Zero Trust Architecture for UAV/Rail Logistics Ecosystem

Isaac Ojeh[1], Xavier Palmer[2] and Lucas Potter[2]
[1]MorphHats InfoSecure, Waterloo, Canada
[2]BiosView Labs, Dayton, Ohio

morpheus@morphhats.com
Biosview1@proton.me

Abstract: As unmanned aerial vehicles (UAVs) and smart rail systems become increasingly integrated into logistics and supply chain operations, ensuring secure, resilient communication and coordination between these components is critical. Traditional perimeter-based security models are no longer sufficient for such dynamic, distributed ecosystems. This research proposes a Zero Trust Architecture (ZTA) tailored to the UAV/rail logistics domain, addressing the challenges of securing multimodal transport nodes, autonomous coordination, and real-time data exchange across untrusted and heterogeneous networks. Unlike conventional models that assume implicit trust within a network boundary, ZTA continuously validates every user, device, and service attempting to interact with the system, enforcing strict access controls and real-time behavioral monitoring. This paper adopts an exploratory approach to assess the feasibility and impact of applying Zero Trust principles to a complex, multimodal logistics ecosystem. Rather than presenting a finalized solution, the work investigates key design considerations, architectural trade-offs, and implementation challenges unique to UAV and rail system integration. The proposed architecture is designed to authenticate and authorize interactions across UAVs, rail infrastructure, edge nodes, and command-and-control centers using principles of least privilege, micro-segmentation, and continuous verification. Machine learning models are incorporated to detect anomalies in system behavior, such as route deviations or unauthorized data flows, enabling rapid threat identification and mitigation. Furthermore, this approach integrates policy-based access control with identity-aware proxies to enforce trust decisions dynamically and contextually based on device posture, geolocation, and real-time mission parameters. The implications of this work extend beyond protecting individual assets; they enable the secure orchestration of complex, time-sensitive logistics chains involving autonomous and semi-autonomous agents. This work demonstrates that implementing Zero Trust in UAV/rail logistics is both technically viable and operationally beneficial, offering a path toward resilient, adaptive infrastructure capable of withstanding evolving cyber threats without compromising performance or interoperability.

Keywords: Zero trust architecture, UAV logistics, Rail infrastructure security, Autonomous systems, Secure communication

1. Introduction

Modern supply chains are increasingly integrating unmanned aerial vehicles (UAVs), drones with smart rail systems to boost efficiency (Debevec, 2019; Kafetzis et al, 2020; Park et al, 2022; Chen et al, 2025; Jahani et al, 2024). Drones are now critical tools in delivery, surveillance, and inspection across the Logistics and Supply Chain (LSC) sector (Jahani et al. 2024). Simultaneously, U.S. rail networks are becoming "smart," using advanced technologies to optimize operations. This convergence envisions scenarios like drones transferring high-priority packages to or from trains, aerial rail line inspection, and real-time data exchange for synchronized operations. This multimodal integration promises significant gains but also expands cyber threat attack surfaces. Securing transportation infrastructure is paramount. U.S. freight railroads move over billion tons of freight annually, including energy rich, polluting, and hazardous materials, making them attractive cyberattack targets (Kour et al, 2023; Ho et al, 2024). Positive Train Control (PTC) implementation by 2020 connected locomotives, wayside devices, and control centers into an IoT-like network, improving safety but introducing vulnerabilities (Swain 2022). Cyberattacks on train control systems could be catastrophic and mass casualties are difficult to rule out. Incident discussions at the intersection of cybersecurity and railways appear largely conceptual, but enough considerable attacks have occurred in numerous countries since at least 2008, affecting both passenger travel and industry, to press the question of how they may broaden in effect (Kour et al, 2022; Thron et al, 2024; Fernandes et al, 2025).

