RESEARCH ARTICLE

# A Structured Framework for Cybersecurity Assessment of Microgrids and Nanogrids

**Plamen Stanchev**[1], **Nikolay Hinov**[2,*], **Atakan Salimov**[3], **Bulbul Ziulqmova**[2] and **Adnan Redjeb**[3]

[1] Department of Intelligent Technology in Industry, Faculty of Computer Systems and Technologies, Technical University of Sofia, 1000 Sofia, Bulgaria
[2] Department of Computer Systems, Faculty of Computer Systems and Technologies, Technical University of Sofia, 1000 Sofia, Bulgaria
[3] Department of Cybersecurity, Faculty of Computer Systems and Technologies, Technical University of Sofia, 1000 Sofia, Bulgaria

## Abstract

**Microgrids and nanogrids are increasingly deployed to support decentralized generation, local resilience, and renewable integration. However, their growing reliance on digital control, communication networks, cloud services, and IT–OT integration exposes them to diverse cybersecurity threats. Unlike traditional utility-scale systems, microgrids and nanogrids often operate under resource constraints, heterogeneous architectures, and limited cybersecurity expertise, making direct application of large-scale security frameworks impractical. This paper proposes a structured cybersecurity assessment framework for small- and medium-scale energy systems, supporting systematic risk identification, evaluation, and prioritization. The framework combines architectural inventory, trust-boundary analysis, threat modeling, and maturity-based assessment across six domains: governance and risk management, identity and access management, network and communication security, control-system and device security, monitoring and incident response, and physical security. Emphasis is placed on proportionality, repeatability, and actionability, enabling application across diverse operational contexts without excessive burden. An illustrative application to a campus microgrid and building nanogrid demonstrates how the framework assesses cybersecurity posture, identifies critical vulnerabilities, and defines staged mitigation roadmaps. Results indicate that a structured, context-aware assessment approach significantly improves cybersecurity awareness, investment prioritization, and resilience-oriented decision-making in decentralized energy environments. The framework offers a practical foundation for operators, designers, and policymakers seeking to enhance micro- and nanogrid security and resilience.**

**Keywords**: cybersecurity, microgrids, nanogrids, IT/OT security, threat modeling, maturity assessment, smart inverters, resilience.

**Submitted:** 12 March 2026
**Accepted:** 24 March 2026
**Published:** 08 April 2026

**Vol.** 2, **No.** 2, 2026.
10.62762/TEPNS.2026.258528

***Corresponding author:**
✉ Nikolay Hinov
hinov@tu-sofia.bg

**Citation**
Stanchev, P., Hinov, N., Salimov, A., Ziulqmova, B., & Redjeb, A. (2026). A Structured Framework for Cybersecurity Assessment of Microgrids and Nanogrids. *ICCK Transactions on Electric Power Networks and Systems*, 2(2), 58–71.

© 2026 ICCK (Institute of Central Computation and Knowledge)

## 1 Introduction

Microgrids and nanogrids are increasingly deployed as core building blocks of decentralized energy systems, enabling local integration of renewable generation, energy storage, and flexible demand [1–3]. Their value proposition is strongly associated with resilience, efficiency, and local energy autonomy. These systems can maintain critical services during disturbances in the main grid, reduce peak demand, improve power quality, and support a more sustainable and distributed energy transition.

At the same time, the operational benefits of microgrids and nanogrids depend on extensive digitalization. Energy management systems (EMS), supervisory control and data acquisition (SCADA) platforms, smart inverters, distributed controllers, sensors, gateways, cloud services, and remote maintenance interfaces form a tightly interconnected IT–OT ecosystem [4, 5]. As decision-making becomes more automated and network-mediated, the cyber-attack surface expands considerably. In such cyber-physical environments, security incidents may no longer remain confined to data confidentiality or service availability in the IT domain; instead, they may propagate into physical processes and affect voltage regulation, frequency stability, islanding capability, protection coordination, and continuity of supply [2, 3].

The cybersecurity challenge in microgrids and nanogrids is not only technical, but also organizational and economic. Compared to traditional utility-scale power systems, these decentralized infrastructures are commonly characterized by heterogeneous vendor ecosystems, evolving architectures, constrained budgets, and limited availability of specialized cybersecurity personnel. Many installations combine legacy industrial protocols with modern IP-based networking and cloud-connected services. In addition, remote vendor support and third-party maintenance channels are often essential for operation, but they also create high-risk entry points. Physical protection can also be weaker than in regulated utility environments, especially in building-scale nanogrids or distributed field installations.

As a result, the direct application of comprehensive cybersecurity frameworks originally developed for enterprise IT or large utility infrastructures often becomes impractical. Such frameworks may be too complex, too costly, or insufficiently tailored to the operational realities of small- and medium-scale distributed energy systems. Nevertheless, the absence of a structured assessment approach leads to fragmented security decisions, inconsistent documentation, limited visibility of critical weaknesses, and poor prioritization of mitigation measures. Existing research on cybersecurity in smart grids and distributed energy resources has provided valuable insights into attack surfaces, inverter vulnerabilities, communication security, and anomaly detection. However, much of this work either addresses utility-scale systems, focuses on isolated technical layers, or assumes organizational capacities that many micro- and nanogrid operators do not possess. In practice, there is a clear need for a framework that is sufficiently structured to be repeatable and auditable, yet lightweight enough to remain feasible under resource constraints. Such a framework should also support actionability by translating assessment findings into prioritized and realistic improvement plans.

This paper proposes a structured framework for cybersecurity assessment of microgrids and nanogrids, designed to bridge IT–OT security considerations with the operational constraints of decentralized energy systems. The framework integrates three complementary components:

- architectural inventory and interface analysis to identify critical assets, dependencies, and trust boundaries;
- threat modeling tailored to common deployment patterns, remote access pathways, and third-party dependencies; and
- a maturity-based assessment across six key cybersecurity domains.

The proposed approach is designed around three central qualities: proportionality, repeatability, and impact orientation. It enables operators to assess their current cybersecurity posture, determine feasible target levels, and plan staged improvements without requiring immediate full compliance with heavyweight standards.

The study is guided by the following research questions:

- RQ1: What cybersecurity assessment dimensions are most critical for microgrids and nanogrids given their specific IT–OT integration and operational constraints?
- RQ2: How can cybersecurity assessment be structured to remain proportional, repeatable,

and actionable for small- and medium-scale energy systems?

- RQ3: How can a structured assessment framework support prioritization of mitigation actions and staged improvement planning in representative micro- and nanogrid scenarios?

