UNITECH SELECTED PAPERS

INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025, GABROVO

REVIEW OF SECURITY METHODS FOR COMPUTER NETWORKS IN RENEWABLE ENERGY PRODUCTION SYSTEMS

Nikolay Hinov[1*], Sinan Salim Salim [2]

[1] Technical University of Sofia, Department of Computer Systems, 8, Kliment Ohridsky blvd. Sofia, Bulgaria
[2] Technical University of Sofia, Department of Cybersecurity, 8, Kliment Ohridsky blvd. Sofia, Bulgaria
**Corresponding author: hinov@tu-sofia.bg*

Abstract
This paper reviews security methods for computer networks used in renewable energy production systems (PV farms, wind parks, hybrid DER plants). We structure threats and countermeasures across field, control, and enterprise layers, considering standards and protocols typical for energy automation (IEC 61850, IEC 60870-5-104, DNP3, Modbus/TCP, MQTT, OPC UA, IEEE 2030.5). The review covers architectural measures (segmentation/zero trust), cryptographic protections (TLS, OPC UA Security, IEC 62351), detection and response (IDS/IPS, anomaly detection, SIEM/SOAR), secure device lifecycle (secure boot, firmware signing, PKI), and governance frameworks (IEC 62443, NIST SP 800-82, NIS2). We provide a comparison matrix of methods vs. attack classes (DoS, MITM, spoofing, ransomware) and outline KPIs for cyber-resilience in DER networks.
Keywords: renewable energy, DER cybersecurity, IEC 61850, IEC 62443, IDS/IPS, zero trust, ICS/SCADA security.

INTRODUCTION

Digitalization and distributed energy production are ushering in a new era in power system management. With the advent of photovoltaic, wind and hybrid power plants based on the Distributed Energy Resources (DER) concept, an increasing part of critical infrastructure is managed through intelligent communication networks based on SCADA, IoT and cloud platforms.

This high connectivity provides significant advantages, the possibility of remote control, predictive maintenance and optimization through artificial intelligence. At the same time, however, it increases the attack surface and requires a new type of approach to security. While traditional IT systems rely on centralized protection and periodic updates, operational technologies (OT) in the energy sector are characterized by high requirements for availability, determinism and low latency, which often excludes classic mechanisms such as antiviruses, IDS agents and heavy cryptographic operations.

In the context of the energy transition and the decentralization of networks, cybersecurity is now seen not simply as technological, but as an element of energy security and sustainability. Possible attacks such as DoS on communication gateways, measurement manipulation, unauthorized control of inverters or ransomware in SCADA systems can lead not only to financial losses, but also to network instability or equipment damage.

A comprehensive and multi-level approach is needed that combines architectural measures (zoning and segmentation), cryptographic protection of communications, mechanisms for monitoring and anomaly detection, vulnerability management and compliance with standards such as IEC 62443,

doi: www.doi.org/10.70456/.....

IEC 62351, NIST SP 800-82 and NIS2.

This article offers a systematic review of computer network security methods used in renewable energy production systems. Architectural, cryptographic, detection and organizational mechanisms applicable to the different layers of energy communications from the field level to the corporate and cloud infrastructure are covered. The aim is to present an integrated framework for increasing the cyber resilience of DER networks and to identify key performance indicators (KPIs) for their assessment.

THREATS AND SPECIFICS OF RES NETWORKS

Modern renewable energy (RES) systems are a combination of physical infrastructure and digital communications, which makes them both technically complex and vulnerable to cyberthreats. RES plants include inverters, controllers, PLC/RTU devices, protections, SCADA systems and communication gateways, connected via a variety of industrial automation protocols.

Many of the industrial protocols used (e.g. Modbus/TCP, "classic" DNP3, IEC 60870-5-104) were designed in an era when security was not a priority. They lack authentication, encryption and integrity mechanisms, making them vulnerable to spoofing, replay and man-in-the-middle (MITM) attacks.

More modern solutions such as OPC UA, MQTT over TLS and IEEE 2030.5 (Smart Energy Profile 2.0) integrate built-in authentication and encryption mechanisms, but require proper configuration and certificate management (PKI).

In addition, the IEC 61850-7-420 profiles adapted for DER introduce additional functional requirements for secure communication and compatibility with energy aggregators and VPP (Virtual Power Plant).