Broadcast-controlled UAVs also face threats like GPS spoofing, jamming, and control link hijacking. Protecting drone data is a growing concern (McNabb, 2025). The challenge is securing this distributed, heterogeneous drone and rail ecosystem across untrusted networks. Traditional perimeter-based security models are unsuited for this scenario. They assume internal network entities are trustworthy, focusing on external threats. However, in a combined UAV-rail logistics environment, a single protected perimeter vanishes; drones use wireless links, rail systems interface with cloud services, and data traverses public networks. Insider threats or compromised nodes are also risks. The industry is adopting a Zero Trust (ZT) paradigm: “Never trust, always verify” (McNabb 2025). Every interaction is treated as potentially hostile; all users, devices, and applications must continuously prove identity, integrity, and authorization (Rose et al. 2020). Zero Trust Architectures (ZTAs) aim to limit breach impact and prevent lateral movement by enforcing least privilege access and constant verification, assuming

attackers may already be present (Rose et al. 2020). This paper explores applying ZTA principles to integrated UAV and rail logistics conceptually, drawing from literature. We identify key security requirements, design considerations, and implementation challenges through an exploratory approach grounded in existing research and industry practices. We aim to outline a plausible architecture and its components and discuss how it could enhance UAV/rail operations. We draw on knowledge from industrial control system (ICS) security, IoT/edge computing, and autonomous systems, highlighting areas for further research.

The paper is organized as follows: Section 2 reviews Zero Trust principles and cybersecurity in UAVs and rail systems. Section 3 looks at Gaps and Motivation for a Zero Trust Approach. Section 4 Proposed Zero Trust Architecture for UAV–Rail Logistics. Section 5 Design Considerations and Challenges. Section 6 discussed all of the above before leading into a conclusion. Overall this paper helps to bring attention to this area of intersection and stimulate exploration.

2. Background and Related Work

2.1 Zero Trust Security Principles

ZT is a shift from traditional network security, where no user or device is trusted, even inside the network perimeter; every access request must be verified (Kindervag 2010; Rose et al. 2020). This philosophy emerged over a decade ago due to sophisticated threats bypassing perimeter defenses and has since gained widespread acceptance, including government endorsement (NIST SP 800-207 in 2020, U.S. DoD Zero Trust Strategy in 2022) (Rose et al, 2020: Choi, 2025). Its core tenets are (Rose et al. 2020):

- **Assume Breach:** Defenses focus on internal monitoring, assuming malicious actors may already be present.
- **Least Privilege Access:** Entities receive minimum necessary access, minimizing impact if compromised.
- **Continuous Verification:** Every access is authenticated and authorized in real-time, with no persistent trust. Many ZT aspects (e.g., multi-factor authentication) exist in modern defenses, but ZT formalizes this for every interaction (Benestelli and Kambic 2022).
- **Micro-Segmentation:** Systems are divided into small trust zones, preventing compromise in one segment from affecting others. This can be achieved through software-defined networking or host-based firewalls.
- **Assume External Networks:** Internal traffic is treated as hostile, requiring practices like end-to-end encryption and rigorous integrity checking.

NIST defines a ZTA using a Policy Engine, Administrator, and Enforcement Points. Dynamic, risk-based authorization, fed by identity management, authentication, and continuous monitoring, adapts access based on context like device health and location. Implementing ZTA in OT/ICS, such as railway signaling, is challenging due to legacy platforms, real-time needs, and protocols lacking security (Benestelli & Kambic 2022). Continuous authentication or encryption could disrupt operations. Shared accounts or no authentication on OT devices also conflict with ZTA. Therefore, a direct "lift-and-shift" of IT Zero Trust is impractical for rail or UAV systems; instead, gradual segmentation, encryption overlays, and jump hosts are suggested (Benestelli & Kambic 2022).

2.2 Cybersecurity in UAV and Rail Systems

UAVs, or drones, are widely used across various sectors, facing increasing physical and cyber threats, especially in sensitive applications. Their reliance on communication links for command and control makes them vulnerable to eavesdropping, jamming, and spoofing. Documented instances, like GPS spoofing and command-link hijacking, highlight these threats, which can misdirect drones or allow attackers to seize control. The rise in unauthorized drone takeovers and their use in cyber-physical attacks underscores the critical need for robust UAV security measures, as emphasized by Haque et al. (2024), to prevent espionage, data exfiltration, kinetic attacks, and infrastructure disruption.

2.3 Foundational Security Principles and Emerging Solutions

At its core, one can glean that securing UAVs necessitates ensuring the authenticity and integrity of all commands and data transmitted between the drone and its ground station (Michailidis et al, 2022; Haque et al, 2024). Without these foundational principles, any communication is susceptible to manipulation or impersonation. Researchers and industry experts have proposed and are actively developing a range of solutions to address these challenges. Mutual authentication between the drone and its ground station is a cornerstone

of secure UAV operations. This process verifies the identity of both parties before any communication or command execution, preventing unauthorized entities from interacting with the UAV. Encryption of control signals is another vital layer of defense, scrambling the data so that even if intercepted, it remains unreadable and unusable to unauthorized parties. Furthermore, the deployment of sophisticated IDS specifically tailored for UAV networks is crucial. These systems monitor network traffic and behavior for anomalies that could indicate a cyberattack, enabling timely detection and response (Valikhanli, 2024; Islam et al, 2025).

