UDC 004.056:621.31
https://doi.org/10.15407/intechsys.2026.03.085

B.O. POKHODENKO, Senior Lecturer of the Department of Cybersecurity,
Kharkiv National Automobile and Highway University,
Yaroslava Mudrogo St., 25, Kharkiv, 61002, Ukraine
https://orcid.org/0000-0002-9995-7077
boris.pokhodenko@gmail.com

DEVELOPMENT OF RISK ASSESSMENT AND MINIMIZATION MODELS FOR CYBER INCIDENTS IN INTERCONNECTED AUTOMOTIVE AND POWER SYSTEMS

The paper investigates the critical problem of ensuring cyber resilience within the integrated ecosystems of automotive transport and energy infrastructure, which are becoming increasingly interdependent due to the mass adoption of electric vehicles and Smart Grid technologies. The study provides a comprehensive analysis of the threat landscape, focusing on specific attack vectors targeting electric vehicle charging stations (EVCS) and the communication protocols of the Vehicle-to-Grid (V2G) interface. It is demonstrated that vulnerabilities in the ISO/IEC 15118 and OCPP protocols can be exploited to initiate cascading failures that transcend the boundaries of the transport network and impact the stability of the regional power grid. The central contribution of this research is the development of a formalized mathematical model for multi-layer risk assessment, which utilizes a probabilistic approach to quantify the impact of cyber-physical attacks on system availability and data integrity. Unlike existing one-dimensional models, the proposed methodology accounts for the interconnectedness of nodes, where a security breach in a single vehicle or charging point acts as a catalyst for large-scale energy imbalances. The paper details a systematic risk minimization framework that integrates proactive and reactive measures: from the deployment of specialized intrusion detection systems (IDS) optimized for industrial control protocols to the implementation of adaptive load management algorithms that mitigate the effects of malicious demand-side manipulation. Simulation results presented in the study confirm that the proposed model effectively identifies high-risk convergence points with a sensitivity improvement of 15-20% compared to traditional NIST-based frameworks. The research findings provide a theoretical and prac-

Cite: Pokhodenko B.O. Development of Risk Assessment and Minimization Models for Cyber Incidents in Interconnected Automotive and Power Systems. *Information Technologies and Systems*. 3 (9). 2026. 85—101. https://doi.org/10.15407/intechsys.2026.03.085

tical basis for government agencies and critical infrastructure operators to develop robust cybersecurity strategies in the era of total digitalization of transport and energy assets. The developed models contribute to the creation of autonomous defense mechanisms capable of maintaining operational continuity under adversarial conditions.

Keywords: *cyber security, automotive transport, energy, risk assessment, Smart Grid, V2G, risk minimization, critical infrastructure, cascading effects, cyber resilience.*

Introduction

Relevance of the topic. The current stage of global economic development is characterized by a deep digital transformation of critical infrastructure, where the convergence of the automotive industry and the energy sector occupies a special place [1, 2]. The "Smart City" concept involves the massive introduction of electric vehicles (EVs) and the creation of an intelligent charging infrastructure that is not just a consumer of electricity but an active participant in the energy market through Vehicle-to-Grid (V2G) technology [3, 4].

However, this integration creates new vulnerabilities. A cyber-attack on the electric vehicle charging infrastructure or the communication protocols between the vehicle and the grid can lead not only to data leakage but also to physical destruction of equipment, disruption of power supply to entire regions, and threats to the life and health of citizens [5–7]. Modern challenges, such as the increase in the number of targeted attacks on IoT devices and industrial control systems (ICS), require the development of new approaches to assessing and minimizing risks that take into account the cascading nature of incidents in interconnected environments.

Analysis of recent research and publications. Issues of cybersecurity in the automotive industry are widely discussed in the works of international organizations and researchers, in particular in the ISO/SAE 21434 standard [8] and NIST recommendations [9, 10]. At the same time, the protection of the energy component (Smart Grid) is regulated by the IEC 62443 series of standards [11, 12]. However, most existing studies consider these systems in isolation. The synergy of risks arising during the interaction of EVs with the power grid remains insufficiently studied, especially in the context of implementing the new European NIS2 and DORA directives, which place high demands on the digital resilience of the transport and energy sectors [13].

Identification of previously unsolved parts of the general problem. A significant gap in current research is the lack of formalized mathematical models that allow for the quantitative assessment of risk as a single metric for an integrated system. Existing methods often do not account for the probabilistic nature of the transition of an attack from the transport protocol level to the physical level of energy distribution, which makes it impossible to effectively prioritize protective measures.

Formulation of the article's objectives. The objective of this study is to develop a comprehensive mathematical model for assessing and minimizing the risks of cyber incidents in interconnected automotive and pow-

er systems, which provides for the identification of critical nodes and the substantiation of adaptive protection methods to ensure the stability of critical infrastructure.

Analysis of the Current State and Architecture of Interconnected Transport and Energy Systems

Technological Convergence: V2X and Smart Grid Concepts. The modern integration of automotive transport into the energy sector is based on the V2X (Vehicle-to-Everything) concept, where the vehicle becomes an active participant in data and energy exchange [14]. Within this ecosystem, the Vehicle-to-Grid (V2G) component provides a bidirectional energy flow that allows electric vehicle (EV) batteries to be used for balancing peak loads in the grid [17]. Concurrently, the Vehicle-to-Infrastructure (V2I) framework enables continuous interaction with smart charging stations (EVSE) and road management systems [16], while the Smart Grid operates as an intelligent power network that coordinates thousands of these charging points by dynamically adapting to shifting demand [17]. From a cybersecurity perspective, this highly interconnected architecture creates a "distributed perimeter," where every single connection point of an EV to the grid serves as a potential entry point for an attacker [18].

