IAES Journal of Electrical and Electronics Engineering
Vol. 9, No. 1, June 2022, pp. 21~25
ISSN: 2338-7432, DOI: 10.11591/jeee.v9i1.pp21-25

Automotive electrical and electronic architectures: a review of embedded systems, vehicle networks, and functional safety

Mulyadi[1], Ahmad Raditya Cahya Baswara[2]
[1]Embedded Systems and Power Electronics Research Group, Yogyakarta, Indonesia
[2]Faculty of Industrial Technology, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

Article Info

Article history:

Received Feb 21, 2020
Revised Jul 23, 2020
Accepted Nov 28, 2020

Keywords:

Automotive architecture
Automotive ethernet
CAN bus
Cybersecurity
Electronic control unit
Embedded systems
Functional safety

ABSTRACT

Modern automobiles rely on increasingly sophisticated electrical and electronic (E/E) architectures to coordinate powertrain operation, vehicle dynamics, connectivity, driver assistance, and safety functions. This evolution has increased the number and complexity of electronic control units (ECUs), embedded software components, and in-vehicle communication networks. Although conventional distributed architectures provide modularity, their growing wiring requirements, communication constraints, and integration complexity create significant engineering challenges. This review examines automotive E/E architectures, focusing on ECU development, embedded systems, controller area network (CAN), local interconnect network (LIN), and automotive Ethernet, together with cybersecurity and functional safety. It compares the capabilities and limitations of established and emerging vehicle networks and discusses the transition from distributed architectures toward domain-based, centralized, and service-oriented designs. Particular attention is given to vulnerabilities in in-vehicle communication, secure software development, and the application of ISO 26262 throughout the automotive safety lifecycle. The review identifies gaps in cross-layer integration, real-time assurance, and safety-security co-engineering. Finally, it proposes research directions for developing scalable, secure, and dependable automotive architectures that can support increasingly connected and automated vehicles.

This is an open access article under the CC BY-SA license.

1. INTRODUCTION

Automotive electrical and electronic architectures have become fundamental to the operation of modern vehicles. Functions that were previously implemented through mechanical or isolated electrical mechanisms are increasingly controlled by embedded processors, software applications, sensors, actuators, and communication networks. These systems coordinate essential operations such as engine management, braking, steering, lighting, driver assistance, infotainment, and vehicle connectivity. Consequently, vehicle performance and reliability now depend substantially on the quality of the underlying E/E architecture [1]–[4].

The increasing integration of electronic functions has also created significant architectural challenges. Conventional vehicles commonly employ distributed ECUs connected through multiple communication buses, resulting in complex wiring harnesses, growing software dependencies, and demanding integration processes. The introduction of automated driving, high-resolution sensing, and connected services further increases requirements for processing capacity, bandwidth, communication reliability, and real-time response. These developments expose limitations in architectures that were originally designed for relatively independent vehicle functions [2], [3], [5].

Previous studies have examined automotive embedded platforms, network protocols, cybersecurity, and functional safety, but these subjects are frequently addressed as separate engineering concerns. For example, communication protocols are often evaluated in terms of bandwidth and latency, whereas ECU architectures are discussed in relation to software deployment and computing resources. Cybersecurity research focuses on unauthorized access and malicious communication, while functional safety examines

hazards caused by malfunctioning electrical and electronic systems. This separation creates a research gap because the reliability of a modern vehicle depends on the interaction of all these architectural layers [1], [6]–[9].

This review therefore examines automotive E/E architectures through an integrated perspective. It discusses ECU organization, embedded software, vehicle communication technologies, cybersecurity mechanisms, and functional-safety engineering. The main objective is to identify how architectural decisions influence system integration, communication performance, security, and safety throughout the vehicle lifecycle. The review also highlights research directions for developing scalable architectures capable of supporting future connected and automated vehicles.

