COLOMBO SCIENTIFIC PUBLISHING

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM (IJCSIS)

E-ISSN: 2536-7919
P-ISSN: 2536-7900

PAGE NO: 13-17

Next-Generation Automotive E/E Architectures: Unifying Zonal Computing, Deterministic Ethernet-TSN, Secure CAN Protocols, and Fault-Tolerant Lockstep Mechanisms

Dr. Arjun V. Menon
Department of Automotive Systems Engineering, Horizon Institute of Technology

ARTICLE INFO

Article history:
Submission: January 21, 2024
Accepted: January 29, 2024
Published: February 12, 2024

VOLUME: Vol.09 Issue 02 2024

Keywords:
Zonal E/E architectures; fault-tolerant lockstep; in-vehicle network security; CAN/TSN coexistence; OTA update scheduling; resilient controllers

ABSTRACT

This article presents a comprehensive, original synthesis of current knowledge and forward-looking propositions for resilient, secure, and economically optimized electrical/electronic (E/E) architectures in modern vehicles. It integrates evidence and theoretical positions from research on zonal architectures, fault-tolerant lockstep processors, in-vehicle networking (CAN, CAN-FD, and TSN over Ethernet), scheduling and update strategies, and security vulnerabilities that threaten vehicle safety and availability. The structured abstract outlines objectives, methodological framing, key findings, and implications. The main contribution is a unified conceptual framework that reconciles reliability-by-design (hardware lockstep and heterogeneous redundancy), secure communications (CAN hardening and secure firmware-over-the-air), and pragmatic system-level optimization (cost, scheduling, and power supply considerations). The framework is supported by detailed discussion of mechanisms—dual-core lockstep, share-driven scheduling, selective denial-of-service attacks and defenses, and OTA update parallelization—and by a critical appraisal of trade-offs between cost savings and safety requirements. The article concludes with prioritized research directions and engineering recommendations for industry and academia aimed at achieving scalable, secure, and verifiable zonal E/E systems.

INTRODUCTION

The automotive electrical/electronic (E/E) landscape has been undergoing a deep transformation driven by the proliferation of advanced driver assistance systems (ADAS), electrification, and connected vehicle services (Jiang, 2019; Navale et al., 2015). Historically, distributed architectures composed of numerous domain controllers and legacy bus systems such as CAN have evolved toward more centralized or zonal topologies that promise reductions in wiring complexity, improved maintainability, and easier feature deployment (Navale et al., 2015; Blank, 2015). At the same time, vehicles increasingly resemble networked cyber-physical systems, exposing them to novel security threats (Palanca et al., 2017; Avatefipour & Malik, 2018) and raising stringent dependability requirements that automotive manufacturers must meet through hardware and software architectural choices (Abdul Salam Abdul Karim, 2023; Marques et al., 2021).

This paper addresses the fundamental problem that emerges at the intersection of safety, security, cost-effectiveness, and maintainability: how to design zonal E/E architectures that are resilient against failures (transient and permanent), robust against malicious network-level attacks, and efficient to operate and update across the vehicle fleet. The literature shows distinct, often siloed contributions—fault-tolerant dual-core lockstep architectures for controllers (Abdul Salam Abdul Karim, 2023; Nikiema et al., 2023), in-vehicle network security studies focused on CAN vulnerabilities (Avatefipour & Malik, 2018; Bozdal et al., 2020), and scheduling/parallelization methods aimed at optimizing OTA updates and network resource sharing (Herberth et al., 2019; Nolte, 2006). However, there is a gap in integrative frameworks that bring these threads together into a system-level design and operational guidance that accounts for cost and power constraints (Blank, 2015; Kilian et al., 2021). This article fills that gap by synthesizing evidence across hardware redundancy techniques, communication-layer defenses, scheduling strategies, and OTA processes to propose a cohesive architecture and implementation roadmap.

Methodology

This research is theoretical and integrative, constructed as a systematic synthesis of the provided corpus of peer-reviewed and technical references. The methodological approach involves four complementary activities:

1. **Conceptual decomposition** — Each reference is analyzed to extract its core contributions, assumptions, and limitations with respect to three axes: (a) reliability mechanisms (hardware/software redundancy, lockstep techniques), (b) communication and security (CAN, CAN-FD, TSN over Ethernet, attack models and defenses), and (c) operational optimization (scheduling, OTA parallelization, power and cost constraints).

