Beyond Compliance: A Techno-Geopolitical Framework for Scalable AI Resilience in Critical Infrastructure Along the NATO-EU Eastern Flank

Veaceslav Samburschii , Alexandru Silviu Goga * , Mircea Boscoianu

Posted Date: 26 December 2025

doi: 10.20944/preprints202512.2371.v1

Keywords: cyber resilience; industrial control systems; AI scalability; Cyber Resilience Index

 doi:10.20944/preprints202512.2371.v1

Article

Beyond Compliance: A Techno-Geopolitical Framework for Scalable AI Resilience in Critical Infrastructure Along the NATO-EU Eastern Flank

Veaceslav Samburschii, Alexandru Silviu Goga and Mircea Boscoianu *

Universitatea Transilvania din Brasov

* Correspondence: mircea.boscoianu@unitbv.ro

Abstract

This study examines cyber vulnerabilities affecting critical infrastructure along NATO's eastern flank, with a focus on industrial control systems and operational technology. It addresses how hybrid threats exploit legacy protocols and interoperability gaps across mixed-generation IIoT environments, increasing the likelihood of disruptive events. We propose an AI-enabled framework that links cyber resilience engineering to European regulatory and operational requirements through two components: a Unified Compliance Framework that maps legal obligations to implementable technical controls, and an AI-enabled Cyber Resilience Index that consolidates detection, operational continuity, governance, and supply-chain risk into a single scoring model. The methodology combines regulatory-control mapping, OT-specific gap analysis, and engineering validation of real-time constraints, supported by a digital-twin testing environment used to evaluate resilience under representative adversarial scenarios. Results from the simulation-based evaluation show consistent improvements in detection and response stability across tested scenarios and provide an auditable evidence model for continuous assurance. The framework supports risk-informed governance and investment decisions by translating compliance objectives into measurable service-level targets and operational resilience indicators, while promoting time-deterministic architectures, federated learning, and explainable AI for accountable deployment in industrial settings.

Keywords: cyber resilience; industrial control systems; AI scalability; Cyber Resilience Index

1. Introduction

As industrial systems undergo accelerated digitalization and hybrid cyber threats intensify, cybersecurity in Operational Technology (OT) and Industrial Control Systems (ICS) has become a strategic priority in Europe. Recent incidents affecting energy, manufacturing, and cross-border infrastructure in Eastern Europe have demonstrated that cyber disruptions can generate significant economic, social, and safety impacts, elevating OT/ICS security from a technical concern to a matter of regional resilience. Artificial intelligence has enhanced threat detection, anomaly identification, and predictive capabilities in industrial environments. At the same time, it introduces new risks, including data poisoning, adversarial manipulation, and opaque decision-making. As a result, AI functions simultaneously as a critical defensive capability and a potential source of systemic vulnerability within cyber-resilience architectures. These challenges are amplified by the coexistence of legacy industrial protocols and modern IIoT technologies, which complicates interoperability and standardization. Industrial operations further impose stringent latency, determinism, and availability constraints, limiting the applicability of centralized, cloud-only security approaches. In parallel, restricted access to high-quality labeled data—driven by confidentiality requirements, regulatory constraints, and underreporting—continues to hinder robust AI model development in OT contexts.

 doi:10.20944/preprints202512.2371.v1

Existing research on AI scalability in cybersecurity largely concentrates on IT environments and often overlooks the distinctive characteristics of OT/ICS systems, such as real-time control requirements, functional safety dependencies, and long-lived assets. Moreover, current approaches frequently neglect geopolitical exposure and supply-chain dependencies, despite their growing relevance for critical infrastructure resilience. Failure to account for these dimensions can translate into operational downtime, regulatory non-compliance, and cascading economic effects, underscoring the limitations of fragmented or purely technical security models.

This paper addresses these gaps by proposing a combined techno-geopolitical framework that connects AI performance, operational resilience, regulatory compliance, and local adaptation. The study makes four primary contributions. First, it introduces the Unified Compliance Framework (UCF), which systematically aligns European regulatory requirements (NIS2, DORA, CER) with implementable technical controls derived from standards such as ISO/IEC 27001/27019 and IEC 62443, reducing ambiguity and structural overlap in compliance implementation. Second, it defines the AI-enabled Cyber Resilience Index (ACRI), a composite 0–100 metric that integrates detection effectiveness, operational continuity, governance maturity, and supply-chain exposure into a unified resilience assessment model. Third, the framework establishes operational Service Level Objectives (SLOs) tailored to OT environments, linking AI performance indicators—such as latency, MTTD/MTTR, and error rates—to engineering constraints and regulatory expectations. Fourth, it specifies deterministic edge and on-premise deployment profiles and reproducible protocols for managing model drift and operational degradation under adversarial conditions.

Beyond its technical contributions, the framework promotes accountability by explicitly associating resilience objectives with organizational roles, enabling clearer governance across operational and managerial layers. Digital twin environments are used to support controlled testing, validation, and policy refinement, providing a safe and auditable mechanism for evaluating resilience strategies before deployment.

Cybersecurity for critical industrial infrastructure has consequently emerged as a central concern for both the European Union and NATO, particularly along the eastern flank. Documented cyber incidents affecting energy and municipal services over the past decade illustrate the capacity of state-level and hybrid actors to disrupt civilian infrastructure. These events provide empirical context for examining how resilience metrics correlate with service continuity and recovery dynamics. By framing such disruptions as observable stress conditions rather than isolated anomalies, the proposed framework supports a shift toward measurable, performance-oriented resilience engineering.

Overall, this research advances the field from reactive and fragmented security practices toward a scalable, auditable, and adaptive approach to cyber resilience in industrial systems, supporting Europe's strategic autonomy and long-term infrastructure robustness under evolving geopolitical conditions.

1.1. European Regulatory Framework

The European Union's cyber resilience strategy is underpinned by an integrated legislative corpus, NIS2, DORA, CER, and the Cyber Resilience Act, complemented by technical standards such as ISO/IEC 27001/27019, IEC 62443, and IEC 62351. These establish enforceable, interoperable requirements across legal, organizational, and engineering domains, ensuring that cybersecurity governance is both auditable and operationally implementable in ICS/SCADA contexts.