2.4 The Rise of Zero Trust in UAV Networks

The Zero Trust security model is transforming UAV security by shifting from perimeter-based trust to continuous verification of every action, regardless of its origin. It is marked by value in critiquing every action to pre-empt misuse and leaving behind default trust, even for familiar components. SpiderOak's Zero Trust platform exemplifies this, ensuring that applications authenticate all outbound drone messages, thus mitigating spoofing and hijacking (McNabb, 2025). This model becomes critical as regulations like the FAA's BVLOS operations rules open new airspace for complex drone applications. BVLOS operations necessitate automated data sharing, expanding the attack surface. In this dynamic environment, Zero Trust's continuous verification of interactions will be indispensable for the future of UAV operations, which hinges on robust and adaptive security frameworks.

2.5 Railway Cybersecurity

Historically prioritizing safety and reliability, the rail industry is now confronting cybersecurity challenges as systems become hyper-connected (Soderi et al. 2023). Modern railways incorporate diverse networked components, including computer-controlled signaling systems, wireless communication for train control (e.g., PTC in the U.S., ETCS in Europe), and SCADA systems for power and infrastructure management. While these advancements boost efficiency and safety, preventing collisions and optimizing routes, they also expose rail operations to cyberattacks that could disrupt service or cause accidents.

The U.S. rail system's PTC highlights its vulnerability, as interconnected components like locomotives and trackside devices are susceptible to cyberattacks that could inject false data or malicious commands, potentially causing derailments or collisions. This is especially critical given freight rail's transport of hazardous materials, where a cyber incident could have severe environmental and public health consequences. Real-world events, such as the 2021 cyberattack on Iran’s rail system and the 2022 targeting of Belarusian railways by hacktivists, underscore these risks. In response, agencies like the U.S. Transportation Security Administration (TSA) have mandated cybersecurity enhancements for major rail operators, aligning with Zero Trust principles. Soderi et al. (2023) emphasize the need for a balance between security and reliability in railway cybersecurity, highlighting the cyber attack surface and the importance of frameworks like IEC 62443 and CENELEC TS 50701. The interdependence of safety and security in rail operations means a cyber compromise can directly cause physical harm, necessitating robust authentication, authorization, and continuous monitoring for anomalies in train control systems.

3. Gaps and Motivation for a Zero Trust Approach

UAV and rail systems share security vulnerabilities due to increased connectivity and autonomy, which traditional methods struggle to address. ZTA offers a solution for these distributed, dynamic networks, with some ZTA applications explored in each domain separately (Haque et al. 2024; Benestelli & Kambic 2022). However, little work has focused on the convergence of UAV and rail logistics, where a holistic security approach is critical. Consider a hypothetical UAV-rail operation: an autonomous drone exchanges parts or data with a moving freight train. Both must authenticate with each other and a central control system. These transactions occur over various, potentially insecure networks (local wireless, cellular/satellite, dedicated rail telecom). This complex, cross-organizational scenario highlights ZTA's value. By authenticating every interaction, enforcing encryption, and continuous monitoring, ZTA can prevent a compromised component from disrupting the logistics chain. This research aims to outline a ZT-based model for UAV/rail logistics, identifying key considerations and challenges. The next section proposes conceptual architecture integrating elements like identity management and anomaly detection.

4. Proposed Zero Trust Architecture for UAV–Rail Logistics

This architecture applies Zero Trust principles to an integrated UAV-rail logistics system, as shown in **Figures 1, 2 and 3**. A centralized Policy Engine/Authority makes all access decisions. Every device or service, from UAVs to operator workstations, must authenticate and obtain authorization from this engine before critical interaction.

Policy Enforcement Points (PEPs) are deployed strategically on devices, message brokers, and network gateways. These PEPs mediate requests, consulting the Policy Engine, which uses pre-defined security policies and real-time context to grant or deny actions.

