International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review of Cybersecurity Threats in Automotive Semiconductor Control Units

Sujan Hiregundagal Gopal Rao

Submitted:08/12/2023 **Revised:**10/01/2024 **Accepted:**20/01/2024

Abstract: The increasing dependence of modern vehicles on electronic control units (ECUs) has transformed automobiles into complex cyber-physical systems. These ECUs are built on automotive-grade semiconductor platforms that execute safety-critical and connectivity-oriented functions. While advancements in semiconductor integration have improved vehicle performance and functionality, they have simultaneously expanded the cybersecurity attack surface. This paper presents a technical review of cybersecurity threats affecting automotive semiconductor control units, focusing on vulnerabilities at the hardware, firmware, and communication levels. Industry trends, safety–security interdependencies, and mitigation strategies are examined from a semiconductor-centric perspective. The review highlights existing research gaps and identifies future directions for developing secure automotive electronic architectures.

Keywords: *Automotive cybersecurity, electronic control units, automotive semiconductors, ECU security, vehicle electronics*

1. Introduction

The automotive industry has undergone a profound transformation over the past few decades, evolving from mechanically dominated systems to highly sophisticated electronically controlled platforms. Modern vehicles are no longer simple mechanical machines; they are complex cyber-physical systems that rely on a network of interconnected electronic control units (ECUs) to manage critical functionalities such as powertrain operation, braking, steering, infotainment, and advanced driver assistance systems (ADAS). Each ECU is implemented using automotive-grade microcontrollers or system-on-chip (SoC) architectures, designed to meet stringent reliability, fault-tolerance, and real-time performance requirements essential for safe vehicle operation.

Traditionally, ECUs operated as isolated modules with limited exposure to external networks. Cybersecurity was not a primary design consideration, as vehicles were largely "air-gapped" from potential remote attacks. However, the integration of wireless connectivity, over-the-air (OTA) software updates, telematics, and vehicle-to-everything (V2X) communication has significantly expanded the attack surface, exposing automotive semiconductor control units to remote cyber threats. A successful attack on an ECU can compromise vehicle functionality, degrade safety-critical operations, or even allow malicious actors to gain full vehicle control.

Automotive semiconductor control units face unique design constraints that distinguish them from conventional IT systems. They must operate reliably over long lifetimes, adhere to strict real-time deadlines, maintain cost-effectiveness, and withstand harsh environmental conditions, such as extreme temperatures, vibration, and electromagnetic interference. These constraints complicate the integration of traditional cybersecurity solutions, which are often resource-intensive and incompatible with embedded automotive hardware.

This review focuses on cybersecurity vulnerabilities inherent to automotive semiconductor control units, with particular emphasis on hardware and embedded system weaknesses rather than purely software-centric issues. By analyzing threats from a hardware perspective, this study underscores the critical importance of incorporating security-aware design practices in ECUs to ensure safe and resilient vehicle operation in an increasingly connected automotive ecosystem.

sujangopalrao@gmail.com
Independent Researcher, USA

Figure 1 illustrates the typical architecture of a modern vehicle's ECUs, showing internal connections, external interfaces, and potential cyberattack vectors.

