Continuous Intrusion Protection Lifecycle (IPL) for Amended Vehicles: A Cyber Resilience Framework

Simeon Okechukwu Ajakwe (SMIEEE)*, and Dong-Seong Kim (SMIEEE)*
*IT-Convergence Engineering Department, Kumoh National Institute of Technology, Gumi, South Korea
Email: {simeon.ajakwe, dskim}@kumoh.ac.kr

***Abstract*—Autonomous Vehicles (AVs) are undergoing continuous evolution through software amendments, Over-the-Air (OTA) updates, and AI-driven functionalities. These dynamic changes expand the attack surface, challenging traditional, static cybersecurity models. This paper proposes a Continuous Intrusion Protection Lifecycle (IPL)—a unified, adaptive framework that integrates Security-by-Design, AI-driven detection, and blockchain-enabled forensic traceability. The lifecycle aligns with ISO/SAE 21434 and UNECE WP.29 standards while leveraging recent advances in federated learning, explainable AI (XAI), and secure OTA. The IPL operates through four interconnected phases—Plan, Implement, Operate, and Amend—ensuring cyber resilience and trustworthy autonomy across the entire vehicle lifespan.**

***Index Terms*—Autonomous vehicles, cybersecurity, intrusion detection, blockchain, explainable AI, ISO/SAE 21434, OTA.**

I. INTRODUCTION

The rise of Software-Defined Vehicles (SDV) and Connected Autonomous Vehicles (AVs) has transformed mobility but introduced unprecedented cybersecurity challenges. Amended AVs—vehicles that receive post-production hardware or software updates—demand continuous protection across their lifecycle. Traditional Intrusion Detection Systems (IDS) fail to adapt to new attack vectors, such as CAN-bus spoofing, AI model poisoning, and compromised OTA channels [1], [2]. Recent global standards (ISO/SAE 21434, UNECE WP.29, NHTSA guidelines) emphasize lifecycle-based protection, yet lack an integrated framework connecting detection, response, and recovery. To address this gap, we present a Continuous Intrusion Protection Lifecycle (IPL)—a closed-loop model embedding proactive threat modeling, AI-powered anomaly detection, blockchain auditability, and secure OTA remediation.

II. PROPOSED CONTINUOUS IPL FRAMEWORK

The proposed IPL (Fig. 1) integrates best practices from industry, AI research, and vehicular cybersecurity standards into a four-phase continuous loop: Plan → Implement → Operate → Amend.

Phase 1: Plan – Security-by-Design and TARA

This phase establishes a proactive cybersecurity baseline. Threat Analysis and Risk Assessment (TARA) is conducted not only during design but also before each amendment. Using fault-tree and attack-graph modeling [3], risks are ranked by functional safety impact. Hardware Security Modules (HSMs) and Root-of-Trust (RoT) components are defined for authentication, key management, and domain isolation.

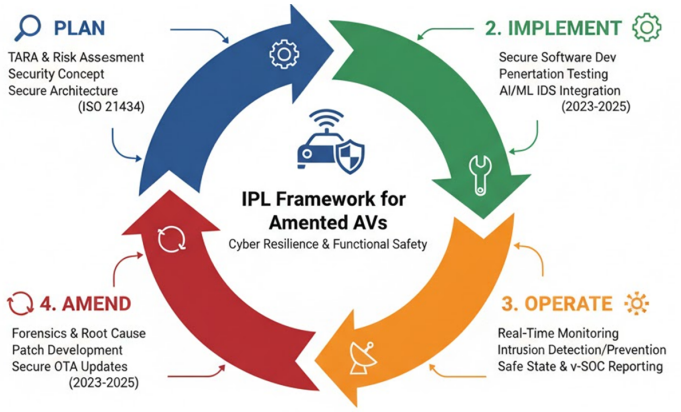

Fig. 1. Proposed Continuous Intrusion Protection Lifecycle (IPL) for amended autonomous vehicles.

2: Implement—Secure Development and IDS Integration

During implementation, code validation, SBOM verification, and secure build pipelines are enforced. AI-based IDS modules—such as CNN-LSTM hybrid models or Transformer-based few-shot detectors—are deployed for in-vehicle networks (IVN) and V2X data streams [4], [5]. Blockchain-based audit logs capture version control and verification hashes for forensic traceability.

