Global Research Journal of Social Sciences
Vol 5(5) pp. 001-010 May, 2025.
https://collegiatejournals.us/assd
Copyright © 2025 Collegiate Research Journals

Full Length Manuscript

Cybersecurity in Smart Grids in Lithuania: A Resilience Framework for the Post-Synchronisation Electricity System

Algirdas Kęstutis

Accepted 25th March 2025

Abstract

Lithuania's electricity system has undergone a major structural transition with important consequences for cybersecurity. On 9 February 2025, Lithuania, Latvia and Estonia synchronised their electricity systems with the Continental Europe Synchronous Area, ending the Baltic states' long-standing synchronous operation with the IPS/UPS system controlled from Russia and Belarus [Litgrid, 2025; ENTSO-E, 2025]. At the same time, the continuing digitalisation of transmission and distribution networks, deployment of intelligent metering and distributed energy resources, and increasing dependence on information and communication technologies expand the cyber-physical attack surface of the electricity sector [ENISA, 2012; ENISA, 2016]. This review examines the cybersecurity challenges of Lithuania's smart-grid environment and develops an integrated framework based on asset visibility, IT/OT segmentation, identity and access management, secure remote maintenance, supply-chain security, continuous monitoring, incident response, resilience engineering, and regulatory alignment. Particular attention is given to the interaction between operational technology (OT), SCADA and protection systems; smart meters and Internet-of-Things devices; distributed energy resources; communications; third-party service providers; and cross-border electricity interconnections. The analysis also considers the implications of the EU NIS2 framework and the evolving European energy-sector cybersecurity architecture. The paper proposes a Lithuania-focused maturity model and a set of measurable indicators that can support transmission and distribution system operators, regulators, energy companies, and public authorities. The central finding is that smart-grid cybersecurity should be treated as a continuous resilience function rather than as a conventional information-security perimeter. Lithuania's post-synchronisation environment makes secure interoperability, coordinated incident response, supply-chain assurance, and recovery capability particularly important.

Keywords: Lithuania; smart grid; cybersecurity; operational technology; SCADA; electricity grid; NIS2; critical infrastructure; cyber resilience

1. Introduction

Electricity networks are becoming increasingly dependent on digital technologies. Modern smart grids combine conventional power-system equipment with supervisory control and data acquisition (SCADA), industrial communication networks, intelligent electronic devices, advanced metering, cloud and edge computing, distributed energy resources, automated protection, and data analytics. This digital integration improves observability, flexibility and operational efficiency, but it also creates additional pathways through which cyber incidents can affect physical electricity services [ENISA, 2012; ENISA, 2016]. ENISA identifies energy infrastructure as a critical sector in which disruptions can have cascading effects across society and the economy [ENISA, 2026].

Lithuania provides an important case for studying these issues because its electricity system has recently experienced a fundamental change in its operating environment. On 9 February 2025 at 14:05 EET, Lithuania, Latvia and Estonia synchronised with the Continental Europe Synchronous Area through Poland [ENTSO-E, 2025; Litgrid, 2025]. Before that date, the Baltic electricity systems operated synchronously with the IPS/UPS system, in which frequency control was centrally coordinated from Moscow [Litgrid, 2025]. The synchronisation strengthens regional integration and changes the technical, organisational and cybersecurity context in which Lithuanian grid operators work.

The objective of this article is to develop a Lithuania-focused framework for cybersecurity in smart grids. The paper addresses five questions: (1) what characteristics of Lithuania's electricity transformation affect cyber risk; (2) which smart-grid assets and interfaces create the most significant cybersecurity exposure; (3) how EU and national cybersecurity requirements shape the governance environment; (4) which technical and organisational controls can improve resilience; and (5) how cybersecurity maturity can be measured in practice.

2. Materials and Methods

This manuscript uses a structured narrative-review approach. Primary and authoritative sources were prioritised, including publications from the European Union Agency for Cybersecurity (ENISA), the European Network of Transmission System Operators for Electricity (ENTSO-E), the European Commission, and Lithuania's transmission system operator Litgrid. The review focuses on sources describing smart-grid cybersecurity, energy-sector cyber risk, communication-network interdependencies, NIS2, and the Baltic synchronisation programme. The evidence is synthesised into a conceptual cybersecurity framework rather than a statistical meta-analysis. Because the Lithuanian electricity environment is evolving rapidly after the February 2025 synchronisation, claims about current infrastructure and governance are explicitly tied to the source year.