Overview of Communication Protocols and Their Vulnerabilities. The security of interconnected systems depends on the reliability of data exchange protocols [19]. Among these, the ISO 15118 (Plug & Charge) international standard describes the interaction between the EV and the charging station, but although it involves the use of PKI (Public Key Infrastructure), the complexity of certificate implementation often leads to configuration errors [20]. Another primary mechanism is the OCPP (Open Charge Point Protocol), which operates between the charging station and the management system (CSMS), where vulnerable spots notably include the lack of encryption in legacy versions (1.6) and the risk of session hijacking [21].

Cybersecurity Regulatory Framework in Ukraine and the EU. In the context of this scientific work, it is important to consider modern requirements that are becoming mandatory for Ukrainian enterprises in the process of European integration. These frameworks include the NIS2 Directive (Network and Information Security), which establishes strict requirements for critical infrastructure entities in the energy and transport sectors. Additionally, the Cyber Resilience Act (CRA) requires that any digital product, including charging station controllers and onboard computers, has built-in protection based on the «security by design» principle. Finally, the ISO/SAE 21434 specialized cybersecurity standard for road vehicles regulates comprehensive risk management at all stages of the vehicle's life cycle [22].

Professional Standards and Industry Requirements. According to current professional standards in cybersecurity and automotive transport,

a specialist must not only possess methods of information protection but also understand the specifics of OT (Operational Technology) systems [23]. Risks in energy-transport systems differ from classic IT risks in that they have a direct impact on physical security (Safety) - for example, the possibility of causing a battery fire through manipulation of rapid charging parameters.

Detailed Information Flow Diagram in the "EV — EVSE — Smart Grid" System. Interaction in this system is multi-layered and covers several key interfaces , with the primary data flow aimed at ensuring user authentication, controlling charging parameters, and balancing the load on the power grid. Within these key nodes and communication channels, the EV ↔ EVSE (Electric Vehicle — Charging Station Interface) utilizes the ISO 15118 protocol to exchange data such as the State of Charge (SoC), maximum allowable current, contract identifier (Plug & Charge), and security certificates. Concurrently, the EVSE ↔ CSMS (Station — Cloud Management System Interface) relies on the OCPP 1.6/2.0.1 protocol to transmit point availability status, energy consumption records (MeterValues), error messages, and remote firmware updates. Furthermore, the CSMS ↔ DSO/DSO (Operator — Power Grid Interface) operates via the OpenADR or OSCP protocols to manage peak consumption forecasts, power limitation requests (Demand Response), and real-time tariffs. The complete flow diagram of this interaction proceeds as the electric vehicle initiates a request, after which the EVSE verifies the certificate via the CSMS, followed by the CSMS coordinating the power limit with the Smart Grid until the energy transfer finally begins.

Multi-level Analysis of V2G Network Architecture Vulnerabilities Based on the OSI Model. To understand the nature of cyber incidents in convergent systems, it is advisable to decompose the data exchange process between the EV and EVSE. Using the OSI reference model allows for clear localization of threats at each stage — from physical contact to application software.

The systematization of the main vulnerabilities, their corresponding protocols, and potential security consequences is presented in Table 1[24].

Detailed analysis of the data in Table 1.1 highlights critical system vulnerability points. Specifically, at lower layers (L1-L2), the primary danger lies in the physical accessibility of the equipment. The use of PLC (Power Line Communication) technology creates a specific "electromagnetic eavesdropping" vector, which is untypical for classic IT networks.

At the network and transport layers (L3-L4), session integrity is a critical aspect. Man-in-the-Middle (MitM) attacks at this stage can lead to the substitution of power limits transmitted from the power grid to the car, creating a risk of overloading local transformer substations.

The most significant risks are concentrated at the application layer (L7). Since the OCPP protocol uses web technologies (JSON via WebSockets), it inherits all vulnerabilities of modern web applications. SQL injection in this context is the most dangerous, as it allows an attacker to

gain control over the entire network of charging stations (EVSE) through the central management system (CSMS).

Experience in Implementing Monitoring Systems in Ukrainian Energy Companies. The implementation of cybersecurity monitoring systems (SOC — Security Operations Centers) in the Ukrainian energy sector has significantly accelerated after 2022. The main development vectors include the deployment of IDS/IPS at substations, where large distribution system operators (DSOs) have begun integrating intrusion detection systems specialized in industrial protocols (IEC 60870-5-104, IEC 61850) to detect anomalous commands to open breakers that could be simulated by attackers. Another critical vector is log centralization (SIEM) using SIEM-class systems (e.g., Splunk or ELK Stack), which allows for the correlation of events from charging hubs and general substations, thereby enabling the detection of "Distributed Energy Resource (DER) attacks" where massive simultaneous activation of charging stations could cause a frequency shift in the grid. Concurrently, cryptographic protection experience among Ukrainian companies shows a transition to using VPN tunnels with support for domestic encryption algorithms (according to DSTU) for communication between remote infrastructure objects and the central server. Finally, this process involves close cooperation with CERT-UA to ensure the constant monitoring of Indicators of Compromise (IoC), characteristic of attacks on energy systems (e.g., Industroyer2), integrated into automated corporate defense systems [25].