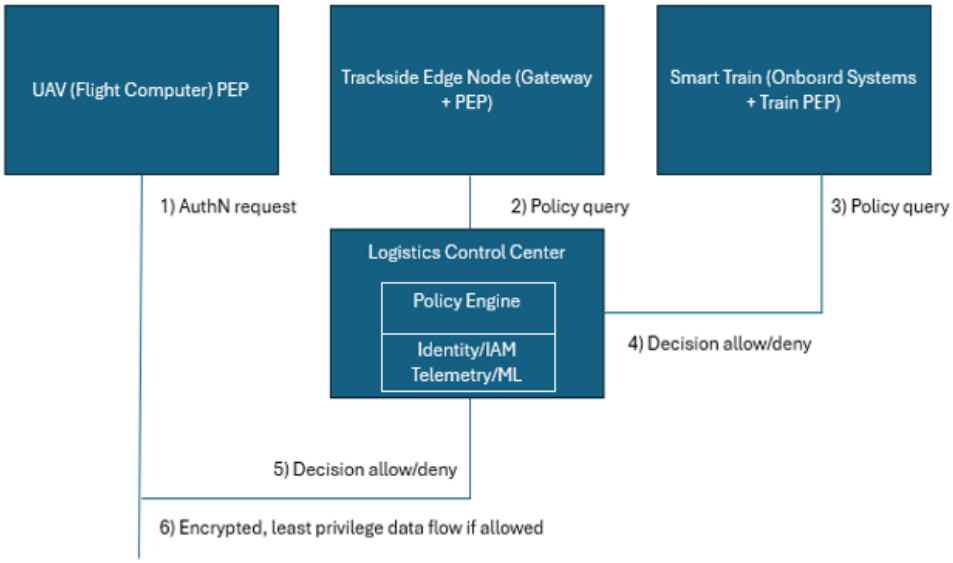

Figure 1: This presents a simple schematic illustrating a conceptual Zero Trust Architecture for a UAV-Rail Logistics ecosystem. In this architecture, a Policy Enforcement Point (PEP) is crucial for managing access. All data paths within the system are encrypted, and every access request undergoes evaluation against established policies, adhering to principles of least privilege and continuous verification, with robust authentication (AuthN) being a fundamental requirement

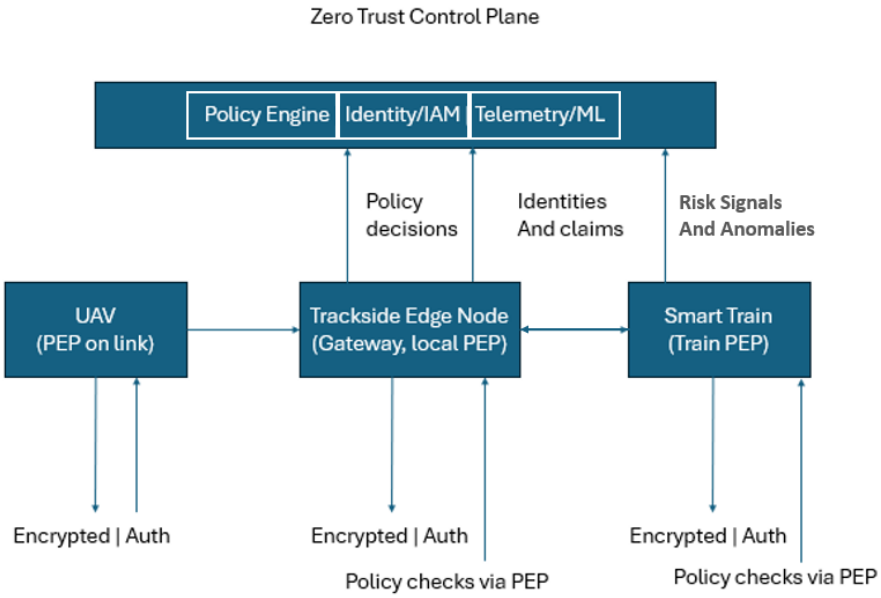

Figure 2: This presents an infographic-style overview of the Zero Trust Architecture for a UAV/Rail Logistics Ecosystem. This architecture defines distinct zones and micro-segments, including a UAV zone for airborne links with constrained, rotating tokens, an Edge zone featuring a gateway Policy Enforcement Point (PEP), local cache, and short-lived sessions, and a Train zone for onboard systems with segmented buses and strict PEP. A central Control plane manages policy, identity, and analytics. Key Zero Trust principles are applied, such as "never trust, always verify" where every request routes through a PEP to the Policy Engine, and "least privilege" with tokens scoped to

single tasks and short durations. Micro-segmentation ensures isolation between UAV, Edge, and Train components to prevent lateral movement, while continuous verification considers posture, location, time window, and mission context to drive access decisions