3. Lithuania's Electricity-System Transformation

3.1 Baltic synchronisation

The February 2025 synchronisation is central to understanding Lithuania's present electricity-security environment. Litgrid reports that the Baltic transmission system operators disconnected from the Russian and Belarusian electricity systems on 8 February 2025 and completed synchronisation with Continental Europe through the LitPol Link on 9 February 2025 [Litgrid, 2025]. ENTSO-E confirmed that the three Baltic states successfully entered the Continental Europe Synchronous Area at 14:05 EET on 9 February 2025 [ENTSO-E, 2025].

Synchronisation is primarily a power-system engineering and energy-security project, but it also has cybersecurity implications. The transition requires dependable control systems, communications, monitoring, protection, time synchronisation, access management, and coordinated incident response across interconnected operators. Lithuania is therefore operating in an environment in which cyber resilience must support both national assets and cross-border system stability.

3.2 Increasing digital dependence

Smart-grid functionality depends on communications and computing systems. ENISA notes that communications networks have become essential to the operation of smart grids and that their interdependencies create additional risks and dependencies [ENISA, 2016]. In practical terms, a cyber incident can affect confidentiality and integrity of data, but in operational technology it can also affect availability, control commands, protection settings, or operator visibility. Consequently, cybersecurity controls must account for safety, real-time constraints, availability requirements and the long life cycles of industrial equipment.

System characteristic	Cybersecurity relevance	Lithuania-specific consideration
Continental European synchronisation	Cross-border operational dependencies and coordinated control	Secure interoperability with Continental Europe and regional TSOs
SCADA/EMS and OT	Compromise may affect physical operations	Protection of high-availability control environments
Smart metering	Large distributed attack surface	Identity, firmware, communications and privacy controls
Distributed energy resources	Many heterogeneous endpoints	Secure inverter, aggregator and remote-management interfaces
Digital substations	Convergence of IT, OT and communications	Segmentation, secure protocols and monitoring
Third-party services	External access can bypass traditional boundaries	Supplier assurance and privileged-access governance

4. Smart-Grid Cybersecurity Threat Landscape

Smart-grid threats should be understood as cyber-physical risks. ENISA's smart-grid work identifies the dependence of power infrastructure on communication networks and highlights risks involving malware, denial-of-service attacks, compromised devices and loss of communications or control [ENISA, 2012; ENISA, 2016]. For Lithuania, the threat model should encompass both direct attacks on energy organisations and indirect attacks through suppliers, communications providers, software, cloud services and connected devices.

4.1 Threat categories

- Ransomware and destructive malware affecting enterprise IT and, where segmentation is weak, pathways toward OT.
- Credential theft and privileged-account compromise involving operators, engineers, contractors or service providers.
- Remote-access abuse through maintenance channels, VPNs, jump servers, engineering workstations or vendor platforms.
- Supply-chain compromise involving software, firmware, managed services, industrial components or update mechanisms.
- Distributed denial-of-service attacks against exposed services or communications infrastructure.
- Manipulation of operational data, including false measurements or altered commands that can mislead operators.

- Compromise of smart meters, IoT devices and distributed-energy-resource interfaces at scale.
- Insider threats and misuse of legitimate administrative privileges.
- Loss or manipulation of time synchronisation, which can affect systems that rely on accurate timing.
- Physical-cyber attacks in which manipulation of digital systems produces consequences in substations, generation, protection or distribution.

4.2 Cyber-physical consequences

The principal difference between smart-grid cybersecurity and conventional enterprise cybersecurity is the possibility of physical consequences. A successful compromise can affect generation dispatch, switching, protection, voltage management, demand response, or operator visibility. The appropriate objective is therefore not absolute prevention of every intrusion; it is layered prevention, rapid detection, containment, safe operation, and recovery.

5. Critical Smart-Grid Assets and Attack Surfaces

Asset/domain	Examples	Primary cyber risks	Priority controls
Transmission OT	SCADA, EMS, RTUs, IEDs, protection systems	Command manipulation, malware, credential abuse	Segmentation, allow-listing, MFA where feasible, monitoring, secure engineering
Distribution OT	RTUs, automation, reclosers, feeder control	Remote compromise, availability attacks	Secure remote access, network zoning, logging, anomaly detection
Smart metering	Meters, head-end systems, concentrators	Mass compromise, fraud, privacy breaches	Device identity, signed firmware, secure communications, lifecycle management
DER/IoT	PV inverters, batteries, EV chargers, aggregators	Botnets, insecure APIs, malicious control	Strong authentication, secure APIs, vendor assurance
Enterprise IT	Email, identity, business systems	Phishing, ransomware, credential theft	EDR, MFA, backup, segmentation, awareness
Supply chain	Vendors, software, firmware, contractors	Backdoors, compromised updates, third-party access	SBOM, contractual controls, provenance, audits
Communications	Fiber, microwave, IP networks, telecom services	DDoS, interception, route disruption	Redundancy, encryption, segmentation, resilient routing