The main contributions of this paper are as follows:

- C1: A domain-specific structured cybersecurity assessment framework tailored to microgrids and nanogrids;
- C2: A maturity-based model designed to support proportional and staged cybersecurity improvement;
- C3: An illustrative application demonstrating how the framework can identify critical weaknesses and prioritize mitigation measures in decentralized energy environments.

In addition to these contributions, the proposed framework explicitly links cybersecurity maturity evaluation with cyber-physical operational impact, enabling security assessments to be directly interpreted in terms of energy system resilience and operational stability.

The remainder of the paper is organized as follows. Section 2 summarizes the background and threat landscape of microgrids and nanogrids. Section 3 discusses the limitations of existing cybersecurity frameworks when applied to decentralized small-scale energy systems. Section 4 presents the proposed assessment framework, including its design principles, domains, and maturity model. Section 5 demonstrates an illustrative application scenario and resulting prioritization logic. Section 6 discusses the findings, limitations, and future research directions. Section 7 concludes the paper.

A related domain-based maturity assessment approach was previously proposed by the authors for evaluating the level of digitalization in electrical networks [18]. That model focused on assessing digital transformation readiness across multiple domains, without explicitly addressing cybersecurity risks or threat scenarios.

## 2 Threat model and attack surface (IT/OT)

### 2.1 IT/OT Convergence and Trust Boundaries

Microgrids and nanogrids increasingly rely on tightly coupled operational technology and information technology components to support monitoring, optimization, and automated control. Typical OT elements include protection relays, programmable logic controllers, inverter controllers, battery management interfaces, and field sensors/actuators. Typical IT elements include SCADA/EMS servers, operator workstations, identity and access management, cloud analytics, and remote maintenance systems. This convergence introduces several trust boundaries between field devices, local control networks, enterprise systems, and third-party services. A practical implication is that these infrastructures inherit vulnerabilities from both IT and OT domains. Traditional IT weaknesses such as credential compromise, insecure remote access, and supply-chain exposure coexist with OT-specific weaknesses such as legacy protocols, weak field-layer

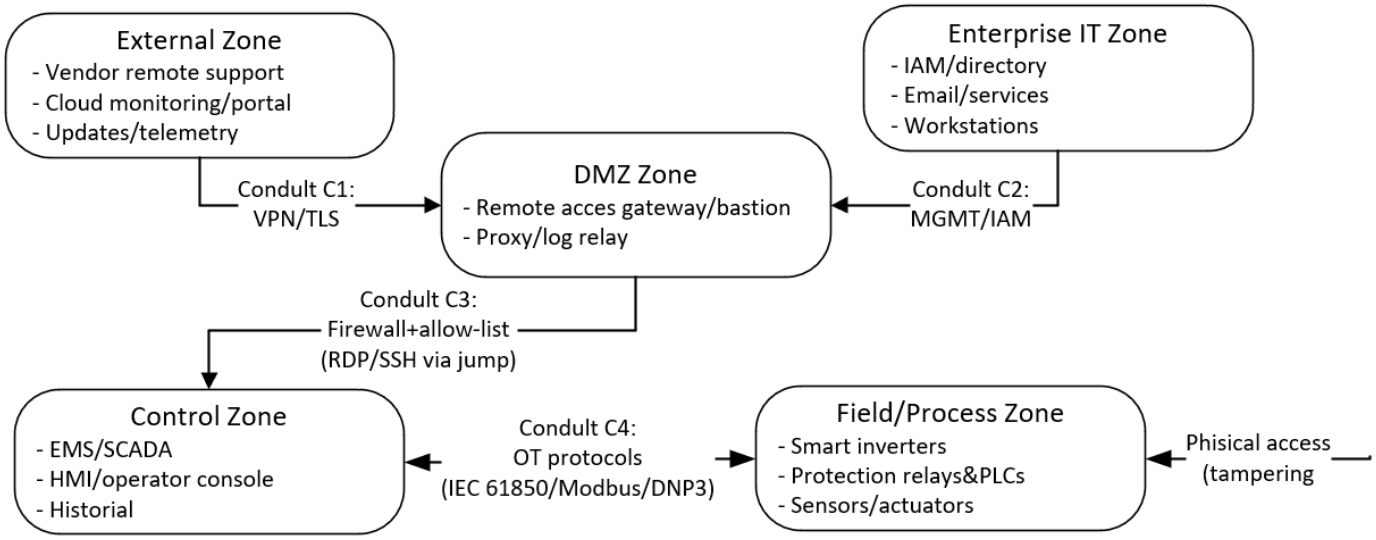


**Figure 1.** ISA/IEC 62443-inspired zoning and conduits map for a representative microgrid deployment.

**Table 1.** Mapping of cybersecurity threat surfaces to representative attack techniques, operational impacts, and assessment focus in microgrids and nanogrids.

| Threat surface | Representative attack techniques | Potential operational impact | Assessment focus |
|---|---|---|---|
| Remote access and third-party connectivity | Credential theft, weak authentication, VPN misconfiguration, supply-chain compromise | Unauthorized control access, lateral movement from IT to OT, loss of operational integrity | Access control policies, identity management, third-party access governance |
| Communication networks and protocols | Spoofing, man-in-the-middle attacks, replay attacks, protocol abuse | Manipulated measurements, delayed or incorrect control signals, degraded stability | Protocol security, encryption, segmentation, latency-aware protection |
| Control systems and embedded devices | Firmware manipulation, unsafe configuration changes, logic modification | Incorrect inverter behavior, protection misoperation, cascading outages | Secure configuration, firmware integrity, control logic protection |
| Monitoring and detection mechanisms | Log evasion, alert suppression, insufficient visibility | Increased dwell time, delayed incident response, undetected compromise | Logging coverage, OT-aware monitoring, anomaly detection |
| Physical and environmental access | Physical tampering, rogue device insertion, local network access | Bypass of cyber controls, direct manipulation of devices | Physical security controls, asset protection, environmental monitoring |
| IT–OT integration points | Privilege escalation, trust boundary violations, insecure gateways | Propagation of IT incidents into OT domain, loss of safety margins | Network zoning, trust boundary enforcement, interface hardening |

authentication, and safety-critical dependence on deterministic communications [1]. Figure 1 provides an ISA/IEC 62443-inspired zoning and conduits view that makes these trust boundaries explicit.

