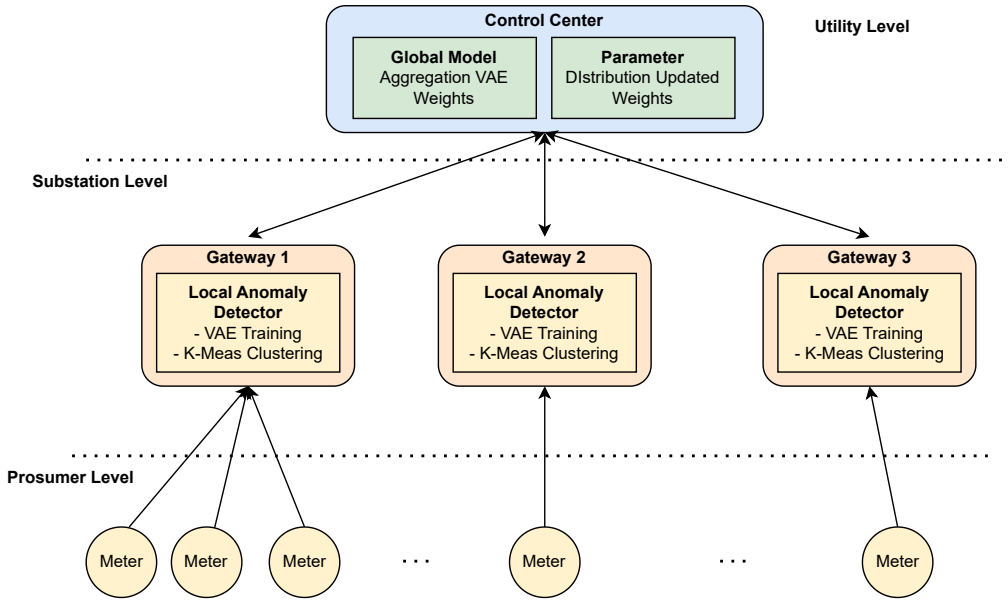


Figure 5.4: Federated learning architecture for smart grid anomaly detection in the Berchidda deployment. The three-layer hierarchy comprises the control centre functioning as the FL server, gateways operating as FL clients with local anomaly detectors, and smart meters performing data collection. Bidirectional communication flows enable secure model weight transmission whilst preserving data privacy by maintaining raw consumption data at local nodes.

The implementation leverages the PySyft library to facilitate secure communication between federated learning clients and the server. Each gateway collects energy consumption measurements at fifteen-minute intervals, performs local preprocessing and normalisation using standard scaling techniques, and trains the VAE model on its local dataset. Following local training, gateways securely transmit only the VAE model weights to the control centre, which aggregates these parameters to refine the global model. The updated global model weights are then redistributed to all gateways, enabling each node to benefit from the collective knowledge derived from distributed data across the entire network. This iterative process enhances detection accuracy over time while maintaining the fundamental privacy-preserving property that raw consumption data never leaves its originating location.

Table 5.2 summarises the specific hyperparameters and configuration settings adopted for the model training in this case study.

Limitations and Challenges While the proposed Federated Learning strategy effectively preserves privacy and detects anomalies, certain limitations warrant discussion. First, the *non-IID*

Table 5.2: Hyperparameters and local training configuration for the Federated Learning model.

Parameter	**Value**
Federated Strategy	FedAvg
Local Epochs	5
Batch Size	32
Optimizer	Adam
Learning Rate	10^{-3}
Input Dimension	96 (24h $\times$ 15min)
Latent Dimension	8

(Independent and Identically Distributed) nature of the data is a significant factor; each prosumer has a unique consumption profile (e.g., residential vs. commercial), meaning local datasets do not represent the global distribution. While our clustering-based user profiling mitigates this by grouping similar behaviours, extreme heterogeneity can still impact the convergence rate of the global model. Second, *communication latency* within the Smart Grid infrastructure can affect the synchronisation of model weights. Although FL significantly reduces bandwidth usage by avoiding raw data transmission, the iterative aggregation process requires reliable connectivity, and network delays could hinder real-time responsiveness in a large-scale deployment. Finally, the dataset is inherently *imbalanced*, as anomalous events are rare compared to normal operations. This imbalance was observed in the variability of the Precision-Recall AUC scores during validation, suggesting that while the system is robust, continuous re-training and careful threshold tuning are necessary to maintain high detection performance across all conditions.

5.4 Simulation Control Unit for What-If Analyses

In Berchidda the SCU was used to generate *what-if* datasets and to drive power-flow checks on the Digital Twin without touching the live network. Two simulation sources were enabled and coupled with the CIM-derived topology and the explicit representation of distribution lines.

Prosumer generation via mathematical model For PV-equipped prosumers, the SCU produced synthetic generation series using a process-informed model parameterised by plant metadata (rated power, orientation, tilt, temperature coefficient) and meteorological drivers (plane-of-array irradiance, air temperature, wind). DC output followed a PVWatts-type relation with temperature correction, then was converted to AC using inverter efficiency and loss factors. The SCU varied inputs and parameters to emulate degradations, sensor bias, curtailment,

and sudden irradiance drops. The resulting traces were injected into the DT as NGSI-LD observations linked to the corresponding prosumer entities.

Prosumer profiles via federated learning To cover consumption and mixed prosumer behaviour, the SCU ingested profiles generated by a federated learning pipeline. Gateways trained local models on meter data, the server aggregated weights, and the global model produced consumption/production trajectories per profile class. These series respect privacy constraints because raw data stayed local during training. The SCU sampled from these models under different calendar and temperature conditions to create realistic load/production inputs for large clusters.

Coupling with network model and disruptive tests Both sources were combined with the CIM-based network model (substations, transformers, switches, line segments, terminals, connectivity nodes). The SCU assembled simulator-ready cases by binding synthetic prosumer injections/loads to the LV nodes defined in the DT and by applying current switch states. Typical disruptive tests included: sharp PV ramp-down on selected feeders, coordinated setpoint shifts across a prosumer clusters, forced outages on a branch, and tap changes at MV/LV transformers. For each case the solver produced node voltages, equipment loading, losses, and limit violations. Results were written back as NGSI-LD entities with `observedAt` and provenance to support replay and comparison.

Outcome This setup allowed repeatable evaluation of BPA thresholds and operating policies under controlled stress. The mathematical model supplied targeted generation perturbations; the federated model supplied realistic demand/production patterns at scale; the CIM topology ensured that impacts were assessed along true electrical paths. The SCU thus provided a safe path to test disruptive events on the DT and measure their effects before any field action.

5.5 Enabling Cross Border Data Sharing via Data Space

The Berchidda connector deployment enables cross-border data exchange between the municipal operator (A.E.C.), upstream DSO/TSO actors, and selected peers by adopting a data space approach. The goal is to share operational context, indicators, and incident information while keeping data owners in control. The method combines trusted identification and authentication, policy-based usage control, encryption in transit and at rest, and semantic interoperability based on NGSI-LD aligned with the Common Information Model (CIM). European building blocks guide the design: governance and interaction patterns follow IDSA concepts, and the technical stack uses FIWARE components where NGSI-LD is required. STRIDE threat modelling is applied to the flows and assets to align controls with risks.

Architecture in Berchidda Each participant exposes a *connector* at its boundary. At the municipality level, the connector fronts the Digital Twin and publishes selected projections (e.g., substation status, feeder-level KPIs, anonymised prosumer cluster, topology deltas). The connector enforces contracts negotiated via a *Broker/Catalogue*, authenticates peers with certificates issued by a *Certification Authority*, and records immutable transaction logs at a *Clearing House*. Usage control is applied before, during, and after transfer (time limits, purpose restriction, geo-scoping, retention). Figure 5.5 summarises this arrangement.

