Evolving and Securing the CAN Bus for Safer More Comfortable Cars

ZHANG ZHONG HENG Independent Researcher
Hong Kong SAR, China
Email: kkzhanghk@gmail.com

***Abstract*—The Controller Area Network (CAN) bus is the backbone of in-vehicle communications, coordinating electronic control units (ECUs) that affect safety, comfort, and the overall driving experience. Originally introduced to reduce wiring complexity and cost, CAN has evolved with CAN FD and the emerging CAN XL to sustain higher data throughput and larger payloads while preserving real-time behavior and robustness. Yet, classical CAN lacks built-in security and is vulnerable to spoofing, replay, and denial-of-service attacks. This paper reviews the evolution of CAN technologies and practical intrusion detection approaches, highlighting how higher bandwidth and stronger defenses translate into human-centered outcomes: safer driving through reliable advanced driver-assistance systems (ADAS), greater comfort via responsive body and infotainment functions, and intuitive ownership supported by diagnostics and software updates. We discuss how CAN XL is positioned to coexist with Automotive Ethernet in zonal architectures and outline how standards and best practices (e.g., ISO/SAE 21434, UNECE WP.29, NHTSA guidance) can be leveraged to mitigate cyber risk. By connecting protocol evolution with human factors, we argue that secure, high-performance CAN-based networks are essential for trustworthy mobility in connected and automated vehicles.**

***Index Terms*—Controller Area Network (CAN), CAN FD, CAN XL, automotive cybersecurity, intrusion detection, machine learning, human-centered design, vehicle safety, comfort**

I. Introduction

Modern vehicles comprise dozens of electronic control units (ECUs) coordinating everything from braking and steering to climate control and infotainment. The Controller Area Network (CAN) bus provides a cost-effective, robust, and real-time communication substrate that enables these functions to work together reliably.

For drivers and passengers, CAN is invisible but decisive: pressing the brake pedal, receiving lane-keeping feedback, or adjusting cabin comfort all rely on dependable message exchange. As vehicles become more connected and automated, demands on in-vehicle networking continue to grow. This paper examines the evolution from classical CAN to CAN FD and CAN XL, the security risks inherent to legacy deployments, and the state of practical defenses, with an emphasis on how these technical changes improve safety, reduce driver workload, and enhance comfort.

II. Historical Evolution and Core Principles of CAN

CAN was developed in the 1980s to reduce wiring harness complexity and cost while improving reliability. Its message-based, multi-master design uses non-destructive bitwise arbitration (often described as CSMA with collision resolution), allowing higher-priority frames to win bus access without corrupting lower-priority ones. Identifiers (11 or 29 bits) encode priority, so urgent traffic (e.g., braking) can preempt less critical messages. Classical CAN includes robust error detection (e.g., CRC), automatic retransmission, and fault confinement, which make it resilient in harsh automotive environments.

These attributes enabled real-time coordination of safety and body systems at scale, supporting mass-market adoption across powertrain, chassis, and comfort domains.

III. From Classical CAN to CAN FD and CAN XL

Classical CAN's nominal 1 Mbit/s data rate and 8-byte payload became limiting for sensor-rich and feature-dense vehicles. CAN FD introduced higher data rates in the data phase and payloads up to 64 bytes while maintaining backward compatibility at the arbitration phase. This substantially improves efficiency for control and diagnostics without abandoning CAN's timing and cost advantages.

CAN XL represents the next step toward significantly larger payloads and higher throughput, designed to better support service-oriented communication and efficient gatewaying with IP/Ethernet domains. Publicly available specifications and standardization work indicate:

- A frame format and PHY concept targeting data rates beyond those of CAN FD, with a header facilitating explicit prioritization and scalable payloads.
- Enhanced integrity protection (e.g., stronger CRC schemes) and features such as frame preemption to preserve real-time responsiveness under load.
- Coexistence with legacy CAN/CAN FD in mixed or bridged networks, enabling gradual migration.

Security for CAN XL can be augmented by community proposals such as CANsec (from CAN in Automation, CiA), which defines a data-link–adjacent security framework tailored to CAN XL's capabilities. While implementation details vary, the direction is clear: more bandwidth with mechanisms that better support secure, software-defined vehicle functions. A high-level mixed-network view is provided in Fig. 1.