2. EVOLUTION OF AUTOMOTIVE E/E ARCHITECTURES AND ECU SYSTEMS

Electronic control units are the primary computing elements of conventional automotive E/E architectures. Each ECU is generally designed to perform a specific function, such as engine control, transmission management, anti-lock braking, airbag deployment, or body electronics. This distributed approach allows individual functions to be developed and validated within relatively independent subsystems. However, the increasing number of ECUs and their interdependencies have made vehicle integration, software maintenance, and communication management more demanding [2], [3], [10].

The traditional distributed architecture is gradually evolving toward domain-based and centralized configurations. In a domain-based architecture, related functions are coordinated by domain controllers, which can reduce duplicated processing resources and simplify communication between subsystems. Centralized architectures take this development further by consolidating selected computing functions into more powerful controllers. Bandur *et al.* [3] explain that centralization can address several limitations of traditional architectures, although it also introduces new requirements for virtualization, software partitioning, networking, and functional safety.

Embedded software architecture is equally important because vehicle functions are implemented through interacting software components. AUTOSAR Classic provides a standardized framework for distributed embedded applications, while AUTOSAR Adaptive supports more flexible software deployment and service-oriented communication. Model-based architecture design can help engineers evaluate processor utilization, memory requirements, communication behavior, and deployment configurations before implementation. Kugele *et al.* [4] demonstrate how model-based resource analysis can support the synthesis of service-oriented automotive software architectures.

3. AUTOMOTIVE EMBEDDED SYSTEMS AND COMMUNICATION NETWORKS

Automotive embedded systems must execute control functions within defined timing, reliability, and resource constraints. Their hardware typically includes microcontrollers, memory, input/output interfaces, communication controllers, and diagnostic mechanisms. Embedded software processes sensor information, executes control algorithms, communicates with other ECUs, and activates vehicle actuators. The increasing complexity of these applications requires coordinated hardware-software design, particularly when safety-critical and non-safety-critical functions share computing resources [1], [4], [11].

In-vehicle communication networks enable ECUs and other electronic devices to exchange information. The controller area network (CAN) is widely used for control applications because it provides message-based communication, arbitration, and error-detection mechanisms. The local interconnect network (LIN) offers a comparatively economical solution for lower-speed applications, including door modules, window controls, seat functions, and other body electronics. FlexRay and automotive Ethernet address different communication requirements, particularly where higher determinism, bandwidth, or integration flexibility is necessary [5], [12].

Automotive Ethernet is becoming increasingly relevant as advanced driver-assistance systems and connected applications generate larger quantities of data. Compared with traditional low-bandwidth vehicle networks, Ethernet provides higher data rates and supports Internet Protocol-based communication and service-oriented software architectures. However, conventional Ethernet does not automatically guarantee the deterministic behavior required by every safety-critical application. Time-sensitive networking (TSN) extends Ethernet with mechanisms for time synchronization, traffic scheduling, and bounded communication delays, making it an important technology for future automotive embedded systems [5], [6], [13].

Table 1 compares the principal characteristics and application areas of common automotive communication technologies. The comparison shows that CAN and LIN remain appropriate for many established control and body-electronics applications, whereas Ethernet is better suited to bandwidth-intensive and increasingly integrated systems. FlexRay provides deterministic communication capabilities for applications with demanding timing requirements, although its role must be considered in relation to the

evolving Ethernet ecosystem. The selection of a network should therefore reflect application criticality, data volume, timing constraints, cost, and security requirements.

Table 1. Comparison of major in-vehicle communication technologies

Technology	Main characteristics	Typical applications	Main limitations
CAN	Message-based communication, arbitration, error detection	Powertrain, chassis, body control	Limited bandwidth; security mechanisms are not inherent
LIN	Low-cost, scheduled communication	Windows, seats, mirrors, door modules	Low data rate and limited network capability
FlexRay	Deterministic communication and time-triggered operation	Selected chassis and safety-related applications	Greater implementation complexity and cost
Automotive Ethernet	High bandwidth and IP-based communication	ADAS, cameras, gateways, infotainment	Requires additional real-time and security mechanisms
Ethernet with TSN	Time synchronization and scheduled traffic	High-performance embedded and control networks	Configuration and verification complexity

The technologies summarized in Table 1 should not be considered mutually exclusive alternatives. Modern vehicle architectures often combine several network types through gateways and domain controllers to satisfy different functional requirements. For example, a high-bandwidth Ethernet backbone may connect domain controllers, while CAN and LIN remain responsible for communication with established subsystems and lower-cost devices. Such heterogeneous architectures require careful gateway design, message prioritization, timing analysis, and end-to-end validation [5], [6].