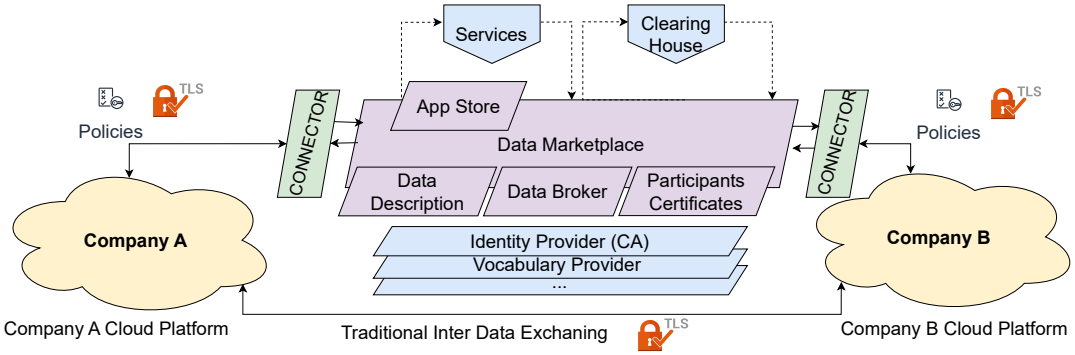


Figure 5.5: Dataspace-based data exchange architecture: connectors, broker, certification, usage control, and clearing [77].

The architecture maps to the IDSA Reference Architecture Model (RAM): business roles and value chains define who publishes or consumes; functional capabilities cover discovery, contract negotiation, and policy enforcement; information defines semantics and governance; process prescribes compliant interaction flows; system identifies the connector and supporting services. FIWARE's Context Broker and IoT Agents integrate on the provider side to normalise heterogeneous telemetry into NGSI-LD; Smart Data Models aligned with CIM keep semantics consistent across parties.

DT integration and data products On the provider side, Orion-LD exposes DT views. The Data Space Connector Builder (DSCB) derives least-privilege projections and binds them to catalogue entries: (i) network state summaries at substation/feeder level; (ii) aggregated indicators from the Business Process Analyzer (alarm counts, tail probabilities); (iii) incident notices and enrichment; (iv) topology updates with versioning. Exports are annotated with provenance (snapshot ID, schema version, issuer) and quality metadata (sampling, units). Prosumer-sensitive data are shared as aggregates or pseudonymised where contracts require it.

Trust boundaries, assets, and controls Figure 5.6 shows an example of data flow diagram that can be used to identify trust boundaries between the municipality, upstream grid operators,

and peers. Assets include real-time grid status, CIM-based topology, device outputs, and demand-response signals. Channels use TLS/mTLS; participants authenticate with CA-issued credentials; authorisation can rely on attributes (role, purpose, geography). Policies constrain access windows, resolution (e.g., aggregated vs. raw), and retention. High-risk assets receive tighter monitoring and additional checks (rate limits, anomaly flags at the connector).

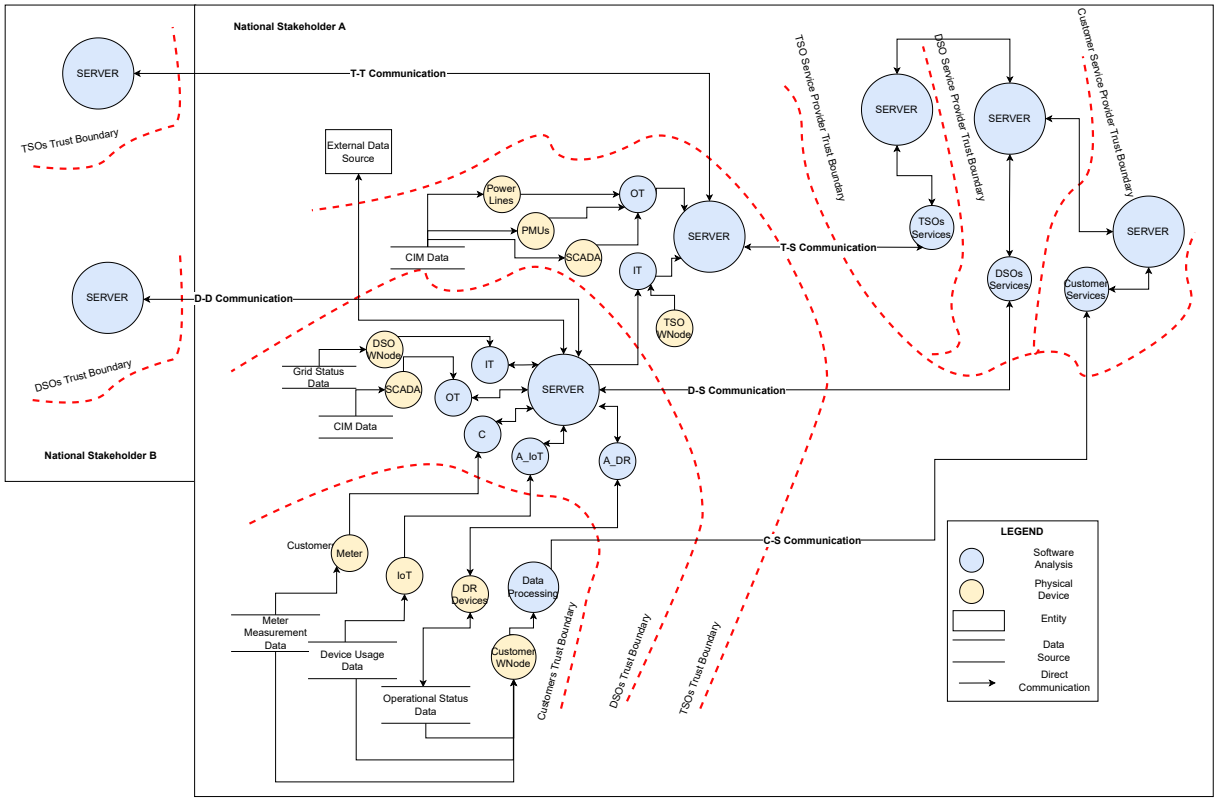


Figure 5.6: Data flows for energy stakeholders in the dataspace with trust boundaries and key assets [77].

Policy enforcement loop Connectors operate a feedback loop that adapts protection to observed conditions. Interaction telemetry and threat insights update the risk model; the connector can then adjust authentication strength, tighten permissions, or change encryption parameters. Figure 5.7 illustrates this policy loop, which keeps the exchange resilient as threats evolve while preserving auditability through the clearing function.

Outcome for Berchidda In Berchidda, the data space setup allows the municipality to publish DT-backed operational views and indicators to upstream operators and peers under clear contracts, while receiving regional context and incident information. The combination of NGSI-LD semantics, connector-level policy enforcement, and audited exchanges keeps ownership and

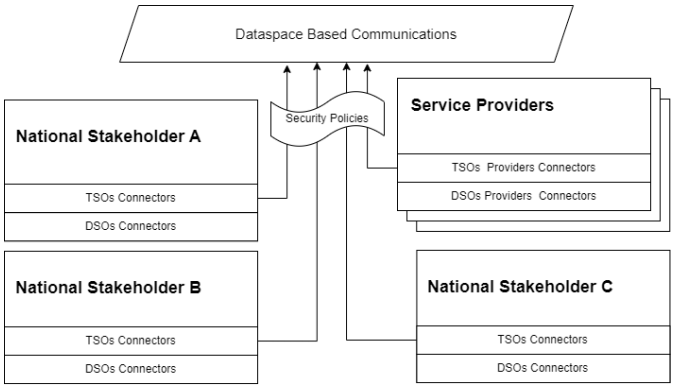


Figure 5.7: Secure cross-border sharing with a dynamic policy-enforcement loop [77].

accountability with the data providers and enables cross-border cooperation without centralised data pooling.

