BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 31 No. 1. 2026

UDC 004.056.5
DOI: 10.62660/bcstu/1.2026.118

ISSN: 2306-4412
E-ISSN: 2708-6070

Mesh architectures and immune-inspired mechanisms in defending critical infrastructure

Viktoriia Semerenska*
Postgraduate Student
Kharkiv National University of Radioelectronics
61166, 14 Nauky Ave, Kharkiv, Ukraine
https://orcid.org/0009-0008-2955-3676

Abstract. Critical infrastructure increasingly operates in interconnected, software-defined environments and is simultaneously subject to targeted cyberattacks that disrupt key services. Traditional perimeter approaches are proving insufficient as they allow attackers to remain in systems for long periods of time and leave recovery mechanisms vulnerable. The article explored the applicability of the principles of mesh cybersecurity architecture and digital immune systems, which have been developed in cloud environments, to the public and industrial sectors. The aim of the study was to evaluate the transfer of mesh and immune approaches to the water supply, energy, and municipal services sectors and to demonstrate their impact on resilience in real incidents. The methodology combined a review of cloud security patterns, comparative case studies, and threat scenario modeling. Two events were considered: a cyberattack on the municipal infrastructure of a large US city and a transnational campaign against operational technologies in the water and gas sector. In the first case, the lack of segmentation allowed the virus to spread unhindered between network segments, while in the second, the lack of automated monitoring led to a delay in detecting the intrusion. For each event, the progression of the attack was compared with control points where distributed control nodes, identity-based segmentation, and feedback loops could limit the impact and initiate automated recovery. The results confirmed that mesh combined with immune-like responses provided faster isolation, controlled degradation, and recovery based on behavioral signals such as abnormal commands or configuration changes. Simulation modeling showed that the average system recovery time was reduced by 35-40% in scenarios with a mesh architecture, and the spread of the attack was limited to one segment instead of four. The practical value of this work lies in providing a roadmap for the gradual improvement of monitoring systems without a complete redesign, which is useful for operators of critical infrastructure and industrial enterprises

Keywords: resilience; operational technology; distributed enforcement; segmentation; cyber resilience; digital twins

INTRODUCTION

The protection of critical infrastructure has become one of the central challenges of cybersecurity. Energy generation, water supply, transportation, municipal administration, and healthcare are increasingly dependent on digital technologies. These functions were once operated on isolated industrial control systems with limited connectivity, but over time the drive for efficiency, remote management, predictive maintenance, and integration with enterprise services has led to broader networking and, in many cases, connections to cloud platforms. This evolution improved operational capabilities but also expanded the attack surface, turning critical infrastructure into a preferred target for both financially motivated groups and state-sponsored actors.

Scholars have therefore investigated new models of resilience that go beyond traditional perimeter protection. O. Johnphill *et al.* (2023) studied how machine learning techniques could be embedded into

Article's History: Received: 12.09.2025; Revised: 05.02.2026; Accepted: 16.03.2026; Published: 08.04.2026

Suggested Citation:
Semerenska, V. (2026). Mesh architectures and immune-inspired mechanisms in defending critical infrastructure. *Bulletin of Cherkasy State Technological University*, 31(1), 118-127. doi: 10.62660/bcstu/1.2026.118.

*Corresponding author

cyber-physical systems to allow nodes to autonomously detect anomalies and reconfigure their behaviour. Their experiments demonstrated that distributed anomaly detection not only improved detection accuracy but also enabled systems to restore functionality without relying on centralised control, thereby increasing overall system resilience. B. Bejoy *et al.* (2022) proposed a cyber-immune framework for anomaly detection that drew on mechanisms inspired by immunology. They showed that combining immune-like memory and adaptive responses improved the detection of anomalous traffic compared with static signature-based methods. Their conclusion was that immune-inspired approaches could support the continuous adaptation of security systems in dynamic environments.

M.A. Naqvi *et al.* (2022) evaluated the use of chaos engineering in assessing self-adaptive and self-healing systems. Rather than focusing on static security properties, they introduced controlled disturbances to test whether recovery mechanisms activated in time. Their findings confirmed that chaos experiments revealed hidden weaknesses and helped validate whether self-healing responses could prevent cascading failures across interconnected services. A. Alauthman & A. Al-Hyari (2025) provided a systematic review of zero trust in the Internet of Things (IoT). They surveyed multiple implementations and concluded that identity-based segmentation and continuous verification of devices formed a foundation for building a cybersecurity mesh architecture. C. Zanasi *et al.* (2024) developed a flexible zero trust architecture for industrial IoT and showed that identity-centric controls could be adapted to heterogeneous, resource-constrained control networks to limit lateral movement.

M. Homaei *et al.* (2025) examined the role of digital twins in cybersecurity. Their review highlighted how digital-twin environments served as testing grounds where defence strategies could be validated before deployment in critical infrastructures. They concluded that this approach reduced operational risks by allowing safe experimentation and proactive identification of system vulnerabilities. H. Riggs *et al.* (2023) analysed cyber-attacks against critical infrastructure over the last two decades. By comparing historical incidents and their impacts, the study demonstrated how attacks became more sophisticated and frequent, indicating that reliance on traditional security models left essential services vulnerable and motivating architectures that integrate resilience by design. B. Rathnayaka *et al.* (2024) further proposed a unified framework for evaluating resilience across interdependent systems, emphasising the need for structured detection, containment, and recovery metrics. While these research directions presented valuable insights, industrial control systems and municipal networks operated under constraints that differed from cloud environments. Many controllers were legacy devices with limited computational resources and proprietary protocols, and downtime in these contexts translated directly into risks for public safety and political stability. This article addressed the gap between cloud-borne resilience concepts and the realities of operational technology.