6. Governance and Regulatory Environment

Cybersecurity governance for Lithuanian smart grids exists within the wider EU regulatory architecture. NIS2 (Directive (EU) 2022/2555) strengthens cybersecurity requirements for essential and important entities, expands sectoral coverage, and emphasises risk management, incident reporting, supply-chain security, vulnerability management, and crisis coordination [European Union, 2022; ENISA, 2026]. ENISA describes energy as one of the critical sectors addressed through European cybersecurity policy and supports coordination among energy stakeholders [ENISA, 2026].

For energy organisations, compliance should not be treated as a documentation exercise. Regulatory controls should be translated into engineering requirements, measurable security objectives, tested incident-response procedures and evidence of operational effectiveness. Particular attention should be paid to the relationship

between NIS2 obligations and OT realities, where patching, authentication changes, system restarts and configuration changes can affect operational availability.

7. A Lithuania-Focused Cybersecurity Framework

This paper proposes an eight-layer framework for Lithuanian smart-grid cybersecurity. The layers are complementary and should be implemented as a defence-in-depth architecture.

Layer	Core measures
1. Governance and accountability	Board-level responsibility, risk ownership, OT cybersecurity policy, regulatory mapping and clear authority during incidents.
2. Asset visibility	Continuously maintained inventories of IT, OT, IoT, communications, software versions, owners and critical dependencies.
3. Identity and privileged access	Strong identity assurance, least privilege, privileged-access management, controlled contractor access and credential lifecycle controls.
4. Network and system architecture	IT/OT segmentation, secure zones, controlled conduits, resilient communications and minimised internet exposure.
5. Secure engineering and lifecycle	Secure procurement, configuration baselines, vulnerability management, firmware assurance and change control.
6. Detection and response	OT-aware monitoring, centralised logging where appropriate, anomaly detection, incident playbooks and coordinated escalation.
7. Resilience and recovery	Offline/immutable backups, restoration testing, manual operating procedures, redundancy and recovery-time objectives.
8. Collaboration and learning	Information sharing, exercises, supplier coordination, cross-border cooperation and post-incident lessons learned.

8. Technical Security Measures

8.1 Network segmentation and zero-trust principles

Segmentation is fundamental because compromise of an enterprise endpoint should not automatically create a pathway to critical OT. Networks should be divided into security zones based on operational criticality, with explicitly controlled communication between zones. Remote administration should pass through monitored access points and dedicated jump infrastructure. Where zero-trust principles are applied, trust should be continuously evaluated rather than inferred solely from network location.

8.2 Identity, authentication and privileged access

Identity compromise is a major pathway into both enterprise and industrial environments. High-risk administrative accounts should be individually attributable, tightly scoped, monitored and reviewed. Multi-factor authentication should be used for remote and privileged access where technically and operationally feasible. Shared accounts should be eliminated or tightly controlled, particularly for engineering and maintenance functions.

8.3 Monitoring and anomaly detection

Traditional IT security monitoring is insufficient for many OT environments because industrial protocols and operational processes have different traffic patterns. Monitoring should therefore establish normal baselines for control traffic, engineering changes, authentication events and critical commands. Detection mechanisms should prioritise high-confidence anomalies and avoid creating excessive false alarms that can overwhelm operators.

8.4 Vulnerability and patch management

Industrial equipment may remain operational for many years and may not support conventional patching. A risk-based process should classify assets according to criticality, exposure, exploitability and compensating controls. Where patching cannot safely occur, organisations should use isolation, application control, monitoring, vendor-supported mitigations and strict access restrictions.

8.5 Backup and recovery

Cyber resilience requires recovery from successful compromise. Critical configurations, protection settings, system images, certificates, keys and essential operational documentation should be backed up securely. Restoration procedures should be tested, including scenarios in which identity infrastructure or central management systems are unavailable.