### 2.2 Threat Modeling for Cyber-Physical Energy Systems

A meaningful threat model for microgrids and nanogrids must identify assets, critical functions, trust boundaries, threat actors, entry points, and operational impacts. Unlike traditional information systems, cyber risk in these environments must be evaluated together with physical consequences, including instability, unsafe switching, inverter misbehavior, or loss of islanding capability.

### 2.3 Attack Surfaces and Threat Paths

Threat modeling should connect attacker techniques to operational impact, prioritizing high-frequency entry points such as remote access, protocol manipulation, device configuration changes, monitoring gaps and physical exposure. Knowledge bases such as MITRE ATT&CK for ICS support a common vocabulary for these techniques and enable consistent mapping to mitigations and detection strategies [2].

Table 1 summarizes representative threat surfaces in microgrids and nanogrids and the associated assessment focus. The mapping is intentionally implementation-agnostic and is used in Section 4 to select illustrative threat paths and derive improvement priorities.

### 2.4 Adversary Techniques and Attack Patterns on ICS

To better structure the threat modeling process, adversary behavior in cyber-physical energy infrastructures can be analyzed using structured knowledge bases, such as the MITRE ATT&CK framework for industrial control systems. This framework provides a taxonomy of attacker tactics and techniques observed in real-world industrial cyber incidents.

Several common attack patterns can be identified in micro- and nano-grid environments. These include compromising remote maintenance interfaces, exploiting insecure industrial communication protocols, manipulating inverter control parameters, and disrupting monitoring and logging systems. Once an attacker gains access to the IT layer, lateral movement in operational networks can allow manipulation of critical energy control functions.

Typical adversarial tactics associated with distributed energy systems include, initial access via remote support channels or compromised credentials, lateral movement through segmented networks, escalation of privileges in management platforms, modification

of device configuration or control logic, impact on operations affecting energy production or grid stability.

The mapping of such attack techniques to operational consequences allows the cybersecurity assessment to focus not only on technical vulnerabilities, but also on the potential impact on system resilience and operational continuity.

### 2.5 Cyber-physical consequences of cyberattacks

A distinctive feature of micro- and nano-grids is the strong connection between digital control and physical energy processes. Consequently, cyber incidents can quickly spread into operational consequences. Examples of cyber-physical impacts include, instability caused by manipulated inverter control signals, improper protection coordination resulting from configuration changes, disruption of load balancing algorithms, forced shutdown of distributed generation assets, failure of islanding transitions during grid disturbances [6–8].

Such events can lead to degradation of system reliability, interruption of critical services, or equipment failure. Therefore, the assessment of cybersecurity in distributed energy infrastructures must explicitly consider the relationship between cyber compromise and the physical behavior of the system.

## 3 Limitations of Existing Cybersecurity Frameworks

Although numerous cybersecurity frameworks and standards have been developed for enterprise information systems and industrial control systems, their direct application to microgrid and nanogrid environments remains challenging [4, 9].

First, many cybersecurity frameworks are designed primarily for enterprise IT environments where confidentiality and data protection are the dominant security objectives. In contrast, operational technology environments prioritize availability, safety, and deterministic system behaviour. Security controls that introduce latency or operational complexity may therefore negatively affect system performance.

Second, frameworks designed for utility-scale power systems often assume standardized architectures, regulated infrastructures, and dedicated cybersecurity teams. Microgrid and nanogrid deployments frequently operate under significantly different conditions. These infrastructures are often owned by municipalities, campuses, small enterprises, or community energy operators who may lack the resources required to implement comprehensive compliance-oriented security programs.

Third, many cybersecurity guidelines focus on extensive catalogues of controls but provide limited support for prioritizing security improvements when resources are constrained. In practice, incremental improvements targeting the most critical attack surfaces often provide the highest benefit for decentralized energy systems.

Finally, existing assessment approaches frequently treat IT and OT security domains separately. However, in microgrid environments the interaction between these domains represents one of the most critical risk factors. Remote access gateways, energy management systems, and cloud monitoring platforms act as integration points through which cyber incidents may propagate from IT systems into operational energy control functions.

These limitations highlight the need for a cybersecurity assessment methodology specifically tailored to the operational and organizational characteristics of decentralized energy systems.

## 4 Proposed cybersecurity assessment framework

Building on the threat landscape and framework limitations discussed in the previous sections, this study introduces a structured cybersecurity assessment methodology tailored to distributed energy infrastructures. The methodology integrates risk evaluation, maturity assessment, and operational context analysis in order to support proportional and actionable cybersecurity improvement in microgrid and nanogrid deployments.

### 4.1 Overview and Outputs

The framework targets repeatable self-assessment and proportional improvement planning. It produces: (O1) a trust-boundary and interface inventory; (O2) a domain maturity profile; (O3) a prioritized list of mitigations mapped to plausible threat paths; and (O4) a staged roadmap aligned with operational constraints. Figure 2 summarizes the workflow and expected outputs.

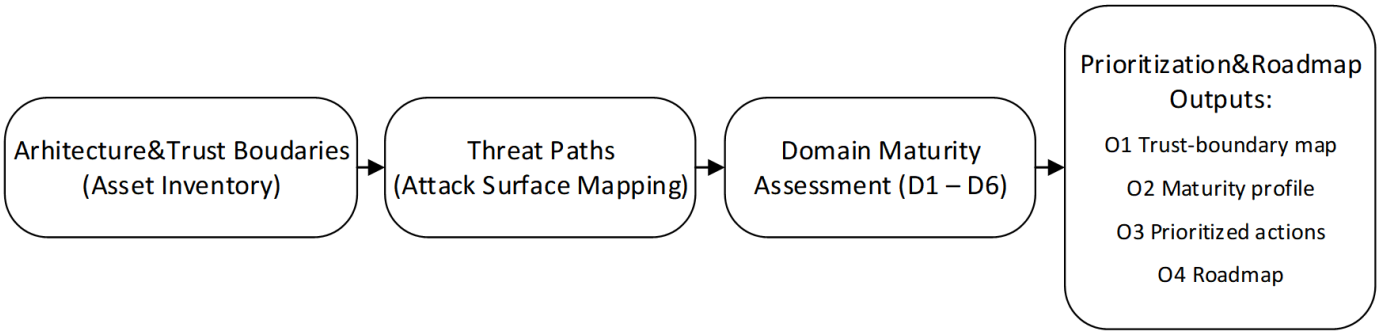


**Figure 2.** Framework workflow and key outputs for cybersecurity assessment of microgrids and nanogrids.

### 4.2 Assessment Domains

Assessment is performed across six domains: D1 governance and roles; D2 identity, privileged access and third-party connectivity; D3 network segmentation and communications security; D4 control systems and device security (firmware, configuration baselines, parameter change protection); D5 monitoring, logging and incident response readiness; and D6 physical security and environmental protection.