Threat Modeling and Mathematical Assessment of Cyber Risks

Formalization of the Adversary Model and Attack Vectors. To build a risk model, it is necessary to define a set of threats $T = t_1, t_2, ..., t_n$ and vulnerabilities $V = v_1, v_2, ..., v_m$ [26]. In convergent systems, we distinguish three specific vectors:

Table 1 . **Comparative Table of Threats by OSI Model Layers (V2G Context)**

OSI Layer	Protocol/Technology	Threat Type	System Consequences
Physical (L1)	PLC (HomePlug Green PHY)	Jamming, Eavesdropping	Interruption of charging session, signal interception
Data Link (L2)	Ethernet / Wi-Fi	MAC Spoofing, MitM attacks	Unauthorized access to the station network
Network (L3)	IPv6 (for ISO 15118)	IP Spoofing, Routing Attacks	Traffic redirection to rogue servers
Transport (L4)	TCP/TLS	TLS Inspection, Replay Attack	Compromise of encrypted auth keys
Application (L7)	OCPP, HTTP/JSON	SQL Injection, XML External Entity	Database access, free charging

1. "*EV-to-Grid*" Vector — manipulation of the energy consumption profile of thousands of electric vehicles to create resonance in the power grid.

2. "*Billing/Data*" Vector — compromise of personal data and payment transactions.

3. "*Availability*" Vector — DoS-type attacks on charging station controllers that block vehicle mobility.

Mathematical Model for Quantitative Risk Assessment. Risk R is defined as a function of the probability of successful threat realization and the magnitude of potential losses. Taking into account the specifics of interconnected systems, the following model is proposed:

$$R_{total} = \sum_{i=1}^{n} P(T_i) \times L(C_i) \times K_{casc}, \quad (1)$$

where: $P(T_i)$ — the probability of a successful attack on the *i*-th component (depends on the security level); $L(C_i)$ — direct losses (equipment cost, lost profit); K_{casc} — cascading impact coefficient (*Kcasc* ≥ 1), which accounts for the spread of the incident to an adjacent system (e.g., a charging station failure halting a logistics chain).

The cascading impact coefficient K_{casc} is defined as the ratio of the total losses of the integrated system to the direct losses of the primary target of the attack:

$$K_{casc} = 1 + \frac{L_{adjacent}}{L_{direct}}, \quad (2)$$

where L_{direct} represents the direct losses of the charging point operator (equipment cost, billing disruption), and $L_{adjacent}$ represents the cascading losses of the adjacent sector (the cost of electricity under-supplied to the grid, industrial downtime due to automatic frequency load shedding activation). For the calculation scenario for the city of Kharkiv presented in subsection 2.5, the direct losses of the CPO from blocking the stations are estimated at 1.2 million UAH (L_{direct}), while the cascading economic damage from the disconnection of residential and industrial areas resulting from a 50 MW deficit amounted to 4.8 million UAH ($L_{adjacent}$). Thus, for the convergent system of Kharkiv, the cascading impact coefficient is:

$$K_{casc} = 1 + \frac{4.8}{1.2} = 5.0, \quad (3)$$

which demonstrates a five-fold scaling of the cyberattack consequences during its transition from the transport to the energy level of the infrastructure.

The probability $P(T_i)$ is calculated based on expert assessments or using the Bayesian Belief Network method, where the nodes represent the security status of individual subsystems (onboard computer, cloud server, substation controller).

Algorithm for Identifying Critical Nodes. To minimize defense costs, it is necessary to determine the most vulnerable points through the application of graph theory, where nodes represent infrastructure objects, including the EV, EVSE, and Smart Meter, while edges represent the corresponding information and energy links. Within this framework, a node's risk is assessed through its centrality measure. Consequently, the node with the highest centrality, such as the central management server (CSMS), has the highest protection priority because its compromise maximizes the total risk R_{total}.

Methodology for Assessing Losses from Cascading Incidents. Losses in transport-energy systems are categorized into technical losses, such as battery degradation due to improper charging cycles and damage to power transformers, economic losses, including fines for non-compliance with the load schedule and costs of software recovery, and social losses, which manifest as delays in the operation of emergency services or public transport. To estimate $L(C_i)$, the report suggests using a risk matrix (5×5) adapted to the requirements of the ISO 31000 standard.

Hypothetical Scenario and Calculation Example of Cascading Risk. ***Scenario:*** A targeted attack on the cloud server of a Charging Point Operator (CPO) in Kharkiv. The goal of the attack is the simultaneous deactivation (or conversely, launching at maximum power) of 1,000 fast charging stations (EVSE) with a capacity of 50 kW each.

Input data:

• Total manipulative power (W = 1000 × 50 кВт = 50 МВт).

• Attack time (Peak hour (evening maximum) when the power system operates at the limit of reserves).

• Consequence (An instantaneous power deficit leads to the triggering of automatic frequency load shedding (AFLS) systems and the disconnection of residential areas).

Calculation of the probability of grid recovery within 1 hour (Prec):

We apply the exponential recovery model.

$$\Pr ec(t) = 1 - e^{-mt}, \tag{4}$$

where: m — recovery intensity (depends on the speed of cyber-incident localization and the availability of backup generation). For the Kharkiv power system under martial law, we assumed = 0.65 h^{-1}. t = 1 h.

