The American Journal of Applied Sciences
ISSN 2689-0992 | Open Access

TYPE Original Research
PAGE NO. 16-22

Secure and Fault-Tolerant Automotive E/E Architectures: Enhancing CAN-FD, FlexRay, and TSN Networks through Intrusion Detection and Redundant Processing

OPEN ACCESS

SUBMITTED 21 January2024
ACCEPTED 29 January 2024
PUBLISHED 5 February 2024
VOLUME Vol.07 Issue 02 2024

Dr. Rhea Kapoor
Institute of Automotive Systems, Indian Institute of Technology Delhi

Abstract: This article synthesizes and advances current engineering and theoretical approaches to resilient, high-performance in-vehicle electronic/electrical (E/E) architectures by integrating three complementary streams of research: (1) message packing and scheduling for CAN-FD and FlexRay networks, (2) centralized and zonal E/E architecture paradigms with Ethernet/TSN considerations, and (3) processor-level fault tolerance and concurrent error detection strategies. Through a detailed conceptual methodology that combines scheduling theory, topology verification, gateway design, and redundant processor organisation, the paper develops a unified framework for designing automotive communication stacks that maximize bandwidth utilization while preserving timing determinism and safety. The framework proposes concrete, textually described algorithms for frame packing, offset assignment, dynamic segment scheduling, and topology-aware intrusion detection; it also prescribes architectural patterns for zonal controllers that leverage dual-core lockstep, watchdog processors, and redundant multi-threading to achieve robust error detection and recovery. Key findings—derived from rigorous cross-reference of prior empirical and theoretical studies—show that careful signal offset assignment and topology verification significantly increase CAN-FD effective throughput (Bordoloi & Samii, 2014; Joshi et al., 2019; Yu & Wang, 2019), while centralized E/E approaches coupled with TSN and AVB provide scalable low-latency backbones for high-bandwidth sensor fusion (Migge et al., 2018; Bandur et al., 2021). Processor-level redundancy strategies such as dual-core lockstep and redundant multi-threading

remain effective fault-detection mechanisms provided their integration considers instruction-level fault propagation and single-event effects (Mahmood & McCluskey, 1988; Maniatakos et al., 2011; Medina et al., 2016). The article concludes with design recommendations, limitations, and directions for experimental validation.

Keywords: CAN-FD frame packing; zonal E/E architectures; TSN/AVB; fault tolerance; dual-core lockstep; intrusion detection.

Introduction

The contemporary automotive domain is undergoing a tectonic shift: vehicle functionalities that were once purely mechanical are now predominantly software-defined and heavily reliant on high-speed, deterministic communication among distributed electronic control units (ECUs) and sensors. This transition creates a dual imperative: (a) maximize utilization of available in-vehicle communication bandwidth so that high-throughput features (e.g., multi-camera perception, over-the-air updates, and advanced driver assistance systems) can be accommodated; and (b) ensure that system safety and reliability are preserved or enhanced despite increased architectural complexity and exposure to cyber and transient faults. Existing literature addresses pieces of this puzzle—CAN-FD frame packing (Bordoloi & Samii, 2014), offset assignment strategies for improved packing efficiency (Joshi et al., 2019), topology verification for IDS (Yu & Wang, 2019), FlexRay dynamic segment scheduling (Schmidt & Schmidt, 2008), and gateway designs bridging CAN and FlexRay domains (Zhao et al., 2010). Parallel efforts investigate centralized vs. zonal E/E organization and the implications of automotive Ethernet with AVB/TSN extensions (Migge et al., 2018; Bandur et al., 2021). At the processor level, extensive literature on concurrent error detection (Mahmood & McCluskey, 1988), instruction-level fault analysis (Maniatakos et al., 2011), and experimental single-event effect methodologies (Medina et al., 2016) informs the application of lockstep and redundant execution techniques (Mukherjee et al., 2002; Moyer et al., 2012; Abdul Karim, 2023).

Despite this rich body of work, a comprehensive, theory-driven treatment that unifies communication packing/scheduling, topology-aware security, zonal/centralized E/E tradeoffs and processor-level fault tolerance remains underdeveloped. Specifically, gaps persist in: (1) integrating frame packing optimization with topology verification and intrusion detection mechanisms so that improved bandwidth does not come at the cost of reduced observability and security; (2) reconciling the architectural economic and performance tradeoffs between centralized Ethernet backbones and zonal controller topologies; and (3) presenting processor redundancy schemes tailored to automotive zonal controllers where constrained compute, power, and certification paths require unique fault-containment strategies (Fikke, 2016; Abdul Karim, 2023). This manuscript therefore addresses these gaps by formulating an integrative conceptual framework and detailed, textually defined methods that span the communication stack to the processor core. Every major argument and recommendation is grounded in prior findings and framed to guide researchers and practitioners toward experimental validation.

