UNITECH SELECTED PAPERS

INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025, GABROVO

METRICS-DRIVEN CYBER-RESILIENCE EVALUATION FOR RENEWABLE ENERGY INFRASTRUCTURES

Evgeni Hristov, Plamen Nakov*

Technical University of Sofia, Department of Computer Systems,
8, Kliment Ohridsky blvd. Sofia, Bulgaria
**Corresponding author: p.nakov@tu-sofia.bg*

Abstract
This paper presents an overview of quantitative and qualitative approaches to assessing the cyber resilience of distributed energy resource (DER) systems, focusing on the integration of KPI indicators, adaptive AI metrics and international security frameworks. A comprehensive resilience analysis model is proposed that combines three assessment levels: technical, organizational and adaptive. In the technical aspect, classic KPIs such as MTTD, MTTR, Detection Rate and Crypto Coverage are used, which measure the speed of detection and response to incidents. The organizational level includes indicators for readiness and recovery, while the adaptive level introduces AI-based indices such as Cyber Resilience Index (CRI), Mean Time to Adapt (MTTA) and Reinforcement Learning Adaptation Efficiency (RAE). These metrics allow for a dynamic comparison of the level of protection and the effectiveness of response to cyber incidents in microgrids, hybrid RES systems and digitally connected DER infrastructures. The proposed methodology supports the transition from reactive to proactive cyber resilience by connecting measurable technical data with artificial intelligence for predictive assessment and adaptive security optimization.
Keywords: DER, cyber resilience, KPI, AI, RL, resilience index.

INTRODUCTION

The rapid adoption of Distributed Energy Resources (DER), such as photovoltaic systems, wind turbines, batteries and smart controllers, is fundamentally changing the way power grids are managed. These systems, connected through communication networks, IoT platforms and SCADA systems, provide high flexibility and efficiency, but at the same time expand the attack surface and require a new level of cyber resilience [1-4].

Cyber resilience is defined as the ability of a system to anticipate, withstand, recover and adapt after cyber attacks or failures. Unlike classic cybersecurity, which focuses on preventing breaches, cyber resilience measures the functional continuity and speed of recovery after an incident. In the context of DER infrastructures, this means maintaining energy availability and control stability even in the event of a partial loss of communication, a compromised gateway or malicious interference with data from sensors and inverters.

As the interconnections between Operational Technology (OT) and IT systems increase, the need for quantitative resilience assessment becomes critical. Traditional security approaches based on static policies and audits are not sufficient for the dynamic environment of DER, where dozens of devices, protocols and cloud services interact in real time [5,6].

An integrated model that combines technical indicators (KPIs), organizational processes and adaptive AI metrics is needed to determine the real level of resilience and readiness for response.

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

This article presents an overview of methods and indicators for quantitative and qualitative assessment of cyber resilience of DER systems. A multi-level approach is proposed, including: technical level, assessment of detection and response speed Mean Time To Detect (MTTD), Mean Time To Respond (MTTR), Detection Rate; organizational level, measurement of readiness and procedural efficiency (Backup Rate, Patch Compliance); adaptive level, introduction of AI-based metrics such as Cyber Resilience Index (CRI), Mean Time to Adapt (MTTA) and Reinforcement Learning Adaptation Efficiency (RAE) [7].

The aim is to propose a unified framework for measuring the resilience of DER networks, allowing comparison between different systems, scenarios and technologies. This framework supports the transition from reactive to proactive protection, based on intelligent monitoring and self-learning mechanisms for adaptation to new threats [8].

CONCEPT AND METHODOLOGICAL FOUNDATIONS OF CYBER RESILIENCE

Cyber resilience in energy systems is considered as the ability of the infrastructure to maintain critical functions, regardless of the presence of cyber incidents, failures or malicious impacts. In contrast to traditional cybersecurity, which aims to prevent attacks, cyber resilience measures the capacity of the system to withstand, recover and adapt after a breach or disturbance.

According to the definitions, a resilient system must perform four sequential functions: Anticipate, identifying threats and vulnerabilities through risk analysis and scenario modeling; Withstand, ensuring continuity through architectural segmentation, redundancy and cryptographic protection; Recover, restoring functionality through backups, DRP and playbook response; Adapt, improving measures based on accumulated data, training and AI analysis.

This four-phase framework corresponds to the security lifecycle, where the Identify–Protect–Detect–Respond–Recover stages form a continuous improvement process.

DERs are cyber-physical systems (CPS) in which electrical, communication and management infrastructure are interconnected. This integration provides operational efficiency, but also leads to a new type of vulnerability, as compromising digital communications can directly affect physical processes. Examples include: telemetry manipulation between inverter and SCADA; time synchronization substitution (PTP spoofing) leading to erroneous protection actions; malicious firmware updates via cloud interfaces.

Therefore, the resilience of DER systems requires the simultaneous provision of physical, communication and logical protection.

The assessment of DER cyber resilience can be formalized through three main levels presented in Table 1.