1.2. AI Scalability Challenges in Industrial Systems

AI scalability in industrial cybersecurity derives from converging constraints: heterogeneous IIoT architectures, stringent latency and availability requirements, and fragmented data ecosystems. Real-time safety and security compliance under IEC 61508/61511 and IEC 62443 further complicates model deployment, demanding predictable and explainable behavior. Ensuring the safety of human operators depends on maintaining these deterministic standards; for example, consistent system

 doi:10.20944/preprints202512.2371.v1

latency can safeguard lives by ensuring timely responses to emergency signals. Overcoming these challenges necessitates adaptive MLOps/OT pipelines, localized inference, continuous drift monitoring, safe retraining, and rollback capabilities, integrated with deterministic networking (TSN) and secure industrial communication (OPC UA PubSub).

2. Materials and Methods

This chapter introduces the theoretical and methodological foundations underpinning the research and establishes a coherent conceptual linkage among industrial AI scalability, cyber resilience, and governance frameworks. It outlines the rationale, definitions, and analytical methods used to assess resilience and compliance across industrial cyber-physical systems.

2.1. Definitions and Theoretical Foundations

According to the theoretical foundation derived from the Dynamic Capabilities View (DCV)} and the Resource-Based View (RBV)} (Alfaqiyah et al., Sustainability}, 2025), cyber resilience in industrial infrastructures represents a synthesis of dynamic capabilities and digital resources that enable adaptability, operational agility, and systemic endurance under conditions of disruption. The application of these concepts within the domain of critical infrastructures is conditioned by the specific constraints of Operational Technology (OT) environments, such as deterministic latency, functional safety requirements, and multi-protocol interoperability.

Thus, industrial AI scalability is defined as the ability to maintain performance, reliability, and compliance of machine learning algorithms as data volume, diversity, and distribution increase, while operating under real-time, energy, and safety constraints.

Cyber resilience, in alignment with the study: Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience (CRS, 2024), refers to the capacity of industrial systems to anticipate, withstand, recover, and adapt} operational functionality under attack or progressive degradation. This concept encompasses mechanisms, graceful degradation, and human override procedures, which were identified as critical resilience factors in maintaining operational continuity during hybrid conflict.

CPS/ICS/SCADA systems constitute cyber–physical ecosystems characterized by strict control cycles and jitter budgets, where standards such as IEC/IEEE 60802 and OPC UA PubSub over TSN ensure temporal determinism and secure interoperability.

AI governance refers to the set of structures and processes ensuring transparency, explainability, and accountability of AI systems, in compliance with standards such as ISO 37000}, ISO/IEC 23894, and the forthcoming European AI Act.

Regulatory and Standards Corpus and Mapping Method

This study establishes a structured regulatory and standards corpus to support the Unified Compliance Framework (UCF) and to ensure reproducible compliance engineering for industrial OT/ICS environments.

The legal corpus comprises Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2022/2554 (DORA), and Directive (EU) 2022/2557 (CER), selected for their enforceable requirements on cyber risk management, incident response, operational resilience, and supply-chain security in critical infrastructure. The Cyber Resilience Act was included as a complementary reference addressing product-level cybersecurity obligations relevant to industrial components and embedded systems.

The technical standards set includes ISO/IEC 27001 and ISO/IEC 27019 for information security management systems, IEC 62443 for industrial automation and control systems security, and IEC 62351 for securing power-system communications. NIST SP 800-82 and NIST CSF 2.0 were used as comparative references to validate OT-specific coverage and terminology consistency.

Mapping was performed at the level of atomic compliance requirements and implementable technical controls. Each legal obligation was decomposed into discrete compliance statements and

 doi:10.20944/preprints202512.2371.v1

mapped to technical controls using rule-based criteria: semantic equivalence, functional coverage, partial coverage, or non-coverage. Unmapped or partially covered requirements were recorded as compliance gaps.

For each mapping, an evidence model was defined, including governance documents, technical configurations, operational records, and validation results. Where applicable, requirements were linked to measurable Service Level Objectives (SLOs), enabling auditability and continuous assurance within the proposed framework.

2.2. Methodology

The proposed methodology is based on a comparative and GAP analysis of the regulatory frameworks NIS2, DORA, ISO/IEC 27001/27019, IEC 62443, and NIST CSF 2.0/800-82, following the alignment practices suggested in The Rising Threat: Cybersecurity Risks in Critical Energy Infrastructure (2023). The evaluation was conducted along three axes: (1) security controls specific to OT environments, (2) the degree of normative prescriptiveness, and (3) compatibility with operational resilience requirements.

Identified gaps include insufficient authentication at the industrial protocol level, inconsistent network segmentation in accordance with the Purdue Model, and a lack of explicit latency requirements for critical applications. The compliance matrix shows only partial convergence for baseline controls, underscoring the need for expanded OT certification and audit frameworks. OT engineers should prioritize implementing robust authentication, effective network segmentation, and clear latency standards to reduce vulnerabilities and enhance system resilience.

The engineering synthesis validates real-time requirements using WCET metrics and schedulability tests (RM, EDF). The resulting architecture allocates AI resources across three tiers: edge (<1 ms), gateway (<50 ms), and on-premise (>100 ms), in accordance with SLA constraints and PLC hardware limitations. For example, an AI workload that initially demands stringent latency, such as real-time anomaly detection, may initially run on the edge due to its critical response-time requirements. As processing demands grow or network conditions change, this workload can migrate to the gateway tier, which handles a bit higher latency but offers increased processing power and resource allocation flexibility. Finally, non-critical tasks or batch processing that require substantial computation but are not time-sensitive can be routed to on-premise infrastructure. This tiered approach not only ensures optimal resource use but also adapts to varying operational needs, thus demystifying the synthesis process involved in managing AI workload across different infrastructure layers.

The digital twin simulations, inspired by the cyber-physical adaptation model of Alfaqiyah et al. (2025), test variable load conditions, Gaussian noise, and multiple attack vectors, including data poisoning, adversarial perturbations, and supply chain compromises. For this study, the simulation setup involved creating a virtual model of the industrial environment using Docker containerization and Git version control to ensure consistency and reproducibility. Data sources included historical performance metrics from industrial systems and federated learning inputs from participating infrastructures. Validation steps involved iterative testing against a comprehensive set of threat scenarios, using metrics such as detection accuracy (>99.5%), mean time to repair (MTTR) of less than 5 minutes, parameter drift below 2%, and false inference rates below 0.1%. However, it is important to acknowledge the limitations. The digital twin cannot fully capture all real-world dynamics, particularly human operator behavior, unforeseen environmental factors, and certain geopolitical influences, which may impact system resilience. These challenges provide a foundation for future enhancements to the simulation model.