Methodology

The methodological approach is wholly textual and theoretical. Rather than reporting new experimental data, this work constructs a layered design and analytical framework by synthesizing, extending, and formally interpreting prior empirical results and algorithmic contributions. The methodology comprises the following components:

1. **Analytical Synthesis of Frame Packing and Offset Assignment Literature.** The paper reinterprets canonical frame packing problems for CAN-FD (Bordoloi & Samii, 2014) and offset assignment techniques (Joshi et al., 2019) under a unified objective function: maximize payload throughput subject to strict deadline constraints and bus arbitration properties. The synthesis identifies the essential variables—signal periods, payload lengths, jitter bounds, ignition-domain priorities—and maps them into a structured optimization metaphors (packing + scheduling) while explicitly avoiding explicit formulae, describing algorithmic steps instead. The methodology extracts from prior work the proven heuristics and constraints that yield high utilization without violating real-time guarantees (Bordoloi & Samii, 2014; Joshi et al., 2019).

2. **Topology Verification and IDS Integration.** A second methodological pillar formalizes the integration of topology verification techniques (Yu & Wang, 2019) with schedule-aware

monitoring. The approach conceptualizes a topology verifier at the gateway/zone boundary that correlates expected scheduling patterns (derived from the packing and offset assignment) with observed bus behavior to detect deviations consistent with intrusion or misconfiguration. The design enumerates monitoring hooks, invariant checks, and anomaly scoring logic, drawing on established detection taxonomies (Wu et al., 2019), and explains how scheduled properties can reduce false positives by narrowing expected behavior profiles

3. **Zonal vs. Centralized E/E Architectural Mapping.** Using insights from architectural analyses (Bandur et al., 2021; Fikke, 2016; Migge et al., 2018), the methodology articulates a decision framework for selecting zonal or centralized topologies. The framework sets evaluation axes—latency, wiring mass, subsystem modularity, fault containment, upgradeability, and cybersecurity surface—and defines how each axis is prioritized for different vehicle classes. The methodology prescribes how to partition communication flows, placing ultra-low latency control messages close to actuators while routing bulk sensory and infotainment traffic over TSN/AVB-enabled Ethernet backbones

4. **Processor-Level Fault Tolerance Design Patterns.** The final methodological strand integrates classical error detection paradigms (Mahmood & McCluskey, 1988; Mukherjee et al., 2002) with modern dual-core lockstep and redundant multi-threading lessons (Moyer et al., 2012; Abdul Karim, 2023). The methodology provides a textually described recipe for implementing watchdog processors, lockstep synchronization policies, error containment regions, and recovery transitions tailored to zonal controller constraints. It further embeds instruction-level impact awareness (Maniatakos et al., 2011) and single-event effect mitigation considerations (Medina et al., 2016; Microchip, 2017) into the design choices.

5. **Gateway and Cross-Domain Interaction Policy.** Recognizing the persistence of legacy buses like CAN and FlexRay, the methodology prescribes gateway design principles (Zhao et al., 2010) that mediate between distinct scheduling and safety requirements. The gateway is described as an active translator and verifier that performs frame aggregation, temporal smoothing, and topology-aware filtering.

Each component of the methodology is described in operational detail so practitioners can implement prototype simulators or bench experiments to quantify tradeoffs. The paper emphasizes the interplay of scheduling, verification, and redundancy: for example, that a tighter packing strategy demands stronger topology verification to preserve detectability, and that zonal controller redundancy must be co-designed with gateway filtering to handle bursty replays or packetization artifacts.

Results

Because this manuscript is conceptual—deriving results through synthesis, inference, and extension of prior empirical knowledge rather than through new experimental trials—the "results" section documents the logical outcomes, predicted benefits, and synthesized performance expectations that follow from applying the methodology. Each result is tied to the underlying literature and described in detail.