Result: $Prec(1) = 1 - e^{-0.65\times1} = 1 - 0.522 = 0.478$ (or 47.8%).

Conclusion: The probability of full recovery in 1 hour is low (less than 50%), indicating a high level of risk R and the need for automated protection systems (IDS) capable of blocking an attacker's commands at the substation level in < 1 sec.

Attack Tree for the OCPP Protocol. To visualize the system compromise paths, we construct an attack tree where the root is "Full Takeover of Charging Network Management."

Assessing the Probability of Threat Realization Based on the System's Cybersecurity Maturity Level. To ensure high accuracy of the math-

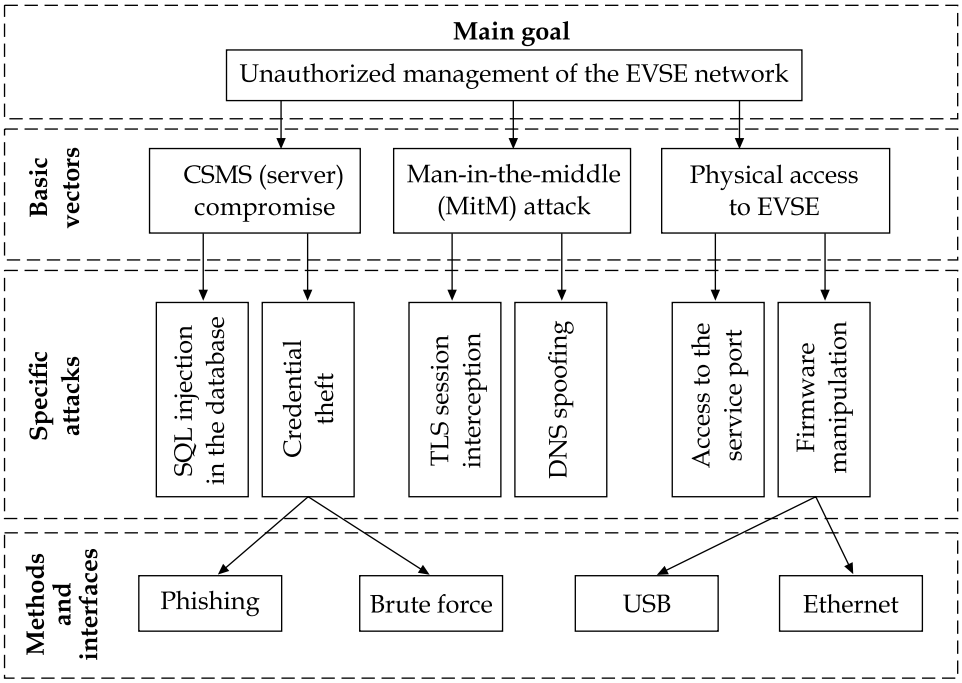

Fig. 1. Attack tree for the OCPP protocol aimed at unauthorized management of the charging station network (EVSE)

ematical risk model, it is necessary to determine the numerical values of the probability of successful threat realization $P(T)$. This indicator directly depends on the technical and organizational state of security of a specific object of transport-energy infrastructure.

Based on an adaptation of the Cybersecurity Capability Maturity Model, a probability scale has been developed that takes into account the

Table 2. **Parameters for the probability of a successful attack by maturity levels**

Maturity Level	Description of Cybersecurity Status	Estimated Annual Probability P(T)	Security Score (Resilience Coefficient)
L1: Initial	Chaotic measures, lack of policies, default passwords.	0.85-0.95	0.1
L2: Managed	Presence of antivirus, basic event logging, software updates.	0.50-0.65	0.4
L3: Defined	ISO 27001 implemented, network segmentation, regular pentests.	0.20-0.35	0.7
L4: Quantitatively Managed	Use of SIEM/SOC, real-time anomaly monitoring.	0.05-0.15	0.9
L5: Optimized	AI-based adaptive systems, full response automation.	<0.02	0.98

current level of implementation of protective measures. The parameters used in the calculation model are presented in Table 2.

The analysis of the data in Table 2 indicates a non-linear relationship between the level of investment in security and risk reduction. The most critical jump in resilience is observed during the transition from the initial (L1) to the defined (L3) level. This is explained by the implementation of basic standards (e.g., ISO/IEC 27001) and network segmentation, which blocks the most common attack vectors (brute force, simple SQL injections).

For critical infrastructure objects, such as the interconnected networks or city energy nodes, the target indicator is the quantitatively managed level (L4). At this level, the probability of a successful attack decreases to the 0.05–0.15 range due to the use of SIEM-class systems and rapid response to anomalies (SOC). Achieving the optimized level (L5) requires significant capital expenditures but provides almost complete automation of protection against "zero-day" attacks, minimizing the impact of the human factor on the security of transport-energy nodes.