5.6 Validation Results

This section reports the results obtained on the Berchidda case study from (i) single–prosumer analysis and (ii) grid–level coordination checks.

Single–prosumer error analysis

For each selected PV prosumer, the Business Process Analyzer generated an expected AC power series from plant metadata and exogenous drivers. Let the residual be

$$r(t) = P_{\text{meas}}(t) - P_{\text{AC}}(t).$$

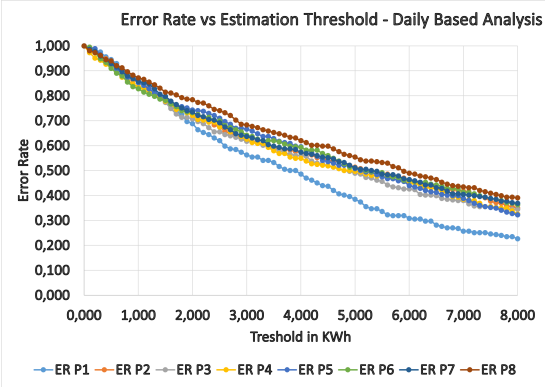
We quantify accuracy with the mean absolute error (MAE) and with an exceedance rate

$$\text{ER}_\tau = \frac{1}{T}\sum_{t=1}^{T} \mathbb{1}\{|r(t)| > \tau\},$$

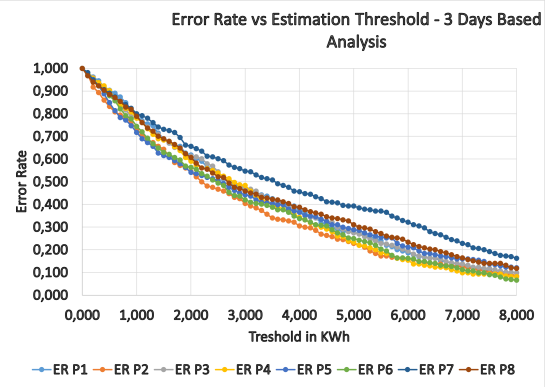
where τ is a tolerance band capturing sensor noise and model mismatch. To reduce short–term volatility, residuals were evaluated after applying a moving–average smoother of length J (MAD $= J$ days).

Figure 5.8 shows the effect of increasing the smoothing window. With $J = 1$, the exceedance rate is high due to intra–day variability and short transients. Increasing J to 3, 5, and 7 days progressively lowers ER_τ and MAE, indicating more stable residuals and fewer spurious exceedances. This reflects the expected trade–off: larger J reduces false positives at the cost of slower reaction to genuine shifts. In practice, J is selected to satisfy an opera-

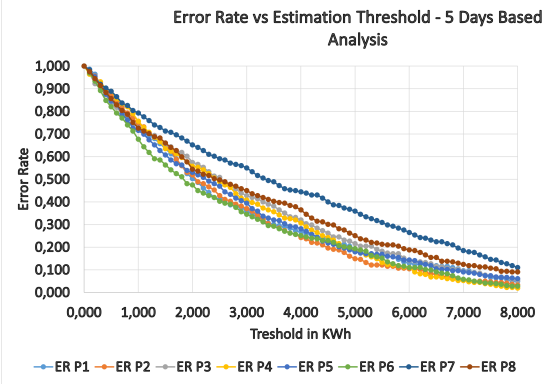
tor–defined bound on ER_τ while keeping detection delay within acceptable limits.



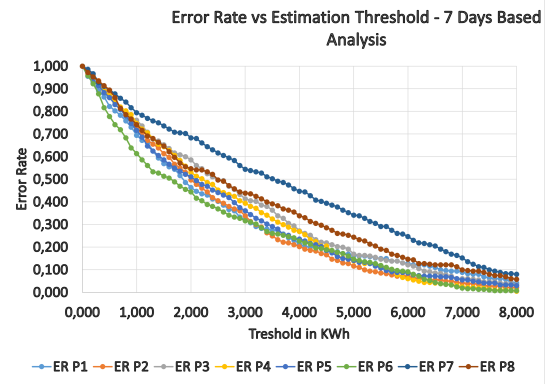
(a) MAD 1



(b) MAD 3



(c) MAD 5



(d) MAD 7

Figure 5.8: Error-rate variation across Moving Average Days (MAD): (a) $J{=}1$ shows higher error due to volatility; (b–d) larger J reduce exceedances coppolino2024increasing.

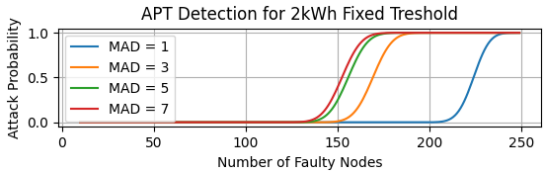
Grid–level coordination check

Grid–level supervision aggregates entity–level alarms within time buckets and tests whether their count is consistent with the background rate. Let n be the cluster size, K the observed alarm count, and p_0 the expected per–entity alarm probability under normal conditions. The binomial tail

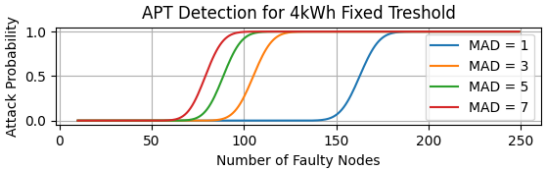
$$\mathrm{P}(X \geq K;\, n, p_0) = \sum_{i=K}^{n} \binom{n}{i} p_0^i (1-p_0)^{n-i}$$

is used to flag coordination when P falls below a fixed significance level. Figure 5.9 summarises detection probabilities obtained for varying energy thresholds (2, 4, 6, 8 kWh) and smoothing (MAD $= 1, 3, 5, 7$) under Berchidda's reference daily consumption of 16.6 MWh. With a 2 kWh threshold and MAD=7, the system tolerates up to ~ 160 prosumer alarms before

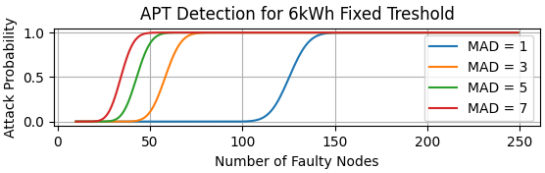
crossing the significance bound, which corresponds to about 320 kWh (1.9% of daily energy). Raising thresholds to 4, 6, and 8 kWh tightens the tolerated count to ~ 80, ~ 45, and ~ 18, respectively (roughly 1.9% down to 0.9% of daily energy). Lower thresholds are more sensitive but increase false positives; higher thresholds reduce false positives but raise the minimum coordinated impact required for detection.



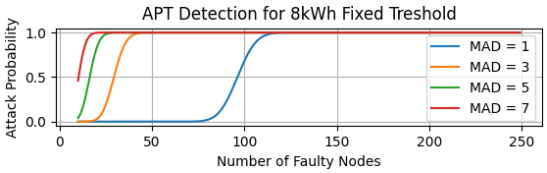
(a) Threshold: 2 kWh



(b) Threshold: 4 kWh



(c) Threshold: 6 kWh



(d) Threshold: 8 kWh

Figure 5.9: Coordination detection probabilities across MAD settings and energy thresholds. Lower thresholds increase sensitivity; higher thresholds reduce false positives coppolino2024increasing.

5.7 Economic impact

The validation results from the Berchidda case study confirm the technical feasibility and effectiveness of the proposed monitoring framework. At the single-prosumer level, the analysis demonstrated a clear, quantifiable trade-off between detection sensitivity and system stability. As shown in Figure 5.8, applying a moving-average smoother (J) is highly effective at reducing false positives (measured by MAE and ER_τ) caused by short-term volatility. Increasing J from 1 to 7 days progressively stabilises the residuals, though this comes at the cost of a slower reaction time, a primary tuning parameter for operators.