IV. Security Challenges and Practical Defenses

Classical CAN lacks native authentication and encryption. As a result, compromised ECUs or external interfaces (e.g.,

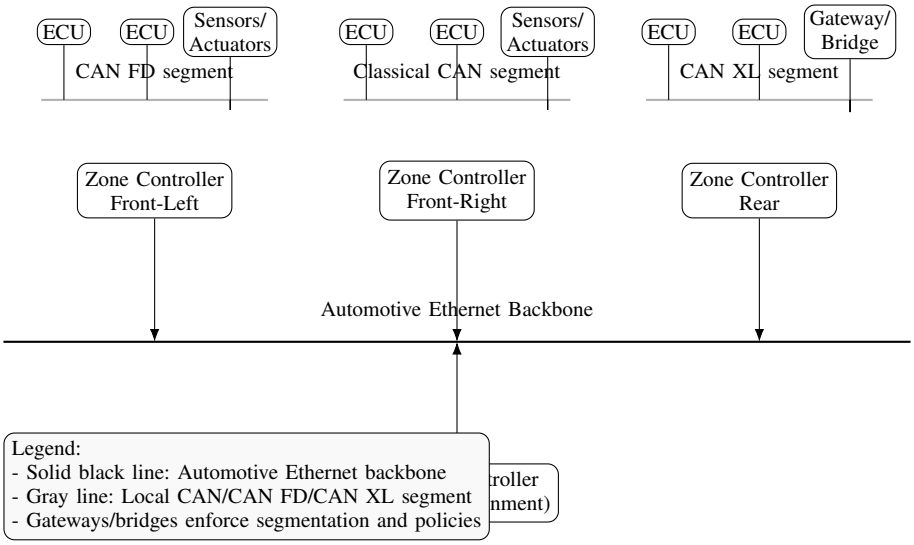

Fig. 1. High-level coexistence of CAN/CAN FD/CAN XL with an Automotive Ethernet backbone in a zonal architecture.

diagnostic access) can be abused for spoofing, replay, fuzzing, or denial-of-service attacks, potentially affecting safety-critical functions if not mitigated. Decade-long research and industry experience (including high-profile demonstrations) have established that in-vehicle networks require systematic cybersecurity engineering and monitoring.

Mitigations span:

- **Secure engineering and governance**: Applying ISO/SAE 21434 processes, adhering to UNECE WP.29 R155/R156, and following NHTSA best practices to manage risks across the vehicle lifecycle.
- **Network hardening**: Segmentation, secure gateways, tightened diagnostics, message authentication where feasible, rate limiting, and fail-safe designs.
- **Intrusion detection**: Lightweight rule-based monitors and data-driven methods (e.g., timing- or payload-modeling, one-class/autoencoder anomaly detection, 1D-CNNs, and RNNs) have shown high detection performance on public and proprietary datasets under realistic constraints. While deployment choices depend on cost, compute, and safety cases, a hybrid of specification- and learning-based detectors is increasingly practical.

A human-centered perspective emphasizes outcomes: robust defenses should operate transparently, preserving the responsiveness of safety features and minimizing nuisance alerts or maintenance burden on drivers. Fig. 2 summarizes a canonical threat surface and IDS placement.

V. Human-Centered Implications: Safety, Comfort, and Trust

A higher-performance, better-defended CAN-based backbone benefits people in tangible ways:

- **Safety**: Deterministic prioritization and resilient communications underpin ADAS features that help avoid or mitigate crashes. Security controls reduce the likelihood and impact of network-borne faults or attacks.
- **Comfort and convenience**: Larger payloads and higher throughput improve responsiveness of body, infotainment, and energy management functions, contributing to a quieter, smoother, and more personalized cabin experience.
- **Trust and usability**: Built-in diagnostics, secure over-the-air updates, and effective monitoring keep vehicles reliable and up-to-date with minimal disruption, reinforcing driver confidence.