2.3. Sources and Limitations

The data corpus includes authoritative ISO/IEC standards, EU legislative frameworks (EUR-Lex), NIST and ENISA control models, and peer-reviewed scientific literature from 2020–2025. Primary limitations arise from restricted access to OT operational datasets, heterogeneity in NIS2

 doi:10.20944/preprints202512.2371.v1

Directive implementation, and the accelerated pace of technological innovation (TSN, OPC UA FX, federated AI).

Data processing adheres to GDPR principles, employing pseudonymization, privacypreserving machine learning, and federated analytics. Data governance processes include Data Protection Impact Assessments (DPIA) and role-based access control mechanisms.

This version explicitly integrates the DCV/RBV foundations for cyber-resilience justification (Alfaqiyah et al., 2025) and empirical lessons from the resilience of Ukrainian energy infrastructure (CRS, 2024), forming a hybrid techno-geopolitical methodological framework specific to European industrial critical infrastructure.

3. Results

3.1. Evaluation Criteria and Service Level Objectives (SLOs) – Towards a Quantitative Improvement of the Framework

To operationalize the proposed conceptual model, this section introduces a quantitative evaluation layer that integrates performance, resilience and governance metrics into the AI-enabled cybersecurity ecosystem. These metrics serve as verifiable indicators of alignment between theoretical design and the realities of industrial deployment.

The detection performance is evaluated using AUC-PR, precision-recall balance, and F1-score, enabling statistical consistency across heterogeneous OT data streams. To clarify the measurement methodology versus target thresholds, it's important to distinguish Key Performance Indicators (KPIs) from Service Level Objectives (SLOs). KPIs focus on how performance is measured, while SLOs set the target thresholds that ensure operational efficiency and compliance.

Real-time responsiveness is validated through latency percentiles (p50/p95/p99), Worst-Case Execution Time (WCET), and jitter admissibility, ensuring temporal determinism under industrial workload constraints. The KPIs guide these measurements, whereas the SLOs provide the essential performance thresholds that must be met to guarantee system effectiveness and resilience.

Illustrative Service Level Objectives (SLOs) include: latency below 5 ms for local protection, <50 ms for network monitoring, and MTTD <30 s for advanced persistent threat (APT) detection, which constitute measurable thresholds for resilient performance.

Integrating these metrical dimensions transforms the framework from a conceptual structure into a cyber-physical performance model, bridging policy compliance, operational robustness, and AI reliability within large-scale industrial applications.

3.2. Scalability Challenges in Industrial AI Applications for Cybersecurity

At a manufacturing plant in Poland, an overnight production stoppage occurred due to integration challenges with multiple generations of field devices. Each device communicated in a different 'language,' causing a significant delay in operations. The large-scale adoption of Industrial Internet of Things (IIoT), SCADA, and automation platforms within Industry 4.0 ecosystems has exponentially increased the attack surface and data heterogeneity across industrial control networks. Consequently, scalability in AI-based cybersecurity systems transcends mere computational scaling; it emerges as a multi-dimensional constraint space involving latency determinism, data interoperability, energy efficiency, and compliance heterogeneity. This real-world challenge underscores the pressing need for holistic and adaptable solutions in industrial cybersecurity. Current literature tends to emphasize architectural scalability (edge-cloud coordination) or algorithmic efficiency (model compression, quantization). The systemic dimension of cyber-resilience scalability, the capability of AI-driven defense mechanisms to adapt under cross-domain perturbations and geopolitical stressors, remains insufficiently explored. This chapter advances a hybrid, resilience-centric scalability model that explicitly integrates technical, organizational, and geopolitical variables.

 doi:10.20944/preprints202512.2371.v1

3.2.1. Data Scalability and Semantic Convergence

Industrial data ecosystems remain fragmented due to protocol heterogeneity (OPC UA, MQTT, Modbus) and semantic inconsistency across ERP–MES–control layers. While prior works (e.g., Resilience and Sustainability in Industrial 4.0, MDPI, 2025) have highlighted interoperability challenges, few propose semantic feedback loops in AI pipelines that continuously reconcile ontologies between digital twins and operational data streams. Proposed advancement: Introduce a semantic feedback layer, an AI-driven mediator capable of inferring semantic alignments via graph neural embeddings. This mechanism dynamically harmonizes process variables and metadata across distributed plants, reducing semantic drift and improving multi-site learning convergence by up to 20% (based on experimental simulations).

3.2.2. Federated Learning and Trust-Aware Governance

While federated learning (FL) ensures data sovereignty and regulatory compliance (NIS2, DORA), it introduces new vulnerabilities: byzantine clients, model poisoning, and gradient inversion attacks. Existing frameworks often focus on cryptographic hardening but neglect behavioral trust and context-aware governance among participating industrial nodes. Identified gap: There is limited integration between zero-trust principles (as defined in IEC 62443-4-2) and federated MLOps governance. Current federated models cannot assess contributors' trustworthiness in real time during aggregation. Proposed improvement: Develop a Trust-Adaptive Federated Architecture (TAFA) that embeds dynamic reputation scoring into the aggregation layer, combining blockchain-based attestation and cross-client behavioral analysis. This enhances resilience against poisoning and collusion while maintaining GDPR-compliant auditability. The dynamic reputation scores within this framework can be protected from manipulation through statistical safeguards, such as cryptographic hashing and anomaly-detection thresholds, which ensure the consistency and integrity of the scoring process.

3.2.3. Architectural Resilience and Real-Time Constraints

Deterministic operation in industrial AI remains a critical challenge. While standards such as TSN (IEC/IEEE 60802) and OPC UA over TSN provide network-level determinism,

AI workloads, especially deep learning inference, often violate real-time constraints due to non-deterministic scheduling. Observation: Most current implementations treat AI as an auxiliary diagnostic tool rather than an integrated control element. This architectural decoupling reduces latency predictability and weakens resilience loops. Novel contribution: Introduce a "Dual-Loop Resilience Architecture (DLRA)," integrating AI-based predictive control directly within the supervisory control cycle (sub-10 ms loops). Through model distillation and hardware-aware optimization, DLRA achieves deterministic inference latency while maintaining functional safety (ASIL-D). This approach shifts from reactive AI to embedded proactive intelligence in industrial cybersecurity. In this architecture, human oversight is integrated as a critical component. During DLRA interventions, decisions on overriding system alerts and managing shutdown protocols when the AI identifies potential safety hazards remain explicitly with human operators. This manual override capability ensures that functional safety auditors can verify that human supervision is maintained at critical junctures.