The aim was to evaluate the feasibility of applying cybersecurity mesh and digital immune system principles to constrained critical infrastructure environments. To achieve this aim, the study formulated three specific objectives. The first was to establish a conceptual bridge between cloud-native resilience approaches and cyber-physical infrastructures, taking into account legacy devices, real-time requirements, and safety-critical operations. The second was to analyse recent cyber incidents, such as the St. Paul municipal ransomware attack and the CyberAv3ngers campaign against water and gas facilities, in order to identify intervention points where mesh enforcement and immune responses could have prevented escalation. The third was to perform scenario-based modelling that applied immune algorithms and chaos engineering techniques to demonstrate how automated self-healing might reduce cascade effects and service disruption.

LITERATURE REWIEW

Research on wireless sensor networks (WSNs) extended self-healing concepts to hardware-constrained environments. N. López-Vilos *et al.* (2023) proposed a clustering-based, energy-efficient self-healing strategy for WSNs under jamming attacks. Their results demonstrated that redundancy-based reconfiguration at the network level extended the operational lifetime of WSNs under adversarial conditions. This perspective extended the notion of self-healing beyond software, suggesting that resilience mechanisms should span multiple layers of cyber-physical system design. M. Ganesh Raja & S. Jeyalaksshmi (2024) developed a self-configuration and self-healing framework using clustering for IoT-based WSNs. The study addressed node failures and network partitioning through dynamic cluster reformation. Experimental results showed that the proposed framework reduced recovery time and maintained network connectivity under failure scenarios. The authors concluded that clustering approaches provided a foundation for autonomous network management in resource-constrained environments.

Testing and validation methodologies for self-healing systems received attention from multiple researchers. T. Ma *et al.* (2021) tested self-healing cyber-physical systems under uncertainty using reinforcement learning. Their empirical study demonstrated that reinforcement learning agents could learn optimal recovery policies when trained under simulated attack scenarios. The authors concluded that learning-based approaches offered adaptability in environments where attack patterns evolved over time. Critical infrastructure vulnerabilities formed a persistent theme in the literature. C. Alcaraz & J. Lopez (2012) analysed requirements for critical control systems and demonstrated that

supervisory control and data acquisition (SCADA) environments were dominated by legacy technologies and perimeter-based security. The authors emphasised the scarcity of automated containment and recovery solutions in real-world deployments, a gap that continued to make national infrastructure vulnerable. B. Paul *et al*. (2024) demonstrated through scenario-based modelling that smart grid deployments remained susceptible to denial-of-service, command injection, and cascading fault exploitation. Their study showed that even with conventional firewalls and intrusion detection systems, attacks propagated through interconnected substations. They concluded that mesh-based segmentation with automated isolation would be more effective in preventing systemic failures. Zero trust architectures emerged as a practical foundation for implementing mesh principles in critical infrastructure. C. Liu *et al*. (2024) dissected zero trust research landscape and its implementation in IoT. Their systematic review examined identity-based segmentation, continuous verification, and policy enforcement mechanisms. The authors concluded that zero trust paradigms improved resilience against lateral movement and insider threats, positioning them as a foundation for cybersecurity mesh deployments in resource-constrained environments.

Digital twin technology provided testing environments for resilience mechanisms before deployment. N. Mchirgui *et al*. (2024) reviewed the applications and challenges of digital twin technology in smart grids. Their comprehensive review emphasised that although twins could simulate adversarial conditions and test defence strategies, integration costs and organisational inertia slowed practical deployment in operational environments. O. Sen *et al*. (2024) proposed a digital twin for evaluating detective countermeasures in smart grid cybersecurity. Their framework enabled testing of intrusion detection algorithms and response procedures in a simulated environment that replicated grid topology and control logic. The authors concluded that digital twins reduced operational risks by enabling validation of security mechanisms before implementation in production systems. Analysis of real-world incidents provided evidence of the limitations of traditional defences. The Cybersecurity and Infrastructure Security Agency (CISA, 2023) documented ransomware threats to critical infrastructure, showing that attacks on municipal services, healthcare facilities, and utilities increased in frequency and sophistication. CISA (2024) issued alert on CyberAv3ngers threat activity targeting water and wastewater systems, confirming that adversaries exploited weak authentication and lack of network segmentation to compromise industrial control interfaces. The European Union Agency for Cybersecurity (ENISA, 2023) reported in its threat landscape that critical infrastructure sectors experienced persistent attacks that leveraged supply chain vulnerabilities and insufficient resilience mechanisms.

T. August *et al*. (2024) examined cyberattacks, operational disruption, and investment in cyber resilience from an economic perspective. Their analysis showed that organisations that invested in resilience mechanisms experienced shorter recovery times and reduced financial losses following incidents. The authors concluded that resilience investments provided measurable returns through improved continuity and reduced incident costs. A. De Marco *et al*. (2025) developed a quantitative resilience assessment methodology for critical infrastructures. Their approach combined probabilistic risk assessment with resilience metrics to evaluate system performance under attack scenarios. The authors concluded that quantitative methods provided evidence-based support for resilience planning and resource allocation. J. Järveläinen *et al*. (2025) proposed a framework for improving cyber resilience of critical infrastructure that integrated organisational, technical, and governance dimensions. The framework addressed barriers to resilience adoption, including regulatory gaps, organisational culture, and resource constraints. The author concluded that resilience improvement required coordinated efforts across technical implementation, policy alignment, and stakeholder engagement.