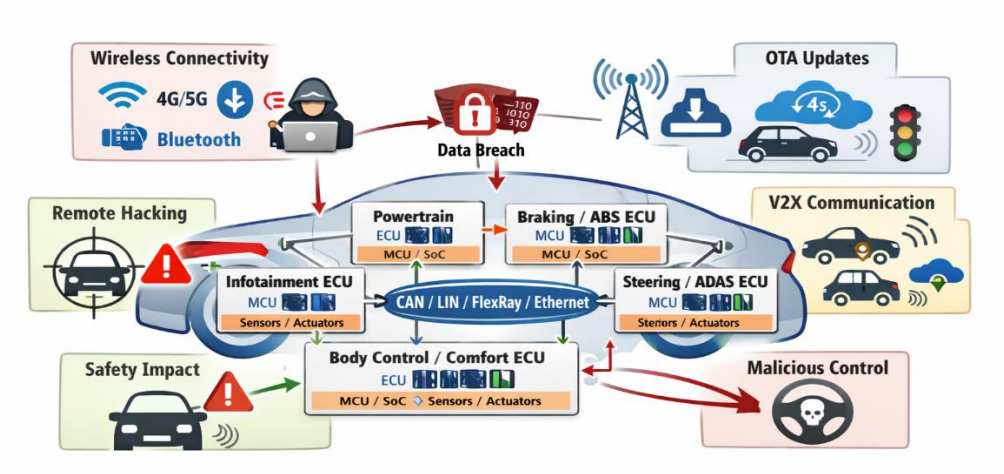

Figure 1. Modern Automotive ECU Network and Cybersecurity Threats

Illustration of interconnected electronic control units in a modern vehicle, highlighting internal network connections (CAN, LIN, FlexRay, Ethernet) and external exposure points such as wireless communication, OTA updates, and V2X interfaces. Potential cybersecurity threats targeting hardware and embedded system components are indicated.

[5]

2. Literature Review

Early research in **automotive cybersecurity** predominantly focused on vulnerabilities in **in-vehicle communication protocols**. The **Controller Area Network (CAN)**, the most widely deployed in-vehicle protocol, was found to lack fundamental security mechanisms such as authentication and encryption. This inherent vulnerability allows attackers to inject, spoof, or manipulate messages, potentially compromising safety-critical vehicle functions including braking, steering, and engine control. Several studies demonstrated proof-of-concept attacks, highlighting the significant risks associated with protocol-level vulnerabilities and the urgent need for security-aware communication designs.

Following these early works, research attention shifted to **ECU software vulnerabilities**. Modern vehicles integrate dozens of ECUs responsible for various functions, making them attractive targets for attackers. Studies revealed that insecure firmware update mechanisms, hardcoded credentials, and inadequate access control policies could allow adversaries to gain persistent control over ECUs. These findings emphasized that automotive cybersecurity cannot be fully addressed at the network layer alone; the integrity and security of ECU software and update processes are equally critical.

In recent years, literature has increasingly emphasized the role of **semiconductor design in shaping ECU security**. Modern ECUs rely on **highly integrated System-on-Chip (SoC)** architectures, which combine processing cores, memory subsystems, hardware accelerators, and third-party intellectual property (IP) blocks. While this integration improves performance, reduces cost, and enables advanced functionalities, it also increases the potential attack surface. Vulnerabilities may arise from complex interactions among integrated subsystems, insecure IP blocks, or low-level hardware flaws. Moreover, **supply-chain security** has emerged as a critical concern. Studies report risks associated with counterfeit components, malicious hardware modifications, and tampering during fabrication or distribution, which can introduce subtle yet dangerous vulnerabilities into vehicle ECUs.

Systematic reviews consistently identify ECUs as **critical attack targets** because they directly control vehicle behavior. Despite this, many surveys adopt a "black-box" perspective, focusing primarily on **network-level attacks** and largely overlooking hardware-specific threats. In contrast,

semiconductor-focused studies advocate for **hardware-rooted security measures**, including secure boot, trusted execution environments, and cryptographic accelerators. These approaches aim to establish a chain of trust starting from the hardware layer, ensuring software integrity, and enhancing resilience against both internal and external attacks.

Building upon prior work, this paper explicitly links **semiconductor architectures to cybersecurity vulnerabilities** in automotive control units. By considering ECUs as hardware-software co-designed systems with complex supply chains, this study highlights emerging threats that go beyond network or software vulnerabilities and proposes strategies for robust and secure ECU design.