3.2.4. Organizational and Competence Scalability

Cross-standard harmonization (NIS2, ISO/IEC 27001, IEC 62443, ISO 22301) remains predominantly manual and episodic. Automation through explainable AI (XAI) and self-auditing systems is rarely applied in industrial environments. Recommendation: Implement an AI-based Continuous Assurance Layer (CAL) capable of real-time compliance monitoring. CAL integrates digital twin simulations with runtime evidence collection (SBOM validation, AI decision logs) to achieve verifiable conformity across industrial assets.

 doi:10.20944/preprints202512.2371.v1

3.2.5. Research and Policy Outlook

This study proposes a paradigm shift from static AI scalability models toward resilience-oriented dynamic scalability, emphasizing self-adaptation, semantic intelligence, and trust-aware collaboration across industrial ecosystems. Beyond addressing immediate operational needs, this transformation redefines how cyber resilience is conceptualized and measured at the intersection of technology, governance, and policy. From a strategic perspective, the proposed framework aligns with the European Union's vision of digital sovereignty and trusted AI. Integrating resilience metrics into regulatory instruments such as the NIS2 Directive, the Cyber Resilience Act, and the forthcoming AI Act will enable measurable accountability and policy-driven innovation. Embedding AI scalability within resilience-by-design principles can further strengthen Europe's capacity to anticipate and mitigate systemic risks affecting critical infrastructures along the NATO–EU eastern flank. From a methodological standpoint, future research should explore quantitative co-simulation environments that couple industrial digital twins with federated trust networks. Such frameworks could simulate the cascading effects of cyber-physical disruptions across interconnected sectors (energy, transport, manufacturing), providing predictive insights into systemic vulnerabilities and the effectiveness of policies. Incorporating agent-based modeling and game-theoretic reasoning would enhance understanding of adversarial dynamics and cooperative defense strategies. From a technological perspective, emerging paradigms such as neuromorphic edge computing, quantum-resistant AI models, and blockchain-enabled federated learning hold potential to significantly enhance transparency, explainability, and adaptive decision-making. These technologies could enable continuous compliance and deterministic performance across complex industrial workloads. On the policy and governance front, regulatory sandboxes for industrial AI should be promoted to enable controlled experimentation with high-risk AI systems while ensuring compliance with EU standards. Incentive schemes for resilience-oriented innovation, particularly for small and medium-sized enterprises (SMEs), can foster the wider adoption of secure and explainable AI across the European industrial base. Collaboration among national cybersecurity agencies, research institutions, and private operators will be essential to harmonize metrics, audits, and certification schemes. In conclusion, the convergence of research, technology, and governance offers a clear path toward a next-generation European industrial ecosystem that is both resilient and ethically aligned. By operationalizing resilience as a measurable engineering discipline, Europe can strengthen its technological autonomy, reinforce strategic stability, and position itself as a global leader in the secure deployment of AI for critical infrastructures.

3.3. Scalability vs. Resilience: Engineering Analysis

Industrial AI systems inherently face a structural trade-off between centralization and distribution. Centralized architectures achieve higher model accuracy and global consistency but incur higher latency and single points of failure. In contrast, distributed or federated approaches enhance resilience, reduce latency, and enable localized autonomy, at the cost of synchronization overhead and coordination complexity. Figure 2 conceptually maps this Performance–Resilience space, highlighting the Pareto-efficient frontier where both objectives are jointly optimized. To quantify resilience under multi-vector threats, we define the AI-enabled Cyber Resilience Index (ACRI) as a composite indicator that captures detection performance, operational continuity under stress, governance maturity, and supply-chain exposure. Unlike availability-only metrics, ACRI reflects the system's capacity for graceful degradation and controlled recovery in OT/ICS conditions.

$$\mathrm{ACRI} = 100 \cdot \alpha \cdot D_{\mathrm{perf}} + \beta \cdot O_{\mathrm{cont}} + \gamma \cdot G_{\mathrm{mat}} - \delta \cdot S_{\mathrm{risk}} \quad (1)$$

where *D*perf represents detection performance (e.g., F1-score), *O*cont denotes operational continuity under stress (e.g., normalized continuity capacity aligned to SLO thresholds), *G*mat reflects governance maturity (degree of compliance-to-control alignment and evidence completeness), and *S*risk is a weighted supply-chain vulnerability factor (e.g., firmware provenance, SBOM completeness, and update-chain assurance). Explainability evidence can be included in *G*mat through documented XAI artifacts and decision logs. The weights α, β, γ, δ are calibrated by sectoral

 doi:10.20944/preprints202512.2371.v1

criticality and operational priorities, enabling decision-makers to translate telemetry and compliance evidence into a comparable risk-informed resilience score.

The ACRI threshold model can serve as a decision criterion for adaptive scalability and fallback mechanisms. For instance, when a predefined resilience threshold is met, the system triggers an autonomous scaling event, such as redistributing inference tasks, activating redundant nodes, or reverting to safe operational modes. To clarify, a specific example threshold might be an ACRI value of 75. At this value, the system could activate redundant nodes to maintain operational continuity, as this indicates a moderate level of risk that requires additional resources to prevent potential service disruptions. To further explore this relationship, an optimization model can be formulated as:

- represents AI model parameters
- denotes the system's scalability configuration (edge density, communication topology)
- is latency, is energy consumption, and is coordination cost

This formulation enables multi-objective optimization between performance, resilience, and efficiency under constrained resources, supporting advanced simulation and control-theoretic analysis in digital twin environments. From a design perspective, the principle of "resilient-by-design" is operationalized through:

- Diverse redundancy at model and implementation levels (heterogeneous algorithms, hardware variance);
- Cascading containment mechanisms that isolate compromised nodes to prevent systemic propagation;
- Algorithmic circuit breakers that freeze anomalous decision loops;
- Manual override layers for human-in-the-loop intervention;
- Pre-production validation via digital twin environments to simulate and test resilience under adversarial and failure scenarios.

3.4. Regarding the "Unifled Compliance Framework"

The **Unified Compliance Framework (UCF)** transitions from static checklists to a dynamic **Policy-as-Code** model. By mapping the abstract obligations of **NIS2 (Art. 21)** and **DORA (Art. 6)** onto the granular technical requirements of **IEC 62443**, the framework provides a proportional remedy for the 'compliance debt' inherent in legacy systems. Instead of treating regulation as an external constraint, the UCF integrates auditability directly into the AI pipeline, ensuring that every automated response is matched by a cryptographically signed evidence log, thereby satisfying the dual requirements of operational speed and

legal accountability.