### 4.3 Maturity Model and Procedure

Domain maturity is scored on five levels: L1 Ad hoc (reactive, undocumented); L2 Basic (partial controls, inconsistent); L3 Defined (documented and consistently applied); L4 Managed (measured, reviewed and verified); L5 Optimized (continuous improvement with automation where feasible).

Assessment proceeds in six steps: (1) define scope and critical functions; (2) document architecture, trust boundaries and interfaces; (3) select representative threat paths using Table 1; (4) gather evidence and score domains on L1–L5; (5) prioritizes mitigation actions based on impact and feasibility; and (6) define a staged roadmap and reassessment cadence. Weighting by criticality is optional but recommended for complex deployments.

In practice, maturity levels are assigned based on evidence collected during the assessment process. Typical evidence includes system configurations (e.g., access control settings, network segmentation rules), documented policies and procedures, authentication mechanisms, firmware and configuration baselines, and available monitoring and logging data. Each domain is evaluated against qualitative indicators that reflect the consistency, completeness, and operational enforcement of cybersecurity controls.

The overall maturity index is calculated as the average value across all assessed domains, optionally weighted according to system criticality. In addition, the minimum domain score is reported to capture critical weaknesses, reflecting the "weakest-link" effect typical for cyber-physical systems.

Modern microgrids are typically organised using a hierarchical control architecture consisting of three main layers: primary, secondary, and tertiary control [17]. The primary control layer operates at the inverter level and is responsible for fast local control functions such as voltage and frequency regulation, typically implemented through droop control mechanisms.

The secondary control layer ensures coordinated operation by restoring system frequency and voltage deviations and enabling proper power sharing among distributed energy resources.

The tertiary control layer performs higher-level energy management functions, including economic dispatch, optimisation, and interaction with the main grid.

From a cybersecurity perspective, each control layer introduces distinct vulnerabilities and potential impact pathways. Compromise at the primary level may directly affect inverter stability and local control dynamics, while attacks targeting the secondary layer may disrupt power sharing and system coordination. At the tertiary level, cyber incidents may lead to incorrect optimisation decisions, economic inefficiencies, or unsafe scheduling of energy resources.

This layered perspective supports a more structured mapping between cybersecurity assessment results and operational consequences in microgrid environments.

## 5 Cyber-Physical Risk Assessment Methodology

Cybersecurity evaluation in distributed energy systems requires an integrated approach that considers both digital vulnerabilities and physical operational consequences. Traditional risk assessment methods developed for information systems often rely on qualitative scoring models that do not fully capture the dynamic interactions present in cyber-physical infrastructures such as microgrids.

To address this limitation, the proposed framework introduces a cyber-physical risk evaluation perspective in which cybersecurity threats are assessed based on three interacting components:

- Attack likelihood – probability that a given vulnerability can be exploited.
- Exposure level – accessibility of the targeted system component.
- Operational impact – severity of consequences for energy system operation.

The overall cyber-physical risk is calculated according to Equation (1):

$$R = P_{\text{attack}} \cdot E_{\text{exposure}} \cdot I_{\text{impact}} \tag{1}$$

where $P_{\text{attack}}$ represents the probability of successful exploitation, $E_{\text{exposure}}$ represents the accessibility of the system interface, and $I_{\text{impact}}$ represents the operational consequence of the compromise.

Similar risk formulations are widely used in cybersecurity risk management and industrial control security assessment [4, 9].

For distributed energy infrastructures, operational impact should be evaluated using system-specific indicators, such as voltage stability degradation, inverter control manipulation, protection coordination failure, islanding capability loss, disruption of energy supply to critical loads.

By combining these factors, the risk model allows cybersecurity findings to be interpreted directly in terms of operational resilience.

## 6 Cybersecurity Maturity Evaluation Metrics

While the maturity model presented in Section 4.3 provides qualitative evaluation levels, a more detailed analysis can be achieved by introducing domain-level scoring metrics.

Each cybersecurity domain $D_i$ can be assigned a maturity score ranging from 1 to 5 corresponding to the maturity levels defined previously. The overall cybersecurity maturity index of the microgrid system can be computed as:

$$CMI = \frac{1}{N} \sum_{i=1}^{N} M_i \tag{2}$$

where $M_i$ represents the maturity score of domain $i$, and $N$ represents the number of evaluated cybersecurity domains.

For the six domains used in this study:

$$CMI = \frac{M_{D1} + M_{D2} + M_{D3} + M_{D4} + M_{D5} + M_{D6}}{6} \tag{3}$$

However, because cyber-physical infrastructures often exhibit weakest-link behaviour, the minimum maturity value may provide a more conservative indicator of system resilience:

$$CMI_{\text{critical}} = \min(M_{D1}, M_{D2}, \ldots, M_{D6}) \tag{4}$$

This approach highlights the domain that requires the most urgent improvement.

Although a wide range of cybersecurity standards and frameworks exist for IT systems, industrial control systems, and critical infrastructure, their direct applicability to microgrids and nanogrids remains limited. The proposed framework contributes beyond existing approaches through several distinguishing elements.

First, the framework introduces an explicit integration of IT–OT trust-boundary modeling into the assessment process. Unlike traditional approaches that treat segmentation conceptually, the proposed method operationalises trust boundaries, gateways, and remote-access interfaces as central elements of risk assessment and attack-path analysis.

Second, the framework combines threat-path reasoning with maturity-based assessment. While existing methodologies often separate threat modeling from control evaluation, the proposed approach links realistic attack scenarios to domain-specific maturity levels, enabling prioritisation based on both likelihood and operational impact.

Third, the framework is designed with proportionality as a core principle. Existing standards are typically oriented toward large-scale or highly regulated environments, whereas the proposed method supports incremental adoption in resource-constrained micro- and nanogrid deployments.

Fourth, the framework explicitly connects cybersecurity findings to energy-system operational consequences. This includes impacts on stability, islanding capability, protection coordination, and service continuity, thereby bridging the gap between cybersecurity assessment and system resilience.

Finally, the framework provides a lightweight and repeatable assessment workflow that is applicable to heterogeneous and evolving distributed energy environments, including those with mixed vendor ecosystems and limited standardisation.

These elements collectively differentiate the proposed framework from existing methodologies and position it as a practical tool for cybersecurity assessment in decentralized energy systems.