Table 1: Summary of Prior Research on Automotive ECU and Semiconductor Security

Focus Area	Key Contribution	Research Gap
In-vehicle network security	Demonstrated CAN message injection attacks	Limited analysis of underlying hardware vulnerabilities
ECU firmware security	Identified insecure firmware update mechanisms	Weak discussion on hardware trust mechanisms
Semiconductor security features	Proposed hardware security modules (HSMs) and secure boot	Limited evaluation of real-world attack scenarios
Supply-chain security	Identified Trojan insertion and counterfeit component risks	Detection and mitigation techniques are immature

3. Automotive Semiconductor Control Unit Architecture

An automotive ECU is an embedded computing system centered around a microcontroller or SoC that executes real-time control algorithms. The processing unit interfaces with flash and RAM memory, sensor inputs, actuator outputs, and in-vehicle communication peripherals such as CAN, LIN, and automotive Ethernet. Many modern ECUs integrate hardware security modules (HSMs) to provide cryptographic services and secure key storage.

Power management circuits ensure reliable operation under varying voltage and temperature conditions. The trend toward domain controllers and centralized vehicle computing has increased the functional responsibility of individual semiconductor platforms. While consolidation improves efficiency, it also increases the potential impact of cyberattacks, making semiconductor-level security essential.

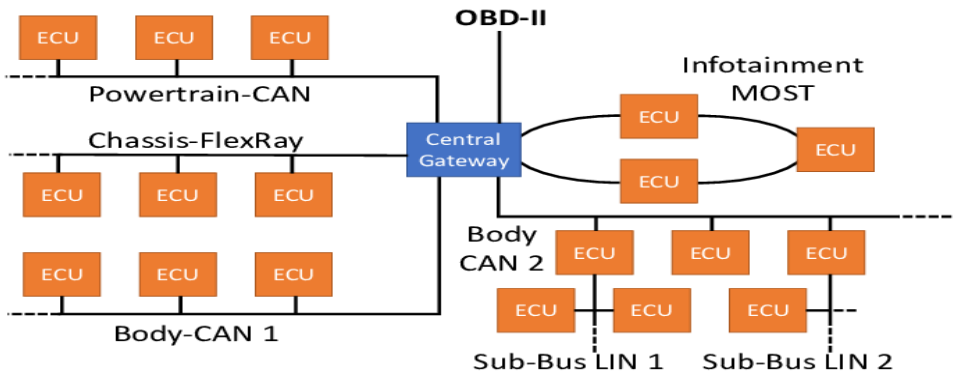

Figure 2. Typical automotive semiconductor-based ECU architecture showing microcontroller/SoC, memory, sensors, actuators, and in-vehicle networks.

(Source: ResearchGate – Automotive E/E architecture diagram)

4. Cybersecurity Threats in Automotive Semiconductor Control Units

4.1 Hardware-Level Threats

Hardware-level attacks exploit the physical properties of semiconductor devices. Side-channel attacks analyze power consumption or electromagnetic emissions to extract cryptographic secrets. Fault injection attacks manipulate voltage or clock signals to bypass security checks. These attacks are difficult to detect and may permanently compromise ECU integrity.

Malicious modifications during manufacturing, commonly referred to as hardware Trojans, represent another serious threat. Such vulnerabilities can remain dormant and evade conventional software-based defenses.

.2 Firmware and Embedded Software Threats

Firmware acts as the interface between semiconductor hardware and application software. Insecure boot processes, weak authentication, and insufficient memory protection can allow attackers to install unauthorized firmware. These attacks often persist across system resets and are challenging to detect during normal operation.

4.3 Communication and Network-Based Threats

ECUs communicate through in-vehicle networks that were not originally designed with security in mind. CAN-based communication lacks message authentication, making it vulnerable to spoofing and denial-of-service attacks. When ECUs interface with external networks, these vulnerabilities can be exploited remotely.