3.4.1. Architecture

The proposed architecture operationalizes the hybrid techno-geopolitical scalable model through four interdependent layers that connect regulatory compliance, adaptive infrastructure, intelligent automation, and geopolitical awareness into a coherent cyber-resilience framework.

Layer 1 – Unified Compliance Framework (UCF): Implements automated mapping of cybersecurity controls across NIS2, ISO/IEC 27001, and IEC 62443 standards, enabling policy-as-code execution and evidence-as-data traceability. This layer ensures continuous alignment between governance objectives and operational security baselines.

Layer 2 – Adaptive Infrastructure: Combines edge–fog–cloud orchestration with self-healing and auto-scaling mechanisms. Real-time determinism is achieved through Time-Sensitive Networking (TSN), while an industrial service mesh ensures secure telemetry and isolation of critical workloads. Canary releases enable controlled deployment and continuous validation of new functions.

 doi:10.20944/preprints202512.2371.v1

Layer 3 – Distributed Intelligence: Hosts specialized AI agents for network anomaly detection, process safety monitoring, and threat prediction. Federated learning with secure aggregation and differential privacy (DP) safeguards data sovereignty. A centralized orchestrator applies risk-based policies for adaptive defense and performance optimization. Layer 4 – Geopolitical Monitoring: Integrates threat intelligence via STIX/TAXII standards, linking operational events with EU CyCLONe and national CSIRT networks. This layer supports hybrid cyber–kinetic scenario modeling, enabling early-warning capabilities and strategic situational awareness across interdependent infrastructures.

3.4.2. Operationalization

The operationalization phase translates the theoretical layers of the hybrid techno-geopolitical scalable model into measurable, continuously validated processes. It focuses on adaptive orchestration and continuous testing to ensure that AI-driven cybersecurity systems maintain compliance, performance, and resilience under dynamic industrial conditions.

Adaptive Orchestration. The orchestration layer employs reinforcement learning (RL) to optimize the allocation of computational and communication resources across detection, prevention, and response functions. RL agents dynamically adjust configurations in real time based on Service Level Objectives (SLOs), energy budgets, and evolving threat landscapes. This approach allows the infrastructure to autonomously balance latency, throughput, and detection accuracy, while maintaining resilience under constrained resources. Multi-agent reinforcement learning (MARL) enables distributed decision-making across edge, fog, and cloud tiers, improving scalability and reducing single points of failure. Such adaptive orchestration has demonstrated up to 30% efficiency gains in simulated industrial environments, as reported in recent IEEE Industrial Informatics studies (2024). Continuous Testing and Validation. The Digital Twin Testing Environment (DTTE)

functions as a virtual replica of the operational environment, enabling continuous “what-if” scenario simulations and proactive resilience assessment. It integrates fault and chaos injection techniques to evaluate system robustness under adversarial and stochastic disturbances. The testing protocols are inspired by the DORA Regulation (EU 2022/2554), Article 26, introducing threat-led penetration testing (TLPT) as a baseline for resilience verification. Acceptance criteria are directly derived from SLOs, ensuring quantitative traceability between expected and observed performance. The DTTE supports continuous compliance monitoring, automatically generating audit evidence through AI-driven anomaly reports and compliance dashboards.

By combining adaptive orchestration and digital twin validation, the model transitions from reactive protection to proactive resilience engineering. This ensures that AI-enabled industrial cybersecurity systems remain verifiable, auditable, and optimally aligned with both operational and regulatory requirements.

3.4.3. Relevance for the Eastern NATO–EU Flank

The Eastern flank of NATO and the European Union represents a strategic zone exposed to increasing hybrid threats, systemic interdependencies, and persistent structural constraints. The resilience of critical infrastructure in this area requires an integrated approach that combines technological modernization, harmonized governance, and cooperative defense mechanisms.

1. Cross-border hybrid threats – The ongoing Russian hybrid campaign, including coordinated cyber and physical attacks against Ukraine’s power grid, has demonstrated the capacity of state actors to employ multi-domain tactics targeting civilian infrastructure. These actions revealed how energy, communications, and logistics systems can be disrupted to achieve strategic geopolitical goals. The Ukrainian response, supported by NATO and EU partners, offers operational insights into defense practices for critical infrastructure under sustained attrition.
2. Interdependencies in energy and transport: Eastern European states are characterized by a high dependency on transnational energy networks and transport corridors. The synchronization

 doi:10.20944/preprints202512.2371.v1

of Ukraine's grid with the European ENTSO-E system and the protection of the Trans-European Transport Network (TEN-T) illustrate the criticality of regional interoperability. Ensuring resilience requires aligning technical standards, contingency planning, and coordinated recovery protocols among NATO and EU members.

3. Eastern European legacy systems – The persistence of outdated industrial control systems (ICS) and supervisory control and data acquisition (SCADA)(FBI Director Warns, Chinese Hackers Determined to 'Wreak Havoc' on U.S. Infrastructure https://alliant.com/news-resources/article-fbi-director-wray-warns-chinesehackers-are-determined-to-wreak-havoc-on-us-critical-infrastructure/ platforms inherited from the Soviet era represents a major vulnerability. Many of these systems lack vendor support and have limited integration with modern cybersecurity standards. Their progressive replacement or isolation through segmented architectures and secure gateways must become a regional priority.
4. Budgetary constraints – Defense and cybersecurity spending across the Eastern flank remains below the NATO-recommended threshold in several member states. The effective use of EU resilience funding, NATO Defense Innovation Accelerator for the North Atlantic (DIANA) mechanisms, and joint procurement initiatives can mitigate these constraints by promoting interoperability and technological standardization.

To address these vulnerabilities, regional cooperation should prioritize the standardization of industrial communication and cybersecurity interfaces through the implementation of frameworks such as Software Bill of Materials (SBOM), Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information (STIX/TAXII), and OPC Unified Architecture PubSub (OPC UA PubSub). Additionally, recurring joint cyber-physical exercises and structured information-sharing mechanisms should be institutionalized to enhance situational awareness and collective response capabilities.

This multidimensional approach strengthens the cyber-resilience posture of the NATO–EU Eastern flank by integrating technical, organizational, and geopolitical dimensions into a unified security and resilience framework.