DER infrastructures are exposed to a wide range of attacks that can be grouped into several categories, such as DoS/DDoS attacks against RTUs, gateways and MQTT brokers leading to loss of visibility and control, MITM and spoofing attacks over TCP/IP or serial tunnels with substitution of commands or measurements, Unauthorized access to HMI, PLC or web interfaces of inverters due to weak passwords, outdated firmware or lack of RBAC, Ransomware and malware in engineering stations and SCADA servers via infected updates or USB media (example: Industroyer2, WannaCry), Supply chain attacks where malicious code is embedded in firmware updates or libraries, Attacks on cloud platforms and APIs used by energy aggregators, including data substitution or misuse of access tokens, Physical attacks and sensor manipulations, e.g. substitution of data from metering devices or manipulation of time synchronization (time spoofing).

RES devices often have limited computing resources (memory, CPU, power consumption), which limits the implementation of classic IT security mechanisms. Additionally, the requirements for high determinism and low latency do not allow for heavy monitoring agents or complex cryptographic algorithms.

In many cases, there is a mixed infrastructure of old and new devices, where the lack of a unified security standard makes key management, authentication and firmware updates difficult.

With the expansion of IoT integration and cloud-based SCADA platforms, threats are no longer limited to local substations, but also cover distributed microgrids that exchange data in real time with external operators.

AI-based attacks using automated vulnerability detection and adversarial traffic generation are also emerging.

In the future, a critical factor will be the protection of time synchronization (NTP/PTP), API interfaces of DER aggregators, as well as the cybersecurity of virtual power plants (VPP)

ARCHITECTURAL METHODS AND ZONING

One of the most effective ways to increase security in energy process control systems is the architectural division of the

doi: www.doi.org/10.70456/.....

network into zones and conduits, in accordance with the IEC 62443 and ISA-95 frameworks. This approach aims to limit the spread of incidents, minimize communications between incompatible environments, and provide clear boundaries for implementing access, monitoring, and protection policies.

Renewable energy production systems such as photovoltaic plants, wind parks and hybrid DER installations rely on heterogeneous communication infrastructures that span from field devices to cloud-based supervisory platforms. Ensuring cybersecurity in such systems therefore requires a multilayered architectural approach aligned with IEC 62443, NIST SP 800-82 and modern Zero Trust principles.

Figure 1 presents an integrated view of the cybersecurity layers in DER/RES networks, from the Field/IED layer (inverters, RTUs, sensors and protection relays) through the Operations/DMZ and Control layers (SCADA, PLCs, IDS/IPS, engineering stations) up to the enterprise and cloud environments (VPP platforms, SIEM/SOAR, PKI). The figure highlights the key security mechanisms applied at each segment, including segmentation, mTLS, IEC 62351 extensions, anomaly detection and certificate-based authentication.

This layered structure reflects the defence-in-depth model and illustrates how secure data flows, trusted communication, monitoring and auditing collectively contribute to cyber-resilience in modern renewable energy systems.

Energy systems are divided into several functional layers, such as Level 0–1 (Field/IED Layer), field-level devices (inverters, protections, RTUs, metering devices). Real-time protocols (IEC 61850-8-1, Modbus RTU/TCP) with low latency requirements are used here. Level 2 (Control Layer): SCADA, PLC, and local operator HMIs, providing process control and visualization. Level 3 (Operations/DMZ), data zone and intersystem exchange (historian, engineering stations, MQTT brokers). Firewalls, IDS and brokers for controlled data transmission are applied here. Level 4–5 (Enterprise/Cloud): corporate systems, ERP, VPP platforms, cloud applications and services of external providers.

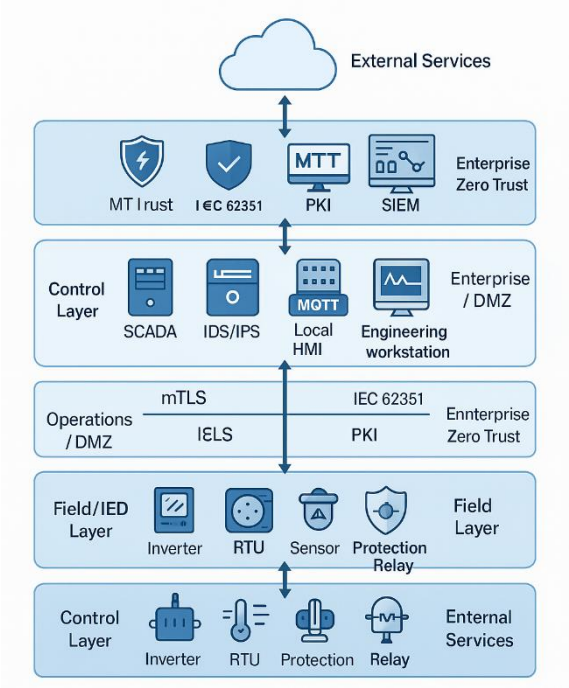

Figure 1. *Multi-layer cybersecurity architecture for DER/RES networks.*

Each level has its own access policy and cryptographic protection. Communication between levels is implemented through controlled channels (conduits) with traffic inspection and strict control of ports and protocols.