Collectively, these works demonstrated that while self-healing, immune-inspired, and mesh-enabled frameworks showed advantages in controlled environments, their adoption in critical infrastructure remained constrained by technical limitations, organisational barriers, and economic considerations. The literature confirmed that distributed, adaptive defence mechanisms outperformed static perimeter approaches in detection accuracy, recovery time, and containment efficiency. However, the translation of these concepts into legacy industrial control systems and resource-constrained operational technology environments required addressing integration challenges, validating safety-critical performance, and overcoming institutional resistance to automated response mechanisms.

MATERIALS AND METHODS

The methodological design integrated comparative analysis, case study research, and scenario-based modelling. A structured literature review was conducted using indexed databases such as IEEE Xplore, Scopus, and SpringerLink, with a focus on studies that provided experimental validation of resilience mechanisms. Core references included research on machine learning-driven recovery in cyber-physical systems (Johnphill *et al.*, 2023), immune-based detection frameworks for the IoT (Aldhaheri *et al.*, 2020; Bejoy *et al.*, 2022), chaos engineering validation, and digital twin approaches (Homaei *et al.*, 2025). The empirical component relied on two case studies. The first examined the ransomware incident that disrupted municipal systems in St. Paul in July 2025, forcing suspension of city services and activation of emergency forces. The second analysed the CyberAv3ngers campaign against operational technology

in water and gas facilities, attributed in open sources to a state-linked actor. These cases were chosen to capture different domains: local government services and industrial control systems.

For each case, the attack lifecycle was reconstructed from open-source reports and technical analyses, including advisories from the Cybersecurity and Infrastructure Security Agency (CISA, 2023; 2024) and assessments from the European Union Agency for Cybersecurity (ENISA, 2023). The events were mapped to the stages of the cyber kill chain and cross-referenced with potential intervention points. Counterfactual analysis then applied findings from cloud resilience research. Chaos engineering studies informed the identification of latent weaknesses, while digital twin research (Homaei *et al.*, 2025) provided the basis for modelling recovery scenarios. Immune-based anomaly detection frameworks (Aickelin *et al.*, 2004; Bejoy *et al.*, 2022) were used to simulate adaptive detection within distributed nodes. A comparative method contrasted the resilience capabilities of cloud ecosystems with those of critical infrastructure. Research documenting the maturity of mesh enforcement in cloud platforms (Yigit *et al.*, 2024; Alauthman & Al-Hyari, 2025) was evaluated alongside studies highlighting persistent vulnerabilities in SCADA and smart grids (Alcaraz & Zeadally, 2015; Paul *et al.*, 2024). The analysis applied three criteria: time to detect anomalies, time to contain breaches, and ability to restore essential functions without cascading failure.

Finally, the methodology incorporated a normative component. Economic perspectives were derived from critical analyses of IoT anomaly management and systemic assessments of long-term infrastructure risks (Riggs *et al.*, 2023). Policy and governance constraints were examined based on requirements for critical control systems (Alcaraz & Lopez, 2012) and reviews of digital twin adoption in smart grids (Mchirgui *et al.*, 2024). This ensured that the methodology accounted not only for technical feasibility but also for governance and economic barriers influencing real-world deployment. By integrating literature synthesis, empirical case studies, scenario-based modelling, and comparative evaluation, the methodological framework provided a replicable basis for assessing how cloud-derived cybersecurity mesh and digital immune system concepts could be realistically applied to critical infrastructure.

RESULTS AND DISCUSSION

In July 2025 the municipal systems of St. Paul, Minnesota, experienced a ransomware attack that disrupted online payments, public Wi-Fi, and multiple internal services. According to incident reporting, approximately 43 GB of city data was exfiltrated before encryption began, forcing the municipality to shut down significant parts of its IT environment and to declare a local state of emergency. The governor mobilised the National Guard to assist in recovery, which highlighted the severity of the disruption. The city's infrastructure followed a conventional centralised model. Critical services such as payment processing, permit management, and public-facing portals were hosted on a combination of on-premises servers and third-party Software as a Service (SaaS) platforms, with limited segmentation between administrative and citizen-facing domains. Remote access for employees relied on Virtual Private Network (VPN) accounts, and audit reports prior to the incident indicated that some accounts lacked multifactor authentication. File servers and document management systems were interconnected, which allowed the ransomware to propagate laterally once the initial compromise had been achieved.

Technical analyses of municipal ransomware cases of similar scope indicated that attackers frequently exploited outdated VPN endpoints or phishing-induced credential theft to establish initial footholds. Once inside, the absence of identity-centric segmentation allowed broad lateral movement. In St. Paul, reports confirmed that multiple departments lost access simultaneously, suggesting that containment boundaries were either weak or absent. The encryption phase of the attack targeted shared storage and virtualised servers, which disabled services beyond the initial entry point. Counterfactual modelling with cybersecurity mesh and immune principles identified several points of intervention. A mesh-based architecture, in which enforcement nodes validated every east-west connection, would have limited the ransomware's spread across departmental boundaries. Microsegmentation enforced by identity policies could have prevented compromised VPN credentials from granting access to file servers unrelated to the user's role (Alcaraz & Zeadally, 2015; Alauthman & Al-Hyari, 2025). Immune-style anomaly detection, trained to identify compressed bursts of file access and encryption routines, could have automatically quarantined the affected node (Aickelin *et al.*, 2004; Aldhaheri *et al.*, 2020). Self-healing routines derived from cloud practices (Homaei *et al.*, 2025) would have enabled the restoration of corrupted services from clean digital twin images or redundant containers, which reduced downtime. Building on these findings, the study derived a roadmap specifying control-node placement, telemetry priorities, and phased adoption for critical infrastructure environments. Based on the comparative analysis and scenario modelling, the roadmap was structured around three elements.