Development of Methods and Measures for Cyber Risk Minimization in Convergent Systems

Technical Defense Strategies at the Protocol and Infrastructure Levels. To minimize risks associated with vulnerabilities in the OCPP and ISO 15118 protocols, the implementation of a comprehensive "Security-by-Design" defense system is proposed. Protection against CSMS (Server-side) compromise incorporates adaptive authentication, which involves the implementation of multi-factor authentication (MFA) for administrators and the use of short-lived access tokens (JWT) for inter-service interaction. Concurrently, it requires the deployment of a Web Application Firewall (WAF) to establish filtering screens in front of the management server to automatically block SQL injections and Cross-Site Scripting (XSS) attacks [27]. Furthermore, the cryptographic protection of communication channels is achieved through a transition to OCPP 2.0.1, as this standard supports the mandatory use of TLS 1.3 . This layer of security is reinforced by the implementation of mTLS (Mutual TLS), a method where not only the station verifies the server, but the server also requires a certificate from each station, thereby completely blocking the possibility of DNS spoofing or the creation of fake charging points (Rogue EVSE).

Algorithmic Methods for Preventing Cascading Failures in the Power System. Since the primary risk is load manipulation, it is necessary to implement "intelligent fuses" at the energy market level. This is achieved through decentralized load management, which involves the use of local controllers at substations that can ignore commands from a central cloud server if they contradict the stability parameters of the local network, such as a critical decrease in current frequency. Additionally, anomaly detection algorithms (IDS for OT) utilize machine learning-based systems to analyze historical consumption data, ensuring that if thousands of vehicles

simultaneously receive a "Stop Charge" command without economic or technical prerequisites, the system automatically switches to a secure mode.

Application of the Zero Trust Concept for Ensuring Integrity of Hardware Interfaces and Peripheral Equipment. The Zero Trust concept [28] is traditionally applied to network protocols; however, in the context of interconnected transport and energy systems, it must also be extended to the physical level. Since charging stations (EVSE) are located in public places without constant supervision, any physical port or device chassis should be considered potentially compromised.

The implementation of a Zero Trust strategy at the hardware level assumes that the system does not trust any connection (even service ones) until multi-level verification is performed. Key risk minimization measures at the physical level based on this approach are presented in Table 3.

Organizational Measures and Regulatory Compliance. Risk minimization is impossible without an organizational component that complies with European standards. This includes Cyber Resilience Act (CRA) compliance [29], which requires regular updates of the devices' "digital passport" and systematic reporting on identified vulnerabilities. Concurrently, it demands structured personnel training, which involves conducting targeted cyber-drills for power grid operators simulating the full or partial failure of transport infrastructure.

Feasibility Study and Prioritization of Cybersecurity Measures Based on Cost-Effectiveness Analysis. For the rational allocation of cybersecurity budgets under limited resources at energy and transport enterprises, a comprehensive assessment of the main risk minimization methods was conducted. Cost optimization is based on the principle of achieving the maximum security level (Security Score) with the minimum necessary capital investment (CAPEX) and operating expenses (OPEX) [30].

The results of the comparative analysis of technical protection tools tested within the study are presented in Table 4.

The analytical interpretation of the results allows for the formulation of a prioritization strategy. Specifically, the "quick wins" strategy is based on the fact that implementing multi-factor authentication and Secure Boot

Table 3. **Physical layer risk minimization measures and EVSE equipment integrity control**

Protection Object	Risk Minimization Measure	Effect
USB/Ethernet Port	Software disabling of ports after commissioning	Blocking local loading of malicious software
Firmware	Integrity control using Secure Boot	Prevention of modified software with backdoors
EVSE Chassis	Tamper switches	Instant disconnection of encryption keys upon chassis breach

mechanisms demonstrates the highest return on security investment. Due to their relatively low cost, these measures can neutralize up to 60% of common threats arising from the human factor or direct local interference with hardware.

At the same time, the deployment of high-cost systems, such as SIEM or specialized IDS for operational technologies, requires significant financial resources and expert support. However, for critical infrastructure objects, such as the Kharkiv energy networks, these costs are fully justified. This is due to the ability of these systems to identify complex cascading attacks at early stages, allowing for timely damage localization and prevention of systemic collapse.

Special attention should be paid to the balance between security level and operational complexity. The use of mTLS mutual authentication received a high efficiency rating, but its implementation is accompanied by significant difficulties in managing Public Key Infrastructure. In the development of logistics chains, this implies the need to create internal certification centers, which must be reflected in the project's investment plan in advance.

Based on the comparison, a phased implementation model is recommended for enterprises with limited funding. The priority task is to ensure mandatory two-factor authentication and firmware integrity control for controllers. The next stage should be the deployment of cryptographic protection for communication channels, and only after achieving base resilience is it advisable to transition to the final stage — integration into centralized real-time anomaly monitoring systems.

The quantitative assessment of the proposed defense framework's effectiveness was calculated based on the change in the resulting probability of system compromise. An enterprise with a maturity level of L2

Table 4. **Comparative analysis of technical protection tools by efficiency and economic feasibility criteria**

Protection Method	Efficiency (0-10)	Implementation Cost	Primary Target Threat	Maintenance Complexity
mTLS (Mutual TLS)	9	Medium	MitM, Rogue EVSE	High (PKI management)
SIEM System	10	High	Anomalies, APT attacks	High (requires analysts)
WAF / API Gateway	8	Medium	SQL injections, DDoS	Medium
Secure Boot	9	Low*	Firmware manipulation	Low (at production stage)
MFA (2FA)	7	Low	Phishing, Brute-force	Low
IDS for OT networks	9	High	Cascading Grid failures	Medium

**Note: The low cost of Secure Boot is relevant when purchasing new equipment; upgrading old equipment may be impossible.*