9. Smart Meters, IoT and Distributed Energy Resources

The expansion of distributed energy resources changes the scale and diversity of the electricity attack surface. Smart meters, photovoltaic inverters, battery systems, electric-vehicle chargers and aggregator platforms can introduce thousands or millions of endpoints. ENISA has specifically examined cybersecurity demand and supply for IoT in distribution grids, underscoring the importance of securing distributed devices [ENISA, 2022].

A Lithuanian security architecture should therefore require device identity, secure onboarding, authenticated communications, signed or otherwise integrity-protected firmware updates, vulnerability disclosure mechanisms, defined support lifetimes and controlled remote administration. Procurement should assess not only the initial security posture of devices but also whether suppliers can maintain security throughout the device lifecycle.

10. Supply-Chain Cybersecurity

Smart grids rely on complex supply chains involving equipment manufacturers, software developers, telecommunications providers, cloud services, engineering firms and maintenance contractors. ENISA identifies supply-chain security as an important component of modern cybersecurity governance, while NIS2 explicitly strengthens supply-chain risk management [ENISA, 2025; European Union, 2022].

Contracts should establish minimum security requirements, incident-notification obligations, secure development expectations, vulnerability disclosure processes, access-control rules, audit rights, software provenance and end-of-life responsibilities. For critical software, organisations should maintain software bills of materials (SBOMs) or equivalent component visibility where feasible. Vendor remote access should be time-limited, attributable and monitored.

11. Incident Response and Regional Coordination

Because electricity systems are interconnected, a major cyber incident can have consequences beyond a single organisation. Lithuania's post-synchronisation environment makes coordination with neighbouring Baltic transmission and distribution operators and Continental European partners especially important. ENISA emphasises cooperation and information sharing across the energy cybersecurity community [ENISA, 2026].

Incident-response plans should include both cyber and power-system scenarios. Exercises should test loss of SCADA visibility, compromise of engineering workstations, malicious configuration changes, ransomware in enterprise environments, compromised third-party access, loss of telecommunications, and coordinated cyber-physical disruption. Exercises should also test decision-making under degraded information rather than assuming that all digital systems remain available.

12. Cybersecurity Maturity Model for Lithuanian Smart Grids

Level	Characteristics	Indicative evidence
1 – Initial	Ad hoc controls; incomplete asset visibility; reactive incident handling	Unmaintained inventories; informal procedures
2 – Managed	Documented policies and basic IT/OT separation	Asset registers; access reviews; backups
3 – Defined	Standardised controls integrated into operational processes	Formal OT security architecture; supplier requirements
4 – Measured	Continuous monitoring and risk-based performance measurement	OT telemetry; tested recovery; KPIs/KRIs
5 – Adaptive	Threat-informed, continuously improving resilience	Regular exercises; predictive risk analysis; lessons integrated into engineering

13. Key Performance and Risk Indicators

Indicator	Possible metric	Purpose
Asset visibility	% of critical OT assets inventoried and owner-assigned	Measures foundational visibility
Privileged access	% of privileged accounts with MFA/strong authentication	Measures identity risk reduction
Remote access	% of vendor sessions recorded and time-limited	Measures third-party exposure
Vulnerability management	Critical vulnerabilities past agreed remediation window	Measures exposure
Detection	Median time to detect defined OT anomalies	Measures monitoring capability
Response	Median time from detection to containment	Measures response effectiveness
Recovery	% of critical systems with tested restoration procedures	Measures resilience
Exercises	Number and scope of cyber-physical exercises per year	Measures preparedness
Supply chain	% of critical suppliers assessed	Measures third-party governance

	against security requirements	

14. Discussion

The Lithuanian case illustrates that smart-grid cybersecurity is inseparable from energy-system transformation. The February 2025 synchronisation did not create cybersecurity risk by itself; rather, it changed the operational context and the set of relationships in which cyber risk must be managed. Lithuania now operates synchronously within the Continental Europe Synchronous Area, making secure interoperability and regional resilience central considerations [Litgrid, 2025; ENTSO-E, 2025].

A second implication is that cybersecurity investment should follow system criticality rather than technology novelty. A highly visible smart-meter programme may attract attention, but a less visible engineering workstation, protection-system interface, identity service, or vendor access pathway can also become a critical dependency. Asset inventories and dependency maps are therefore prerequisites for sensible investment decisions.

Third, cybersecurity and reliability engineering should converge. Controls that reduce cyber risk but introduce unacceptable operational instability are not appropriate for critical OT. Conversely, reliability measures that create unmanaged remote-access channels or excessive technical privilege can increase cyber risk. The appropriate approach is joint engineering governance involving cybersecurity, control engineering, operations, telecommunications and safety personnel.