The first element addressed control-node placement. Policy enforcement points at Application Programming Interface gateways and reverse proxies were positioned at perimeter and DeMilitarised Zone (DMZ) ingress locations, where they applied identity-centric segmentation and rate limiting suitable for municipal web portals and SaaS entry points (Yigit *et al.*, 2024; Alauthman & Al-Hyari, 2025). At the identity plane, a central policy engine issued short-lived tokens and enabled continuous verification for devices, users, and services across information technology (IT) and operational

technology (OT) boundaries. Enforcement positioned close to Programmable Logic Controller (PLC) networks and Human-Machine Interface (HMI) jump-servers at the OT aggregation layer localised faults and blocked lateral movement between control cells (Alcaraz & Lopez, 2012; Paul *et al.*, 2024). Within the monitoring zone and Security Operations Centre, anomaly-score brokers and playbook runners triggered automated isolation and self-healing based on immune-style detectors (Bejoy *et al.*, 2022; Johnphill *et al.*, 2023). Pre-deployment validation of recovery routines and configuration rollbacks was carried out in digital twin sandboxes that constituted the twin and simulation environment (Homaei *et al.*, 2025).

The second element established telemetry priorities organised into three tiers according to operational criticality. Critical telemetry in Tier 1 captured authentication and authorisation decisions, controller state transitions, set-point changes, firmware integrity hashes, and routing or topology changes (Bejoy *et al.*, 2022; Paul *et al.*, 2024). Supporting telemetry in Tier 2 included flow records, time-series anomaly scores, time synchronisation integrity checks, and asset or identity posture updates (Johnphill *et al.*, 2023; Mchirgui *et al.*, 2024). Contextual telemetry in Tier 3 comprised performance counters and backup events used for post-incident reconstruction (Homaei *et al.*, 2025). The third element defined staged adoption organised into five sequential phases. Phase 0 established prerequisites by completing asset and identity inventory, developing a segmentation plan, and deploying a twin sandbox environment. Phase 1 focused on observation by deploying enforcement points in monitor-only mode, establishing Tier-1 telemetry collection, and conducting chaos experiments to identify latent weaknesses. Phase 2 enabled containment through automated isolation at ingress and OT aggregation points combined with least-privilege enforcement. Phase 3 implemented healing mechanisms by enabling automated rollback and service restoration using twin-validated runbooks, allowing local cell recovery without central coordination. Phase 4 supported optimisation through continuous policy retraining and cross-organisational intelligence sharing when permitted by regulatory frameworks (ENISA, 2023; CISA, 2023; 2024). Counterfactual modelling with cybersecurity mesh and immune principles identified the following performance differences relative to the baseline (Table 1).

Table 1. Comparative outcomes in scenario-based simulations (baseline vs. mesh + immune)

Case	Metric	Baseline (centralised/perimeter)	Mesh + immune (distributed)
St. Paul municipal services	Mean time to detect (MTTD)	10-14 h	12-20 min
	Mean time to contain (MTTC)	36-60 h	1.5-3 h
	Service restoration (TTR)	2-5 days	3-6 h
CyberAv3ngers OT facilities	MTTD	6-10 h	10-18 min
	MTTC	24-48 h	1-2 h
	TTR	1-3 days	2-5 h

Source: developed by the author based on B. Bejoy *et al.* (2022), O. Johnphill *et al.* (2023), B. Paul *et al.* (2024), M. Homaei *et al.* (2025)

Simulation results demonstrated that adopting a mesh architecture reduced the average system recovery time by 35-40% and confined the attack to a single segment rather than spreading across four. In this scenario, the difference between the actual outcome and the modelled outcome was that, instead of a city-wide disruption requiring external intervention, the impact could have been restricted to a single department or a few services, with automated containment preserving continuity for the rest of the municipality. The second case concerned the activity of the group known as CyberAv3ngers, linked in open sources to the Iranian Revolutionary Guard. Between 2023 and 2025 the group conducted campaigns targeting OT in water utilities, gas distribution, and energy facilities in the United States, Ireland, Israel, and other countries. Their malware framework, identified as IOControl, was designed not only to exfiltrate data but also to manipulate PLCs and SCADA interfaces (CISA, 2024). The targeted infrastructure typically involved legacy industrial control systems with limited security integration. Water treatment plants, for example, often operated with HMIs connected through outdated Windows workstations, while PLCs communicated over Modbus or proprietary protocols without encryption. Gas distribution networks showed similar architectures, with engineering workstations accessible via remote desktop protocols for maintenance. In many cases, IT and OT networks were insufficiently segmented, which allowed adversaries who compromised business systems to pivot into control networks. Forensic evidence indicated that CyberAv3ngers used phishing and credential theft to access administrative accounts, followed by deployment of IOControl to manipulate controller logic and disable safety interlocks. In certain facilities, operators reported abnormal readings in water flow and pressure, consistent with unauthorised PLC reprogramming. The campaign illustrated the systemic weakness of industrial environments: once attackers reached the control layer, they faced few automated barriers.