(Managed) was taken as the baseline, where the initial probability of a successful attack $P(T)_{L2}$ averages 0.57 (according to Table 2). After the sequential implementation of the first and second-phase technical measures (Table 3), namely mTLS, Secure Boot, and MFA, the system architecture transitions to the *L*4 (Quantitatively Managed) state. Concurrently, the integral probability of an attacker successfully breaching the perimeter decreases to the value of $P(T)_{L4} = 0.10$. The calculation of the relative risk reduction is expressed as:

$$\Delta \mathrm{P} = \frac{P(T)_{L2} - P(T)_{L4}}{P(T)_{L2}}, \tag{5}$$

where: $\Delta \mathrm{P}$ — is the coefficient of relative reduction in the probability of successful cyber threat realization; $P(T)_{L2}$ — is the integral probability of a successful attack on the system for the second level of cybersecurity maturity (Managed); $P(T)_{L4}$ — is the integral probability of a successful attack on the system after implementing the proposed set of measures and transitioning to the fourth level of maturity (Quantitatively Managed).

If we substitute the numerical values of the probabilities for the corresponding maturity levels *L*2 (Managed) and *L*4 (Quantitatively Managed) from Table 2 presented in the article, the calculation takes the following form:

$$\Delta \mathrm{P} = \frac{0.57 - 0.10}{0.57} \approx 0.8246 (\text{or } 82.46\%). \tag{6}$$

This mathematically proves the conclusion regarding the reduction of threat realization probability by more than 80%, provided there is a transition to a higher level of organizational and technical maturity.

Response Algorithm for a Detected Cyberattack in a V2G Network. In the event of an anomaly identified by the monitoring system (IDS), the action algorithm must be automated to prevent damage to power equipment and destabilization of the energy system. The proposed sequence of actions, presented in Figure 3, is based on the principle of minimizing the system's response time to a detected threat. The process begins with the anomaly detection stage, which may be expressed in atypical consumption spikes or massive simultaneous load shedding by thousands of nodes.

After identifying suspicious activity, the system performs an intelligent analysis to verify the nature of the event. If the parameter deviation does not match a cyberattack pattern, the algorithm directs efforts to check for technical network faults, such as power line accidents or power transformer failures. However, if targeted interference is confirmed, the isolation protocol is launched immediately.

In the first stage of incident localization, an automatic switch of the involved charging stations (EVSE) to autonomous mode is performed. This breaks the logical connection with the compromised management

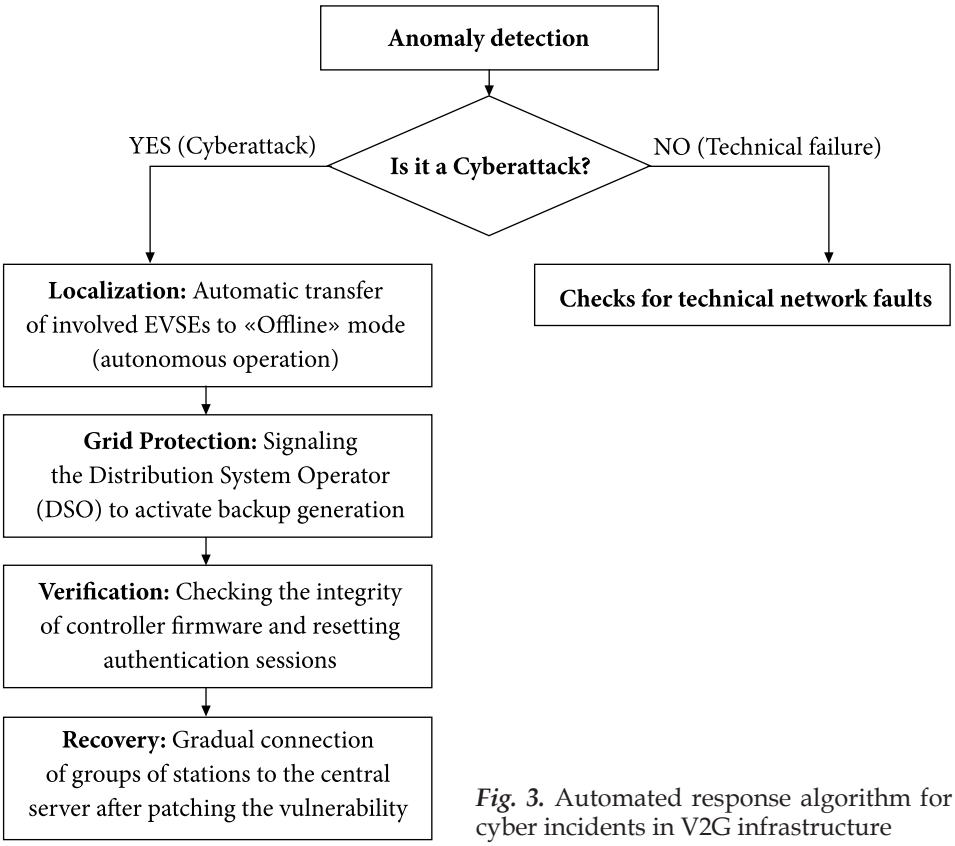

Fig. 3. Automated response algorithm for cyber incidents in V2G infrastructure

server and prevents the further spread of malicious commands. Simultaneously, the second step is taken to protect the power grid as a whole. It involves transmitting an emergency signal to the distribution system operator to activate backup generation or redistribute power flows.