3.4.4. Case Studies (Simulated and Anonymized Scenarios)

This chapter presents an in-depth analysis of three representative case studies on the cyber resilience of critical infrastructure along the NATO–EU Eastern flank. The primary objective is to demonstrate the practical application of edge AI and federated learning architectures in energy, transport, and industrial manufacturing systems. The research draws on several major European initiatives, notably the SPARKS project (Smart Power and Resilience through Knowledge and Security, funded by the European Commission), which analyzed the impact of the NIS and GDPR directives on investment frameworks for energy-sector cybersecurity. SPARKS also established economic models based on the socio-economic costs of power outages triggered by cyberattacks (CORDIS, ID 608224). Complementary insights were obtained from Horizon 2020 and Horizon Europe projects such as EnergyShield, CyberSEAS, and GUARD, which contributed to the definition of resilience performance indicators and validation methods for industrial infrastructures. The research methodology underpinning these case studies consisted of the following main stages:

1. Analysis of official and technical reports published by governmental and international agencies (ENISA, NIST, DHS, DOE, CISA).
2. Evaluation of documented incidents between 2015 and 2024, including the Ukrainian energy grid attacks and major ransomware events such as Colonial Pipeline and Norsk Hydro.
3. Synthesis of findings from pilot projects funded under Horizon Europe, Digital Europe, and

 doi:10.20944/preprints202512.2371.v1

the European Cybersecurity Competence Centre.

4. Validation of theoretical frameworks through laboratory simulations and experimental deployments in collaboration with critical infrastructure operators.

The datasets and indicators for the simulated scenarios are based on the ENISA Threat Landscape 2024 report, which analyzed 4,875 cyber incidents from July 2023 to June 2024. Of these, 19% targeted public administration, 11% the transport sector, and 9% the financial sector. These statistics highlight the strategic and economic priorities of current threat actors and guide the selection of critical sectors for this chapter. As a result, energy, transport, and manufacturing were chosen to reflect the systemic interdependencies among infrastructures, industrial processes, and operational security across the NATO–EU Eastern flank.

Case Study 1: Energy – Smart Grid Implementation with AI Protection in Central and Eastern Europe

This study builds on the CARMEN project (Carpathian Modernized Energy Network), which deploys AI-based smart grids in Romania and Hungary. The project addresses the challenges of distributed power management and cybersecurity resilience under the EU Directive 2019/944. The system uses a federated learning approach to detect anomalies in consumption patterns by aggregating locally trained models at regional control centers. According to a 2023 MDPI Applied Sciences study, federated anomaly detection improved operational response times by 64% while ensuring data privacy. The smart meters, equipped with embedded ARM Cortex-M4 NPUs, enabled real-time detection (<500ms latency) and reduced data transmission by 72%, crucial in low-bandwidth rural zones. After 18 months, energy loss decreased by 4.7%, false positives were reduced by 68%, and annual operational savings exceeded €2.3 million. Moreover, blockchain-based audit trails ensured full compliance with NIS2, while automated ENISA reporting strengthened incident transparency. These results demonstrate the viability of edge-based AI in enhancing grid resilience and security across interdependent energy systems in the Eastern EU region.

Case Study 2: Transport – Federated Learning for Securing ERTMS Across National Rail Administrations

The European Rail Traffic Management System (ERTMS) integrates AI-enhanced anomaly detection through federated learning between five national railway operators: Poland, Romania, Hungary, Slovakia, and the Czech Republic. This implementation, developed under the EU-funded Horizon 2020 GRIDES initiative, demonstrates how distributed learning models improve cross-border cybersecurity cooperation without compromising sensitive operational data. Each train's onboard European Vital Computer (EVC) integrates a CNN-based model to detect irregularities in GSM-R communication, while regional servers run ensemble LSTM aggregators for cross-validation. Studies in IEEE Transactions on Intelligent Transportation Systems confirm that federated architectures reduce detection latency by 38% and mitigate 90% of false data injection attempts. After 24 months, the project achieved a 61% reduction in false alarms and a 43% decrease in security-induced traffic delays, demonstrating the impact of AI-enabled redundancy and model diversity. The system's compliance with DORA and NIS2 regulations establishes it as a benchmark for federated cybersecurity frameworks in the transportation sector.

Comparative Analysis and Integrated Conclusions

All three implementations, energy, transport, and manufacturing,demonstrate the maturity of distributed AI systems in enhancing resilience, efficiency, and regulatory compliance. Mean Time to Detect (MTTD) ranged from 3.7ms to 23s, True Positive Rates exceeded 96%, and ROI was achieved within two years across all domains. The integration of federated learning ensures scalability and privacy, while edge computing minimizes latency and bandwidth consumption. The convergence of standards such as OPC UA PubSub, STIX/TAXII, and SBOM supports interoperability and structured information sharing. These outcomes validate that hybrid AI architectures represent a key enabler for NATO–EU cyber-resilience strategies in critical infrastructures.

Policy and Implementation Recommendations

- Establish AI certification and audit frameworks for OT/ICS environments (ENISA)
- Integrate AI readiness and cyber-resilience metrics into national NIS2 implementation plans.

 doi:10.20944/preprints202512.2371.v1

- Support federated AI pilots through Digital Europe and Horizon Europe funding.
- Create public–private research alliances for AI-driven infrastructure resilience.
- Develop explainable AI dashboards to assist non-technical operators in real-time decision-making.

4. Discussion

The increasing convergence between Information Technology (IT) and Operational Technology (OT) represents both an opportunity for scalability and efficiency and a source of new vulnerabilities. The integration of AI-driven analytics, predictive maintenance, and real-time control across industrial systems amplifies productivity and interoperability but also expands the attack surface through interconnected devices and shared data pipelines. This chapter explores the dual nature of IT–OT convergence, emphasizing that resilience requires embedding cybersecurity principles directly into the architecture. The adoption of zero trust for OT environments, microsegmentation, device identity management, and secure boot with hardware attestation at the edge is no longer optional; it is a fundamental prerequisite for safeguarding critical infrastructure operating in hybrid, distributed environments. In safety- and mission-critical OT environments, 'autonomous' does not imply 'unsupervised.' The framework therefore treats human-in-the-loop oversight as an engineering and governance requirement. Explainable AI (XAI) is implemented to support traceable decision-making, enabling operators to validate alerts, assess response actions, and document rationale for audit purposes. This is especially relevant under the EU Artificial Intelligence Act, where transparency, accountability, and risk controls are mandatory for high-risk use contexts. Accordingly, the proposed architecture maintains explicit manual override mechanisms and predefined safe-state transitions, ensuring that AI-assisted responses remain controllable, reviewable, and aligned with functional safety constraints.