1. **Throughput Gains from Integrated Frame Packing and Offset Assignment.** Prior studies on the frame packing problem demonstrate that intelligent aggregation of signals into CAN-FD frames yields substantial bandwidth savings, particularly when variable payload lengths and flexible arbitration windows are exploited (Bordoloi & Samii, 2014). When offset assignment heuristics are applied—assigning offsets to signals so that their transmission windows align favorably—empirical work has shown notable reductions in the number of frames transmitted and improved bus occupancy (Joshi et al., 2019). The integrated framework presented here predicts that, for typical mid-range vehicle signal matrices, combining packing heuristics with offset assignment will reduce effective bus load by a conservative estimate of 10–30% relative to naïve packing strategies, depending on signal period heterogeneity and payload variance (Bordoloi & Samii, 2014; Joshi et al., 2019). This conceptual result arises because offset assignment reduces fragmentation and enables

multi-signal coalescence into single frames, while packing heuristics optimize selection under deadline constraints.

2. **Improved Anomaly Detection via Schedule-Aware Topology Verification.** Topology verification techniques designed for CAN-FD networks compare observed message flows against a verified topology and report discrepancies indicative of tampering (Yu & Wang, 2019). Integrating schedule expectations into the verification process reduces detector uncertainty: messages that arrive within expected offset windows and with expected packing composition are less likely to be false alarms than messages that violate those expectations. By coupling packing and offset information with topology checks, the combined approach enables a narrower, more discriminating profile of legitimate behavior—thereby decreasing false positives while preserving sensitivity to injection and replay attacks (Yu & Wang, 2019; Wu et al., 2019). The anticipated operational benefit is a measurable improvement in detector precision, especially in complex busy buses where naive IDS approaches otherwise suffer elevated false-alarm rates

3. **Zonal E/E with Ethernet/TSN Backbones Balance Wiring and Latency.** The literature on zonal vs. centralized E/E architectures outlines a trade space where zonal topologies reduce wiring harness mass and localize fault domains but can increase system complexity and cost when middleboxes (gateways) proliferate (Fikke, 2016; Bandur et al., 2021). Centralized architectures—often with Ethernet/TSN backbones—simplify global traffic engineering and facilitate high-bandwidth sensor aggregation (Migge et al., 2018). The framework presented here recommends a hybrid approach: local control loops and timing-critical signals remain in zone-local buses (CAN, CAN-FD, FlexRay dynamic segments), while high-bandwidth perception and domain aggregation utilize a TSN backbone with carefully provisioned AVB classes for multimedia. This hybrid mapping retains low-latency control and improves overall bandwidth scalability without exponential growth in wiring mass.

4. **Gateway Policies That Preserve Timing and Security.** Gateways between legacy buses and Ethernet backbones can be active participants in safety and security. By performing deterministic coalescing, temporal smoothing, and signature-preserving translations, gateways can maintain timing invariants for downstream consumers and enforce topology verification invariants for IDS probes (Zhao et al., 2010; Yu & Wang, 2019). The result is an architecture where legacy traffic is preserved with minimal jitter, and injected traffic patterns that attempt to exploit packing heuristics to obfuscate attacks are more readily detected.

5. **Processor Redundancy Effectiveness and Constraints.** Classical concurrent error detection and watchdog processors remain valuable primitives in detecting transient and permanent faults (Mahmood & McCluskey, 1988). Recent implementations of dual-core lockstep in zonal controllers demonstrate that, when properly designed, such strategies can deliver deterministic error detection with manageable area and power overhead (Abdul Karim, 2023). However, the framework highlights that lockstep strategies must be augmented with instruction-level impact analysis to avoid silent data corruption scenarios where high-level correctness masks low-level errors (Maniatakos et al., 2011). Redundant multi-threading (Mukherjee et al., 2002) provides alternative tradeoffs that may better utilize multispectral cores but demand careful synchronization and recovery semantics. The overall synthesized result is that processor redundancy is effective but must be co-designed with system-level observability mechanisms and single-event mitigation strategies (Medina et al., 2016; Microchip, 2017).

6. **Combined System Predictions.** When the above components are integrated, the paper predicts a system posture where: (a) effective in-vehicle bandwidth utilization increases while timing determinism is maintained; (b) IDS false positives decrease through schedule-aware verification; (c) zonal controllers with processor redundancy provide fast local recovery and minimize vehicle-wide impact of faults; and (d) gateways and TSN backbones enable orderly

scaling of sensor bandwidth demands. These predicted outcomes align with reported empirical observations (Migge et al., 2018; Bandur et al., 2021; Bordoloi & Samii, 2014) and extend them by describing necessary interlocks among packing, verification, and redundancy.

Discussion

This section interrogates the synthesized results, exploring theoretical implications, counter-arguments, operational limitations, and directions for empirical validation.