In a counterfactual scenario where cybersecurity mesh and digital immune systems had been deployed,

several improvements were observed. Mesh enforcement could have separated IT and OT domains with strict identity-based gateways, preventing lateral movement from compromised enterprise accounts (Paul *et al.*, 2024). Immune-inspired anomaly detection, embedded directly into PLC firmware or edge devices, could have flagged deviations from expected instruction sequences, such as sudden parameter changes outside of operational norms (Aldhaheri *et al.*, 2020; Bejoy *et al.*, 2022). Digital twin models of water and gas systems (Homaei *et al.*, 2025) would have enabled operators to validate whether anomalies observed in telemetry were consistent with safe operation or indicative of malicious interference, allowing rollback of controller states.

Self-healing in this environment did not mean simply rebooting a server but restoring safe configurations to PLCs and HMIs while isolating compromised nodes from the rest of the process network. Approaches combining anomaly detection with resilience engineering, as described in the literature, suggested that systems could distinguish between benign faults and targeted attacks, thereby triggering precise responses. In practice, this could have limited CyberAv3ngers' ability to manipulate water or gas flows, containing disruptions before they endangered public safety. Taken together, the two cases demonstrated the practical gap identified in the literature review. In both a municipal IT setting and an industrial OT environment, reliance on perimeter defences and manual recovery produced large-scale disruptions. The counterfactual modelling indicated that cybersecurity mesh and digital immune systems could have limited propagation, preserved essential functions, and accelerated recovery. Counterfactual modelling with cybersecurity mesh and immune principles identified the following performance differences relative to the baseline (Table 2).

Table 2. Mapping cloud security practices to critical infrastructure adaptations

Cloud security approach	Implementation in cloud environments	Challenges for critical infrastructure	Potential adaptation in critical infrastructure
Cybersecurity mesh	Distributed policy enforcement with identity as the primary perimeter. Fine-grained service segmentation, continuous verification, policy as code, local decisions at many enforcement points	Legacy SCADA has weak or absent identity layers. Flat networks, vendor protocols without native authentication, limited change windows, certification constraints	Introduce identity-centric gateways at IT-OT conduits. Enforce role-based and least-privilege access per zone and conduit, align with segmentation concepts in IEC 62443. Deploy lightweight policy decision and enforcement at DMZ and cell boundaries to confine lateral movement
Digital immune system	Behavioural analytics with adaptive baselines, automated containment in cybersecurity platform pipelines, feedback loops that refine detection and response over time)	PLCs and remote control units have limited compute and strict real-time constraints. Safety interlocks must not be disrupted by false positives. Limited telemetry fidelity on legacy controllers	Move detection to edge taps or gateway appliances that learn normal command sequences and interlock states. Use immune-inspired anomaly models to flag deviations and quarantine only the affected segment. Keep controllers deterministic while containment occurs at the network and gateway layers
Self-healing	Orchestrated rollback of workloads, immutable builds, automated failover. Resilience validated with fault injection and recovery drills in staging and production	Critical processes cannot be restarted aggressively. Manual recovery dominates. Risk-averse operations resist automation without prior assurance	Pre-authorised recovery playbooks for specific assets. Automatic restoration of known-good Virtual Machines and file services in municipal IT. For OT, safe re-imaging of controller logic to validated states with process-aware interlocks. Validation of timings and safety limits before enabling automation
Digital twins	High-fidelity replicas for safe validation of detection and automated responses. Replay of real telemetry, what-if attack simulation, measurement of mean time to repair improvements	Twin modelling is costly. Many utilities lack accurate asset inventories and process models. Limited expertise to maintain twins	Start with reduced-order twins for water flow, pressure, and feeder load. Validate immune detection thresholds and healing playbooks off-line, then promote to production with guardrails. Use twins to demonstrate safety and earn certification confidence
Zero trust	Continuous authentication, device posture checks, context-aware access, microsegmentation. Identity and policy follow the workload across environments	Operator accounts lack multi-factor authentication. Legacy HMIs cannot federate to modern Identity Providers. Shared credentials and jump hosts persist in OT	Phase in multi-factor authentication for all privileged accounts. Place protocol-aware proxies in front of HMIs and engineering workstations to enforce step-up authentication and session recording. Replace shared accounts with per-operator identities and time-bound access grants

Source: developed by the author based on the research of U. Aickelin *et al.* (2004), C. Alcaraz & S. Zeadally (2015), S. Aldhaheri *et al.* (2020), B. Bejoy *et al.* (2022), O. Johnphill *et al.* (2023), B. Paul et al. (2024), A. Alauthman & A. Al-Hyari (2025), M. Homaei *et al.* (2025)

The mapping presented in Table 2 illustrated how established cloud security practices could be systematically translated into the context of critical infrastructure. While direct transfer was limited by legacy devices, strict safety requirements, and regulatory inertia, the table highlighted feasible adaptation paths. These included the placement of identity-centric gateways IT-OT boundaries, deployment of immune-inspired anomaly detection at edge devices, pre-authorised recovery playbooks, reduced-order digital twins, and phased enforcement of zero trust controls. Collectively, these adaptations outlined a structured roadmap that aligned advanced resilience concepts with the operational realities of cyber-physical systems. The comparative analysis of the two cases showed that the absence of fine-grained segmentation was a primary factor enabling large-scale disruption. In the St. Paul incident, centralised file servers and shared virtualised environments allowed ransomware to propagate across departments without encountering isolation boundaries. In the CyberAv3ngers campaign, weak separation between enterprise IT and OT domains permitted adversaries to pivot from administrative systems into control networks. B. Ramos-Cruz *et al*. (2024) conducted a comprehensive survey of cybersecurity mesh architecture and examined scalability challenges in distributed security systems. Their analysis demonstrated that federated mesh architectures improved interoperability across heterogeneous environments but required careful integration of cryptographic protocols and artificial intelligence methods to achieve effective coordination. The authors concluded that mesh implementations faced three fundamental challenges related to scalability, distributed coordination, and technology integration, which aligned with the findings of the present study regarding segmentation enforcement in legacy infrastructures.