4. AUTOMOTIVE CYBERSECURITY AND IN-VEHICLE NETWORK PROTECTION

Cybersecurity has become a fundamental requirement because modern vehicles increasingly interact with external devices, wireless networks, diagnostic equipment, and cloud-based services. These connections expand the potential attack surface and create opportunities for unauthorized access to vehicle communication systems. CAN networks are particularly important in this context because conventional CAN communication does not inherently provide message authentication or encryption. An attacker who gains access to an appropriate network entry point may therefore attempt message injection, spoofing, replay, or denial-of-service attacks [8], [9], [14].

Automotive cybersecurity requires protection of communication confidentiality, integrity, authenticity, and availability. Authentication mechanisms can help verify the identity of communicating devices, while message-integrity checks can reveal unauthorized modifications. Intrusion detection systems monitor network behavior to identify suspicious traffic patterns, unexpected message frequencies, or abnormal communication sequences. Research has investigated statistical, rule-based, and machine-learning-based approaches, although practical deployment remains constrained by computational resources, detection latency, false alarms, and the need for representative attack datasets [9], [15].

Security must also be considered across gateways, diagnostic interfaces, software updates, and external communication channels. A secure ECU cannot guarantee vehicle-wide protection if another connected subsystem provides an unprotected path into the internal network. Consequently, security mechanisms should be incorporated into the architecture from the initial design stage rather than added after the vehicle has been integrated. Cross-layer approaches that connect hardware, software, communication, and system-level security analysis offer a promising direction for reducing architectural vulnerabilities [8], [16].

5. FUNCTIONAL SAFETY AND ISO 26262

Functional safety addresses risks caused by malfunctioning behavior of electrical and electronic systems. In automotive engineering, ISO 26262 provides a structured framework for managing these risks throughout the product lifecycle. Its activities include hazard analysis and risk assessment, safety-goal definition, system development, hardware and software requirements, verification, validation, and production-related processes. The automotive safety integrity level (ASIL) provides a means of classifying safety requirements according to the assessed risk associated with hazardous events [17].

The application of functional safety principles is particularly important for ECUs responsible for braking, steering, powertrain control, and other safety-related functions. Hardware and software failures may result from random component faults, systematic design errors, timing violations, or incorrect system integration. Techniques such as fault-tree analysis, failure-mode analysis, diagnostic monitoring, redundancy, and safety mechanisms can help identify and control these risks. Hardware reliability assessment under

ISO 26262 also requires consideration of random hardware failures and the effectiveness of diagnostic measures [18]-[22].

The transition toward centralized and service-oriented architectures introduces additional functional-safety challenges. Consolidating multiple applications within a shared computing platform can improve resource utilization, but it also creates concerns about interference, fault containment, and the independence of software components. Safety-critical applications must remain protected from failures in less critical applications that share processors, memory, and communication resources. Therefore, architectural design should incorporate appropriate partitioning, timing analysis, safety monitoring, and verification before deployment [3], [4], [7].

Cybersecurity and functional safety are closely related but should not be treated as interchangeable concepts. Functional safety primarily addresses hazards resulting from system malfunction, whereas cybersecurity addresses threats arising from malicious actions and unauthorized access. A cyberattack can nevertheless trigger unsafe vehicle behavior by manipulating sensor information, ECU commands, or communication traffic. An integrated engineering approach should therefore evaluate both accidental faults and intentional attacks while maintaining clear safety and security requirements [8], [17], [18].