2. **Cross-domain mapping** — Findings are mapped across axes to identify compatibilities, conflicts, and integration points. For instance, the hardware-level dual-core lockstep strategies are evaluated for their interaction with zonal controller topologies and the implications for OTA update strategies. Scheduling methods such as share-driven scheduling (Nolte, 2006) and automated parallelization for updates (Herberth et al., 2019) are examined for their applicability in zonal architectures.

3. **Trade-off modeling (qualitative)** — Rather than mathematical or empirical modeling, which the constraints of this article prohibit, trade-offs are elaborated descriptively and at high resolution (e.g., the cost implications of adding lockstep cores versus the reduced certification and recall risk). This includes sensitivity discussion for variables like cost per vehicle, additional power draw, and latency constraints.

4. **Synthesis and prescription** — The final step synthesizes an architecture-level design and recommended practices. The prescription is justified by the cross-domain mapping and qualitative trade-off assessment and is positioned against security threats such as selective link-layer DoS attacks (Palanca et al., 2017) and CAN anomalies (Markovitz & Wool, 2017).

Throughout this methodology, rigorous citation of claims to specific references ensures traceability and anchors theoretical propositions in published work.

Results

The integration of the reviewed literature yields several major interrelated findings that form the backbone of the proposed framework:

1. **Zonal controllers augmented with fault-tolerant lockstep processors provide a superior balance of cost and safety compliance compared with naive centralization.** The zonal approach lowers wiring complexity and enables modular deployment (Navale et al., 2015; Blank, 2015), while lockstep strategies—particularly dual-core lockstep (Abdul Salam Abdul Karim, 2023; Nikiema et al., 2023)—offer deterministic fault detection and tolerance appropriate for safety-critical functions. Importantly, heterogeneous lockstep concepts (Marques et al., 2021; Marques, 2020) suggest avenues for combining different ISAs (e.g., Arm + RISC-V) to enhance fault isolation and diversity, improving resilience to correlated failures.

2. **Coexistence of CAN-based networks with Ethernet TSN must be explicitly managed through security hardening and scheduling.** CAN and CAN-FD remain pervasive for many control functions due to cost and determinism (Zeng et al., 2016; Bozdal et al., 2020), yet Ethernet TSN is gaining traction for high-bandwidth, time-sensitive functions (Jiang, 2019; Brunner et al., referenced). This heterogeneity introduces attack surfaces—CAN's broadcast model and lack of built-in authentication are documented vulnerabilities (Avatefipour & Malik, 2018; Bozdal et al., 2020), and novel attack forms like stealth selective link-layer DoS demonstrate how attackers can exploit protocol characteristics (Palanca et al., 2017). A layered defense—secure gateways, intrusion detection on CAN (Markovitz & Wool, 2017), and TSN's deterministic scheduling—emerges as necessary.

3. **Parallelized OTA update strategies, when combined with intelligent scheduling, drastically reduce update durations and minimize vehicle downtime.** Automated scheduling for optimal parallelization reduces update time by leveraging parallel write and validation across distributed ECUs while respecting bus bandwidth constraints (Herberth et al., 2019). Share-driven scheduling concepts (Nolte, 2006) applied to mixed-criticality environments enable fair and deterministic allocation of network resources during updates.

4. **Economic and power supply constraints are non-trivial and must be evaluated as first-order design factors.** Cost savings from zonal consolidation are compelling (Blank, 2015), but the introduction of additional compute (for lockstep or heterogeneous processors) and increased OTA/communication capability can increase per-vehicle cost and power draw. Safe power supply design guidelines (Kilian et al., 2021) provide necessary constraints for architecting power budgets for redundant processors and zonal modules.

5. **Holistic security that encompasses firmware updates, intrusion detection, and communication-layer protections is essential to prevent escalation of network-level attacks into safety failures.** Secure firmware-over-the-air mechanisms and robust key management tie directly into preventing firmware tampering that could subvert lockstep defenses (Kornaros et al., 2020). Studies of driverless vehicle security highlight the multiplicity of attack vectors and the need for layered security throughout stack (De La

Torre et al., 2020).

Each of these findings is elaborated below with conceptual mechanisms, illustrative scenarios, and explicit linkage to the source literature.