15. Research Agenda

- Develop empirical inventories of Lithuanian smart-grid attack surfaces and critical cyber dependencies.
- Evaluate cybersecurity architectures for distributed energy resources, EV charging infrastructure and aggregators in Lithuania.
- Study the effectiveness of OT anomaly-detection techniques under realistic Lithuanian grid traffic conditions.
- Assess cybersecurity implications of cross-border operational dependencies following Baltic synchronisation.
- Develop secure-by-design procurement requirements for smart meters, grid-edge devices and industrial control equipment.
- Measure the relationship between cybersecurity maturity and electricity-system reliability or restoration performance.
- Develop cyber-physical exercises that combine technical attacks with realistic power-system contingencies.
- Investigate privacy-preserving security mechanisms for advanced metering and consumer energy data.

16. Practical Recommendations

Maintain a continuously updated inventory of critical IT, OT, IoT and communication assets and their dependencies.
Separate enterprise IT from operational networks using clearly defined zones, controlled conduits and monitored gateways.
Strengthen privileged-access governance, especially for engineering and third-party maintenance accounts.
Require security-by-design and lifecycle security in procurement of smart meters, DER equipment and industrial systems.

Implement OT-aware detection and response rather than relying exclusively on enterprise security tooling.
Test recovery from cyber incidents, including restoration of configurations and operation when central digital services are unavailable.
Conduct joint cyber-power exercises with relevant Lithuanian and regional stakeholders.
Translate NIS2 and other regulatory obligations into measurable engineering controls and operational evidence.
Develop supplier-security requirements that cover software provenance, vulnerabilities, remote access, incident reporting and end-of-life support.
Use maturity metrics and risk indicators to direct investment toward the most consequential dependencies.

17. Limitations

This is a review and conceptual framework rather than an empirical security assessment of a specific Lithuanian operator. Detailed architectural information about critical electricity infrastructure is not publicly available and should not be inferred. The paper also does not claim that the controls proposed here are uniformly applicable to every Lithuanian energy organisation; requirements should be adapted to asset criticality, operational constraints, regulatory obligations and risk assessments. Finally, the electricity and cybersecurity environment is evolving rapidly, so future studies should update the evidence base as post-synchronisation operational experience develops.

18. Conclusion

Lithuania's smart-grid cybersecurity challenge is shaped by three interacting trends: increasing digitalisation of electricity networks, expansion of distributed and connected energy technologies, and the country's integration into the Continental Europe Synchronous Area in February 2025. These developments increase the importance of secure communications, resilient operational technology, trustworthy supply chains, controlled remote access, effective monitoring and coordinated incident response.

A resilient Lithuanian smart-grid cybersecurity strategy should therefore move beyond perimeter defence and compliance checklists. It should treat cybersecurity as a continuous cyber-physical resilience capability covering governance, asset visibility, identity, architecture, secure engineering, detection, response, recovery and collaboration. The framework proposed in this paper provides a practical basis for future empirical research and for organisations seeking to translate European cybersecurity expectations into measurable protection of Lithuania's electricity infrastructure.

References

ENISA. (2012). Smart Grid Security: Recommendations for Europe and Member States. European Union Agency for Cybersecurity.

ENISA. (2016). Communication Network Interdependencies in Smart Grids. European Union Agency for Cybersecurity.

ENISA. (2022). EU Cybersecurity Market Analysis: IoT in Distribution Grid. European Union Agency for Cybersecurity.

ENISA. (2024). 2024 Report on the State of Cybersecurity in the Union. European Union Agency for Cybersecurity.

ENISA. (2025). Supporting NIS2 implementation through actionable guidance. European Union Agency for Cybersecurity.

ENISA. (2026). Energy: Cybersecurity of Critical Sectors. European Union Agency for Cybersecurity.

ENTSO-E. (2025). ENTSO-E confirms successful synchronization of the Continental European electricity system with the systems of the Baltic countries. European Network of Transmission System Operators for Electricity.

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union.

European Commission. (2023). Commission, Baltic States and Poland commit to accelerated Baltic grid synchronisation with Continental Europe. Directorate-General for Energy.

Litgrid. (2025). Synchronisation. Lithuanian electricity transmission system operator.

Litgrid. (2025). Estonian, Latvian and Lithuanian power systems successfully synchronised with Continental Europe. Lithuanian electricity transmission system operator.