1. **Theoretical Implications and Systemic Interactions.** The principal theoretical insight is that optimizations applied at different abstraction layers have emergent interactions that can be leveraged beneficially or can conflict if designed in isolation. For instance, frame packing and offset assignment (Bordoloi & Samii, 2014; Joshi et al., 2019) improve utilization but reduce the independent observability of individual signals—potentially complicating intrusion detection if the IDS expects single-signal atomicity. Conversely, schedule-aware topology verification (Yu & Wang, 2019) leverages knowledge of packing and offsets to actually increase detectability by reducing the expected behavioral space. Therefore, the architecture designer must view packing and verification as co-dependent design knobs. Similarly, processor redundancy choices affect how much diagnostic information is available to system monitors: a crash-fail that results in immediate fail-safe is easy to detect, but subtle instruction-level errors (Maniatakos et al., 2011) require richer runtime signatures and possibly software-level assertions to detect.

2. **Security Tradeoffs.** Integrating packing optimizations with IDS creates both defensive opportunities and potential attack vectors. An intelligent adversary might craft packet sequences that mimic legitimate packed frames, exploiting the aggregation to hide malicious signals. The countermeasure is a topology verifier that checks not only frame headers and timing but also internal packing composition and signal consistency across related channels. Additionally, gateways should enforce strict provenance and temporal coherence rules—e.g., rejecting frames whose internal signal offsets contradict canonical assignments (Yu & Wang, 2019; Wu et al., 2019). Such defenses strengthen the system but impose computational overhead and can increase latency; a careful cost-benefit analysis is therefore necessary

3. **Architectural Economics.** While centralized Ethernet/TSN backbones promise easier scaling for high bandwidth, their adoption is constrained by cost, certification complexity, and the need to maintain deterministic behavior for safety-critical flows (Migge et al., 2018; Bandur et al., 2021). Zonal controllers reduce wiring mass and physically localize failure modes, which lowers repair costs and can improve manufacturability (Fikke, 2016). The recommended hybrid approach aims to retain the best of both worlds but introduces the complexity of gateways and management planes. Practitioners must weigh the up-front cost of gateways and TSN configuration against the life-cycle benefits of modular upgrades and sensor expansions.

4. **Limitations and Open Problems.** The framework is limited by its reliance on prior empirical results rather than new experimental evidence. While the synthesized predictions are consistent with published findings (Bordoloi & Samii, 2014; Joshi et al., 2019; Yu & Wang, 2019; Migge et al., 2018), implementation details—such as precise offset assignment algorithms' sensitivity to jitter, or the precise computational cost of topology verification at scale—require quantification. Furthermore, the interaction between TSN scheduling and CAN-FD packing at gateway boundaries raises subtle timing composition problems that await formal modeling and tool support. At the processor level, the effectiveness of dual-core lockstep depends on the microarchitecture and workload characteristics—single-event effects (Medina et al., 2016) and modern complex core pipelines (Maniatakos et al., 2011) introduce failure modes that are not fully mitigated by simple lockstep. Another open problem is establishing standardized interfaces and exchange formats for conveying packing and offset assignments to

IDS and gateways so that cross-supplier interoperability is achievable.

5. **Future Scope and Experimental Roadmap.** To validate the framework, a prioritized experimental roadmap is advised:
   • Develop a modular simulator that models CAN-FD packing heuristics, offset assignment policies, gateway translation jitter, and a TSN backbone. The simulator should allow parameter sweeps over signal heterogeneity, vehicle classes (economy to premium), and fault injection to measure IDS precision/recall and latency impacts (Bordoloi & Samii, 2014; Joshi et al., 2019; Yu & Wang, 2019).
   • Implement a prototype gateway that performs topology verification and schedule-aware filtering in real time, measuring CPU and memory overheads for typical automotive message matrices (Zhao et al., 2010; Yu & Wang, 2019).
   • Benchmark zonal controllers with dual-core lockstep and redundant multi-threading across automotive workloads, injecting instruction-level faults and single-event transients to quantify detection latency and false negative rates (Mahmood & McCluskey, 1988; Maniatakos et al., 2011; Medina et al., 2016; Abdul Karim, 2023).
   • Conduct case studies comparing pure centralized Ethernet/TSN, pure zonal, and hybrid architectures across cost, mass, latency, and cybersecurity axes (Migge et al., 2018; Fikke, 2016; Bandur et al., 2021).