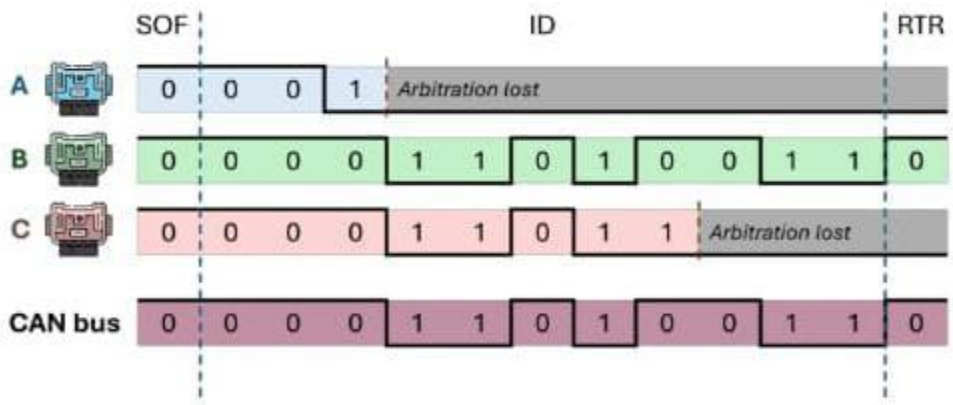

Figure 3. CAN arbitration policy illustrating contention among ECUs on the CAN bus (adapted from Canino et al., *Electronics*, 2025).

(Source: MDPI Electronics – CAN attack surface illustration)

This figure *illustrates the CAN arbitration mechanism*, which is a key part of understanding how in-vehicle networks can be exploited as part of a broader attack surface.

5. Safety and Cybersecurity Interdependence

Automotive safety and cybersecurity are closely linked. Cyberattacks targeting safety-critical ECUs can directly lead to hazardous situations such as unintended braking or steering malfunction. Conversely, safety mechanisms designed to trigger fail-safe behavior may be abused to disrupt vehicle operation.

From a semiconductor perspective, integrating safety and security requires careful co-design. Redundancy, diagnostics, and fault tolerance must coexist with secure execution environments and access control. Addressing these challenges requires security-by-design approaches aligned with automotive safety standards.

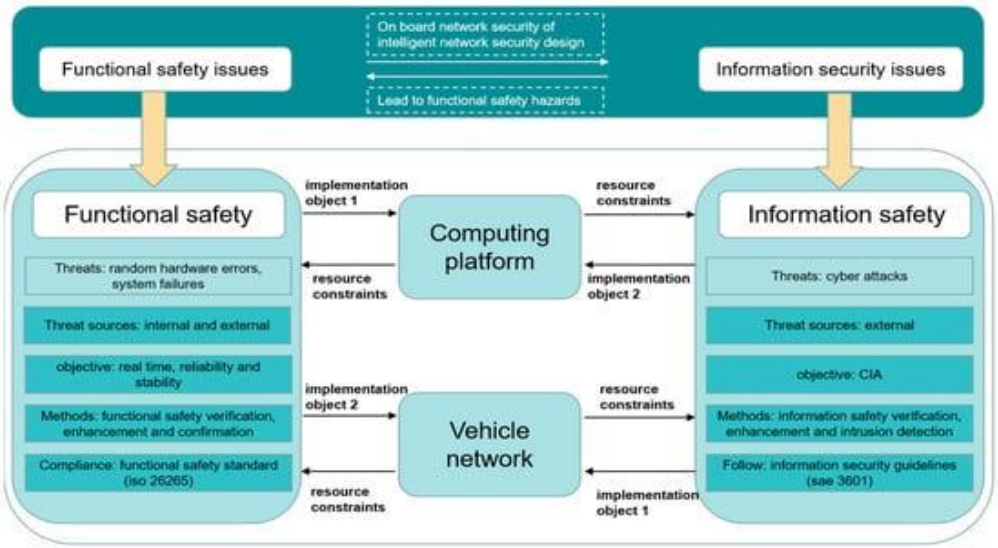

Figure 4. Relationship between cybersecurity threats to ECUs and their impact on vehicle safety functions.

6. Mitigation Strategies

Mitigating cybersecurity threats in automotive semiconductor control units requires a layered defense strategy. Hardware-based mechanisms such as secure boot, trusted execution environments, and cryptographic accelerators establish a root of trust. Firmware security is enhanced through code signing and secure update processes.