At the grid level, the coordination check successfully aggregates these individual alarms to detect systemic patterns. The binomial tail probability test provides a statistically robust method for flagging coordinated events that would be missed by entity-level monitoring alone. The results in Figure 5.9 highlight the system's tunability: by adjusting the energy threshold and smoothing factor (MAD), operators can configure the system's sensitivity. For instance, a higher threshold (e.g., 8 kWh) can detect coordinated events representing a smaller total energy impact (approx. 0.9% of daily energy) composed of large individual deviations. Conversely, a lower threshold (e.g., 2 kWh) is tuned to detect widespread events of smaller individual

magnitude, even if they require a larger cumulative impact (approx. 1.9% of daily energy) to be flagged as statistically significant. These findings validate the framework's capability to identify subtle, coordinated attacks.

Building on this, the economic imperative for such detection is significant. A quantitative assessment of the financial repercussions from energy production deficits was conducted. The model assumes a collective of n prosumers, each with an average annual energy output of E (in kWh), resulting in a total baseline production of $E_{\text{total}} = nE$. If this collective experiences a uniform production shortfall of R percent, the total volume of lost energy can be calculated as:

$$E_{\text{lost}} = \frac{R}{100} E_{\text{total}}$$

The corresponding economic impact, I, is subsequently determined by multiplying this lost energy by the prevailing energy cost, C (e.g., in USD/kWh), yielding the relationship:

$$I = E_{\text{lost}} \times C$$

This model was applied to the Berchidda scenario, with the results illustrated in Figure 5.10. Considering a community of $n = 260$ prosumers, each with a mean annual production estimated at $E = 4018$ kWh. The analysis explores the financial loss across a range of plausible disruption scenarios, specifically for production reductions (R) between 1% and 10%, and for energy costs (C) spanning from 0.10 to 0.20 USD/kWh. As demonstrated by the loss surface

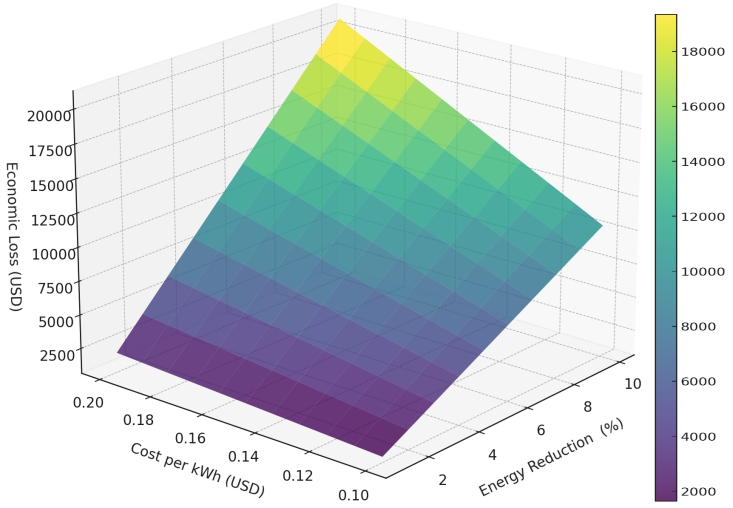


Figure 5.10: Economic loss as a function of production reduction (%) and cost per kWh. [66]

in the figure, the total financial impact scales linearly with both the magnitude of the production cut (R) and the unit cost of energy (C). Notably, at the upper boundary of the simulated parameters—that is, a 10% reduction at a cost of 0.20 USD/kWh—the resulting monetary

losses become substantial (5% of the total municipality expenses). This impact is significant when contextualized against the municipality's typical expenses for energy distribution. This finding underscores the critical value of implementing robust, early-warning detection and response mechanisms—as validated in this chapter—to mitigate such production anomalies before they escalate.

While this analysis focuses on a single municipality, the model's linear nature has critical implications when scaled to larger scenarios. The financial impact I is directly proportional to the total energy baseline E_{total}, which in turn is a function of the number of prosumers n. In the context of a large metropolitan area or a coordinated attack targeting multiple municipalities simultaneously, the value of n would increase by orders of magnitude. This direct scalability means that the absolute economic losses from an equivalent percentage-based shortfall (R) would be dramatically magnified. Such an event could transition from a localised material loss to a systemic financial disruption, further reinforcing the necessity of scalable, multi-region security analytics.

5.8 Framework Validation Summary

This chapter presented the design, implementation, and validation of the proposed prosumer-oriented cybersecurity monitoring framework through a real-world case study on the Berchidda distribution network. The validation successfully demonstrated the technical feasibility and effectiveness of all four core architectural artifacts by applying them to the operator's environment and data. The key objectives and the corresponding results validated within the case study are summarised in Table 5.3.

The requirement for a high-fidelity, semantically-rich Digital Twin was validated by successfully constructing a model of the Berchidda network. This was achieved through a model-driven pipeline that transformed the operator's CIM export into a dynamic NGSI-LD graph. We demonstrated the implementation of decoupled southbound, Kafka-based ingestion and northbound Orion-LD subscription interfaces, proving the DT's capability to serve as a central, real-time state representation for all other framework components.

This Digital Twin served as the foundation for the Business Process Analyzer, whose effectiveness in detecting anomalous and coordinated prosumer behaviour was validated using the operator's real-world data. Single-entity detection was demonstrated using two distinct approaches: a process-informed mathematical model and a privacy-preserving federated learning model. The results in Section 5.6 confirmed the ability to establish accurate baselines and quantify the trade-off between detection sensitivity and stability. Furthermore, grid-level coordination detection was validated using a binomial tail test, which successfully aggregated single-entity alarms to identify systemic patterns consistent with a coordinated attack.

The Simulation Control Unit's capability to orchestrate what-if analyses was also validated. We demonstrated that the SCU could couple the CIM-based network model from the Digital Twin with synthetic data sources, both mathematical and federated learning-generated. This allowed for the execution of controlled, disruptive scenarios, such as coordinated PV ramp-downs, to test framework resilience and BPA tuning, providing a safe environment for the operator to evaluate responses.

Finally, the feasibility of enabling secure, cross-border data sharing via the Data Space Connector Builder was demonstrated. A data space connector, aligned with IDSA principles, was deployed at the utility's boundary. This validation confirmed the framework's ability to share least-privilege projections and indicators based on NGSI-LD semantics, thereby enforcing the operator's data sovereignty and usage control requirements with external stakeholders.

Table 5.3: Framework Validation Results by Artifact, Key Result, and Beneficiary.

Artifact	**Key Result 1**	**Key Result 2**	**Key Result 3**	**Beneficiary(s)**
DT Builder	Live CIM-to-NGSI-LD Model	Decoupled Ingestion	Real-time State Query	Operator, Integrator
BPA	Tunable Anomaly Detection	Statistical Coord. Alert	FL Model Privacy	Sec. Analyst, Operator
SCU	Repeatable 'What-if' Test	Safe Policy Validation	DT-Coupled Scenarios	Operator, Sec. Analyst
DSCB	Sovereign Data Sharing	NGSI-LD Indicator Exch.	IDSA Policy Enforcement	Operator, Stakeholders

Conclusions

This thesis has systematically addressed the critical cybersecurity challenges of the high pervasive distributed energy resources integration affecting the contemporary Electric Power and Energy Systems. It employs a multidisciplinary research approach that integrates technical vulnerability analysis, formal threat modelling, and regulatory gap analysis to bolster the cybersecurity posture of the energy critical infrastructure.

The research develops a reference Advanced Persistent Threat scenario, provides a comprehensive regulatory critique, and delivers a novel cybersecurity monitoring framework. The technical contributions of this framework were subsequently validated using a real-world case study within the municipality of Berchidda, demonstrating both its detection efficacy and the quantifiable economic impact of the threats it is designed to address.