The integration of artificial immune systems into IoT security formed another research direction. S. Aldhaheri *et al*. (2020) provided a structured evaluation of how biologically inspired mechanisms could detect intrusions in IoT ecosystems. Their analysis showed that artificial immune systems achieved detection accuracy with resource consumption appropriate for devices with constrained processing power and memory. However, they also emphasised the need for hybrid models that combined immune algorithms with lightweight cryptography to meet the requirements of IoT nodes. U. Aickelin *et al*. (2004) developed one of the first structured immune system frameworks for anomaly detection. Their review and experimental models demonstrated how immune principles such as self/non-self discrimination and clonal selection could be codified into reference models. They concluded that immune-style orchestration reduced detection latency and provided a conceptual basis for subsequent frameworks addressing cyber resilience in smart infrastructures.

Y.Y. Yigit *et al*. (2024) examined generative artificial intelligence (AI) and its challenges and opportunities for critical infrastructure protection. Their analysis demonstrated that AI-driven threat detection enhanced the identification of advanced persistent threats in distributed environments. The authors concluded that generative AI could scale beyond information technology infrastructures into operational technology contexts, supporting mesh-based monitoring and automated response. Anomaly detection provided a second point of divergence between observed outcomes and simulated scenarios. In St. Paul, encryption activity generated statistical anomalies in file access patterns, yet no automated containment was triggered. In the water and gas facilities, manipulation of programmable logic controllers produced command sequences that deviated from established operational baselines. The scenario modelling demonstrated that immune-inspired detection mechanisms embedded at network edges could have identified these deviations within detection windows measured in seconds rather than hours. B. Krauze & J. Grabis (2024) proposed a conceptual model of digital immune systems to increase resilience in technology ecosystems. Their framework integrated adaptive immunity principles with observability, artificial intelligence-augmented testing, and chaos engineering to create self-healing capabilities. The authors emphasised that digital immune systems required continuous learning mechanisms to adapt to evolving threats, which supported the conclusion that immune-inspired approaches could have enabled near-real-time quarantine of compromised nodes in the cases analysed in this study.

Recovery and restoration processes further highlighted the difference between actual and modelled outcomes. In St. Paul, recovery required manual reinstallation of systems over several days, while in the OT case operators reloaded safe controller configurations by hand. The digital twin validation performed in this study showed that automated self-healing routines could restore known-good states through rollback of virtual machines or safe re-imaging of programmable logic controllers. The simulation indicated that downtime could be reduced from days to minutes through pre-validated recovery playbooks executed without human intervention, thereby minimising service disruption and operational losses. Domain-specific constraints influenced the feasibility of implementing mesh and immune mechanisms across different infrastructure types. Municipal IT infrastructures could feasibly adopt cloud-derived approaches with limited adaptation, as demonstrated by the St. Paul case simulation. In contrast, industrial networks relied on legacy controllers with limited computational capacity, which complicated embedding anomaly detection directly into devices. The economic dimension of resilience adoption emerged as another factor influencing practical implementation. K. Singh *et al*. (2025)

examined cybersecurity resilience and innovation ecosystems in the context of macroeconomic changes. Their cross-sectional study demonstrated that cybersecurity resilience positively influenced innovation capabilities, which in turn enhanced sustainable business excellence. However, the authors also found that macroeconomic policies and regulations moderated these relationships, indicating that external economic factors shaped organisational decisions regarding resilience investments. The scenario modelling in the present study quantified potential reductions in recovery time and containment costs, providing evidence that mesh and immune mechanisms offered measurable operational benefits. However, initial deployment required investments in identity infrastructure, monitoring capabilities, and digital twin environments. The analysis suggested that unfavourable cost-benefit perceptions among decision-makers could discourage adoption despite demonstrated technical feasibility, which aligned with the economic barriers identified by K. Singh *et al*. (2025). Governance and regulatory factors also shaped the adoption landscape. The cases examined in this study occurred in jurisdictions where cybersecurity standards for critical infrastructure emphasised compliance with baseline controls rather than adaptive resilience mechanisms. The research demonstrated that existing regulatory frameworks were not aligned with mesh and immune concepts, creating institutional barriers to implementation. Overcoming these barriers would require coordinated efforts among technical operators, policy-makers, and standards bodies to update requirements in ways that recognised the value of automated detection, containment, and recovery.

The findings of this research contributed to the broader discourse on critical infrastructure protection by demonstrating that cloud-native resilience concepts could be adapted to cyber-physical environments through systematic translation and domain-specific customisation. The scenario-based approach validated the technical feasibility of mesh enforcement and immune-inspired self-healing in constrained operational contexts, while also identifying economic, governance, and integration challenges that required attention for successful deployment. The comparative analysis with existing research confirmed that distributed, adaptive security architectures outperformed static perimeter defences in detection accuracy, recovery time, and containment efficiency. However, the translation of these concepts into resource-constrained environments demanded addressing legacy system limitations, validating safety-critical performance, and overcoming institutional resistance to automated response mechanisms.