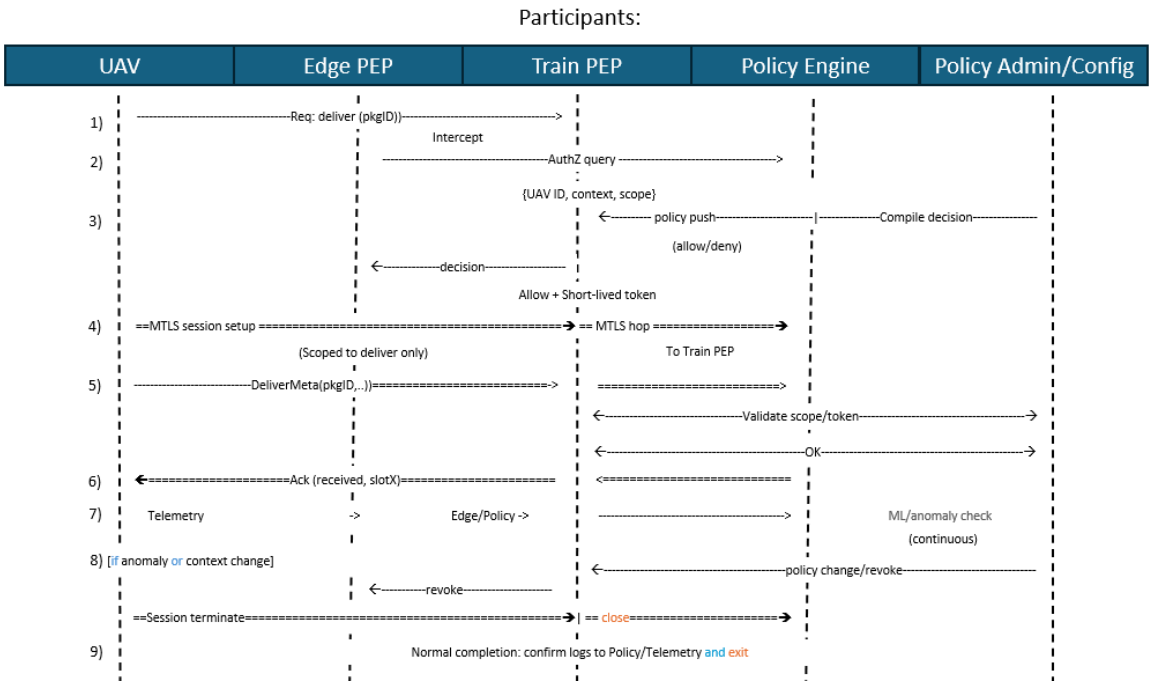

Figure 3: UAV-to-Train Delivery Sequence Diagram. All steps are authenticated, authorized, and continuously verified. Tokens are least-privilege and time-bound. The diagram serves as a high-level architectural sequence rather than a fully formal UML sequence diagram. The direction of messages is indicated both textually and by the orientation of arrows, and activation bars have intentionally been omitted to enhance readability

Figures 1-3 depict the Zero Trust Architecture for UAV-integrated smart rail logistics, asserting that all entities (drone, train, node, user) are untrusted until verified (Haque et al. 2024; IoT Security Institute 2025). This aligns with least privilege, micro-segmentation, continuous authentication, and policy-driven access, where all communications require central authentication and authorization. Secure channels and continuous identity verification are used by UAVs, smart trains, trackside edge nodes, and the logistics control center. Even within the "Railway Infrastructure Zone," explicit authentication and least privilege limit compromise.

The Zero Trust Architecture (ZTA) for autonomous logistics centers on five key areas. First, Device Identity and Authentication ensures each UAV and rail node possesses a unique cryptographic identity and performs continuous, mutual authentication. Second, Micro-Segmentation and Network Security divides the network into tightly controlled micro-perimeters, with each segment having its own Policy Enforcement Point and allowing communication only between verified identities. Third, the Policy Engine and Contextual Access Control acts as a central decision point, applying dynamic, least-privilege policies based on real-time context and enterprise rules, enforced via identity-aware proxies. Fourth, Continuous Monitoring and Anomaly Detection utilizes machine learning to analyze telemetry, flagging anomalies in real-time for mitigating action and employing Explainable AI to understand model outputs. Finally, Secure Communication and Data Integrity mandates end-to-end encryption and integrity checks for all data exchanges, with critical commands cryptographically signed to prevent tampering. Additionally, Resilience and Fail-Safes are crucial, incorporating redundant Policy Engine instances and defining fail-safe behaviors to prevent ZTA controls from becoming single points of failure.