Phase 3: Operate – Real-Time Detection and Automated Response

Once deployed, the AV operates under multi-layered surveillance through embedded IDS and in-vehicle SOC (v-SOC). Detected anomalies trigger graduated responses: (1) alert and log, (2) isolate compromised domains, (3) transition to a minimal-risk safe state. Explainable AI (XAI) techniques such as SHAP and LIME increase operator trust by revealing the reasoning behind detections [6]. Event metadata is immutably recorded on-chain for later forensic validation. In-vehicle sensors and IDSs collect vast amounts of data for real-time monitoring. The AI-based IDS identifies anomalies for safety-critical threat detection. Then, containment and a safe state for severe or uncertain intrusions are performed. All incident data is securely and promptly transmitted for reporting to v-SOC, necessary for intrusion recovery to return the vehicle to a normal and secure operational state.

Phase 4: Amend – Secure OTA and Continuous Learning

After incident verification, the v-SOC generates countermeasures and securely distributes updates via cryptographically signed OTA channels [7]. Federated learning (FL) enables fleet-wide model retraining without raw data exchange, achieving 99% accuracy in recent studies [8]. Lessons learned

are fed back into Phase 1, reinforcing the lifecycle's adaptability and continuous improvement.

III. DISCUSSION AND INDUSTRY IMPLICATIONS

The proposed IPL embodies the principle of cyber resilience through continuity. Its cyclic design ensures each amendment enhances—rather than weakens—security posture. Compared to static IDS models, the continuous IPL is positioned to achieve dynamic protection for real-time adaptation via FL and OTA updates. It will ensure blockchain-backed forensic logging for auditability. Also, XAI-assisted trust in autonomous decisions will provide feedback explainability. Seamless alignment with ISO/SAE 21434 and UNECE WP.29 will ensure compliance. When deployed across smart mobility ecosystems, this lifecycle minimizes Mean Time To Remediation (MTTR), strengthens fleet-wide situational awareness, and ensures sustainable safety assurance.

IV. ROADMAP & REQUIREMENTS FOR IPL ADOPTION

The shift from discrete hardware products to Software Defined Vehicles (SDVs) makes the Continuous Intrusion Protection Lifecycle (IPL) a fundamental requirement for legal compliance (UN Regulation No. 155) and market viability. The IPL is not merely a technical process; it demands a significant organizational and collaborative restructuring across the automotive value chain.

A. Organizational and Regulatory Imperatives

The IPL necessitates a seamless integration of Cybersecurity Management Systems (CSMS) from the Original Equipment Manufacturer (OEM) down through the entire supply chain (Tier 1, Tier 2, etc.). Suppliers must align their TARA and development processes with the OEM's master V&V (Verification & Validation) plan. Compliance with ISO/SAE 21434 [9] must be rigorously enforced and audited at every interface where software or electronic components are integrated. Also, the central role of the Vehicle Security Operations Center (v-SOC) for fleet-level incident management cannot be overstated. The v-SOC must evolve beyond basic log aggregation to become a high-velocity threat intelligence hub. It needs to process telemetric data from thousands of vehicles in real-time to correlate suspicious activities, distinguish true attacks from false positives, and issue fleet-level security directives [12]. This centralized approach is essential for guaranteeing that the Amend phase is executed rapidly and uniformly.

B. Guarantees for a Robust and Resilient IPL

To guarantee a truly robust and resilient secured IPL for amended vehicles, the following strategic and technical advancements must be universally adopted.

1) Adaptive AI-based Intrusion Detection: Resilience requires adaptive AI-driven IDSs on high-performance controllers, continuously refined via federated learning across fleets while preserving data privacy [11]. These systems detect evolving and adversarial attacks in real time with ultra-low latency, ensuring reliable perception, decision integrity, and adherence to automotive safety and cybersecurity standards [10].