To properly situate these findings, the following sections will first define the specific scope and boundaries of the research. Following this, the distinct, actionable insights generated by this work for both policymakers and technical operators are detailed, leading to a final summary of the work's primary contribution.

Limitations and Scope of the Research

To fully contextualise the contributions of this thesis, it is important to define its specific scope boundaries. The successful validation in the Berchidda case study was subject to several deliberate limitations, which, far from diminishing the results, clarify their precise applicability and the foundation laid by this work.

First, the validation's focus on the Berchidda municipal network was a strategic choice. This environment provided a controlled, real-world testbed with clear governance and accessible operator data, which was essential for a first-of-its-kind feasibility and efficacy validation. Consequently, while the framework's principles are designed for scalability, its performance and operational dynamics in a larger, multi-operator national grid—with its attendant political and commercial complexities—were outside the direct scope of this validation.

Second, the research prioritised the demonstration of technical feasibility and detection efficacy over a formal economic analysis of the solution itself. The proposed architecture is

technologically advanced, and its implementation implies costs in terms of capital and expertise. This thesis successfully quantifies the economic risk (the cost of an attack), providing the justification for such a framework. However, a formal Total Cost of Ownership (TCO) analysis for the monitoring solution was considered a separate, subsequent business-case activity, not a primary research question.

Third, the framework's validation was predicated on the availability of high-quality, CIM-compliant data. This 'greenfield' data environment was necessary to establish a clear, unambiguous baseline for the Business Process Analyzer's performance. The framework's robustness and the significant pre-processing effort required in typical 'brownfield' scenarios—which are often dominated by noisy data, incomplete telemetry, or non-standard protocols—was therefore not assessed.

Finally, the framework was intentionally specified at a logical and functional level to ensure its principles remain stack-agnostic. The research focused on defining the core artifacts, their interactions, and proving their function. The design and prototyping of the specific Application Layer, including the Human-Machine Interfaces and operational workflows for an analyst, was considered a subsequent, implementation-specific activity, and thus beyond the architectural and validation scope of this thesis.

National Security Implications for Prosumer-oriented Critical Infrastructure

This work has provided evidence-based insights for policymakers and national security strategists, highlighting how prosumer infrastructure introduces systemic vulnerabilities with profound implications for the energy critical infrastructure protection.

The Prosumer as the Weakest Link While the energy infrastructure is designed to be fault-tolerant and can easily withstand the failure or compromise of a single prosumer, its resilience does not account for multiple, coordinated attacks leveraging a single, widespread vulnerability. The true foundational threat is this systemic risk. The vast new class of non-technical prosumers shares a common, critical vulnerability: low cybersecurity awareness and a lack of security training. This creates a massive, uniform attack surface. An attacker doesn't need to find a unique flaw in each device; they only need one strategy—such as an AI-enhanced social engineering campaign impersonating a utility—to exploit this shared human factor at scale. Therefore, the critical danger is not an isolated breach but a coordinated compromise that hijacks thousands of prosumers simultaneously, enabling an attacker to manipulate load or generation in a way that could destabilize the entire grid.

Insecure Management and Operational Gaps This human vulnerability directly undermines device-level security. While a manufacturer may follow rigorous security-by-design principles and, for example, provide promptly security patches, the system's integrity is compromised by insecure operational practices. Attackers can leverage social engineering to convince a prosumer to bypass security controls, such as disabling safety features or installing unauthorized software under the guise of "maintenance." This effectively neutralizes manufacturer-side protections, creating a critical gap between the device's theoretical security and its real-world installations. Another operational risk arises from the third-party companies that often manage prosumer devices on behalf of homeowners. These entities may lack robust security practices, further exposing the infrastructure to compromise.

Concentrated Risk in Cloud Platforms and Supply Chains The reliance on third-party management creates a massive, concentrated risk. The market is dominated by a few major manufacturers, each operating centralized cloud platforms to manage their device fleet. This architecture represents an unprecedented vulnerability concentration; the compromise of a single cloud platform could grant an adversary simultaneous, coordinated control over hundreds of thousands or even millions of distributed energy assets. This concentrated supply chain structure means a single breach can be leveraged for a systemic, grid-scale attack.

Geopolitical and Data Sovereignty Threats Finally, policymakers must contend with a novel geopolitical risk. These critical cloud control platforms are frequently hosted in foreign jurisdictions, placing energy data and command infrastructure outside the nation's legal and regulatory control. This absence of guaranteed data sovereignty makes the energy infrastructure vulnerable to foreign state influence or direct manipulation. This dependency can be weaponised as diplomatic leverage or as an asymmetric attack vector, inextricably linking national energy security to the jurisdictional location of cloud data centres.

Lessons Learnt for Regulatory Bodies

This research provides evidence-based insights for governing bodies tasked with securing distributed energy infrastructure. A primary lesson is the inadequacy of current entity-based regulations, such as the NIS2 Directive. These frameworks fail to classify prosumer agglomerations as critical entities, even though, as this thesis demonstrates, their collective, coordinated behaviour can have systemic impacts on grid stability. The analysis confirms that the most vulnerable nodes in the infrastructure currently receive the least regulatory protection.

This gap is mirrored in device certification and market access regulations. While the Cyber Resilience Act introduces mandatory baseline security and lifecycle management, it shares a limitation with the Cybersecurity Act: a predominantly product-centric focus that does not

adequately address the concept of *collective criticality*. A single prosumer device may warrant only 'basic' certification or standard conformity assessment under the CRA, yet the aggregated risk of thousands of such devices necessitates a systemic security posture that current product-oriented frameworks do not effectively mandate. Securing the individual component does not automatically secure the aggregated system behavior.

Furthermore, the analysis highlights the practical limitations of applying corporate-grade compliance to individual prosumers. The requirements of the Cybersecurity Act, the AI Act, and GDPR, while appropriate for large organizations, are not economically or technically scalable to thousands of distributed installations. For instance, GDPR's comprehensive security requirements, with their emphasis on 'appropriate technical and organizational measures,' assume organizational capabilities that individual prosumers may lack, creating potential compliance gaps when their activities extend beyond the household exemption scope. This creates a systemic governance gap.

The research also points to a need for clearer multi-stakeholder accountability models, which are not sufficiently defined in frameworks like the EU Network Code on Cybersecurity or GDPR. Specifically for GDPR, its traditional, individual-centric approach to data controller identification and accountability is ill-suited for the complex, multi-stakeholder environment of distributed energy. This creates both significant multi-stakeholder liability coordination difficulties—with unclear responsibility distribution between Transmission System Operators, Distribution System Operators, aggregators, manufacturers, and the prosumers themselves—and collective impact accountability deficiencies. The regulation's focus on individual data processing fails to adequately address the aggregated privacy and security risks that emerge when numerous prosumer data processing activities combine to create systemic risks affecting critical infrastructure.

Generic regulations, such as the AI Act and GDPR, also require specific sectoral guidance to address the unique real-time operational and security needs of the energy domain, such as clarifying the 'household exception' for prosumers providing grid services. This household exception boundary ambiguity arises from unclear criteria for determining when prosumer activities exceed 'purely personal or household purposes,' a line that becomes increasingly blurred as prosumer participation in sophisticated grid services, demand response programs, and virtual power plant operations grows.

The key takeaway is that future legislation should evolve from an individual entity or product-centric view to a risk-based, systemic-impact perspective. This includes developing frameworks that formally address collective risk and establish clear, scalable responsibilities for the security of aggregated prosumer infrastructure.

Lessons Learnt for Security and Energy Operators

For technical stakeholders, this thesis highlights the insufficiency of conventional, aggregate-level monitoring for prosumer-driven grids, advocating instead for a data-centric, behaviour-based paradigm. The validation in Berchidda provides empirical evidence that manipulation-of-demand attacks are not merely theoretical. A subtle 10% production reduction across a small prosumer group was shown to have a measurable 5% impact on general municipal expenditure, confirming the economic and operational materiality of this threat vector.