Classical segmentation is often insufficient in dynamic environments such as hybrid RES systems and microgrids. Microsegmentation applies access policies at the application or service level (Layer 7), allowing east-west control between individual virtual machines, containers or edge devices. With the help of Software-Defined Networking (SDN) and service mesh architectures, administrators can centrally manage routing, filtering, and encryption policies, as well as dynamically isolate compromised services without

doi: www.doi.org/10.70456/.....

disrupting the entire process. This approach is especially effective when implementing virtual DER gateways, edge brokers, and local analytics nodes with ML/AI functions.

The concept of Zero Trust means that no device, user, or service is considered trusted by default, regardless of whether it is located inside or outside the network perimeter. The main principles applicable to OT environments include, Authentication of each communication session via mTLS or device identity (certificates, TPM-based keys). Least privilege and context-sensitive access control. Continuous trust evaluation through correlation of behavior and access policies. Segmentation of control and monitoring: for example, separation of SCADA administration from telemetry channels. Zero Trust in the context of RES systems is often implemented through gateway levels with identification and signing of all MQTT or OPC UA sessions.

The DMZ (Demilitarized Zone) serves as an intermediate layer between OT and IT networks, through which only strictly defined data exchange passes. In DER infrastructures, unidirectional gateways (data diodes) are often used for one-way transmission of telemetry to SCADA or the cloud; MQTT brokers with TLS and client certificates, which provide asynchronous exchange without a direct connection between the systems; Reverse proxy servers and API gateways for filtering and controlling incoming traffic. This minimizes the risk of compromising critical systems, even in the event of a breach in the corporate network.

Architectural segmentation should be considered in synergy with physical access measures, because compromising a cabinet, RTU or PLC can bypass all logical security. Therefore, IEC 62443 recommends a combination of network zoning, physical restriction and procedural control, including access auditing, video surveillance and asset inventory.

The combination of architectural zoning, microsegmentation and Zero Trust provides: Localization of incidents and limiting their spread; Flexibility in integrating new DER modules and IoT devices; Centralized management of policies and cryptographic keys; Increased visibility and the ability to apply SIEM/SOAR analyses in real time.

CRYPTOGRAPHIC PROTECTION AND PROTOCOLS

Cryptographic protection is a fundamental element of cybersecurity in RES management systems, ensuring confidentiality, integrity and authenticity of data exchanged between field devices, SCADA systems and cloud services. Unlike in classic IT environments, here cryptography must be efficient, deterministic and compatible with devices with limited resources (inverters, RTU, IED).

The most common cryptographic protection mechanism in DER networks is Transport Layer Security (TLS), used in protocols such as HTTPS, MQTT over TLS, OPC UA and IEEE 2030.5 SEP2.0. Modern implementations use TLS versions 1.2/1.3 with support for Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for perfect forward secrecy, and symmetric encryption algorithms such as AES-GCM or ChaCha20-Poly1305. Mutual TLS is recommended for communication between brokers, aggregators, and DER gateways, where both the client and server authenticate each other with X.509 certificates. IPsec in tunnel or transport mode can also be used to protect traffic between subnets or between different entities, especially for VPN connections between substations and central dispatch centers.

Open Platform Communications Unified Architecture (OPC UA) is a protocol widely used in energy SCADA and gateway environments. Its security layer supports a combination of mechanisms for: Message Signing and Encryption; User/Application

doi: www.doi.org/10.70456/.....

Certificates; Key rotation and management via an integrated trust store; Secure channels and sessions that isolate all communication between client and server.

To evaluate the effectiveness of different protection mechanisms in renewable energy and DER network environments, it is essential to compare how each method responds to distinct classes of cyberattacks. Renewable energy systems combine legacy industrial protocols with modern cloud-integrated platforms, which exposes them simultaneously to DoS, spoofing, unauthorized access, malware and supply-chain attacks.