6. INTEGRATED ARCHITECTURAL CHALLENGES AND FUTURE RESEARCH

The reviewed literature indicates that automotive E/E architecture is moving toward greater centralization, higher communication capacity, and more flexible software deployment. However, this transformation requires coordinated development of embedded hardware, software platforms, communication networks, and safety mechanisms. The principal research challenge is no longer simply increasing the performance of individual ECUs or networks, but ensuring that the complete architecture operates reliably under realistic vehicle conditions. This requires cross-layer engineering methods that connect functional requirements with hardware allocation, network configuration, cybersecurity, and safety validation [2]–[7].

Future research should prioritize scalable architectures that support both legacy vehicle networks and emerging high-performance communication technologies. Model-based systems engineering and automated verification could help assess timing, resource utilization, fault propagation, and communication behavior before physical implementation. Lightweight security mechanisms are also needed to protect resource-constrained ECUs without compromising real-time performance. Furthermore, safety and cybersecurity engineering should be coordinated through shared threat analysis, fault analysis, and system-level validation procedures [8], [11], [13], [17].

Another important direction is the development of more effective methods for managing software complexity throughout the vehicle lifecycle. Service-oriented architectures and centralized computing platforms can simplify the deployment of new functions, but software updates must not compromise previously validated safety requirements. Continuous verification, secure update mechanisms, traceable software configurations, and hardware-software co-design will therefore become increasingly important. These capabilities can support vehicles that remain maintainable, secure, and dependable despite changing operational requirements and technological advances [4], [7], [11].

7. CONCLUSION

Automotive electrical and electronic architectures provide the foundation for coordinating the embedded systems, ECUs, and communication networks used in modern vehicles. Distributed architectures have enabled modular vehicle control, but growing software complexity, wiring requirements, and communication demands have encouraged the adoption of domain-based, centralized, and service-oriented approaches. CAN and LIN remain important for established control functions, while automotive Ethernet and TSN offer capabilities for higher-bandwidth and more time-sensitive applications. The integration of these technologies requires careful consideration of communication performance, resource allocation, and system compatibility. Cybersecurity and functional safety are essential to the dependable operation of increasingly connected automotive architectures. Security mechanisms must protect ECUs and in-vehicle networks against unauthorized access and malicious communication, while ISO 26262 provides a systematic framework for controlling hazards caused by malfunctioning E/E systems. Neither discipline can be implemented effectively in isolation because faults and attacks may propagate across hardware, software, and communication layers. Future automotive architectures should therefore adopt integrated engineering methods that combine scalable embedded platforms, deterministic networking, cybersecurity protection, and lifecycle-based functional-safety assurance.

REFERENCES

[1] L. Lo Bello, R. Mariani, S. Mubeen, and S. Saponara, "Recent advances and trends in on-board embedded and networked automotive systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 1038–1051, Feb. 2019, doi: 10.1109/tii.2018.2879544.

[2] H. Zhu, W. Zhou, Z. Li, L. Li, and T. Huang, "Requirements-driven automotive electrical/electronic architecture: a survey and prospective trends," *IEEE Access*, vol. 9, pp. 100096–100112, 2021, doi: 10.1109/access.2021.3093077.

[3] V. Bandur, G. Selim, V. Pantelic, and M. Lawford, "Making the case for centralized automotive E/E architectures," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1230–1245, Feb. 2021, doi: 10.1109/tvt.2021.3054934.

[4] S. Kugele, P. Obergfell, and E. Sax, "Model-based resource analysis and synthesis of service-oriented automotive software architectures," *Software and Systems Modeling*, vol. 20, no. 6, pp. 1945–1975, 2021, doi: 10.1007/s10270-021-00896-9.

[5] M. Ashjaei, L. Lo Bello, M. Daneshtalab, G. Patti, S. Saponara, and S. Mubeen, "Time-Sensitive Networking in automotive embedded systems: State of the art and research opportunities," *Journal of Systems Architecture*, vol. 117, p. 102137, Aug. 2021, doi: 10.1016/j.sysarc.2021.102137.