## 7 Cybersecurity Integration with Microgrid Control Architecture

Microgrid cybersecurity cannot be evaluated independently of the control architecture used to operate the energy system. Modern microgrids typically rely on hierarchical control architectures consisting of three layers:

- Primary control layer – inverter-level voltage and frequency regulation.
- Secondary control layer – power sharing and voltage restoration.
- Tertiary control layer – energy management and economic optimization.

Cybersecurity threats affecting these layers may have different operational consequences [1, 10].

Attacks targeting the tertiary control layer may manipulate optimization algorithms or scheduling decisions. Such attacks may lead to inefficient energy dispatch or financial losses.

Attacks targeting the secondary control layer may affect power balancing mechanisms and voltage restoration algorithms. These events may reduce system stability [11].

Attacks targeting the primary control layer represent the most critical scenario because they directly influence inverter behaviour and power electronic control loops.

Therefore, cybersecurity assessment must consider the relationship between cyber vulnerabilities and control architecture layers.

In microgrids and nanogrids, cybersecurity incidents can directly affect physical system behaviour due to the tight coupling between control, communication, and power electronic devices. Identified vulnerabilities in access control, communication channels, or device configuration may translate into concrete operational impacts.

For instance, unauthorized modification of inverter control parameters (e.g., voltage–reactive power (Q–V) or frequency–active power (P–f) characteristics) may degrade voltage stability and reduce the ability of the system to provide grid-support functions. Similarly, manipulation of EMS control signals or measurement data may lead to incorrect dispatch decisions, resulting in load-generation imbalance or inefficient energy management.

Weaknesses in protection coordination may also arise if relay settings or protection logic are altered, potentially causing delayed tripping, false trips, or loss of selectivity. In islanded operation, such effects can significantly compromise system stability and resilience.

In addition, communication-level attacks such as delay, replay, or data injection may introduce control instability or oscillatory behavior, particularly in systems with high penetration of inverter-based resources.

Standardized security extensions for power system communication protocols, such as those specified in IEC 62351-6 for IEC 61850-based networks, provide mechanisms for authentication, encryption, and access control that can mitigate these communication-level attack vectors [16].

These observations highlight that cybersecurity assessment should not only identify vulnerabilities but also evaluate their potential impact on key operational functions, including inverter control, protection coordination, voltage regulation, and system resilience.

## 8 Resilience-Oriented Cybersecurity Strategy

Cybersecurity strategies for microgrids should not focus exclusively on preventing attacks but also on

ensuring resilient system operation during cyber incidents [12].

Resilience-oriented cybersecurity strategies typically include the following mechanisms:

- **Segmentation of IT and OT Networks**

  Strict separation between enterprise networks and operational control networks significantly reduces the likelihood of lateral movement during cyber intrusions [13].

- **Secure Remote Access Management**

  Remote access channels represent one of the most common entry points for attackers. Implementing multi-factor authentication and time-limited vendor access sessions can significantly reduce the attack surface [14].

- **Secure Configuration Baselines**

  Maintaining verified configuration baselines for inverter settings, protection parameters, and EMS configurations allows operators to detect unauthorized modifications and quickly restore normal operation.

- **Continuous Monitoring and Anomaly Detection**

  Cyber-physical anomaly detection systems can identify abnormal control behaviour or unexpected power system responses that may indicate cyber compromise [15].

- **Incident Response and Recovery Planning**

  Prepared incident response procedures ensure that operators can quickly isolate compromised components and restore safe system operation.

## 9 Illustrative assessment examples

### 9.1 Representative Threat Path

To illustrate the method, we consider a representative threat path in which a remote-access channel (vendor VPN or cloud portal) is used to obtain privileged access, leading to unauthorized configuration changes on an inverter or DER controller [4, 11]. The operational outcome may include altered protection settings, loss of grid-support functions, unsafe switching, or forced disconnects during disturbances.

### 9.2 Domain Maturity Summary

Two illustrative assessments are used to demonstrate the output format: (A) a campus microgrid with mixed DER and a local EMS, and (B) a building-level nanogrid with a small inverter and a gateway managed by a third party. Table 2 summarizes the resulting domain maturity profiles (L1–L5 as defined in Section 4.3).

**Table 2.** Summary of illustrative maturity assessment results.

| Domain | Campus microgrid | Building nanogrid |
|---|---|---|
| D1 Governance | L2 | L1–L2 |
| D2 Identity/Access | L2 | L1–L2 |
| D3 Network/Comms | L3 | L2 |
| D4 Control/Devices | L2–L3 | L2 |
| D5 Monitoring/IR | L2 | L1–L2 |
| D6 Physical | L3 | L2 |

Figure 3 visualises the maturity profiles from Table 2 using a radar representation. For ranges (e.g., L1–L2) an intermediate value (e.g., 1.5) is used for visualisation. Figures 4 and 5 provide simple correlation and gap-based views that support prioritisation.

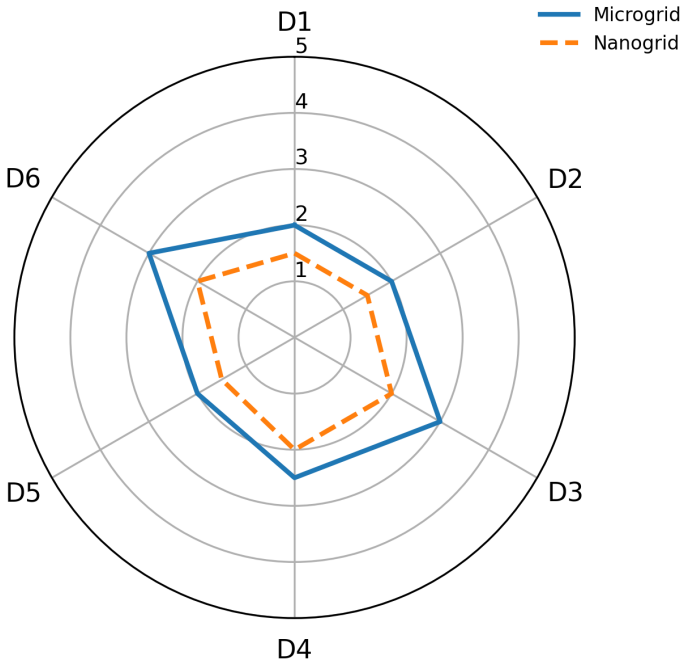


**Figure 3.** Radar plot of illustrative maturity profiles across assessment domains (D1–D6).

### 9.3 High-Leverage Gaps and Priorities

For the campus microgrid, the main priorities relate to privileged access governance for remote maintenance, segmentation between enterprise and control networks, and systematic logging of