CONCLUSIONS

The analysis of the St. Paul ransomware incident and the CyberAv3ngers campaign confirmed that both municipal IT and industrial OT infrastructures were highly exposed to targeted disruption. In each environment, the absence of effective segmentation allowed adversaries to move laterally and escalate the impact of their attacks. Scenario-based modelling demonstrated that identity-centric mesh enforcement could have contained ransomware propagation in a municipal context and restricted adversarial pivoting between IT and OT domains in industrial networks. Anomaly detection emerged as a second critical factor. In the municipal case, bursts of encryption activity, and in the industrial case, unauthorised reprogramming of controllers, produced measurable deviations from baseline behaviour. Yet no automated containment was activated. The modelling indicated that immune-inspired detection frameworks, if implemented, could have identified such deviations under constrained resources and initiated near-real-time quarantine of compromised nodes. Recovery processes further highlighted the disparity between actual and modelled outcomes. In both cases, restoration required extensive manual intervention. By contrast, scenario simulations suggested that validated self-healing mechanisms, supported by digital twin replicas and rollback routines tested in advance, could have restored essential functions automatically, reducing downtime from days to minutes. Overall, the findings of this study showed that cybersecurity mesh and digital immune system concepts, which have been successfully implemented in cloud ecosystems, could also be adapted to critical infrastructure. Their application would not eliminate all risks but would significantly reduce the scale and duration of service disruption. By combining segmentation, anomaly detection, and self-healing, operators of municipal and industrial systems could move from reactive recovery toward proactive resilience. Future work should extend the digital twin modelling to additional infrastructure sectors, conduct field trials in operational environments with appropriate safety protocols, and develop economic assessment frameworks that support resilience investment decisions.

ACKNOWLEDGEMENTS

None.

FUNDING

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Aickelin, U., Greensmith, J., & Twycross, J. (2004). Immune system approaches to intrusion detection: A review. In G. Nicosia, V. Cutello, P.J. Bentley & J. Timmis (Eds.), *Artificial immune systems* (pp. 316-329). Berlin: Springer. doi: 10.1007/978-3-540-30220-9_26.

[2] Alauthman, A., & Al-Hyari, A. (2025). Intelligent fault detection and self-healing mechanisms in wireless sensor networks using machine learning and flying fox optimization. *Computers*, 14(6), article number 233. doi: 10.3390/computers14060233.
[3] Alcaraz, C., & Lopez, J. (2012). Analysis of requirements for critical control systems. *International Journal of Critical Infrastructure Protection*, 5(3), 137-145. doi: 10.1016/j.ijcip.2012.08.003.
[4] Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, 8, 53-66. doi: 10.1016/j.ijcip.2014.12.002.
[5] Aldhaheri, S., Alghazzawi, D., Cheng, L., Barnawi, A., & Alzahrani, B.A. (2020). Artificial immune systems approaches to secure the Internet of Things: A systematic review of the literature and recommendations for future research. *Journal of Network and Computer Applications*, 157, article number 102537. doi: 10.1016/j.jnca.2020.102537.
[6] August, T., Noh, D., Shamir, N., & Shin, H. (2024). Cyberattacks, operational disruption, and investment in resilience measures. *Management Science*, 71(9), 7390-7413. doi: 10.1287/mnsc.2022.00430.
[7] Bejoy, B.J., Raju, G., Swain, D., & Acharya, B. (2022). A generic cyber immune framework for anomaly detection using artificial immune systems. *Applied Soft Computing*, 130, article number 109680. doi: 10.1016/j.asoc.2022.109680.
[8] CISA. (2023). *Critical infrastructure security and resilience*. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.
[9] CISA. (2024). *Alert (AA24-121A): CyberAv3ngers threat activity targeting water and wastewater systems*. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.
[10] De Marco, A., Berardi, D., Galuppi, M., & Lombardi, M. (2025). Quantitative resilience assessment on critical infrastructures: A systematic literature review of the last decade (2014-2024). *Journal of Safety Science and Resilience*, 6(3), article number 100201. doi: 10.1016/j.jnlssr.2025.02.002.
[11] ENISA. (2023). *ENISA threat landscape 2023*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.
[12] Ganesh Raja, M., & Jeyalaksshmi, S. (2024). Self-configuration and self-healing framework using clustering for IoT-based wireless sensor networks. *International Journal of Sensor Networks*, 24(3), article number 2350022. doi: 10.1142/S0219265923500226.
[13] Homaei, M., Mogollón-Gutiérrez, Ó., Sancho, J.C., Ávila, M., & Caro, A. (2025). A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*, 57, article number 201. doi: 10.1007/s10462-024-10805-3.
[14] Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems*, 34(1), aticle number 2479546. doi: 10.1080/12460125.2025.2479546.
[15] Johnphill, O., Sadiq, A.S., Al-Obeidat, F., Al-Khateeb, H., Taheir, M.A., Kaiwartya, O., & Ali, M. (2023). Self-healing in cyber-physical systems using machine learning. *Future Internet*, 15(7), article number 244. doi: 10.3390/fi15070244.
[16] Krauze, B., & Grabis, J. (2024). A conceptual model of digital immune system to increase the resilience of technology ecosystems. In J. Araújo, J.L. de la Vara, M.Y. Santos & S. Assar (Eds.), *Research challenges in information science* (pp. 82-96). Cham: Springer. doi: 10.1007/978-3-031-59465-6_6.
[17] Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., & Liu, Q. (2024). Dissecting zero trust: Research landscape and its implementation in IoT. *Cybersecurity*, 7, article number 20. doi: 10.1186/s42400-024-00212-0.
[18] López-Vilos, N., Valencia-Cordero, C., Souza, R.D., & Montejo-Sánchez, S. (2023). Clustering-based energy-efficient self-healing strategy for WSNs under jamming attacks. *Sensors*, 23(15), article number 6894. doi: 10.3390/s23156894.
[19] Ma, T., Ali, S., & Yue, T. (2021). Testing self-healing cyber-physical systems under uncertainty with reinforcement learning: An empirical study. *Empirical Software Engineering*, 26, article number 52. doi: 10.1007/s10664-021-09941-z.
[20] Mchirgui, N., Quadar, N., Kraiem, H., & Lakhssassi, A. (2024). The applications and challenges of digital twin technology in smart grids: A comprehensive review. *Applied Sciences*, 14(23), article number 10933. doi: 10.3390/app142310933.
[21] Naqvi, M.A., Malik, S., Astekin, M., & Moonen, L. (2022). On evaluating self-adaptive and self-healing systems using chaos engineering. In *2022 IEEE international conference on autonomic computing and self-organizing systems (ACSOS)* (pp. 1-10). California: IEEE. doi: 10.1109/ACSOS55765.2022.00018.
[22] Paul, B., *et al.* (2024). Potential smart grid vulnerabilities to cyber attacks: Current threats and mitigation strategies. *Heliyon*, 10(19), article number e37980. doi: 10.1016/j.heliyon.2024.e37980.
[23] Ramos-Cruz, B., Andreu-Perez, J., & Martínez, L. (2024). The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research. *Neurocomputing*, 581, article number 127427. doi: 10.1016/j.neucom.2024.127427.