Discussion

Zonal Architectures and the Rationale for Lockstep Augmentation

Zonal architectures restructure vehicle E/E networks by grouping sensors and actuators physically into zones, each served by a local zonal controller. This arrangement reduces cabling mass and supports modular upgrades (Navale et al., 2015; Blank, 2015). However, moving intelligence towards zones heightens the importance of per-zone compute reliability because a zonal controller failure can incapacitate many functions. The literature supports integrating fault-tolerant hardware at zonal nodes. Dual-core lockstep (Abdul Salam Abdul Karim, 2023; Nikiema et al., 2023) enforces instruction-level redundancy: two cores execute the same instruction stream in lockstep and mismatch detection triggers failover. While classical lockstep imposes area and power overhead, its determinism is highly valuable for functions that have real-time and safety-critical constraints.

Heterogeneous lockstep approaches (Marques et al., 2021; Marques, 2020) propose using different processor architectures in lockstep to reduce the possibility of common-mode failures arising from microarchitectural design bugs. This diversity enhances resilience against certain classes of design faults and software-level attacks that target specific ISA features. Practically, the adoption of heterogeneous lockstep increases system complexity: cross-compilation, compiler correctness, and verification across heterogeneous cores require sophisticated toolchains. Nevertheless, for zonal nodes that host mixed-criticality workloads (safety-critical control and non-critical infotainment), diverse lockstep can be selectively applied to safety partitions while leaving non-safety workloads on single cores—balancing cost and reliability. From a certification standpoint, deterministic architectures facilitate ISO 26262 argumentation because they make timing and failure modes analyzable. Dual-core lockstep aligns well with ASIL D requirements for many control functions, thereby potentially simplifying compliance burdens even if initial hardware costs rise (Abdul Salam Abdul Karim, 2023).

CAN Security, Detection, and Coexistence with TSN

CAN bus security continues to surface as a critical vulnerability due to its original design assumptions that parties on the bus were trusted (Avatefipour & Malik, 2018; Bozdal et al., 2020). Research demonstrates that an attacker with access to the bus can inject messages, impersonate ECUs, and disrupt vehicle behavior. Novel attack classes—such as the stealth, selective link-layer DoS—demonstrate that attackers can target link-layer properties to create denial-of-service without obvious intrusion patterns (Palanca et al., 2017).

To mitigate these risks, a combination of intrusion detection and protocol hardening is recommended. Field classification and anomaly detection work (Markovitz & Wool, 2017) demonstrates unsupervised methods to model unknown CAN networks and detect deviations. However, anomaly detection alone is insufficient because sophisticated adversaries can craft low-and-slow attacks that mimic benign traffic characteristics; thus, defense-in-depth remains essential. Gateways that translate CAN and TSN traffic must enforce message authentication and rate limiting and must be designed to fail-safe, ensuring that a compromised gateway does not provide an attacker with a bridge into high-assurance TSN domains (Kornaros et al., 2020).

Ethernet TSN (Time-Sensitive Networking) promises deterministic scheduling for high-bandwidth functions (Jiang, 2019). When TSN is used alongside CAN, careful partitioning is necessary: high-assurance control loops should be retained in deterministic domains (either hardened CAN-FD with strong protections or TSN with cryptographic authentication and precise scheduling). The move toward mixed networks requires that scheduling policies consider security trade-offs—e.g., gating high-rate diagnostic traffic during critical driving phases—to prevent resource exhaustion attacks. Share-driven scheduling concepts (Nolte, 2006) can be adapted to ensure predictable allocation across CAN and TSN domains during peak load and OTA activity.

OTA Updates: Parallelization, Scheduling, and Security

OTA capability transforms the automotive lifecycle by enabling software fixes, new features, and security patches in the field. However, large-scale fleet updates require careful orchestration to avoid overwhelming vehicle networks and to guarantee integrity. Herberth et al. (2019) show that automated scheduling for optimal parallelization meaningfully reduces update duration by distributing update activities across multiple ECUs concurrently when safe and allowed by bandwidth and safety constraints. The qualitative logic is straightforward: overlapping non-conflicting update tasks can proceed in parallel while preserving deterministic communication for real-time functions.

Implementing robust OTA requires several system properties: cryptographic verification of payloads (to prevent malicious firmware installs), authenticated boot chains (to preserve trust across reboots), and rollback mechanisms (to recover from faulty updates). Kornaros et al. (2020) emphasize securing both CAN communication and OTA mechanisms to prevent an attacker from using update channels to escalate privileges. Furthermore, share-driven scheduling offers a theoretical foundation to assign temporal windows and bandwidth shares to updates versus operational traffic (Nolte, 2006), enabling conservative but efficient update scheduling that respects

safety-critical timing requirements.