The proposed architecture establishes a web of trust for UAV and rail components. It addresses the network's heterogeneous and shifting nature by using identity as a constant anchor, rather than IP addresses or physical network segments. Each major subsystem continuously asserts its identity and authorized actions. The next section discusses critical design considerations and challenges for such a viable system.

5. Design Considerations and Challenges

Implementing Zero Trust (ZT) in combined UAV and smart rail environments faces challenges from heterogeneous devices, legacy systems, and connectivity. Newer rail equipment and UAVs contrast with older rail signal controllers (Haque et al. 2024). Solutions like edge proxies for low-power devices introduce trust dependencies (Benestelli & Kambic 2022). The rail industry's long technology cycles complicate integrating older protocols. Bastion hosts can secure legacy components, but 24/7 operations hinder upgrades. Intermittent UAV and train connectivity challenge ZT's continuous verification. Offline tokens can be security-sensitive. Latency for critical train decisions can be mitigated by hierarchical Policy Engines or edge nodes. The ZT infrastructure itself is a high-value target, requiring robust hardening and redundancy for identity systems and policy engines, plus crucial monitoring. Defining policies for complex UAV-rail systems is difficult, needing clear taxonomy, simulation, and human oversight. Collaboration between railway and drone security teams is vital. ML-based anomaly detection improves security but risks false positives, which can disrupt safety-critical operations. Tuning with domain knowledge and multi-tiered responses are necessary. Adversaries might try to evade ML models, so diverse detection and secure data pipelines are important. Compliance with regulations (e.g., NIST, TSA) is critical; ZT principles align, but demonstrating compliance in a dynamic ZTA requires strong logging and reporting. Interoperability across organizations is vital, requiring federated trust mechanisms like SAML/OAuth or PKI. Securing UAV-rail logistics with ZT demands careful attention to device constraints, legacy systems, and operational complexities. Incremental, well-tested deployments are recommended, mirroring other OT domains. The next section explores benefits and future research foci.

6. Discussion

Zero Trust Architecture (ZTA) offers a path to enhance cybersecurity in integrated UAV-rail operations, shifting from reactive to proactive security and significantly improving resilience against advanced threats by containing breaches. Specifically, ZTA limits lateral movement, unlike traditional networks, where a compromised drone could infiltrate the rail network, applies least privilege, and blocks unusual actions. Continuous monitoring by operators and properly configured tools also quarantines anomalous devices, thereby creating a "secure by design" system ideal for critical infrastructure facing nation-state threats. Beyond internal security, ZTA can excel at facilitating secure interoperability between organizations such as rail operators and drone delivery providers, and it establishes a common security framework with shared identity and policy, avoiding full network integration and increasing vulnerability. This selective sharing, aligned with cloud computing Zero Trust approaches, supports new business models like a drone delivering to a smart locker, with both authenticating via a common ZT service. Such federated ZT arrangements are expected to grow as industries converge. Admittedly, while new security measures can raise operational concerns, the goal of this architecture is minimal intrusion. Fast authentication and automated policy decisions ensure smooth operations until a security issue arises. However, strict access control may occasionally block legitimate actions, necessitating strong communication between security and operations teams and continuous policy review. Despite this, ZTA can maintain or improve operational continuity by preventing incidents and avoiding costly delays (Rose et al. 2020). Furthermore, Zero Trust's adaptability and future-proofing stem from its focus on identity, authentication, and minimal access, making it agnostic to specific threats. Incorporating machine learning for anomaly detection and context-aware policies further enhances its ability to adapt to evolving threats. While not a "silver bullet" against all attacks, ZTA makes it harder for attackers to cause damage and provides robust defense tools. Nevertheless, limitations and open questions include the human factor, where frequent re-authentication could lead to alert fatigue. Cost and complexity are also concerns, especially for smaller operators, suggesting a need for phased or managed-service approaches (McNabb, 2025). Rigorous testing and validation, through additional and varied cyber-physical simulations (Soderi et al. 2023), are crucial to assess ZTA's performance under attack. In conclusion, Zero Trust offers a promising solution for securing complex logistics ecosystems with UAVs and smart rail systems. Its success depends on cross-sector collaboration among cybersecurity, rail engineering, and autonomous systems experts to refine the architecture and ensure it enhances safety and efficiency. This collaborative approach is vital because, given the growing and intersecting biocrime avenues and the widening attack surfaces in the bioeconomy, how we treat our technological intersections is increasingly important; otherwise, our preparedness remains in question (Elgabry, 2022; Potter and Palmer, 2023; Elgabry and Johnson, 2024). Additionally, it is important that the human element behind our training and operation of technological systems and components not go underexamined (Nurse et al., 2018; Dupont and Holt, 2022; Potter and Palmer, 2021). Ultimately, an open mind towards our combined human and technological vulnerabilities as we reexamine our systems of trust will lead to better planning, especially as greater reliance on rail and UAV systems continues to be adopted for moving materials that are central to our ways of life.