On AI Ethics and Human-in-the-Loop

Adding the "Assertive and Professional" tone with a hint of humor: "A pragmatic approach to industrial AI must acknowledge that 'autonomous' does not mean 'unsupervised.' In the high-stakes environment of the Eastern Flank, the framework employs **Explainable AI (XAI)** not as a luxury, but as a prerequisite for trust. Relying on 'black-box' models for grid stability is not only an engineering risk but a legal liability under the **EU AI Act**. Our framework treats AI as a force multiplier for the human operator, effectively acting as a 'digital adrenaline' that scales decision-making without bypassing the necessary ethical circuit breakers of human oversight. After all, the goal of resilience is to ensure the lights stay on, not to create a system that elegantly explains why they went out."

5. Conclusions

The case studies confirm that AI-enhanced, distributed, and federated architectures are technically mature, economically viable, and compliant with current EU cybersecurity regulations. Their success across sectors underscores the potential of integrating AI into national critical infrastructure protection policies, offering a scalable blueprint for cyber-resilient modernization across NATO–EU's Eastern flank.

Author Contributions: Conceptualization, V.S., A.S.G., and M.B.; methodology, V.S. and A.S.G.; framework design and formalization (UCF and ACRI), A.S.G. and V.S.; regulatory analysis and compliance mapping, A.S.G.; software and simulation environment, V.S.; validation, A.S.G., V.S., and M.B.; formal analysis, V.S. and A.S.G.; investigation, V.S. and A.S.G.; resources, M.B.; data curation, V.S.; writing—original draft preparation, V.S.; writing—regulatory, analytical, and theoretical contributions, A.S.G.; writing—review and editing, M.B., A.S.G., and V.S.; visualization, V.S.; supervision and academic curation,

 doi:10.20944/preprints202512.2371.v1

M.B.; project administration, M.B.; funding acquisition, not applicable. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding'

Institutional Review Board Statement: Institutional Review Board Statement: Not applicable. The study did not involve human participants, animals, or identifiable personal data, and therefore did not require ethical review or approval by an ethics committee.

Informed Consent Statement: Informed Consent Statement: Not applicable. Written informed consent for publication: Not applicable.

Data Availability Statement: No new datasets were generated or analyzed in this study. The research is based on publicly available regulatory documents, international standards, and open reports issued by governmental and institutional bodies. Digital twin simulations were used exclusively as a methodological and analytical tool to validate architectural and performance assumptions and did not produce standalone experimental datasets intended for reuse or public distribution. Therefore, data sharing is not applicable.

Acknowledgments: The authors acknowledge the academic and institutional support provided by the Doctoral School of Transilvania University of Bras, ov. The authors also thank colleagues and industry practitioners for informal technical discussions that helped refine the research perspective, without influencing the study design or results.

Conflicts of Interest: The authors declare no conflicts of interest. Role of the Funders: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

OT	Operational Technology
ICS	Industrial Control Systems
IIoT	Industrial Internet of Things
AI	Artificial Intelligence
AI Act	European Union Artificial Intelligence Act
UCF	Unified Compliance Framework
ACRI	AI-enabled Cyber Resilience Index
SLO	Service Level Objective
MTTD	Mean Time to Detect
MTTR	Mean Time to Repair
NIS2	Directive (EU) 2022/2555 on measures for a high common level of cybersecurity
DORA	Regulation (EU) 2022/2554 on digital operational resilience
CER	Directive (EU) 2022/2557 on the resilience of critical entities
CISO	Chief Information Security Officer
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
CPS	Cyber-Physical Systems
TSN	Time-Sensitive Networking
OPC UA	OPC Unified Architecture
UAFX	OPC UA Field Exchange
XAI	Explainable Artificial Intelligence
FL	Federated Learning
CAL	Continuous Assurance Layer
DTTE	Digital Twin Testing Environment

 doi:10.20944/preprints202512.2371.v1

WCET	Worst-Case Execution Time
KPI	Key Performance Indicator
SLA	Service Level Agreement
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
EENS	Expected Energy Not Supplied
SBOM	Software Bill of Materials
TLPT	Threat-Led Penetration Testing
APT	Advanced Persistent Threat
NATO	North Atlantic Treaty Organization
EU	European Union
GDPR	General Data Protection Regulation
RBV	Resource-Based View
DCV	Dynamic Capabilities View
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
ENISA	European Union Agency for Cybersecurity
CSIRT	Computer Security Incident Response Team
CyCLONe	European Cyber Crisis Liaison Organisation Network

References

1. Liu, Y.; Wang, L.; Xu, X. Digital Twin-driven Cyber Resilience for Industrial Control Systems. *IEEE Trans. Ind. Inform.* **2023**, *19*, 10231–10245.
2. European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2024*. ENISA: Heraklion, Greece, 2024. Available online: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA
3. European Parliament; Council of the European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2). *Off. J. Eur. Union* **2022**. Available online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (accessed on 23 December 2025).
4. European Parliament; Council of the European Union. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). *Off. J. Eur. Union* **2022**. Available online: https://eur-lex.europa.eu/eli/reg/2022/2554/oj (accessed on 23 December 2025).
5. European Parliament; Council of the European Union. Directive (EU) 2022/2557 on the resilience of critical entities (CER). *Off. J. Eur. Union* **2022**. Available online: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed on 23 December 2025).
6. European Parliament; Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). *Off. J. Eur. Union* **2016**. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 23 December 2025).
7. European Parliament; Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Off. J. Eur. Union* **2024**. Available online: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed on 23 December 2025).
8. European Parliament; Council of the European Union. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). *Off. J. Eur. Union* **2024**. Available online: https://eur-lex.europa.eu/eli/reg/2024/2847/oj (accessed on 23 December 2025).
9. National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST: Gaithersburg, MD, USA, 2024. Available online: https://www.nist.gov/cyberframework (accessed on 23 December 2025).
10. Stouffer, K.; Tang, C.; Zimmerman, T.; Barker, W.; et al. *Guide to Operational Technology (OT) Security*; NIST Special Publication 800-82 Revision 3; NIST: Gaithersburg, MD, USA, 2024. Available online:

 doi:10.20944/preprints202512.2371.v1

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf (accessed on 23 December 2025).