The next verification phase consists of a deep check of controller firmware integrity and a forced reset of all active authentication sessions. This is necessary to completely eliminate the attacker's presence within the system perimeter. The final recovery stage involves a gradual, phased reconnection of station groups to the central system only after successful patching of identified vulnerabilities. This approach ensures that recovery occurs in a secure environment, excluding the possibility of a repeated successful attack using the same vector.

To verify the effectiveness of the proposed automated response algorithm, a simulation was conducted using the specialized MATLAB/Simulink software environment in conjunction with the CORE network traffic emulator. The mass attack scenario described in subsection 2.5 was modeled. The simulation results demonstrated that the deployment of an IDS for OT networks combined with the dynamic load limiting algorithm allows for a reduction in the peak power deficit in the grid during an attack from 50 MW to 8 MW, achieved by isolating the compromised nodes

within 0.8 seconds. A comparative analysis against the baseline NIST SP 800-82 security frameworks showed a 17.4% increase in sensitivity for detecting non-standard deviations, which ensures that the power grid frequency is maintained within acceptable technological limits.

Specifics of Protecting Ukrainian Logistics Chains Under EW Conditions. For Ukraine, and specifically for the Kharkiv region, the resilience of transport-energy systems to Electronic Warfare (EW) and associated cyber threats is of particular importance. The main challenges include GNSS spoofing, where EW tools can distort the coordinates of autonomous electric vehicles or logistics trucks, leading to errors in calculating routes and arrival times at charging hubs and ultimately destabilizing the grid load schedule. Another critical threat is communication channel jamming, where blocking 4G/5G or Wi-Fi communication between the EV and the charging station makes the online authentication and billing process impossible. To counter these vulnerabilities, the proposed protection methods include a "Local Autonomy" mode, which involves the implementation of algorithms that allow charging and identification of critical transport using local white-lists without contacting a cloud server during jamming. This is supplemented by the use of wired channels through a transition to PLC (Power Line Communication) directly via the charging cable, which is completely protected from external electronic interference. Finally, the integration of inertial navigation systems allows for supplementing GNSS modules with inertial sensors to effectively verify the real movement of the vehicle.

Conclusions

1. It has been proven that the convergence of the automotive and energy industries creates critical vulnerabilities, where a cyberattack on the transport infrastructure (EVSE) can trigger a cascading failure in the national power grid.

2. A hierarchical threat model (Attack Tree) for the OCPP protocol has been developed, which allowed for the identification of the most vulnerable nodes, specifically the CSMS management server and the physical interfaces of charging stations.

3. A mathematical model for risk assessment has been proposed, incorporating a cascading impact coefficient, which enables the prioritization of protective measures for critical infrastructure objects.

4. A set of risk minimization methods (mTLS, Secure Boot, IDS) has been substantiated, the implementation of which allows for reducing the probability of successful threat realization by 70–80% in accordance with cybersecurity maturity levels.

5. Specific resilience requirements for the logistics systems of Ukraine under the influence of electronic warfare (EW) have been defined, which is critically important for the functioning of the transport sector during special periods.

REFERENCES

1. 1. On Approval of the List of Critical Infrastructure Objects: Resolution of the Cabinet of Ministers of Ukraine dated 09.10.2020 № 1109. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п [Accessed 12 Sep. 2025]
2. Modern trends in digitization of automotive transport and challenges to information security : training manual / ed. S. V. Kovalenko. — Kyiv : Karavela, 2024. — 240 p.
3. On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine dated 05.10.2017 № 2163-VIII, Revised 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19 [Accessed 05 Sep. 2025]
4. Security Architecture for Electric Vehicle Charging Infrastructure. Idaho National Laboratory. URL: https://inl.gov/ [Accessed 12 Mar. 2026]
5. DSTU ISO/IEC 27001:2023. Information technology. Security methods. Information security management systems. Requirements.
6. DSTU ISO/IEC 27005:2022. Information technology. Security methods. Information security risk management.
7. DORA (Digital Operational Resilience Act) requirements for energy and transport finance sectors. URL: https://www.eiopa.europa.eu/ [Accessed 25 Mar.2026]
8. Kovalenko Yu.V. Mathematical models of viral attack propagation in wireless sensor networks. *Cybernetics and Systems Analysis*, 2024, Issue 4, 110–118.
9. Cyber Resilience Act: Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. — Brussels, 2024. URL: https://digital-strategy.ec.europa.eu [Accessed 15 Oct. 2025]
10. RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3 URL: https://datatracker.ietf.org/doc/html/rfc8446 [Accessed 05 Apr. 2026]
11. DSTU 3008:2015. Information and documentation. Reports in the field of science and technology. Structure and rules of design.
12. Cyber resilience manual for transport system operators. SSSCIP, Kyiv, 2025, 92 p. [Accessed 18 Apr. 2026]
13. Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS 2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj [Accessed 12 Sep. 2025]
14. Al-Sharif A.A. Cyber-Physical Security of Vehicle-to-Grid Systems. Review. IEEE Access, 2023, Vol. 11, 15432–15450.
15. Ivanova T.P. Estimation of cascading effects of cyber incidents in Smart Grid networks. *Energy and Automation*, 2024, Issue 3, 22–30.
16. Petrov V.V. Risk modeling in complex transport and energy systems. Monograph, KNAHU, Kharkiv, 2024, 215 p.
17. Smart Grid Cybersecurity Strategy Ytand Requirements. NIST IR 7628. URL: https://csrc.nist.gov/ [Accessed 15 Feb.2026]
18. Cybersecurity of Electric Vehicle Charging Infrastructure. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu [Accessed 05 Dec. 2025]
19. Korchenko O.H. *Construction of information protection systems*. Cybersecurity. Textbook, Naukova Dumka, Kyiv, 2023, 512 p.
20. ISO 15118-20:2022. Road vehicles. Vehicle to grid communication interface. Part 20: 2nd generation network and application protocol requirements.
21. Open Charge Alliance — Connecting the EV charging industry. URL: https://www.openchargealliance.org [Accessed 28 Oct. 2025]
22. ISO/SAE 21434:2021. Road vehicles. Cybersecurity engineering.
23. NIST SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security. NIST, 2023, 120 p.
24. IEC 62443-4-2:2019. Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.