[6] H.-J. Kim, M.-H. Choi, M.-H. Kim, and S. Lee, "Development of an ethernet-based heuristic time-sensitive networking scheduling algorithm for real-time in-vehicle data transmission," *Electronics*, vol. 10, no. 2, p. 157, Jan. 2021, doi: 10.3390/electronics10020157.

[7] J. Walrand, M. Turner, and R. Myers, "An architecture for in-vehicle networks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 7, pp. 6335–6342, 2021, doi: 10.1109/tvt.2021.3082464.

[8] Y. Xie, Y. Zhou, J. Xu, J. Zhou, X. Chen, and F. Xiao, "Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: State-of-the-art and future challenges," *Software: Practice and Experience*, vol. 51, no. 11, pp. 2108–2127, Mar. 2021, doi: 10.1002/spe.2965.

[9] N. Khatri, R. Shrestha, and S. Y. Nam, "Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain," *Electronics*, vol. 10, no. 8, p. 893, Apr. 2021, doi: 10.3390/electronics10080893.

[10] A. Buczacki and P. Piątek, "Proposal for an integrated framework for electronic control unit design in the automotive industry," *Energies*, vol. 14, no. 13, p. 3816, 2021, doi: 10.3390/en14133816.

[11] A. Bucaioni and P. Pelliccione, "Technical architectures for automotive systems," Mar. 2020, doi: 10.1109/icsa47634.2020.00013.

[12] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, "Intrusion detection system for automotive controller area network (CAN) bus system: a review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 2019, doi: 10.1186/s13638-019-1484-3.

[13] L. Lo Bello, G. Patti, and G. Vasta, "Assessments of real-time communications over TSN automotive networks," *Electronics*, vol. 10, no. 5, p. 556, Feb. 2021, doi: 10.3390/electronics10050556.

[14] A. Martínez-Cruz, K. A. Ramírez-Gutiérrez, C. Feregrino-Uribe, and A. Morales-Reyes, "Security on in-vehicle communication protocols: Issues, challenges, and future research directions," *Computer Communications*, vol. 180, pp. 1–20, Dec. 2021, doi: 10.1016/j.comcom.2021.08.027.

[15] Z. Pethő, Á. Török, and Z. Szalay, "A survey of new orientations in the field of vehicular cybersecurity, applying artificial intelligence based methods," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, 2021, doi: 10.1002/ett.4325.

[16] Z. Wang, H. Liang, C. Huang, and Q. Zhu, "Cross-layer design of automotive systems," *IEEE Design & Test*, vol. 38, no. 5, pp. 8–16, Oct. 2021, doi: 10.1109/mdat.2020.3037561.

[17] R. Debouk, "Overview of the second edition of ISO 26262: functional safety— road vehicles," *Journal of System Safety*, vol. 55, no. 1, pp. 13–21, Mar. 2019, doi: 10.56094/jss.v55i1.55.

[18] G. Xie, Y. Li, Y. Han, Y. Xie, G. Zeng, and R. Li, "Recent advances and future trends for automotive functional safety design methodologies," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5629–5642, 2020, doi: 10.1109/tii.2020.2978889.

[19] J. Famfulik *et al.*, "Application of hardware reliability calculation procedures according to ISO 26262 standard," *Quality and Reliability Engineering International*, vol. 36, no. 6, pp. 1822–1836, Mar. 2020, doi: 10.1002/qre.2625.

[20] M. Vogel *et al.*, "Metrics in automotive software development: A systematic literature review," *Journal of Software: Evolution and Process*, vol. 33, no. 2, Aug. 2020, doi: 10.1002/smr.2296.

[21] A. Saber, F. Di Troia, and M. Stamp, "Intrusion detection and CAN vehicle networks," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*, Springer International Publishing, 2020, pp. 125–154.

[22] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "Long short-term memory-based intrusion detection system for in-vehicle controller area network bus," in *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2020, pp. 10–17, doi: 10.1109/compsac48688.2020.00011.