VI. Future Directions

Zonal architectures will combine CAN XL and Automotive Ethernet, using gateways to place each technology where it fits best in terms of cost, determinism, and bandwidth. Standardization and regulation (ISO/SAE 21434, UNECE WP.29) will continue to shape security requirements. On the defense side, hybrid intrusion detection—combining rules, physical invariants, and efficient ML/AI—offers a path to robust, explainable protection that respects real-time constraints. Future work should integrate human-factors evaluation (e.g., workload, trust, perceived safety) into networking and security design to ensure technology delivers clear benefits to drivers and passengers.

VII. Conclusion

CAN has evolved from a wiring reduction strategy into a foundational enabler of safe, comfortable, and intuitive mobility. With CAN FD and CAN XL, the ecosystem can support richer features and software-defined vehicles while preserving real-time behavior and cost efficiency. Complemented by cybersecurity engineering, best practices, and practical intrusion detection, modern CAN-based networks can more reliably deliver the human-centered outcomes that matter most on the road.

References

[1] International Organization for Standardization (ISO), “Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling,” ISO 11898-1, latest edition.

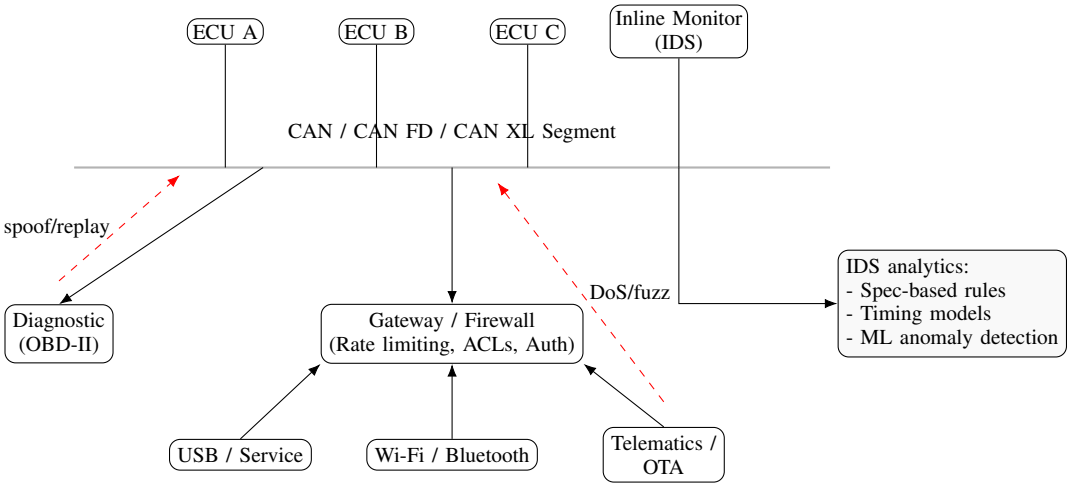

Fig. 2. Canonical threat surface and IDS placement across a mixed in-vehicle network.

[2] International Organization for Standardization (ISO), "Road vehicles — Controller area network (CAN) — Part 2: High-speed medium access unit," ISO 11898-2, latest edition.

[3] CAN in Automation (CiA), "CAN XL – CAN with eXtra Long Data Field," White Paper, accessed Mar. 2026. [Online]. Available: https://www.can-cia.org

[4] ISO/SAE, "Road vehicles — Cybersecurity engineering," ISO/SAE 21434, 2021.

[5] UNECE WP.29, "UN Regulation No. 155 (Cybersecurity) and UN Regulation No. 156 (Software Updates)," 2020.

[6] U.S. DOT, National Highway Traffic Safety Administration (NHTSA), "Cybersecurity Best Practices for the Safety of Modern Vehicles," 2022.

[7] K. Koscher, A. Czeskis, F. Roesner, et al., "Experimental security analysis of a modern automobile," in *Proc. IEEE Symposium on Security and Privacy*, 2010.

[8] S. Checkoway, D. McCoy, B. Kantor, et al., "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Security Symposium*, 2011.

[9] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat USA, 2015.

[10] M. Müter and N. Asaj, "Entropy-based anomaly detection for in-vehicle networks," in *Proc. IEEE Intelligent Vehicles Symposium*, 2011.