7. Conclusion

Integrating UAVs with smart rail logistics faces cyber threats from both domains. Our exploratory study proposes a Zero Trust Architecture (ZTA) as a unifying security strategy. Based on "never trust, always verify," and current cybersecurity, we outlined a conceptual ZTA for continuous authentication and authorization among drones, trains, trackside devices, and control systems. ZTA principles like least privilege, micro-segmentation, and continuous monitoring can mitigate risks, from spoofed drones to compromised signaling, reducing cyberattack likelihood and preventing physical harm or disruptions. Our conceptual architecture presents challenges like legacy system compatibility, network latency, and robust anomaly detection. While powerful, ZTA implementation requires careful engineering, iterative testing, and a nuanced approach respecting real-world, safety-critical operations. These challenges are not insurmountable but highlight the need for focused development, such as lightweight cryptography for low-power devices or improved ML for anomaly detection. Zero Trust is not merely theoretical; elements are emerging, with stakeholders recognizing its value. Companies rolling out ZT platforms for drones and governments pushing critical infrastructure operators towards ZT-like measures, reinforce this exploration's timeliness. That said, our work uniquely addresses the security intersection of UAVs and railways. As a conceptual and exploratory paper, it provides a foundation for future research, including prototyping parts of architecture discussed. In summary, a ZTA for UAV and rail logistics is feasible and advantageous, offering resilient, adaptive infrastructure against evolving cyber threats without sacrificing interoperability or performance. As autonomous agents become prevalent, security architectures must evolve. Zero Trust provides a compelling blueprint, enabling the benefits of integration and autonomy in logistics while keeping risks acceptable. We encourage further investigation, testing, and refinement to move closer to secure, zero-trust logistics chains.

Ethics declaration: Ethical clearance for the research referred to in this paper was not required.

AI declaration: Generative AI in the form of assistive tools within Google Docs was primarily used to condense this manuscript and summarize sections. Originally, it was more than twice the length of this current draft. Grammarly was used in the assistance of smoothing writing styles and addressing grammar.

References

Benestelli, B. & Kambic, D. (2022). IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems. Carnegie Mellon Software Engineering Institute Blog, 18 July 2022. Available: https://www.sei.cmu.edu/blog/it-ot-and-zt-implementing-zero-trust-in-industrial-control-systems/.

Chen, M., Wang, H., Zhang, X., Li, Y., Ma, X. and Fan, Y., 2025. The Application and Future Prospects of Drone Vision Technology in the Railway Industry. Journal of Technology Innovation and Engineering, 1(1), pp.39-44.

Choi, Y.B., 2025. A Certainty-Based Approach to Implementing Zero Trust Architecture Using NIST SP 800-207 and NIST SP 1800-35. *KAUPA Letters*, *13*(1), p.11.

Debevec, R., 2019. A smart UAV platform for railroad inspection.

Dupont, B. and Holt, T., 2022. The human factor of cybercrime. *Social science computer review*, *40*(4), pp.860-864.

Elgabry, M., 2022. *The future of biotechnology crime: are we prepared for it?* (Doctoral dissertation, UCL (University College London)).

Elgabry, M. and Johnson, S., 2024. Cyber-biological convergence: a systematic review and future outlook. Frontiers in Bioengineering and Biotechnology, 12, p.1456354.