The proposed four-artifact framework (DT, BPA, SCU, DSCB) was validated as a viable and effective solution. The Digital Twin Builder emerges as the foundational enabler. The case study demonstrated the critical importance of mapping legacy operator data (CIM) to a standard, semantic, real-time model (NGSI-LD). This Digital Twin is not merely a static model but the central data hub that enables all subsequent analytics and simulations to operate on a single, trusted source of truth.

From this foundation, the Business Process Analyzer (BPA) demonstrates effective detection capabilities at two levels. Single-entity baselines, using both mathematical and AI-based models, are effective at identifying individual prosumer deviations. Furthermore, the validation of the grid-level coordination check (the binomial tail test) shows this to be a reliable method for detecting the coordinated, low-and-slow nature of an advanced attack, which would be missed by isolated, single-device alarms. This highlights the need to move beyond simple thresholding to a more aggregated, statistical approach.

The Simulation Control Unit (SCU) was validated as an essential tool for proactive defense. It allows for the safe testing and validation of response procedures against "what-if" attack scenarios (such as a coordinated PV ramp-down) on a high-fidelity model of the network. This provides a repeatable, safe environment for training and policy refinement without any risk to live operations.

Finally, the validation of the Data Space Connector Builder (DSCB) points to advances in collaborative security. The case study demonstrated the feasibility of sharing curated security intelligence (e.g., aggregated BPA alerts, DT-derived indicators) with external stakeholders without sacrificing data sovereignty. This addresses a major operational barrier, showing that operators can participate in a trusted, cross-border ecosystem, gaining collective situational awareness without exposing sensitive raw operational data.

Final Remarks

This research has demonstrated a significant structural vulnerability within contemporary energy grid architectures, specifically concerning the aggregated behavior of distributed prosumer devices. Through empirical analysis and validation, the study has established that current regulatory frameworks, which predominantly focus on individual entity compliance, inadequately address the emergent systemic risks posed by coordinated device networks. The data-centric security architecture developed and tested within this work represents a departure from conventional approaches, offering a technically viable pathway for managing these distributed vulnerabilities while maintaining operational efficiency. The findings underscore the inherently interdisciplinary nature of energy grid security challenges. Technical solutions alone prove insufficient without corresponding evolution in regulatory structures and economic incentives. The research reveals that effective mitigation of these vulnerabilities requires simultaneous consideration of technological implementation, policy adaptation, and market mechanisms. By demonstrating the viability of collaborative, data-centric security architectures in this context, this research contributes to an expanding body of evidence that challenges conventional siloed approaches to critical infrastructure protection, suggesting that systemic vulnerabilities demand correspondingly systemic responses.

Bibliography

[1] Oluleke Babayomi, Zhenbin Zhang, Tomislav Dragicevic, Jiefeng Hu, and Jose Rodriguez, "Smart grid evolution: Predictive control of distributed energy resources—a review," *International Journal of Electrical Power & Energy Systems*, vol. 147, pp. 108812, 2023.

[2] Azwirman Gusrialdi and Zhihua Qu, "Smart grid security: Attacks and defenses," in *Smart Grid Control: Overview and Research Opportunities*, pp. 199–223. Springer, 2018.

[3] Kaibin Bao, Sid Chi-Kin Chau, Ghada Elbez, Qi Liu, and Veit Hagenmeyer, "Advanced persistent threats on consumer energy resources in decentralized energy systems," in *Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems*, 2025, pp. 838–845.

[4] Alfredo Petruolo, Luigi Coppolino, Roberto Nardone, and Luigi Romano, "Regulating prosumer device security: a key priority in power grid protection," in *2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*. IEEE, 2025, pp. 105–111.

[5] Heribert Vallant, Branka Stojanović, Josip Božić, and Katharina Hofer-Schmitz, "Threat modelling and beyond-novel approaches to cyber secure the smart energy system," *Applied Sciences*, vol. 11, no. 11, pp. 5149, 2021.

[6] Lazar Gitelman, Elena Magaril, and Mikhail Kozhevnikov, "Energy security: new threats and solutions," *Energies*, vol. 16, no. 6, pp. 2869, 2023.

[7] Kirsi Kotilainen, "Energy prosumers' role in the sustainable energy system," in *Affordable and clean energy*, pp. 1–14. Springer, 2019.

[8] Dong Liu, Xi Zhang, and K Tse Chi, "Effects of high level of penetration of renewable energy sources on cascading failure of modern power systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 1, pp. 98–106, 2022.

[9] Ersan Kabalci and Yasin Kabalci, "Introduction to smart grid architecture," in *Smart grids and their communication systems*, pp. 3–45. Springer, 2018.

[10] Arastoo Zibaeirad, Farnoosh Koleini, Shengping Bi, Tao Hou, and Tao Wang, "A comprehensive survey on the security of smart grid: Challenges, mitigations, and future research opportunities," *arXiv preprint arXiv:2407.07966*, 2024.

[11] Chenthamarai Selvam, Kota Srinivas, GS Ayyappan, and M Venkatachala Sarma, "Advanced metering infrastructure for smart grid applications," in *2012 International Conference on Recent Trends in Information Technology*. IEEE, 2012, pp. 145–150.

[12] Gordan Štruklec and Joško Maršić, "Implementing dlms/cosem in smart meters," in *2011 8th International Conference on the European Energy Market (EEM)*. IEEE, 2011, pp. 747–752.

[13] Cristian-Dragoș Dumitru and Adrian Gligor, "Scada based software for renewable energy management system," *Procedia Economics and Finance*, vol. 3, pp. 262–267, 2012.

[14] Gnana Swathika OV, Aayush Karthikeyan, K Karthikeyan, P Sanjeevikumar, Sajju Karapparambil Thomas, and Amin Babu, "Critical review of scada and plc in smart buildings and energy sector," *Energy Reports*, vol. 12, pp. 1518–1530, 2024.

[15] Mengxiang Liu, Fei Teng, Zhenyong Zhang, Pudong Ge, Mingyang Sun, Ruilong Deng, Peng Cheng, and Jiming Chen, "Enhancing cyber-resiliency of der-based smart grid: A survey," *IEEE Transactions on Smart Grid*, 2024.

[16] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response and Office of Energy Efficiency and Renewable Energy, "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid," Tech. Rep., U.S. Department of Energy, October 2022.

[17] European Network of Transmission System Operators for Electricity (ENTSO-E), "Frequency Stability Evaluation Criteria for the Synchronous Zone of Continental Europe," Tech. Rep., ENTSO-E, March 2016.

[18] International Renewable Energy Agency (IRENA), "Renewable Capacity Statistics 2025," Tech. Rep., IRENA, Abu Dhabi, March, Accessed on 30 June 2025.

[19] Forescout Research, "Sun:down: New vulnerabilities in solar power systems," March 2025, Accessed: November 30, 2025.

[20] Ioannis Zografopoulos, Nikos D Hatziargyriou, and Charalambos Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, 2023.

[21] Yuanliang Li and Jun Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, no. 2, pp. 2364–2383, 2022.

[22] Su Zin Zin Win, Zaw MM Htun, and HlaMyo Tun, "Smart security system for home appliances control based on internet of things," *International journal of scientific & technology research*, vol. 5, no. 06, pp. 102–107, 2016.

[23] SOCRadar Cyber Intelligence Inc., "Top 10 Exploited Vulnerabilities of 2024," `https://socradar.io/top-10-exploited-vulnerabilities-of-2024/`, January 2025, Accessed: 30 June 2025.

[24] Aldar C-F Chan and Jianying Zhou, "Toward safe integration of legacy scada systems in the smart grid," in *International Conference on Applied Cryptography and Network Security*. Springer, 2022, pp. 338–357.