A pragmatic example: a zonal controller designated for body-control functions could receive staged updates where background services are updated first in low-traffic periods, while safety-critical modules wait until a safe state or are updated in lockstep across redundant hardware. Such staged and partitioned update strategies minimize the likelihood of introducing inconsistencies that could lead to system-level failures.

Economic and Power Trade-offs

Blank (2015) quantifies savings achievable by E/E system optimization and wiring consolidation, arguing that mass-market cost targets can be met through zoning and consolidation of function. However, the introduction of redundant processors, cryptographic accelerators, and enhanced network interfaces increases both capital cost and steady-state power draw. Power supply design guidelines (Kilian et al., 2021) remind designers that redundant architectures must be considered from the power-system perspective: cold redundancy, warm redundancy, and active-active configurations each have distinct power and availability profiles.

Cost-benefit analysis in automotive design is multi-faceted. While hardware costs increase with redundancy, potential benefits include reduced recall risk, lower warranty costs, and fewer in-field safety incidents—all of which can offset upfront investment. Moreover, the strategic use of heterogeneous cores (Marques et al., 2021) may reduce costs if lower-cost RISC-V cores can be used for certain safety partitions while more expensive Arm cores are reserved for compute-heavy or legacy-compatible tasks. Nonetheless, supply-chain maturity for emerging ISAs and toolchain verification costs must be accounted for.

Limitations and Counter-Arguments

Several counter-arguments and limitations require attention. First, lockstep and heterogeneous redundancy complicate software toolchains and verification processes; cross-compilation and consistent behavior across divergent ISAs is non-trivial (Marques, 2020). Second, anomaly detection systems are susceptible to false positives and drift over time—need for adaptive models and human-in-the-loop validation is critical (Markovitz & Wool, 2017). Third, the reliance on OTA mechanisms introduces its own risk profile: while OTA enables rapid patching, it also opens an attack surface that must be hardened (Kornaros et al., 2020). Finally, economic constraints for mass-market vehicles constrain the extent of hardware redundancy that can be deployed; therefore, architectural choices must be calibrated to acceptable safety targets and market segmentation (Blank, 2015).

Future Research Directions

From the synthesis, several research priorities emerge:

- **Toolchain and verification research for heterogeneous lockstep**: automated proofs of behavioral equivalence across divergent CPU architectures would reduce the verification burden for heterogeneous lockstep designs (Marques et al., 2021).
- **Adaptive anomaly detection robust to low-and-slow attacks**: combining temporal, semantic, and physical-layer signals (e.g., sensor fusion) may increase detection fidelity for stealthy attacks that mimic benign CAN traffic (Markovitz & Wool, 2017; Palanca et al., 2017).
- **Integrated scheduling algorithms for mixed CAN/TSN domains**: algorithms that can reason about multi-bus topologies, mixed-criticality workloads, and security constraints simultaneously are required. Extending share-driven scheduling to account for cryptographic processing latency and OTA bandwidth is an open area (Nolte, 2006; Herberth et al., 2019).
- **Quantitative lifecycle cost modeling**: rigorous models that capture upfront hardware costs, expected reduction in recalls, OTA patching cost, and liability exposure will help OEMs make evidence-based design decisions (Blank, 2015).
- **Power-aware redundancy strategies**: optimizing redundancy schemes with respect to vehicle-level power budgets and thermal constraints (Kilian et al., 2021) will be important for electric vehicles where energy is a premium.

Conclusion

The transition to zonal E/E architectures in contemporary vehicles offers substantial benefits in wiring reduction, modularity, and upgradeability; however, it also concentrates the importance of per-zone reliability and security. By integrating fault-tolerant dual-core and heterogeneous lockstep techniques at zonal controllers, applying layered communication defenses across CAN and TSN domains, and orchestrating OTA update processes with intelligent parallelization and scheduling, a robust and economically rational architecture can be realized. The literature reviewed here provides complementary insights: hardware redundancy for deterministic failure detection (Abdul Salam Abdul Karim, 2023; Nikiema et al., 2023), deep awareness of CAN vulnerabilities (Avatefipour & Malik, 2018; Bozdal et al., 2020), the importance of secure OTA and holistic network security (Kornaros et al., 2020; De La Torre et al., 2020), and scheduling strategies that minimize update downtime (Herberth et al., 2019; Nolte, 2006). Achieving an industrial-strength realization of this integrated framework requires advances in verification, tooling, adaptive security, and cost modeling—areas that constitute crucial research agendas for both academic and industry partners. The recommendations provided herein are actionable: adopt selective lockstep for safety partitions, enforce gateway-level authentication between

CAN and TSN, implement parallelized OTA pipelines with share-driven scheduling, and evaluate redundancy from a holistic cost-power-safety perspective.