Figure 2 presents a comparative matrix that maps the major cybersecurity methods discussed in the paper—segmentation/DMZ, Zero Trust with mTLS, IEC 62351 and OPC UA Security, IDS/IPS, machine-learning-based anomaly detection, SIEM/SOAR platforms, and secure boot & firmware signing—against the most common attack categories affecting DER infrastructures.

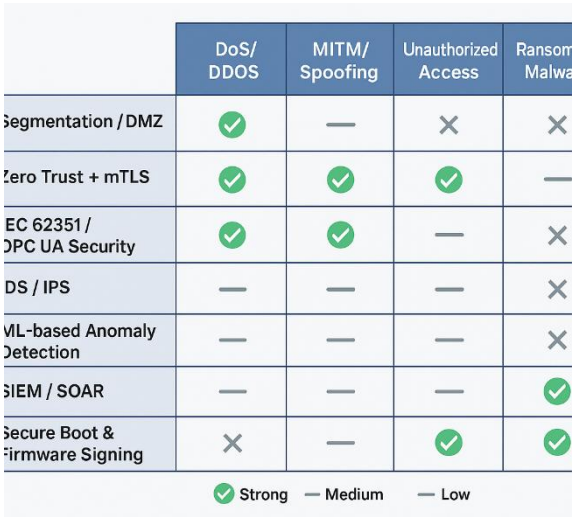

Figure 2. *Matrix illustrating the effectiveness of key cybersecurity methods against major attack classes in DER/RES networks.*

The visual comparison highlights that no single method provides complete protection. Instead, defence-in-depth is achieved by combining architectural isolation, cryptographic trust, behavioural monitoring, and secure device lifecycle mechanisms. The matrix clearly illustrates which controls are strong, moderately effective, or insufficient against specific attack vectors, supporting informed prioritization and strategic planning for cyber-resilience.

OPC UA offers different security policy profiles (e.g. Basic256Sha256, Aes128_Sha256_RsaOaep) that define the specific algorithms and key lengths. In the DER context, OPC UA is often used for secure integration between inverters, energy managers and SCADA, allowing simultaneous authentication, access control and auditing.

The IEC 62351 family of standards defines security extensions to the IEC 60870-5-104, IEC 61850, DNP3 and other protocols used in the energy industry. The main functional groups include: IEC 62351-3: cryptographic protection of TCP/IP communications using TLS profiles optimized for real-time systems; IEC 62351-5: Authentication and integrity of messages in DNP3 and IEC 60870-5 telemetry; IEC 62351-6: Protection of GOOSE and Sampled Values by signing and time-limiting packets; IEC 62351-8: Role-Based Access Control (RBAC) for SCADA operators and devices; IEC 62351-9: Management of certificates and cryptographic keys in OT infrastructure. The implementation of these extensions ensures compatibility between different vendors and layers in the system, while minimizing latency and load on devices.

Public Key Infrastructure (PKI) is a fundamental element for large-scale authentication and cryptographic key management in DER systems. A typical architecture includes a hierarchy of Certification Authorities (CA), a root, intermediate and local CA located in a substation or operator center. Certificates can be issued and renewed automatically via Simple Certificate Enrollment Protocol (SCEP) or EST (Enrollment over Secure Transport). Hardware protection of keys is achieved with Hardware Security Modules

doi: www.doi.org/10.70456/.....

(HSM) integrated into gateways or controllers. It is a good practice to periodically rotate keys and automatically revoke them when a device is compromised.

Time synchronization is a critical element in power grids, especially with IEC 61850 Sampled Values (SV) and Time-Sensitive Networking (TSN). Time spoofing attacks can cause incorrect protection actions or synchronization errors between substations. The following are applied for protection: Signing and authentication of PTP messages (IEEE 1588v2 Annex K); Filters and white-list for NTP/PTP sources; Timestamping and clock correlation mechanisms, ensuring time trustworthiness verification.

Due to the limited computational capabilities of field devices, lightweight cryptographic algorithms (e.g. Elliptic Curve Cryptography (ECC), Ed25519, AES-CCM) and hardware encryption accelerators are required in DER systems. In the future, the gradual introduction of Post-Quantum Cryptography (PQC) for long-term key protection is expected, especially in the context of the NIST SP 800-208 standard and the ENISA initiative for quantum-resistant cryptography.

DETECTION & RESPONSE

While architectural and cryptographic measures reduce the probability of a successful attack, effective detection and response are crucial to limit the consequences of a real breach.