[25] National Institute of Standards and Technology (NIST), "Guidelines for Smart Grid Cybersecurity – Volume 1, Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," NIST Interagency Report 7628, National Institute of Standards and Technology, Gaithersburg, MD, August 2010, Accessed: 30 June 2025.

[26] Corinne N Johnson, "The benefits fo pdca," *Quality Progress*, vol. 35, no. 5, pp. 120, 2002.

[27] James McCarthy, Jeffrey Marron, Don Faatz, Daniel Rebori-Carretero, Johnathan Wiltberger, and Nik Urlaub, "Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems," Tech. Rep. 8498, National Institute of Standards and Technology, 2024.

[28] Saleh Soltan, Prateek Mittal, and H Vincent Poor, "{BlackIoT}:{IoT} botnet of high wattage devices can disrupt the power grid," in *27th USENIX security symposium (USENIX security 18)*, 2018, pp. 15–32.

[29] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al., "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[30] Tohid Shekari, Celine Irvene, Alvaro A Cardenas, and Raheem Beyah, "Mamiot: Manipulation of energy market leveraging high wattage iot botnets," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, 2021, pp. 1338–1356.

[31] Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan, "Security analysis of internet-of-things: A case study of august smart lock," in *2017 IEEE conference on computer communications workshops (INFOCOM WKSHPS)*. IEEE, 2017, pp. 499–504.

[32] Gaoqi Liang, Steven R Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE transactions on power systems*, vol. 32, no. 4, pp. 3317–3318, 2016.

[33] Joseph Devanny, Luiz Rogério Franco Goldoni, and Breno Pauli Medeiros, "The 2019 venezuelan blackout and the consequences of cyber uncertainty," *Revista Brasileira de Estudos de Defesa*, vol. 7, no. 2, 2020.

[34] El-Nasser S Youssef, Fabrice Labeau, and Marthe Kassouf, "Detection of load-altering cyberattacks targeting peak shaving using residential electric water heaters," *Energies*, vol. 15, no. 20, pp. 7807, 2022.

[35] European Parliament and Council of the European Union, "Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union, amending regulation (eu) no 910/2014 and directive (eu) 2018/1972, and repealing directive (eu) 2016/1148 (nis 2 directive)," 2022.

[36] European Union, "Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU," June 2019, Text with EEA relevance.

[37] European Commission, "Commission recommendation (eu) 2019/553 - cybersecurity in the energy sector," apr 2019, Official Journal of the European Union, L 94/137.

[38] European Commission, "Commission delegated regulation (eu) 2024/1366 establishing a network code on cybersecurity for the electricity sector," may 2024, Official Journal of the European Union, L, 2024/1366.

[39] European Parliament and Council of the European Union, "Regulation (eu) 2019/881 on enisa (the european union agency for cybersecurity) and on information and communications technology cybersecurity certification and repealing regulation (eu) no 526/2013 (cybersecurity act)," apr 2019, Official Journal of the European Union, L 151/1.

[40] European Parliament and Council of the European Union, "Regulation (eu) 2024/1689 of the european parliament and of the council of 13 june 2024 laying down harmonised rules on artificial intelligence (artificial intelligence act)," jun 2024, Official Journal of the European Union, L, 2024/1689.

[41] European Union, "General data protection regulation (gdpr)," `https://gdpr.eu/`, 2018, Accessed: 2024-10-08.

[42] U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response, "Cybersecurity baselines for electric distribution systems and distributed energy resources," Tech. Rep., U.S. Department of Energy, February 2024.

[43] Federal Energy Regulatory Commission, "Order no. 2222: Participation of distributed energy resource aggregations in markets operated by regional transmission organizations and independent system operators," 2021.

[44] Federal Energy Regulatory Commission, "Cybersecurity incentives program," 2023.

[45] National Development and Reform Commission and National Energy Administration, "Action plan for accelerating the new type power system (2024-2027)," Tech. Rep., Government of China, 2024.

[46] Parliament of Canada, "Bill c-8: An act respecting critical cyber systems protection," June 2025.

[47] Natural Resources Canada, "Cyber energy security policy and outreach," Accessed August 2025.

[48] Ministry of Economy, Trade and Industry, "Cybersecurity guidelines for energy resource aggregation business version 3.0," Tech. Rep., Government of Japan, May 2025.

[49] Solar Mounting System Design, "How to design solar pv system," Blog post, `https://solarmountingdesign.wordpress.com/2017/11/15/how-to-design-solar-pv-system/`, 2017, Accessed: August 19, 2025.

[50] Jay Johnson, Bob Fox, Kudrat Kaur, and Jithendar Anandan, "Evaluation of interoperable distributed energy resources to ieee 1547.1 using sunspec modbus, ieee 1815, and ieee 2030.5," *IEEE Access*, vol. 9, pp. 142129–142146, 2021.

[51] Maryam Mohammadi Maghanki, Barat Ghobadian, Gholamhassan Najafi, and Reza Janzadeh Galogah, "Micro combined heat and power (mchp) technologies and applications," *Renewable and Sustainable Energy Reviews*, vol. 28, pp. 510–524, 2013.

[52] Jiří Libich, Josef Máca, Jiří Vondrák, Ondřej Čech, and Marie Sedlaříková, "Supercapacitors: Properties and applications," *Journal of energy storage*, vol. 17, pp. 224–227, 2018.

[53] Ji Hoon Yoon, Ross Baldick, and Atila Novoselac, "Dynamic demand response controller based on real-time retail price for residential buildings," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 121–129, 2014.

[54] Harshit Singh Jadon, Himanshu Prajapati, Kishan Agarwal, Vipul Tyagi, and Geetika Aswani, "Automatic home load management system," in *2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*. IEEE, 2020, pp. 934–939.

[55] Luigi Coppolino, Valerio D'Alessandro, Salvatore D'Antonio, Leonid Levy, and Luigi Romano, "My smart home is under attack," in *2015 IEEE 18th International Conference on Computational Science and Engineering*. IEEE, 2015, pp. 145–151.

[56] Iliana Shandurkova, Bernt A Bremdal, Rainer Bacher, Stig Ottesen, and Andreas Nilsen, "A prosumer oriented energy market," *IMPROSUME: NCE smart energy markets*, 2012.

[57] Esteban A Soto, Lisa B Bosman, Ebisa Wollega, and Walter D Leon-Salas, "Peer-to-peer energy trading: A review of the literature," *Applied energy*, vol. 283, pp. 116268, 2021.

[58] Khizir Mahmud, Behram Khan, Jayashri Ravishankar, Abdollah Ahmadi, and Pierluigi Siano, "An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview," *Renewable and Sustainable Energy Reviews*, vol. 127, pp. 109840, 2020.

[59] Younes Zahraoui, Tarmo Korõtko, Argo Rosin, Tekai Eddine Khalil Zidane, Hannes Agabus, and Saad Mekhilef, "A competitive framework for the participation of multi-microgrids in the community energy trading market: A case study," *IEEE Access*, vol. 12, pp. 68232–68248, 2024.

[60] Subhash Lakshminarayana, Yexiang Chen, Carsten Maple, Andrew Larkins, Daryl Flack, Christopher Few, Kenny Awuson-David, and Anurag K Srivastava, "Threats to power grid operations from the demand-side response ecosystem: A comprehensive overview," *IEEE Industrial Electronics Magazine*, 2025.

[61] Wood Mackenzie, "Tesla takes sungrow's crown as lead global producer of battery energy storage systems in 2023," 2024.

[62] Ahmed Hadi Ali AL-Jumaili, Yousif I. Al Mashhadany, Rossilawati Sulaiman, and Zaid Abdi Alkareem Alyasseri, "A conceptual and systematics for intelligent power management system-based cloud computing: Prospects, and challenges," *Applied Sciences*, vol. 11, no. 21, 2021.