Table 1 Assessment model of DER cyber resilience

Assessment Level	Focus	Metric Type
Technical	Speed and efficiency of detection, response and recovery	KPI: MTTD, MTTR, Detection Rate, Crypto Coverage
Organizational	Policies, training, procedures and incident management	KPI: Backup Success Rate, Patch Compliance, Tested Playbooks
Adaptive (intelligent)	Self-learning and dynamic optimization through AI	Metrics: CRI, MTTA, RAE, ASI

This three-tier model combines quantitative measurements (KPIs) and qualitative indices of adaptability, providing a balanced assessment of the real resilience of the system.

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

Modern regulatory requirements, place cyber resilience at the center of critical infrastructure management. They recommend integrating: systematic risk management (risk-based security management); measurable performance indicators (performance monitoring); continuous improvement processes.

In the context of DER, this means building a dynamic monitoring system that can measure resilience not only statically, but also over time through automatic collection and analysis of KPIs and AI metrics.

METHODOLOGY AND MODEL FOR QUANTITATIVE ASSESSMENT OF CYBER RESILIENCE

The aim of the proposed method is to provide an objective and comparable assessment of the cyber resilience of distributed energy resource (DER) systems by combining operational KPIs, organizational indicators and adaptive AI metrics. The method allows both quantitative measurement of the current state and dynamic tracking of trends when threats, policies or architecture change.

The assessment process consists of five main stages: Identification of assets and critical flows, determination of key components in the DER infrastructure (inverters, SCADA, communication gateways, cloud platforms). Data collection, extraction of operational logs, IDS alarms, update indicators and access events. Calculation of KPIs and AI metrics, use of standardized formulas for MTTD, MTTR, Detection Rate, etc. Normalization and weighting, transformation of all values to the range [0,1] and setting weights according to criticality. Calculation of a composite Cyber Resilience Index (CRI), a summary value indicating the overall level of readiness and adaptability.

They are calculated by:

$$MTTD = \frac{\sum(t_{find} - t_{\text{emergence}})}{N} \quad (1)$$

$$MTTR = \frac{\sum(t_{\text{recovery}} - t_{\text{find}})}{N} \quad (2)$$

$$DR = \frac{N_{find}}{N_{total}} \cdot 100\% \quad (3)$$

$$FPR = \frac{N_{\text{false alarms}}}{\text{N}_{\text{total alarms}}} \cdot 100\% \quad (4)$$

Since different indicators have different scales, all values need to be normalized in the interval [0,1]:

$$N_i = 1 - \frac{X_i - X_{\min}}{X_{\max} - X_{\min}} \quad (5)$$

After normalization, weights ω_i are assigned, reflecting the priorities of the organization, presented in Table 3.

Table 2 Weighted indices

Group	Weight
Technical KPIs	0.4
Organizational KPIs	0.3
Adaptive AI Metrics	0.3

The combined CRI index is calculated as a weighted sum of the normalized metrics:

$$CRI = \sum_{i=1}^{n} \omega_i \cdot N_i \quad (6)$$

where:

- Ni is the normalized value of the indicator;
- ω_i – the weight determined according to the priority;
- n – the number of indicators included.

It is possible to extend the model through a dynamic version of the index, which also includes a rate of change (adaptability):

$$CRI_{dyn} = CRI + \alpha \frac{dCRI}{dt} \quad (7)$$

The parameter α reflects the sensitivity to the rate of adaptation (measured by MTTA and RAE).

The interpretation scale is presented in Table 3

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

The calculated CRI can be mapped to the security levels in IEC 62443 (SL1–SL4) or to the C2M2 maturity levels presented in Table 4.

Thus, the CRI index can be used as a unified tool for assessing compliance with international standards and regulatory requirements.

Table 3 Rating ranges

CRI Value	Interpretation	System Status
0.90 – 1.00	Excellent cyber resilience	Autonomous adaptive protection, low risk
0.75 – 0.89	Good resilience	Timely response and effective recovery
0.60 – 0.74	Medium resilience	Partial control, needs optimization
< 0.60	Low resilience	High risk of impaired functionality

Table 4 CRI index metric

CRI range	IEC 62443 SL	C2M2 Maturity Level
0.90–1.00	SL 4 (Resilient)	Level 5 – Optimized
0.75–0.89	SL 3 (Secure)	Level 4 – Managed
0.60–0.74	SL 2 (Controlled)	Level 3 – Defined
<0.60	SL 1 (Initial)	Level 1–2 – Ad hoc/Repeatable

CYBER RESILIENCE ASSESSMENT OF A DER MICROGRID

The studied system is a smart microgrid, consisting of: Photovoltaic plant (300 kW), controlled by inverters with Modbus/TCP profile; Battery pack (150 kWh, Li-ion) with local EMS controller; SCADA/EMS system, with organized central server for monitoring and management; MQTT broker and OPC UA gateway connecting field devices with a cloud VPP aggregator; Communication environment, IP-based local area network with TLS protection and IDS/IPS module (Suricata).

The microgrid operates autonomously in normal mode, but maintains a two-way connection with the aggregator for forecasting and energy trading.