In RES systems, where communication processes are continuous and distributed, a combination of passive and active monitoring methods specialized for OT environments, as well as mechanisms for correlation and automated response, are required.

Intrusion detection and prevention systems (IDS/IPS) adapt to the specifics of industrial protocols. Traditional IT network solutions are not suitable for DER environments due to the lack of understanding of protocols such as IEC 60870-5-104, DNP3, IEC 61850 MMS/GOOSE, Modbus/TCP, OPC UA. Therefore, specialized OT IDS solutions such as Zeek (Bro), Suricata and Snort ICS modules are used, extended with parsers for industrial protocols and rules based on the state of communication (stateful inspection). Example: by analyzing the sequence of GOOSE messages or DNP3 packets, the system can detect anomalous commands or replay attacks without disrupting the real-time process. IPS (Intrusion Prevention Systems) are often implemented in border zones (DMZ, SCADA firewall) and perform deep inspection (Deep Packet Inspection – DPI) to block unauthorized protocols or ports.

Traditional signature systems cannot detect new or modified attacks. For this purpose, behavioral and ML-based approaches are used that model the normal operation of the system and detect deviations in real time. Examples of such methods include: Statistical baselining – determining normal ranges of parameters (e.g. command frequency, traffic volume); Machine learning models – autoencoders, Isolation Forest, LSTM/GRU networks that analyze time sequences of traffic or sensor values. Stateful ICS anomaly detection – checking a logical sequence of events (e.g. impossible order of ON/OFF commands). Federated learning approaches, in which local agents in substations or microgrids train local models without sharing sensitive data. AI-based methods also allow for predictive threat detection by analyzing combined indicators from communication, SCADA tags and system logs.

For comprehensive incident analysis, Security Information and Event Management (SIEM) platforms are used that collect and correlate data from: IDS/IPS systems; SCADA logs and telemetry; firewalls, brokers and MQTT gateways; vulnerability management systems (CVE/SBOM). Event correlation allows for the identification of complex scenarios – for

doi: www.doi.org/10.70456/.....

example, a combination of anomalous traffic, failed authentication, and a change in PLC configuration. Integration with Security Orchestration Automation and Response (SOAR) platforms allows for automatic actions in the event of an incident – isolating the affected node, restarting a process, activating a fallback mode, or notifying an operator.

Energy organizations are increasingly using external Threat Intelligence platforms (ENISA, MITRE ATT&CK for ICS, ISAC for the Energy Sector), which provide: lists of indicators of compromise (IoC) – IP addresses, hashes, domains, signatures of known attacks; tactics, techniques, and procedures (TTPs) of known adversaries; information about active campaigns and vulnerabilities related to OT components (e.g. vulnerabilities in SolarEdge, Siemens, Schneider). Integrating these indicators into SIEM/SOAR systems increases the speed and accuracy of detection.

After detecting an anomaly or attack, an Incident Response Plan is activated, which includes: Isolation of affected systems (network quarantine, switch-off); Collection of artifacts – logs, memory, configurations for subsequent forensic analysis; Impact assessment and switching to "safe mode" or fallback control; Restoration and integrity verification through backups and firmware verification; Reporting and learning – updating playbooks and tabletop exercises.

The effectiveness of detection and response systems can be measured by: MTTD (Mean Time to Detect) and MTTR (Mean Time to Respond); Detection Rate / False Positive Rate of IDS/ML models; Coverage Rate – percentage of protocols and zones that are monitored; Number of successfully executed playbooks – annually exercised scenarios; Correlation Efficiency Index – ratio between detected combined incidents and total alarms.

In the context of DER systems, the following trends are emerging: Use of Edge AI IDS, local ML models , implemented directly in gateway devices; Self-learning SOAR systems that adapt responses based on previous incidents; Integration of digital twins for cyberattack simulation and resilience assessment; Transition to Cloud-Native Security architectures with automatic scaling and continuous model training.

SECURE DEVICE LIFECYCLE

Cybersecurity of DER systems cannot be guaranteed only through network or software measures; it starts from the design, manufacturing and deployment phase of the devices. The concept of secure device lifecycle covers the entire life cycle of the equipment from its creation and initial configuration, through operation, updates and maintenance, to decommissioning and decommissioning.

The basis of hardware security is the trusted boot (Secure Boot), which ensures that when turned on, the device loads only signed and verified firmware. This function is implemented through Trusted Platform Module (TPM) or Root of Trust (RoT) elements that store cryptographic hashes of the permissible firmware versions. If a change is detected during boot, the system blocks the boot and signals a compromise. In the DER context, Secure Boot is critical for inverters, gateways, edge controllers and communication processors, which can be targets of supply-chain attacks.