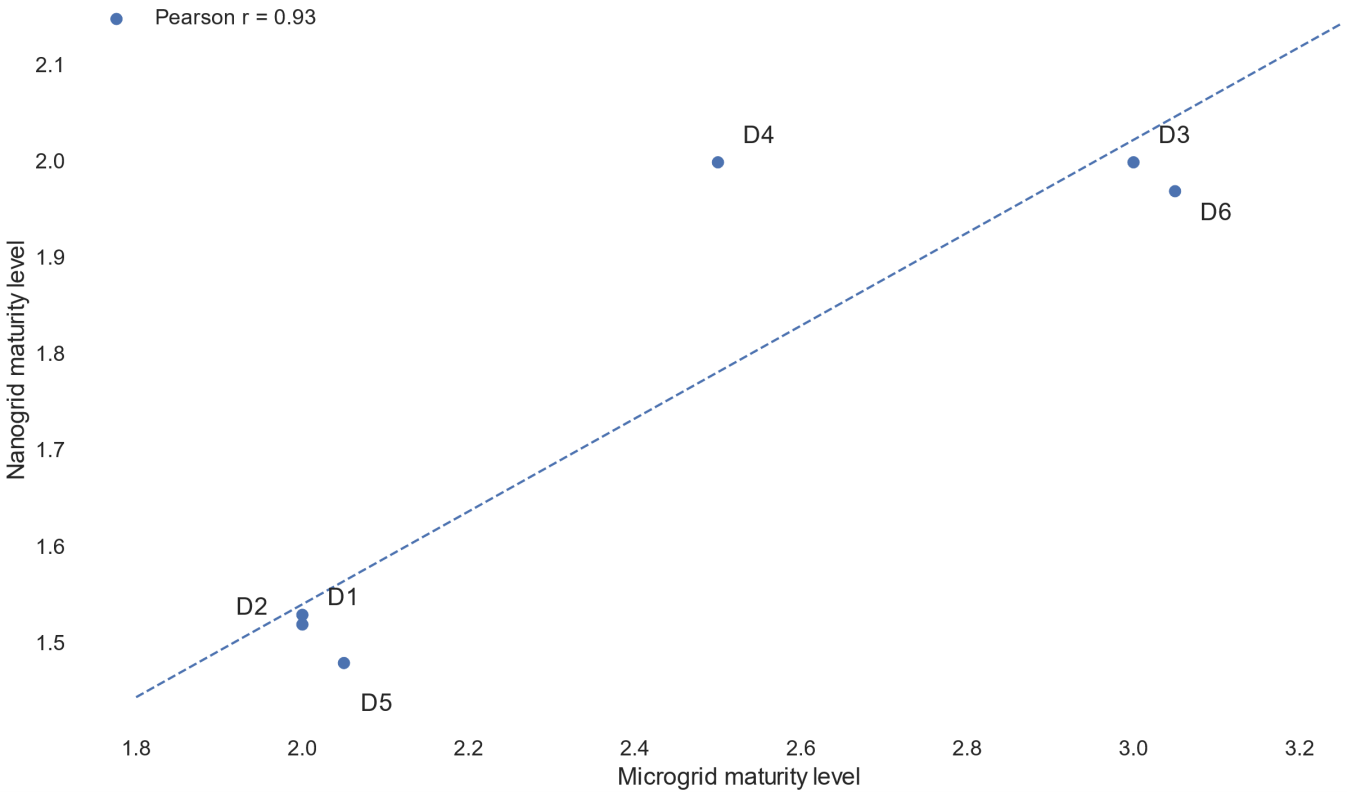


**Figure 4.** Correlation between cybersecurity maturity levels of microgrid and nanogrid domains.

configuration changes (D2–D5). These controls reduce the likelihood that an IT compromise or third-party account misuse propagates into inverter or protection settings.

For the building nanogrid, the weakest domains are governance and access control (D1–D2) and monitoring/incident readiness (D5), compounded by cloud-portal exposure, limited segmentation, and higher physical accessibility of assets.

Figure 4 presents the correlation between the cybersecurity maturity levels evaluated for the microgrid and nanogrid scenarios across the six assessment domains (D1–D6). Each point in the scatter plot corresponds to one cybersecurity domain defined in the proposed framework: governance (D1), identity and access management (D2), network and communication security (D3), control systems and device security (D4), monitoring and incident response (D5), and physical security (D6).

The horizontal axis represents the maturity level of the campus microgrid, while the vertical axis represents the maturity level of the building nanogrid. The dashed line illustrates the linear regression trend between the two maturity profiles.

Figure 4 provides an illustrative comparison of the maturity profiles of the two assessment scenarios across domains D1–D6. The reported Pearson correlation coefficient (r=0.93) is used only as a compact summary of similarity between the two illustrative profiles and should not be interpreted as a statistical generalisation beyond these examples. The main value of the comparison is to show that both scenarios exhibit relatively stronger performance in D3 and D6 and weaker performance in D1, D2, and D5.

Domains D3 (network and communication security) and D6 (physical security) show relatively higher maturity levels in the two illustrative scenarios, reflecting the presence of basic segmentation measures and physical access controls. In contrast, domains related to governance, identity and access management, and monitoring readiness (D1, D2, and D5) exhibit lower maturity, indicating limited formal security policies, insufficient access-control mechanisms, and incomplete monitoring capabilities. Domain D4 (control systems and device security) remains particularly important because it is directly related to inverter configuration, firmware integrity, and control logic; even moderate maturity gaps in this domain may lead to significant operational risks, including unstable control behaviour or misoperation of protection mechanisms.

The strong correlation observed in the figure highlights that cybersecurity challenges in distributed energy infrastructures are largely systemic rather than site-specific. Consequently, improvements targeting high-leverage domains such as access management, network segmentation, and monitoring infrastructure can significantly enhance the overall cybersecurity posture of both microgrid and nanogrid environments.

From a methodological perspective, the strong correlation also indicates that cybersecurity maturity improvements implemented in one deployment type may be transferable to similar distributed energy environments. This observation suggests that standardized assessment approaches and shared cybersecurity practices could significantly accelerate security improvements across multiple microgrid and nanogrid installations.