2) Secure and Atomic OTA-FOTA: The Amend phase relies on a tamper-resistant OTA/FOTA infrastructure ensuring cryptographic integrity and atomicity. Each patch must be HSM-signed and verified through a Root of Trust, guaranteeing that updates either complete securely or revert to the last trusted state. This prevents bricking and new vulnerabilities. To mitigate bandwidth and resource limits, differential patching techniques minimize download size and installation time [13].

3) Safety-Security Co-Engineering and Redundancy: System robustness arises from integrating safety and security as interdependent elements. Treating attacks as potential faults mandates redundant, fail-operational designs where fallback channels maintain control, ensuring a secure transition to a minimal risk condition (MRC) through Defense-in-Depth.

4) Standardization of Incident Data: Unified standards for incident reporting across OEMs and suppliers—covering CAN logs, ECU IDs, and attack taxonomy—enable shared intelligence, rapid zero-day mitigation, and continuous IPL-driven cyber resilience for autonomous mobility.

V. CONCLUSION

This paper presents a novel Continuous Intrusion Protection Lifecycle (IPL) for amended autonomous vehicles—an adaptive, explainable, and auditable cybersecurity framework bridging design-time risk assessment with runtime defense and recovery. Future work includes implementing a blockchain-XAI-integrated prototype validated using Car-Hacking and OTIDS datasets, and measuring its performance on real-time vehicular testbeds.

ACKNOWLEDGMENT

This research was supported by the Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003) (50%) and by the Institute of Information & Communications Technology Planning & Evaluation (IITP)-Innovative Human Resource Development for Local Intellectualization program grant funded by the Korea government(MSIT)(IITP-2025-RS-2020-II201612) (50%).

REFERENCES

[1] G. Karopoulos *et al.*, "Demystifying In-Vehicle Intrusion Detection Systems," *Electronics*, vol. 11, no. 19, 2022.

[2] W. Luo *et al.*, "In-Vehicle Network Intrusion Detection Using Deep Learning: A Review," *IEEE Access*, vol. 11, pp. 153822–153840, 2023.

[3] H. Kim *et al.*, "Cybersecurity Risk Assessment for Automated Driving Systems," *IEEE Trans. Intell. Veh.*, vol. 8, no. 1, 2023.

[4] Q. Liu *et al.*, "Intrusion Detection System for Autonomous Vehicles Using Sensor Spatio-Temporal Information," *Computers & Security*, 2025.

[5] A. Althunayyan *et al.*, "Multi-Class Intrusion Detection Using Few-Shot Learning and Anomaly Transformers," *ScienceDirect*, 2025.

[6] S. O. Ajakwe *et al.*, "Medical IoT Record Security and Blockchain: Milieu, Milestones, and Momentum," *Big Data and Cognitive Computing*, vol. 8, no. 9, 2024.

[7] T. Chen *et al.*, "A Secure and Efficient Over-The-Air (OTA) Update Scheme for Vehicular Networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, 2023.

[8] R. Akinie *et al.*, "Fine-Tuning Federated Learning-Based Intrusion Detection for Transportation IoT," *arXiv preprint*, 2025.

[9] ISO/SAE 21434:2021, "Road vehicles — Cybersecurity engineering." (Current industry standard).

[10] H. Kim et al., "Cybersecurity Risk Assessment for Automated Driving Systems based on Fault Tree Analysis and Attack Graph," *IEEE Trans. Intell. Veh.*, vol. 8, no. 1, pp. 202-215, 2023.

[11] C. K. G. Anthony, W. Elgenaidi, and M. Rao, "Intrusion Detection System for Autonomous Vehicles Using Non-Tree Based Machine Learning Algorithms," *Electronics*, vol. 13, no. 5, p. 809, 2024.

[12] D. Lee and M. Park, "Designing a Collaborative v-SOC Architecture for Fleet-Wide Cybersecurity Incident Response in CAVs," *Proc. KICS Fall Conf. 2025* (Conceptual Reference).

[13] T. Chen, S. Wu, and P. Li, "A Secure and Efficient Over-The-Air (OTA) Update Scheme for Vehicular Software-Defined Networks," *IEEE Trans. Veh. Technol.*, vol. 72, no. 10, pp. 13628-13642, 2023.