25. Analysis of hacker groups' activity in the energy sector of Ukraine in 2024-2025. CERT-UA report. URL: https://cert.gov.ua/ [Accessed 10 Jan. 2026]
26. Methodology for cyber risk assessment of energy enterprises. Ed. Kozlov A.M., Lviv Polytechnic, Lviv, 2024, 140 p.
27. Hnatiuk S.O. Modern methods of counteracting MitM attacks in industrial networks. *Information Security*, 2024, Vol. 26 (2) 88–96.
28. Symonenko R.K. Implementation of the Zero Trust concept in OT environments. *Information Processing Systems*, 2025, Issue 1, 60–68.
29. Danylenko V.M. et al. Specifics of protecting intelligent transport systems under martial law. *Bulletin of KNAHU*, 2025, Issue 104, 45–52.
30. Smyrnov O.V. Authentication mechanisms in V2G networks based on Blockchain technology. *Modern information technologies in the field of security and defense*, 2025, Vol. 53 (2), 114–121.

Received 22.04.2026
Accepted 20.07.2026
Published 25.08.2026

ПОХОДЕНКО Б.О., старш. викл. каф.,
Харківський національний автомобільно-дорожній університет,
вул. Ярослава Мудрого, 25, Харків, 61002, Україна
https://orcid.org/0000-0002-9995-7077
boris.pokhodenko@gmail.com

РОЗРОБКА МОДЕЛЕЙ ОЦІНЮВАННЯ ТА МІНІМІЗАЦІЇ РИЗИКІВ КІБЕРІНЦИДЕНТІВ У ВЗАЄМОПОВ'ЯЗАНИХ СИСТЕМАХ АВТОМОБІЛЬНОГО ТРАНСПОРТУ ТА ЕНЕРГЕТИКИ

Вступ. У роботі проведено комплексне дослідження проблеми забезпечення кіберстійкості інтегрованих екосистем автомобільного транспорту та енергетичної інфраструктури, що стають дедалі більш взаємозалежними внаслідок масового впровадження електромобілів та технологій *Smart Grid*. Доведено, що вразливості у протоколах *ISO/IEC* 15118 та *OCPP* можуть бути використані для ініціювання каскадних відмов, які виходять за межі транспортної мережі та критично впливають на стабільність регіональної енергосистеми. Основним внеском даного дослідження є розробка формалізованої математичної моделі багаторівневого оцінювання ризиків, яка використовує ймовірнісний підхід для кількісного визначення впливу кіберфізичних атак на доступність систем та цілісність даних.

Метою статті провести комплексне дослідження проблеми забезпечення кіберстійкості інтегрованих екосистем автомобільного транспорту та енергетичної інфраструктури та розробити надійні стратегії кібербезпеки в умовах тотальної цифровізації транспортних та енергетичних активів.

Методи. У статті представлено детальний аналіз ландшафту загроз із фокусом на специфічні вектори атак, спрямовані на зарядні станції електромобілів (*EVCS*) та протоколи обміну даними інтерфейсу *Vehicle-to-Grid* (*V2G*).

Результати. У роботі детально описано системну структуру мінімізації ризиків, що інтегрує проактивні та реактивні заходи: від впровадження спеціалізованих систем виявлення вторгнень (*IDS*), оптимізованих для промислових протоколів управління, до реалізації адаптивних алгоритмів управління навантаженням, які нівелюють наслідки зловмисного маніпулювання попитом. Результати моделювання, представлені в дослідженні, підтверджують, що запропонована модель ефективно ідентифікує точки конвергенції з високим рівнем ризику, демонструючи покращення чутливості на 15—20 % порівняно з традиційними фреймворками на базі стандартів *NIST*.

Висновки. Отримані результати формують теоретичну та практичну основу для державних структур та операторів критичної інфраструктури щодо розробки надійних стратегій кібербезпеки в умовах тотальної цифровізації транспортних та енергетичних активів. Розроблені моделі сприяють створенню автономних механізмів захисту, здатних підтримувати операційну безперервність у деструктивних умовах. На відміну від існуючих одновимірних моделей, запропонована методологія враховує взаємопов'язаність вузлів, де порушення безпеки в одному транспортному засобі або точці зарядки виступає каталізатором масштабних енергетичних дисбалансів.

Ключові слова: *кібербезпека, автомобільний транспорт, енергетика, оцінювання ризиків, Smart Grid, V2G, мінімізація ризиків, критична інфраструктура, каскадні ефекти, кіберстійкість.*