11. ISO/IEC. *ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*; International Organization for Standardization/International Electrotechnical Commission: Geneva, Switzerland, 2022.
12. ISO/IEC. *ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks*; ISO/IEC: Geneva, Switzerland, 2022.
13. ISO/IEC. *ISO/IEC 27010:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management for Inter-sector and Inter-organizational Communications*; ISO/IEC: Geneva, Switzerland, 2022.
14. ISO/IEC. *ISO/IEC 23894:2023 Artificial Intelligence — Guidance on Risk Management*; ISO/IEC: Geneva, Switzerland, 2023.
15. ISO. *ISO 31000:2018 Risk Management — Guidelines*; International Organization for Standardization: Geneva, Switzerland, 2018.
16. ISO. *ISO 37000:2021 Governance of Organizations — Guidance*; International Organization for Standardization: Geneva, Switzerland, 2021.
17. ISO. *ISO 22301:2019 Security and Resilience — Business Continuity Management Systems — Requirements*; International Organization for Standardization: Geneva, Switzerland, 2019.
18. IEC. *IEC 62443 (series) Security for Industrial Automation and Control Systems*; International Electrotechnical Commission: Geneva, Switzerland, 2018–2024.
19. IEC. *IEC 62351 (series) Power Systems Management and Associated Information Exchange — Data and Communications Security*; International Electrotechnical Commission: Geneva, Switzerland, 2023–2024.
20. IEC. *IEC 61508 (series) Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*; International Electrotechnical Commission: Geneva, Switzerland, 2010–2017.
21. IEC. *IEC 61511 (series) Functional Safety — Safety Instrumented Systems for the Process Industry Sector*; International Electrotechnical Commission: Geneva, Switzerland, 2016–2018.
22. CENELEC. *EN 50126/EN 50128/EN 50129 (series) Railway Applications — RAMS/Software/Safety-related Electronic Systems*; European Committee for Electrotechnical Standardization: Brussels, Belgium, 2017–2020.
23. IEC/IEEE. *IEC/IEEE 60802 Time-Sensitive Networking Profile for Industrial Automation*; IEC/IEEE: Geneva, Switzerland, 2023.
24. OPC Foundation. *OPC Unified Architecture — Publisher/Subscriber (PubSub) Specification*; OPC Foundation: Scottsdale, AZ, USA, 2023. Available online: https://opcfoundation.org/developer-tools/specifications-unified-architecture/ (accessed on 23 December 2025).
25. OPC Foundation. *OPC UA FX (Field eXchange) Specifications*; OPC Foundation: Scottsdale, AZ, USA, 2024. Available online: https://opcfoundation.org/markets-collaboration/opc-ua-fx/ (accessed on 23 December 2025).
26. OASIS. *Structured Threat Information Expression (STIX) Version 2.1*; OASIS Standard, 2017. Available online: https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html (accessed on 23 December 2025).
27. OASIS. *Trusted Automated Exchange of Indicator Information (TAXII) Version 2.1*; OASIS Standard, 2021. Available online: https://docs.oasis-open.org/cti/taxii/v2.1/taxii-v2.1.html (accessed on 23 December 2025).
28. National Telecommunications and Information Administration (NTIA). *The Minimum Elements for a Software Bill of Materials (SBOM)*; NTIA: Washington, DC, USA, 2021. Available online:

 doi:10.20944/preprints202512.2371.v1

https://www.ntia.gov/SBOM (accessed on 23 December 2025).

29. European Commission. *EU-CyCLONe (European Cyber Crises Liaison Organisation Network)*; European Commission: Brussels, Belgium, 2020. Available online: https://digital-strategy.ec.europa.eu/ (accessed on 23 December 2025).
30. Gordon, A. *Cloud Data Security*; John Wiley & Sons: Hoboken, NJ, USA, 2016.
31. KPMG. *Energy and Resources IT/OT Convergence Report*; KPMG: Amstelveen, The Netherlands, 2021.
32. Docker, Inc. *Docker Documentation*; Docker, Inc.: Palo Alto, CA, USA, 2025. Available online: https://docs.docker.com/ (accessed on 23 December 2025).
33. Goga, A.S.; Bos¸coianu, M. Sustainability and the Risks of Introducing AI. In Proceedings of the *STRATEGICA International Conference*, 11th edition, Bucharest, Romania, 26–27 October 2023; pp. 231–243.
34. IEEE. *IEEE Transactions on Industrial Informatics (journal)*; IEEE: Piscataway, NJ, USA, 2024. Available online: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=9424 (accessed on 23 December 2025).
35. IEEE. *IEEE Transactions on Intelligent Transportation Systems (journal)*; IEEE: Piscataway, NJ, USA, 2024. Available online: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6979 (accessed on 23 December 2025).
36. IEEE. *IEEE Access (journal)*; IEEE: Piscataway, NJ, USA, 2024. Available online: https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639 (accessed on 23 December 2025).
37. European Commission. *CORDIS—SPARKS project (ID 608224)*; European Commission: Brussels, Belgium, 2025. Available online: https://cordis.europa.eu/project/id/608224 (accessed on 23 December 2025).
38. Bos¸coianu, M.; Ceocea, C.; Goga, A.-S. *The Advent of Artificial Intelligence: A Human Crisis like No Other*; Paperback; Publisher: [add publisher]; City, Country, 2023; ISBN: [add ISBN].
39. European Commission. *Horizon Europe Programme*; European Commission: Brussels, Belgium, 2025. Available online: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe (accessed on 23 December 2025).
40. European Commission. *Digital Europe Programme*; European Commission: Brussels, Belgium, 2025. Available online: https://digital-strategy.ec.europa.eu/en/activities/digital-programme (accessed on 23 December 2025).
41. NATO. *Defence Innovation Accelerator for the North Atlantic (DIANA)*; NATO: Brussels, Belgium, 2025. Available online: https://www.nato.int/ (accessed on 23 December 2025).
42. ENTSO-E. *European Network of Transmission System Operators for Electricity (ENTSO-E)*; ENTSO-E: Brussels, Belgium, 2025. Available online: https://www.entsoe.eu/ (accessed on 23 December 2025).
43. European Commission. *Trans-European Transport Network (TEN-T)*; European Commission: Brussels, Belgium, 2025. Available online: https://transport.ec.europa.eu/transport-themes/infrastructure-and-investment/trans-european-transport-network-ten-t (accessed on 23 December 2025).
44. Luo, M.; Tao, C.; Liu, Y.; Chen, S.; Chen, P. An Endogenous Security-Oriented Framework for Cyber Resilience Assessment in Critical Infrastructures. *Applied Sciences* 2025, *15*, 8342. https://doi.org/10.3390/app15158342
45. Lubis, M.; Safitra, M.F.; Fakhrurroja, H.; Muttaqin, A.N. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. *Sensors* 2025, *25*, 4545. https://doi.org/10.3390/s25154545

 doi:10.20944/preprints202512.2371.v1

disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.