The assessment is performed under three realistic scenarios:

- Scenario A, base mode (without AI protection): traditional segmentation, cryptographic protection, without adaptive monitoring.
- Scenario B, with IDS/IPS and SIEM: added event correlation and automatic notification.
- Scenario C, with ML-based adaptive model (RL agent): system with Reinforcement Learning agent that optimizes access policies and response to detected anomalies.

After two weeks of monitoring, the average values reported for the main metrics are presented in Table 5 and Table 6.

Table 5 Average values reported for the main metrics

Metric	Scenario A	Scenario B	Scenario C (AI)	Units
MTTD	140	45	15	min
MTTR	210	80	35	min
Detection Rate	0.72	0.89	0.95	-
False Positive Rate	0.18	0.10	0.06	-
Patch Compliance	0.80	0.85	0.92	-
Backup Success Rate	0.75	0.86	0.93	-
MTTA	-	-	0.30	hours
RAE	-	-	0.85	-

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

Table 6 Calculated CRI values

Scenario	CRI (0–1)	Interpretation
A	0.63	Average resilience – reactive protection, high response time
B	0.78	Good resilience – timely detection and recovery
C	0.91	Excellent resilience – autonomous adaptation, low MTTR

The implementation of ML-based adaptive protection improves the overall cyber resilience index by about 45% compared to the baseline architecture.

The detection time (MTTD) is reduced by almost nine times when introducing an RL agent that analyzes the correlation between traffic and events in real time. The mean time to recovery (MTTR) is reduced from 210 to 35 minutes thanks to automated SOAR playbooks. The Detection Rate increases from 72% to 95%, and the False Positive Rate drops below 6%, demonstrating the effectiveness of the AI model. Patch and Backup metrics are also improved due to integration with a centralized update management system. RAE = 0.85 indicates high efficiency of the RL agent training against real incidents.

This targeted example confirms that quantitative assessment through KPI and CRI index allows not only measurement, but also optimization of resilience in a real DER microgrid. AI-based models provide dynamic adaptation to new types of attacks and minimize human intervention in incident response. The methodology can be used as a tool for: monitoring cyber resilience over time; assessing the impact of new policies or technologies; maintaining compliance with standards.

CONCLUSION

The presented work considers an integrated model for quantitative and qualitative assessment of cyber resilience of distributed energy resource (DER) systems, which combines technical KPIs, organizational indicators and adaptive AI metrics in a single analytical framework. The developed methodology allows not only measurement, but also comparison of resilience between different architectures and technologies in microgrids, based on standards.

The results of the targeted example show that the integration of AI/ML-based adaptive mechanisms can increase the value of the Cyber Resilience Index (CRI) by over 40%, significantly reducing the time to detection (MTTD) and recovery (MTTR) after incidents. This confirms that the combination of monitoring, automation and self-learning is key to building a resilient energy infrastructure.

The proposed approach represents a step towards an objective, measurable and automated assessment of cyber resilience in the context of smart energy systems and can serve as a basis for future standards and regulatory requirements in the renewable energy and microgrid sectors.

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, INNOVATION AND GREEN ENERGY IN ICT "DUNIZVICT".

REFERENCE

[1] J. Chen, J. Yan, A. Kemmeugne, M. Kassouf, and M. Debbabi, "Cybersecurity of distributed energy resource systems in the smart grid: A survey," Applied Energy, vol. 383, p. 125364, Jan. 2025, doi: 10.1016/j.apenergy.2025.125364.

[2] M. Liu et al., "Enhancing Cyber-Resiliency of DER-based SmartGrid: a survey," arXiv

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

(Cornell University), Jan. 2023, doi: 10.48550/arxiv.2305.05338.
[3] A. Vosughi, A. Tamimi, A. B. King, S. Majumder, and A. K. Srivastava, "Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs," Renewable and Sustainable Energy Reviews, vol. 168, p. 112794, Aug. 2022, doi: 10.1016/j.rser.2022.112794.
[4] V. J. Nair et al., "Resilience of the electric grid through trustable IoT-coordinated assets," Proceedings of the National Academy of Sciences, vol. 122, no. 8, Feb. 2025, doi: 10.1073/pnas.2413967121.
[5] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber-Physical Energy Systems Security: threat modeling, risk assessment, resources, metrics, and case studies," IEEE Access, vol. 9, pp. 29775–29818, Jan. 2021, doi: 10.1109/access.2021.3058403.
[6] V. Tzavara and S. Vassiliadis, "Tracing the evolution of cyber resilience: a historical and conceptual review," International Journal of Information Security, vol. 23, no. 3, pp. 1695–1719, Feb. 2024, doi: 10.1007/s10207-023-00811-x.
[7] K. Gupta, S. Sahoo, and B. K. Panigrahi, "A monolithic cybersecurity architecture for power electronic systems," IEEE Transactions on Smart Grid, vol. 15, no. 4, pp. 4217–4227, Feb. 2024, doi: 10.1109/tsg.2024.3368277.
[8] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," Computers & Security, vol. 132, p. 103372, Jun. 2023, doi: 10.1016/j.cose.2023.103372.

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