[63] Lea Müller, Stefan Sütterlin, and Holger Morgenstern, "Towards a proof-of-principle of an llm-powered low resource social engineering attack coach," in *International Conference on Human-Computer Interaction*. Springer, 2025, pp. 205–217.

[64] Tharindu Kumarage, Cameron Johnson, Jadie Adams, Lin Ai, Matthias Kirchner, Anthony Hoogs, Joshua Garland, Julia Hirschberg, Arslan Basharat, and Huan Liu, "Personalized attacks of social engineering in multi-turn conversations–llm agents for simulation and detection," *arXiv preprint arXiv:2503.15552*, 2025.

[65] Darren Steve Dsouza, Ayman El Hajjar, and Hamid Jahankhani, "Deepfakes in social engineering attacks," in *Space Law Principles and Sustainable Measures*, pp. 153–183. Springer, 2024.

[66] Luigi Coppolino, Roberto Nardone, Alfredo Petruolo, and Luigi Romano, "Increasing the cybersecurity of smart grids by prosumer monitoring," *IEEE Transactions on Industrial Informatics*, 2024.

[67] Industrial Internet Consortium and Plattform Industrie 4.0, "Digital twin and asset administration shell concepts and application in the industrial internet and industrie 4.0," `https://www.iiconsortium.org/pdf/`

Digital-Twin-and-Asset-Administration-Shell-Concepts-and-Application-Joint-Whitepaper.pdf, 2020, [Online; accessed August 8, 2025].

[68] Digital Twin Consortium, "The definition of a digital twin," https://www.digitaltwinconsortium.org/initiatives/the-definition-of-a-digital-twin/, 2023, [Online; accessed August 8, 2025].

[69] Luigi Coppolino, Roberto Nardone, Alfredo Petruolo, and Luigi Romano, "Building cyber-resilient smart grids with digital twins and data spaces," *Applied Sciences*, vol. 13, no. 24, pp. 13060, 2023.

[70] Luigi Coppolino, Adelaida Parreño-Rodríguez, Alfredo Petruolo, Juan Sánchez-Valverde, and Antonio F Skarmeta-Gómez, "Simulation as a service in data spaces: A digital twin-based approach," *Data Science and Engineering*, pp. 1–19, 2025.

[71] Fabian Stadtmann, H. A. G. Wassertheurer, and Adil Rasheed, "Demonstration of a standalone, descriptive, and predictive digital twin of a floating offshore wind turbine," in *Volume 8: Ocean Renewable Energy*. June 2023, American Society of Mechanical Engineers.

[72] "The digital twin in industry 4.0: A wide-angle perspective," *Quality and Reliability Engineering International*, vol. 38, no. 3, pp. 1357–1366, April 2022.

[73] ETSI ISG CIM, "GR CIM 017 - V1.1.1 - Context Information Management (CIM); Feasibility of NGSI-LD for Digital Twins," Tech. Rep., ETSI, 2022.

[74] EPRI, "Common information model (cim) primer: Eighth edition," 2011.

[75] L. Coppolino, Roberto Nardone, Alfredo Petruolo, L. Romano, and A. Souvent, "Exploiting digital twin technology for cybersecurity monitoring in smart grids," *ACM Digital Library*, 2023.

[76] Anna Gieß, Marius Hupperz, Thorsten Schoormann, and Frederik Möller, "What does it take to connect? unveiling characteristics of data space connectors," 2024.

[77] Luigi Coppolino, Alessandro De Crecchio, Roberto Nardone, Alfredo Petruolo, Luigi Romano, and Federica Uccello, "Exploiting data spaces to enable privacy preserving data exchange in the energy supply chain," *Proceedings of the ITASEC*, 2024.

[78] Emilio Ghiani, Andrea Giordano, Andrea Nieddu, Luca Rosetti, and Fabrizio Pilo, "Planning of a smart local energy community: The case of berchidda municipality (italy)," *Energies*, vol. 12, no. 24, pp. 4629, 2019.

List of Publications

Journal Papers

2023 Coppolino, Luigi; Nardone, Roberto; **Petruolo, Alfredo**; Romano, Luigi, "Building cyber-resilient smart grids with digital twins and data spaces," Applied Sciences, vol. 13, no. 24, pp. 13060, 2023, MDPI.

2024 Coppolino, Luigi; Nardone, Roberto; **Petruolo, Alfredo**; Romano, Luigi, "Increasing the Cybersecurity of Smart Grids by Prosumer Monitoring," IEEE Transactions on Industrial Informatics, 2024, IEEE.

2025 Coppolino, Luigi; Parreño-Rodríguez, Adelaida; **Petruolo, Alfredo**; Sánchez-Valverde, Juan; Skarmeta-Gómez, Antonio F, "Simulation as a Service in Data Spaces: A Digital Twin-based Approach," Data Science and Engineering, pp. 1-19, 2025, Springer Nature Singapore.

2025 Coppolino, Luigi; Iannaccone, Antonio; Nardone, Roberto; **Petruolo, Alfredo**, "Asset Discovery in Critical Infrastructures: An LLM-Based Approach," Electronics, vol. 14, no. 16, pp. 3267, 2025.

Conference Papers

2023 Coppolino, Luigi; Nardone, Roberto; **Petruolo, Alfredo**; Romano, Luigi; Souvent, Andrej, "Exploiting digital twin technology for cybersecurity monitoring in smart grids," Proceedings of the 18th International Conference on Availability, Reliability and Security, pp. 1-10, 2023.

2023 Coppolino, Luigi; Nardone, Roberto; **Petruolo, Alfredo**; Romano, Luigi, "Securing FIWARE with TEE technology," New Trends in Intelligent Software Methodologies, Tools and Techniques, pp. 149-160, 2023, IOS Press.

2024 De Crecchio, Alessandro; Cristiano, Giovanni Maria; **Petruolo, Alfredo**, "Mobile Phones in the Cloud-Edge Continuum: Understanding the TEE's Role," International Conference on Advanced Information Networking and Applications, pp. 234-243, 2024, Springer Nature Switzerland Cham.

2024 Coppolino, Luigi; De Crecchio, Alessandro; Nardone, Roberto; **Petruolo, Alfredo**; Romano, Luigi; Uccello, Federica, "Exploiting Data Spaces to Enable Privacy Preserving Data Exchange in the Energy Supply Chain," Proceedings of the ITASEC, 2024.

2024 Nardone, Roberto; **Petruolo, Alfredo**; Uccello, Federica, "Secure and Transparent Data Sharing Among Connected Devices: Integrating Data Spaces and Provenance," 2024 IEEE International Conference on Cyber Security and Resilience (CSR), pp.

670-675, 2024, IEEE.

2024 Coppolino, Luigi; Nardone, Roberto; **Petruolo, Alfredo**; Romano, Luigi, "Connecting the Mobility and the Refuelling/Recharging Infrastructures: The Role of Data Spaces," 2024 IEEE International Conference on Environment and Electrical Engineering and 2024 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe), pp. 1-6, 2024, IEEE.

2024 Mineo, Carmelo; Nardone, Roberto; Paoletti, Michele; Paragliola, Giovanni; **Petruolo, Alfredo**, "Advanced Monitoring with Enhanced Security in Critical Infrastructures: the DOSSIER framework," 2024 IEEE International Workshop on Technologies for Defense and Security (TechDefense), pp. 165-170, 2024, IEEE.

2025 **Petruolo, Alfredo**; Coppolino, Luigi; Nardone, Roberto; Romano, Luigi, "Regulating Prosumer Device Security: a Key Priority in Power Grid Protection," 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S), pp. 105-111, 2025, IEEE.

2025 **Petruolo, Alfredo**; Iannaccone, Antonio; D'Antonio, Salvatore. Towards a Privacy-Preserving Health Data Sharing: Architecture and Critical Implementation Factors. In: 2025 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 2025. p. 725-730.