### 9.4 Condensed Improvement Roadmap

A staged roadmap can be derived directly from the weakest domains and the selected threat paths. Short term (0–3 months): eliminate default credentials, enforce MFA for remote access, restrict vendor access to time-bound sessions, and create verified configuration backups. Medium term (3–12 months): implement segmentation and allow-listing, centralize logs, and introduce configuration change approval and periodic review. Longer term (>12 months): integrate continuous monitoring and anomaly detection, exercise incident response, and embed cybersecurity requirements in supplier and maintenance contracts. Figure 5 highlights the largest maturity gaps to a minimum target Level 3.

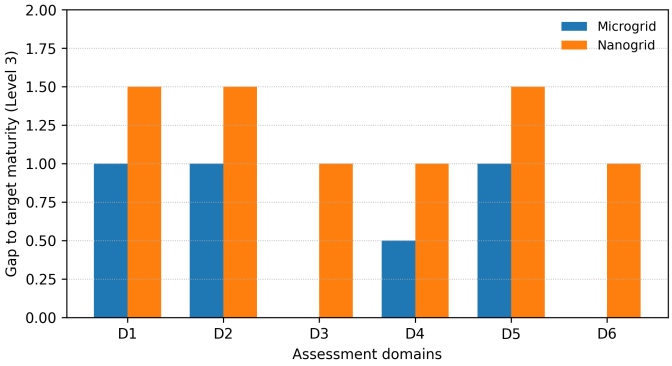


**Figure 5.** Maturity gaps to a minimum target Level 3 (Defined) for each domain (illustrative).

## 10 Discussion and limitations

The proposed framework is intended to bridge established industrial control security guidance and the practical realities of microgrid and nanogrid deployments. Rather than replacing existing standards and recommended practices, it provides a structured operational layer for their interpretation in decentralized energy environments. In this context, the framework emphasizes proportionality: operators can begin with a minimum viable control set and progressively improve cybersecurity maturity as system criticality, interconnection complexity, and available resources increase. The resulting domain profile also supports communication among asset owners, operators, IT/OT personnel, integrators, and vendors by providing a shared structure for requirements, evidence, and improvement priorities.

A key practical advantage of the framework is that it combines domain-based maturity assessment with representative threat modeling and operational context. This makes the output more actionable than a checklist-only review, because mitigation priorities can be linked not only to missing controls, but also to plausible attack paths and their potential operational consequences. In this way, cybersecurity investment can be aligned more closely with resilience objectives, which is particularly important in decentralized energy infrastructures where resources are often limited. The illustrative scenarios suggest that meaningful improvements may frequently be achieved through relatively focused measures, such as stronger privileged-access governance, improved segmentation, verified configuration baselines, and better logging and incident preparedness.

The framework is also designed to remain compatible with established cybersecurity standards and guidance, including NIST SP 800-82, IEC 62443, and the Cybersecurity Capability Maturity Model (C2M2). However, instead of reproducing these frameworks in full, it aims to support their practical interpretation in settings where operators may not have dedicated cybersecurity teams or the capacity to implement compliance-oriented control catalogues in a single step. This is particularly relevant in campus, municipal, community, commercial, and building-scale distributed energy environments, where mixed ownership structures and operational constraints often require staged and risk-informed improvement planning.

At the same time, the present study has important limitations. First, the maturity assessment remains partly qualitative and depends on the quality and completeness of the available evidence. In practical

application, scoring should therefore be supported by explicit artefacts such as policies, access-control settings, network configurations, firmware and parameter baselines, logging records, and test results. Where feasible, the assessment should also be complemented by technical validation activities, including configuration audits, penetration testing, recovery exercises, or targeted security testing. Second, the current paper demonstrates the framework through illustrative scenarios rather than through empirical validation across operational deployments. The presented examples are intended to show the structure of the method, the assessment workflow, and the form of the outputs in a controlled and reproducible manner, but they do not constitute field validation using operational data from real industrial sites.

Future work should therefore focus on applying the framework across multiple real-world microgrid and nanogrid deployments with different architectures, governance models, and operational constraints. Such studies would allow refinement of the domain indicators, better calibration of maturity scoring, and more robust comparison between scenario-based and field-based assessment outcomes. Additional research may also explore integration with automated monitoring tools, configuration scanning platforms, and evidence collection mechanisms, as well as stronger linkage between cybersecurity maturity assessment and explicit resilience or operational performance metrics. Another relevant direction is the interaction between cybersecurity controls and advanced control strategies, including AI-based energy management systems, where security weaknesses may have amplified operational consequences.

While the proposed framework shares a domain-based maturity structure with earlier work on digitalisation assessment, it differs fundamentally in its objective and analytical logic. The earlier model focused on technological adoption and integration readiness in electric power networks, whereas the present framework is specifically designed for cybersecurity assessment in microgrids and nanogrids. It extends beyond digitalisation assessment by incorporating threat modeling, IT–OT trust-boundary analysis, and explicit mapping between vulnerabilities and cyber-physical operational effects. In this sense, the framework should be understood not as a renaming of a previous maturity model, but as a security-oriented extension tailored to decentralized energy systems.

## 11 Conclusions

Microgrids and nanogrids increase the flexibility and resilience of modern energy systems, but their growing IT/OT integration also expands the cyber-attack surface and increases the possibility that cyber compromise may translate into operational disruption. In response to this challenge, this paper presented a lightweight and repeatable cybersecurity assessment framework that combines trust-boundary analysis and threat-path reasoning with a six-domain maturity model tailored to distributed energy environments. The framework produces a structured maturity profile together with a prioritised improvement roadmap and was demonstrated through illustrative campus microgrid and building nanogrid scenarios.

The proposed approach is intended as a practical tool for supporting consistent self-assessment, staged security improvement, procurement planning, and system integration in resource-constrained distributed energy deployments. By translating high-level cybersecurity principles into a domain-based and operationally interpretable assessment process, the framework can help operators identify high-leverage weaknesses and prioritise mitigation actions in a more systematic and resilience-oriented manner.

Future research should focus on empirical validation across diverse real-world deployment contexts, refinement of the maturity indicators using operational evidence, and integration with automated monitoring and configuration analysis tools. Such developments would further strengthen the scalability, robustness, and practical applicability of cybersecurity assessment for microgrid and nanogrid systems.

## Data Availability Statement

Data will be made available on request.

## Funding

This work was supported by the Bulgarian National Scientific Fund under Grant KP-06-M87/2/06.12.2024 for the project “Optimization of energy consumption in small and medium enterprises based on micro and nano grids”.

## Conflicts of Interest

The authors declare no conflicts of interest.

## AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

## Ethical Approval and Consent to Participate

Not applicable.