Signing firmware with digital certificates (code signing) guarantees the integrity and origin of updates. The process should include: Verifying the digital signature before installation; Verifying the CA/PKI hierarchy from which the signature comes; Maintaining a secure update channel – typically via HTTPS or TLS tunnel with two-way authentication; Rollback protection that prevents reverting to old, vulnerable versions. There are industry standards such as IEC 62443-4-2 and IEEE 2654 that describe the requirements for secure updates in industrial environments. Hardening is the process of minimizing the attack surface by:

doi: www.doi.org/10.70456/.....

Disabling unnecessary services and ports; Using role-based access (RBAC) or attribute-based access control (ABAC); Segregating users and roles – operator, engineer, administrator; Restricting physical access through passwords, tokens, smart cards or biometrics; Logging and remotely auditing every action on the device. It is particularly important to record all actions on SCADA and RTU configurations in a tamper-proof log for subsequent forensic analysis.

One of the latest and most important practices is real-time vulnerability management by maintaining a Software Bill of Materials (SBOM), a structured information about all software components, libraries and versions in the firmware of a given device. Through SBOM, manufacturers and operators can: Identify dependencies containing known CVE vulnerabilities; Assess the risk of new public exploits; Automate the process of patch management and vulnerability scanning. Regulatory frameworks such as the EU Cyber Resilience Act (CRA) and NIS2 already introduce an obligation to maintain SBOM for critical devices.

Many attacks in the energy sector occur along the supply chain. Examples include the introduction of malicious code in updates (SolarWinds, 2020) or compromised drivers in the manufacturing process. To prevent such attacks, it is necessary to: Use only trusted manufacturing partners and suppliers with valid certification (IEC 62443-2-4); Verify firmware and libraries using cryptographic hashes; Conduct periodic integrity checks in the operational phase.

DER systems require careful planning of maintenance windows to avoid disrupting energy production. It is recommended to use automated firmware distribution platforms that apply updates in stages and provide the ability to safely rollback in the event of an error. Ideally, each update should be digitally signed, tested, and checksum verified.

Physical protection is an integral part of the life cycle: Locked cabinets and substations; Tamper detection – sensors for opening, impact, or vibration; Shielding of communication lines; Geolocation control and alarms when moving devices. Even the best cyber protection can be bypassed with physical access, so physical security is considered the first level of protection.

When replacing or decommissioning equipment, the following must be ensured: Deleting keys and certificates from memory (secure erase); Deactivating accounts and deleting identifiers from the management system; Documenting the process in the asset management system (Asset Management).

In the development of firmware and SCADA applications, the DevSecOps approach is increasingly being applied, which integrates security into every stage of development, design, testing, deployment and maintenance. This includes automated vulnerability testing, code analysis (SAST/DAST) and continuous integration with PKI systems.

Key indicators for life cycle management (Lifecycle KPIs) are: Patch Compliance Rate (% devices with up-to-date firmware); MTTV (Mean Time to Validate) – average time for checking and approving new firmware; Firmware Integrity Success Rate – percentage of successfully verified updates; Tamper Detection Incidents – number of detected physical manipulations; SBOM Coverage (%) – share of devices with up-to-date SBOM record.

GOVERNANCE FRAMEWORKS AND COMPLIANCE

Technical protection measures must be integrated into a comprehensive governance framework that ensures sustainability, traceability and compliance with international and national requirements. In the context of renewable energy (RES) systems, cybersecurity is considered an integral part of critical infrastructure

doi: www.doi.org/10.70456/.....

management, which includes policies, procedures, risk assessment and performance control.

The IEC 62443 family of standards is the main international framework for industrial cybersecurity applicable to all OT/ICS systems, including DER and SCADA infrastructures. It defines: Zones & conduits – a structural approach to segmentation and control of flows; Security Levels (SL 1–4) – degree of resilience to defined threats; Security lifecycle – from design to decommissioning; Roles and responsibilities for manufacturers, integrators and operators (parts 2-4 and 3-3).

The application of IEC 62443 in power systems allows: building a structured access policy (SL-by-zone mapping); maturity assessment using the IEC 62443-2-1/4-1 standard; creating integrated programs for audit and certification of components (conformity assessment).