References

1. Jiang, S.: Vehicle E/E architecture and its adaptation to new technical trends. SAE Tech. Paper (2019).
2. Palanca, A., Evenchick, E., Maggi, F., et al.: A stealth, selective, link-layer denial-of-service attack against automotive networks. Paper presented at 14th International Conference, DIMVA 2017, Bonn, Germany, 6–7 July 2017.
3. Herberth, R., Körper, S., Stiesch, T., et al.: Automated scheduling for optimal parallelization to reduce the duration of vehicle software updates. IEEE Trans. Veh. Technol. 68(3), 2921–2933 (2019).
4. De La Torre, G., Rad, P., et al.: Driverless vehicle security: challenges and future research opportunities. Future. Gener. Comp. Syst. 108, 1092–1111 (2020). https://doi.org/10.1016/j.future.2017.12.041
5. Abdul Salam Abdul Karim. (2023). Fault-Tolerant Dual-Core Lockstep Architecture for Automotive Zonal Controllers Using NXP S32G Processors. International Journal of Intelligent Systems and Applications in Engineering, 11(11s), 877–885. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/7749
6. Byun, J.Y., Park, J.W., Kim, D.Y., et al.: Effective in-vehicle network training strategy for automotive engineers. IEEE Access 10, 29252–29266 (2022). https://doi.org/10.1109/ACCESS.2022.3158269
7. Avatefipour, O., Malik, H.: State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vulnerabilities. arXiv:1802.01725 (2018).
8. Nolte, T.: Share-Driven Scheduling of Embedded Networks. Institutionen för Datavetenskap och Elektronik (2006).
9. Blank, R.: How to save $20 per car by optimization of the E/E system? SAE Int. J. Passenger Cars Electron. Electr. Syst. 8, 51–55 (2015). https://doi.org/10.4271/2015-01-0153
10. Navale, V.M., Williams, K., Lagospiris, A., et al.: Revolution of E/E architectures. SAE Int. J. Passenger Cars Electron. Electr. Syst. 8, 282–288 (2015). https://doi.org/10.4271/2015-01-0196
11. Bozdal, M., Samie, M., Aslam, S., Jennions, I.: Evaluation of can bus security challenges. Sensors 20, 2364 (2020). https://doi.org/10.3390/s20082364
12. Markovitz, M., Wool, A.: Field classification, modeling and anomaly detection in unknown CAN bus networks. Veh. Commun. 9, 43–52 (2017).
13. Kornaros, G., Tomoutzoglou, O., Mbakoyiannis, D., et al.: Towards holistic secure networking in connected vehicles through securing CAN-bus communication and firmware-over-the-air updating. J. Syst. Architect. 109, 101761 (2020). https://doi.org/10.1016/j.sysarc.2020.101761
14. Zeng, W., Khalid, M.A.S., Chowdhury, S.: In-vehicle networks outlook: achievements and challenges. IEEE Commun. Surveys Tutor. 18(3), 1552–1571 (2016). https://doi.org/10.1109/COMST.2016.2521642
15. Kilian, P., Köhler, A., Van Bergen, P., Gebauer, C., Pfeufer, B., Koller, O. and Bertsche, B., 2021. Principle guidelines for safe power supply systems development. IEEE Access, 9, pp.107751-107766.
16. Marques, I., Rodrigues, C., Tavares, A., Pinto, S. and Gomes, T., 2021. Lock-V: A heterogeneous fault tolerance architecture based on Arm and RISC-V. Microelectronics Reliability, 120, p.114120.
17. Marques, I.D.C., 2020. A Loosely-Coupled Arm and RISC-V Locksteping technology (Doctoral dissertation).
18. Mohsan, S.A.H., Othman, N.Q.H., Li, Y., Alsharif, M.H. and Khan, M.A., 2023. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. Intelligent Service Robotics, 16(1), pp.109-137.
19. Nikiema, P.R., Kritikakou, A., Traiola, M. and Sentieys, O., 2023, June. Design with low complexity fine-grained Dual Core Lock-Step (DCLS) RISC-V processors. In 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S) (pp. 224-229). IEEE.
20. Nishiyama, H., Fujimoto, D., Sone, H. and Hayashi, Y., 2023. Efficient noninvasive fault injection method utilizing intentional electromagnetic interference. IEEE Transactions on Electromagnetic Compatibility, 65(4), pp.1211-1219