## References


[1] Stouffer, K. A., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V. Y., Lightman, S., ... & Thompson, M. (2023). Guide to Operational Technology (OT) Security. [CrossRef]

[2] MITRE. (2026). ATT&CK® for ICS: Techniques. Retrieved from https://attack.mitre.org/techniques/ics/ (accessed: Jan. 2026).

[3] ISA Global Cybersecurity Alliance (ISAGCA). (2020). Quick Start Guide: An Overview of ISA/IEC 62443 Standards—Security of Industrial Automation and Control Systems.

[4] Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST cybersecurity framework (CSF) 2.0. [CrossRef]

[5] Pillitteri, V., & Brewer, T. (2014). Guidelines for smart grid cybersecurity (NIST Interagency/Internal Report (NISTIR)). National Institute of Standards and Technology, Gaithersburg, MD. In *Guidelines for smart grid cybersecurity. NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology*. [CrossRef]

[6] McCarthy, J., Marron, J., Faatz, D., Rebori-Carretero, D., Wiltberger, J., & Urlaub, N. (2024). *Cybersecurity for smart inverters: Guidelines for residential and light commercial solar energy systems* (No. NIST Internal or Interagency Report (NISTIR) 8498 (Withdrawn)). National Institute of Standards and Technology. [CrossRef]

[7] Powell, C., Hauck, K., Sanghvi, A. D., Hasandka, A., Van Natta, J., & Reynolds, T. L. (2019). *Guide to the distributed energy resources cybersecurity framework* (No. NREL/TP–5R00-75044). National Renewable Energy Laboratory (NREL), Golden, CO (United States). Retrieved from https://docs.nrel.gov/docs/fy20osti/75044.pdf (accessed: Jan. 2026).

[8] Veitch, C. K., Henry, J. M., Richardson, B. T., & Hart, D. H. (2013). *Microgrid Cyber Security Reference Architecture (V. 1.0)* (No. SAND–2013-5472). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States). [CrossRef]

[9] U.S. Department of Energy. (2021). Cybersecurity Capability Maturity Model (C2M2) (Version 2.0). Retrieved from https://www.energy.gov/ceser/downloads/cybersecurity-capability-maturity-model-c2m2-version-20

[10] Zhang, Z., Turnbull, B., Kermanshahi, S. K., Pota, H., Damiani, E., Yeun, C. Y., & Hu, J. (2025). A survey on resilient microgrid system from cybersecurity perspective. *Applied Soft Computing, 175*, 113088. [CrossRef]

[11] Chen, J., Yan, J., Kemmeugne, A., Kassouf, M., & Debbabi, M. (2025). Cybersecurity of distributed energy resource systems in the smart grid: A survey. *Applied Energy, 383*, 125364. [CrossRef]

[12] Li, Y., & Yan, J. (2023). Cybersecurity of Smart Inverters in the Smart Grid: A Survey. *IEEE Transactions on Power Electronics, 38*(2), 2364–2383. [CrossRef]

[13] Karumba, S., Chau, S. C. K., Pearce, H., Ahmed, M., & Janicke, H. (2024, June). Systematic study of cybersecurity threats for smart inverters. In *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems* (pp. 669-675). [CrossRef]

[14] Tuyen, N. D., Quan, N. S., Linh, V. B., Tuyen, V. V., & Fujita, G. (2022). A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access, 10*, 35846–35875. [CrossRef]

[15] International Electrotechnical Commission. (2013). *IEC 62443-3-3:2013, Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels*. IEC Webstore. Retrieved from https://webstore.iec.ch/en/publication/7033

[16] International Electrotechnical Commission. (2020). *IEC 62351-6:2020, Power systems management and associated information exchange—Data and communications security—Part 6: Security for IEC 61850*. IEC Webstore. Retrieved from https://webstore.iec.ch/en/publication/63742

[17] Guerrero, J. M., Vasquez, J. C., Matas, J., De Vicuña, L. G., & Castilla, M. (2010). Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization. *IEEE Transactions on industrial electronics, 58*(1), 158-172. [CrossRef]

[18] Stanchev, P., Hinov, N., & Zlatev, Z. (2025). A Model for Assessing the Degree of Digitalization in Electric Power Networks. *ICCK Transactions on Electric Power Networks and Systems, 1*(2), 93–108. [CrossRef]

**Plamen Stanchev** received his PhD in Energy Systems from the Technical University of Varna, Bulgaria, in 2023. He has published articles in various journals; his research focuses on modern optimization, simulation, and artificial intelligence methods in power grids. His interests include reliability of photovoltaic inverters, energy efficiency in small and medium-sized enterprises, reinforcement learning-based controllers for distributed generation, and feasibility assessments of storage systems such as lithium-ion, lead-acid, and hydrogen technologies. (Email: p.stanchev@tu-sofia.bg)

**Nikolay Hinov** is a Professor in the Department of Computer Systems at the Faculty of Computer Systems and Technologies at the Technical University of Sofia, Bulgaria. Born in 1970 in Lukovit, he graduated with a Master's degree in "Electronics and Microelectronics" at the Technical University of Sofia in 1995 and defended his PhD dissertation in 1998 in the field of high-power electrical energy converters with industrial application. In 2024, he also defended his dissertation for the degree of "Doctor of Science", dedicated to the model-based design of power electronic devices with the application of artificial intelligence techniques. (Email: hinov@tu-sofia.bg)

**Atakan Salimov** received his Master's degree in Computer Systems and Technologies from the Technical University of Sofia, Bulgaria in 2023. His research interests are in the field of cybersecurity and advanced computing technologies. His work focuses on secure communication systems, cyber threat detection, quantum computing, and the development of post-quantum cryptographic techniques for protecting future digital infrastructures. (Email: atakan.salimov@tu-sofia.bg)

**Bulbul Ziulqmova** received her PhD from the Technical University of Sofia, Bulgaria, in 2015. Her PhD thesis focused on the development and analysis of cryptographic techniques for secure information distribution. Her research interests include modern cryptography, secret sharing schemes, information security, and methods for secure data protection for distributed systems. (Email: bulbul@tu-sofia.bg)

**Adnan Redjeb** received his PhD from the Technical University of Sofia, Bulgaria, in 2017, in the professional field of Communication and Computer Engineering. His PhD thesis focused on improving computational efficiency and resource utilization in computer architectures. His research interests include computer system optimization, task scheduling algorithms, performance analysis of computing systems, and efficient resource management in modern computing environments. (Email: adnan@tu-sofia.bg)