The document "Guide to Industrial Control Systems Security" (NIST SP 800-82 Rev.2) provides a framework for assessing and managing risk in industrial and power systems. It offers: models for identifying assets, threats and vulnerabilities; prioritizing risk according to the impact on safety, availability and data; procedures for monitoring and continuous improvement.

The NIST model is successfully combined with IEC 62443 - the first provides a risk-oriented process, and the second - specific technical and organizational requirements.

The new Directive (EU) 2022/2555 – NIS2 introduced in 2023–2024 significantly expanded cybersecurity requirements in the energy sector, including for operators of renewable energy capacity, microgrids and energy aggregators. The main highlights include: Mandatory risk assessment and implementation of technical and organizational measures; Incident reporting – notification of national authorities within 24 hours of detection of an incident; Appointment of a security officer (CISO / Security Manager); Requirements for training, monitoring and management of suppliers; Regular compliance audits.

The introduction of NIS2 obliges operators of renewable energy systems to build a formal cyber resilience program, including policies, KPIs and reporting to national CERT/CSIRT structures.

In parallel with NIS2, the Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for connected devices and software. It affects manufacturers of inverters, controllers and edge gateways, who must now: maintain an SBOM and a vulnerability management process; provide updates throughout the product lifecycle; implement a secure development lifecycle (SDL); ensure compliance through CE marking with a cyber component.

ENISA (European Union Agency for Cybersecurity) provides operational guidelines, such as: ENISA Threat Landscape for Energy Sector; Good Practices for Security of Smart Grids; Guidelines for Cybersecurity Certification of Energy Devices.

These serve as practical tools for implementing policies based on NIS2 and CRA.

In North America, the NERC CIP (Critical Infrastructure Protection) standards define detailed technical requirements for the energy sector, which are also used as a reference in Europe. These include: access control to critical systems (CIP-004, CIP-007); communication protection and incident management; disaster recovery policies (CIP-009).

Although the NERC CIP is geared towards large transmission grid operators, its principles can be adapted for distributed DER infrastructures.

According to IEC 62443-2-4 and NIS2, security must be ensured not only internally, but also throughout the supply chain. Key measures include: certification of suppliers according to Security Level (SL);

doi: www.doi.org/10.70456/.....

requirement for documented security development and testing processes; inclusion of cybersecurity clauses in contracts with subcontractors; regular testing by red-team and penetration testing exercises and attack simulations to check staff readiness.

These policies ensure operational resilience (cyber-resilience) even in the event of a temporary loss of control or in a controlled environment.

Table 1. Relationship between security methods and typical attacks in DER systems

Method	DoS/DDoS	MITM/Spoofing	Unauthorized access	Ransomware/ Malware
Segmentation/DMZ	High (limits spread)	Medium	Medium	High (localizes incident)
Zero Trust + mTLS	Medium	High (encryption/ authentication)	High	Medium
IEC 62351/OPC UA Security	Medium	High	High	Medium
IDS/IPS (ICS protocols)	Medium	High (pattern/state)	High	Medium
Anomaly detection (ML)	High (behavioral)	High	Medium	Medium
SIEM/SOAR	Medium	Medium	High (correlation/ response)	High (reaction)
Secure boot/signature	Low	Low	Medium	High (anti-persistence)

Ratings:
High – the method effectively prevents or localizes the attack;
Medium – the method partially limits the effect or assists in detection;
Low – the method has minimal direct contribution (but may contribute indirectly in combination with others).

Organizations can assess their cybersecurity maturity using models such as: IEC 62443 Maturity Model (CSM2); NIST Cybersecurity Framework (Identify–Protect–Detect–Respond–Recover); Cybersecurity Capability Maturity Model (C2M2).

Typical maturity levels range from "ad hoc" practices (Level 1) to fully integrated and teamed processes (Level 5). Regular audits and resilience assessments ensure that the system does not simply comply with the requirements, but dynamically adapts to new threats.

As part of the management framework, the following are developed: Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP); Playbooks for specific types of incidents – ransomware, DoS, compromised gateway; Tabletop communication with part of the DER network.

Management KPI metrics for compliance are: % systems certified according to IEC 62443; Mean Time to Incident Response (MTTR) compared to the regulatory limit; Percentage of suppliers with a contractual clause for cybersecurity; Number of successfully conducted tabletop tests/year; Maturity Level Score according to the C2M2 or IEC 62443 model.