[24] Rathnayaka, B., Robert, D., Adikariwattage, V., Siriwardana, C., Meegahapola, L., Setunge, S., & Amaratunga, D. (2024). A unified framework for evaluating the resilience of critical infrastructure: Delphi survey approach. *International Journal of Disaster Risk Reduction*, 110, article number 104598. doi: 10.1016/j.ijdrr.2024.104598.
[25] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M.A., Amir, A., Vuda, K.V., & Sarwat, A.I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-attacks on critical infrastructure: A 20-year perspective. *Sensors*, 23(8), article number 4060. doi: 10.3390/s23084060.
[26] Sen, O., Bleser, N., & Ulbig, A. (2024). Digital twin for evaluating detective countermeasures in smart grid cybersecurity. *ArXiv*. doi: 10.48550/arXiv.2412.03973.
[27] Singh, K., Chatterjee, S., Mariani, M., & Wamba, S.F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. *Technovation*, 143, article number 103219. doi: 10.1016/j.technovation.2025.103219.
[28] Yigit, Y.Y., Ferrag, M.A., Sarker, I.H., Maglaras, L.A., Chrysoulas, C., Moradpoor, N., & Janicke, H. (2024). Generative AI, challenges, and opportunities for critical infrastructure protection. *ArXiv*. doi: 10.48550/arXiv.2405.04874.
[29] Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, 156, article number 103414. doi: 10.1016/j.adhoc.2024.103414.

Сітчасті архітектури та імунно-натхненні механізми у захисті критичної інфраструктури

Вікторія Семеренська
Аспірант
Харківський національний університет радіоелектроніки
61166, просп. Науки, 14, м. Харків, Україна
https://orcid.org/0009-0008-2955-3676

Анотація. Критична інфраструктура дедалі більше функціонує у взаємопов'язаних, програмно-орієнтованих середовищах і водночас зазнає цілеспрямованих кібератак, що зупиняють ключові сервіси. Традиційні периметральні підходи виявляються недостатніми, оскільки дозволяють атакувальникам перебувати в системах тривалий час і залишають вразливими механізми відновлення. Метою дослідження було оцінювання перенесення mesh- та immune-підходів у сфери водопостачання, енергетики та муніципальних послуг і демонстрація їхнього впливу на стійкість у реальних інцидентах. Методологія поєднувала огляд шаблонів безпеки у хмарі, порівняльний аналіз кейсів та сценарне моделювання загроз. Було розглянуто дві події: кібератаку на муніципальну інфраструктуру великого міста США та транснаціональну кампанію проти операційних технологій у сфері води й газу. У першому випадку відсутність сегментації дозволила вірусу безперешкодно поширитися між мережевими сегментами, тоді як у другому брак автоматизованого моніторингу призвів до затримки у виявленні вторгнення. Для кожної події прогресія атаки була зіставлена з контрольними точками, де розподілені вузли контролю, сегментація на основі ідентичності та петлі зворотного зв'язку могли б обмежити наслідки та ініціювати автоматизоване відновлення. Отримані результати підтвердили, що mesh у поєднанні з імуноподібними реакціями забезпечував швидшу ізоляцію, контрольовану деградацію та відновлення на основі поведінкових сигналів, таких як аномальні команди чи зміни конфігурацій. Симуляційне моделювання показало, що середній час відновлення системи скорочувався на 35-40 % у сценаріях із сітчастою архітектурою, а поширення атаки обмежувалося одним сегментом замість чотирьох. Практична цінність роботи полягає у наданні дорожньої карти для поступового вдосконалення систем моніторингу без повного редизайну, що є корисним для операторів критичної інфраструктури та промислових підприємств

Ключові слова: стійкість; операційні технології; розподілений контроль; сегментація; кіберстійкість; цифрові двійники