At the system level, intrusion detection systems monitor in-vehicle network traffic for abnormal behavior. Supply-chain security practices, including component authentication and IP verification, reduce the risk of malicious hardware modifications. Standards such as ISO 26262 and ISO/SAE 21434 provide structured frameworks for integrating safety and cybersecurity.

Table 2: Security Mechanisms for Automotive Semiconductor Control Units

Layer	Security Mechanism	Purpose
Hardware	HSM, secure boot	Establish root of trust
Firmware	Code signing	Prevent unauthorized execution
System	Intrusion detection	Detect abnormal behavior

7. Research Challenges and Future Directions

Despite progress, several challenges remain. Hardware-level attacks are difficult to evaluate due to their complexity and cost. Standardized methods for assessing semiconductor security in ECUs are lacking. Furthermore, security mechanisms often introduce trade-offs in power consumption and cost.

Future research should focus on lightweight hardware security solutions, formal verification of secure semiconductor designs, and cross-layer security frameworks that integrate hardware, firmware, and network defenses.

8. Conclusion

This paper reviewed cybersecurity threats in automotive semiconductor control units from a technical and industry-oriented perspective. As vehicles evolve into connected and autonomous platforms, ECUs will remain prime targets for cyberattacks. Addressing these challenges requires semiconductor-level security integration, close collaboration between automotive and chip manufacturers, and continued research into emerging vulnerabilities. A semiconductor-centric approach is essential for building secure and resilient automotive systems.

References

[1] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., … Savage, S. (2010). Experimental security analysis of a modern automobile. *Proceedings of the IEEE Symposium on Security and Privacy*, 447–462.

[2] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., … Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *USENIX Security Symposium*, 77–92.

[3] Miller, C., & Valasek, C. (2015). *Remote exploitation of an unaltered passenger vehicle*. Black Hat USA.

[4] Petit, J., & Shladover, S. (2015). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems, 16*(2), 546–556.

[5] Abhishake Reddy Onteddu. (2021). AI and Deep Learning-Based Intelligent Drug Recommendation System for Patient Health Monitoring in IoT-Enabled Healthcare. *Journal of Informatics Education and Research*, 1(3).

[6] Wolf, M., Weimerskirch, A., & Paar, C. (2004). Security in automotive bus systems. *Workshop on Embedded Security in Cars (ESCAR)*.

[7] D. Dhabliya, A. Gupta, Sharyu Ikhar, R. Sharma, M. Soni, and S. S. Dari, "The impact of 5G technology on telemedicine and mobile health apps," in *Revolutionary Impact of 5G on Advancement of Technology in Healthcare*, 1st ed., Apple Academic Press/Taylor & Francis, 2025, pp. –, doi: 10.4018/979-8-3693-1297-1.ch011.

[8] Herkle, M., Kuntz, A., & Schaumont, P. (2020). Automotive semiconductor security: Challenges and trends. *IEEE Design & Test, 37*(3), 72–80.

[9] Ruddle, A., Ward, D., & Weyl, B. (2017). Cyber security in automotive embedded systems. *IET Conference Proceedings*.

[10] ISO. (2018). *ISO 26262: Road vehicles – Functional safety*. International Organization for Standardization.

[11] ISO. (2021). *ISO/SAE 21434: Road vehicles – Cybersecurity engineering*. International Organization for Standardization.

[12] Sommer, R., Paxson, V., & Weaver, N. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*.

[13] Kunchi, S., Aher, V. N., Ikhar, S., Pathak, K., Gandhi, Y., & Wanjale, K. (2024). *Risk factor prediction for heart disease using decision trees*. In Proceedings of the 5th International Conference on Information Management & Machine Intelligence (ICIMMI '23). Association for Computing Machinery. https://doi.org/10.1145/3647444.3647937

[14] Arm Ltd. (2020). *TrustZone technology for automotive SoCs*. Arm White Paper.

[15] Bosch. (2020). *Automotive cybersecurity: Challenges and solutions*. Bosch Industry Report.