METHODS, ATTACKS MATRIX (OVERVIEW)

Table 1 presents a comparison between the main security methods and their effectiveness against typical attack classes observed in RES and DER infrastructures. The purpose of the matrix is to show that there is no universal solution, and a combined approach including architecture,

doi: www.doi.org/10.70456/.....

cryptography, detection, response and management is mandatory to achieve resilience.

Multi-layered protection (Defense-in-Depth). No method provides complete protection on its own. The most effective combinations are: (Segmentation + Zero Trust + IDS/IPS) – for prevention of MITM and DoS attacks; (IEC 62351 + Secure Boot + SBOM) – for protection of the chain of trust; (ML Detection + SOAR Response) – for dynamic response to new types of threats.

Technical level of effectiveness. The strongest contribution to technical protection is made by TLS/mTLS, IEC 62351, OPC UA Security and Secure Boot. IDS/IPS and ML-analyses are operational tools for early detection.

Organizational level. SIEM, SOAR and DRP belong to the management layers, ensuring response, coordination and resilience. They should be linked to KPIs and procedures from the IEC 62443 and NIS2 frameworks.

Adaptive (AI) level. ML and RL (reinforcement learning) models are starting to be used for automated adaptation of access policies and incident response. These systems can "self-train" SOAR processes, analyzing the behavior of DER devices and predicting threats.

A recommended strategy for DER operators is: Short-term: implement segmentation, OPC UA security and IDS/IPS. Medium-term: integrate SIEM/SOAR with ML anomaly models. Long-term: implement RL-based adaptive controllers for cyber resilience and dynamic risk management.

KPI FOR CYBER RESILIENCE OF DER NETWORKS

The assessment of cyber resilience of distributed energy resources (DER) is based on a set of key performance indicators (KPIs) that allow for quantitative measurement and comparison of the level of protection. The main operational KPIs include: MTTD/MTTR, mean time to detect and recover from an incident; Detection Rate and False Positive Rate, effectiveness of IDS/ML systems; Crypto Coverage and Patch Compliance, coverage of encrypted flows and updates; Backup/Restore Success Rate, reliability of recovery procedures. At the adaptive level, AI-based indices such as Mean Time to Adapt (MTTA) and Cyber Resilience Index (CRI) are used, which assess the system's ability to adapt to new threats. Combining these indicators supports continuous improvement and creates a basis for dynamic risk management in DER networks.

CONCLUSION

Grid security in renewable energy requires an integrated, multi-layered approach that combines architectural zoning, cryptographic protection, anomaly detection, and effective device lifecycle management.

The review shows that the joint implementation of standards such as IEC 62443, IEC 62351, and NIS2 is key to building a resilient infrastructure.

AI and ML methods are already emerging as an important tool for predictive protection and adaptive response to new threats.

In the future, cybersecurity of DER systems will evolve through intelligent automation, digital twins, and quantum-resistant cryptography, aimed at achieving full cyber resilience in the energy sector.

Funding: The authors gratefully acknowledge the support provided by the project: BG05SFRP001-3.004-0025-C01 DOCTORAL SCOOLS FOR SCIENCE, INNOVATION AND GREEN ENERGY IN ICT "DUNIZVICT".

Acknowledgments: The authors gratefully acknowledge the support provided by the project: BG05SFRP001-3.004-0025-C01 DOCTORAL SCOOLS FOR SCIENCE,

doi: www.doi.org/10.70456/.....

INNOVATION AND GREEN ENERGY IN ICT "DUNIZVICT".

REFERENCE

[1] IEC 62443 Series, Industrial Communication Networks – IT Security for Networks and Systems, International Electrotechnical Commission (IEC), Geneva, 2018–2023.
[2] IEC 62351 Series, Power Systems Management and Associated Information Exchange – Data and Communications Security, IEC, 2019–2024.
[3] NIST SP 800-82 Rev.2, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, Gaithersburg, MD, 2015.
[4] ENISA, Threat Landscape for the Energy Sector, European Union Agency for Cybersecurity, latest edition, 2023.
[5] European Union, Directive (EU) 2022/2555 (NIS2 Directive) – On Measures for a High Common Level of Cybersecurity across the Union, Official Journal of the European Union, 2023.
[6] European Commission, Cyber Resilience Act (CRA) – Regulation on Cybersecurity Requirements for Products with Digital Elements, Brussels, 2024.
[7] IEEE Std 2030.5-2021, Smart Energy Profile Application Protocol, IEEE Standards Association, 2021.
[8] OPC Foundation, OPC UA Security Architecture, Version 1.05, OPC Specification, 2023.

doi: www.doi.org/10.70456/.....