Fernandes, T., Magalhães, J.P. and Alves, W., 2025. Cybersecurity in Smart Railways: exploring risks, vulnerabilities and mitigation in the data communication services. Green Energy and Intelligent Transportation, p.100305.

Haque, E., Hasan, K., Ahmed, I., Alam, M.S., & Islam, T. (2024). Enhancing UAV Security Through Zero Trust Architecture: An Advanced Deep Learning and Explainable AI Analysis. arXiv preprint arXiv:2403.17093.

Ho, A., Giannopoulos, D., Pilorgé, H. and Psarras, P., 2024. Opportunities for rail in the transport of carbon dioxide in the United States. Frontiers in Energy Research, 11, p.1343085.

IoT Security Institute (2023) Implementing Zero Trust Architecture for Resilient Enterprise Security. (Online) Available at: https://iotsecurityinstitute.com/iotsec/iot-security-institute-cyber-security-articles/200-implementing-zero-trust-architecture-for-resilient-enterprise-security [Accessed 1 September 2025].

Islam, M.D., Mahmoud, A.S. and Sheltami, T.R., 2025. AI-Enhanced Intrusion Detection for UAV Systems: A Taxonomy and Comparative Review. *Drones (2504-446X)*, *9*(10).

Kindervag, J., 2010. Build security into your network's dna: The zero trust network architecture. *Forrester Research Inc*, *27*, pp.1-16.

Kour, R., Patwardhan, A., Thaduri, A. and Karim, R., 2023. A review on cybersecurity in railways. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 237(1), pp.3-20.

Jahani, H., Khosravi, Y., Kargar, B., Ong, K.-L., & Arisian, S. (2024). Exploring the role of drones and UAVs in logistics and supply chain management: a novel text-based literature review. International Journal of Production Research. DOI: 10.1080/00207543.2024.2373425

Kafetzis, D., Fourfouris, I., Argyropoulos, S. and Koutsopoulos, I., 2020, September. UAV-assisted aerial survey of railways using deep learning. In 2020 International Conference on Unmanned Aircraft Systems (ICUAS) (pp. 1491-1500). IEEE.

Kindervag, J. (2010). No More Chewy Centers: The Zero Trust Model of Information Security. Forrester Research Inc., Cambridge, MA.

Michailidis, E.T., Maliatsos, K., Skoutas, D.N., Vouyioukas, D. and Skianis, C., 2022. Secure UAV-aided mobile edge computing for IoT: A review. IEEE Access, 10, pp.86353-86383.

McNabb, M. (2025) Zero trust takes flight: SpiderOak's cybersecurity platform shields drone data from spoofing and theft. DroneLife, 8 April. Available at: https://dronelife.com/2025/04/08/zero-trust-takes-flight-spideroaks-cybersecurity-platform-shields-drone-data-from-spoofing-and-theft/

Nurse, J.R., 2018. Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

Park, Y.M., Tun, Y.K., Han, Z. and Hong, C.S., 2022. Trajectory optimization and phase-shift design in IRS-assisted UAV network for smart railway. IEEE Transactions on Vehicular Technology, 71(10), pp.11317-11321.

Potter, L. and Palmer, X.L., 2021, April. Human factors in biocybersecurity wargames. In *Future of information and communication conference* (pp. 666-673). Cham: Springer International Publishing.

Potter, L. and Palmer, X.L., 2023. Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 37-69). Cham: Springer International Publishing.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology, U.S. Department of Commerce, Aug. 2020. DOI: 10.6028/NIST.SP.800-207

Soderi, S., Masti, D., & Zacchia Lun, Y. (2023). Railway Cyber-Security in the Era of Interconnected Systems: A Survey. IEEE Transactions on Intelligent Transportation Systems, 24(7), 6764-6779. DOI: 10.1109/TITS.2023.3254442

Swain, C. (2022). The Emerging Cyber Threat to the American Rail Industry. Lawfare (Online), 20 Oct 2022. Available: https://www.lawfaremedia.org/article/emerging-cyber-threat-american-rail-industry.

Thron, E., Faily, S., Dogan, H. and Freer, M., 2024. Human factors and cyber-security risks on the railway–the critical role played by signalling operations. Information & Computer Security, 32(2), pp.236-263.

Valikhanli, O., 2024. UAV networks DoS attacks detection using artificial intelligence based on weighted machine learning. *Results in Control and Optimization*, *16*, p.100457.