6. **Standards and Industry Considerations.** The success of the proposed integrative approach depends on industry alignment. Standardizing descriptors for packing and offsets, gateway verification contracts, and redundancy signaling will enable suppliers and OEMs to implement interoperable solutions. Additionally, certification authorities must consider how packing and aggregation affect traceability and evidence for safety analyses. For example, auditors will need methods to trace a failed signal back through aggregated frames—a nontrivial bookkeeping task that must be addressed through standardized diagnostics and metadata.

conclusion

This article presents a unified, richly detailed framework for designing resilient and efficient in-vehicle communication systems. By synthesizing advances in CAN-FD frame packing and offset assignment, topology verification for intrusion detection, zonal and centralized E/E architectural tradeoffs, and processor-level fault tolerance, the work clarifies how improvements at one layer influence observability, security, and fault detection at other layers. The principal recommendations are: (1) co-design packing and topology verification to preserve detectability while improving bandwidth utilization; (2) adopt hybrid E/E architectures that localize timing-critical control while leveraging TSN backbones for high-bandwidth sensor aggregation; (3) implement gateways as active timing and security enforcers; and (4) design processor redundancy strategies that incorporate instruction-level impact awareness and single-event mitigation. The conceptual results align with and extend prior empirical findings, but require rigorous experimental validation through simulators, prototypes, and industry pilots. Addressing standardization, certification, and the subtle composition of timing across domains remains an urgent next step for practical deployment. The overarching message is that robust automotive systems arise from integrated design—only by jointly optimizing packing, verification, architecture, and redundancy can future vehicles meet the twin demands of functionality and safety.

References

1. Bordoloi, U.D., Samii, S.: The frame packing problem for CANFD. Paper presented at 35th IEEE Real-Time Systems Symposium (RTSS), Rome, Italy, 2–5 December 2014.
2. Yu, T., Wang, X.: Topology verification enabled intrusion detection for in-vehicle CAN-FD networks. IEEE Commun. Lett. 24(1), 227–230 (2019). https://doi.org/10.1109/LCOMM.2019.2953722
3. Joshi, P., Ravi, S.S., Liu, Q., et al.: Approaches for assigning offsets to signals for improving frame packing in CAN-FD. IEEE Trans. Comput. Aided D. 39, 1109–1122 (2019). https://doi.org/10.1109/TCAD.2019.2907921
4. Schmidt, E.G., Schmidt, K.: Message scheduling for the FlexRay protocol: the dynamic segment. IEEE Trans. Veh. Technol. 58(5), 2160–2169 (2008).

5. Zhao, R., Qin, G.H., Liu, J.Q.: Gateway system for CAN and FlexRay in automotive ECU networks. Paper presented at 2010 International Conference on Information, Networking and Automation (ICINA), Kunming, 18–19 October 2010.
6. Fikke F S.: Electric/electronic-architectures-automating and optimizing communication matrices. Dissertation, Delft University of Technology (2016).
7. Migge, J., Villanueva, J., Navet, N., et al.: Insights on the performance and configuration of AVB and TSN in automotive ethernet networks. Paper presented at 9th European Congress on Embedded Real Time Software and Systems (ERTS 2018), Toulouse, France, January 2018.
8. Wu, W., Li, R., Xie, G., et al.: A survey of intrusion detection for in-vehicle networks. IEEE Trans. Intell. Transp. Syst. 21(3), 919–933 (2019). https://doi.org/10.1109/TITS.2019.2908074
9. Bandur, V., Selim, G., Pantelic, V., et al.: Making the case for centralized automotive E/E architectures. IEEE Trans. Veh. Technol. 70(2), 1230–1245 (2021).
10. MAHMOOD, A.; MCCLUSKEY, E. J.: Concurrent error detection using watchdog processors—a survey. IEEE Transactions on Computers, v. 37, n. 2, p. 160–174, Feb 1988.
11. MANIATAKOS, M., et al.: Instruction-level impact analysis of low-level faults in a modern microprocessor controller. IEEE Transactions on Computers, v. 60, n. 9, p. 1260–1273, Sept 2011.
12. MEDINA, N. H., et al.: Experimental Setups for Single Event Effect Studies. Journal of Nuclear Physics, Material Sciences, Radiation and Applications, v. 4, n. 1, p. 13–23, Aug 2016.
13. Abdul Salam Abdul Karim. 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 (2023).
14. MICROCHIP. Rad Hard Processors. 2017. Available from: http://www.microchip.com/design-centers/rad-hard/processors.
15. MONDRAGON, A. F.: AC 2012-4835: Hard Core Vs. Soft Core: A Debate. 2012. Available from: https://www.researchgate.net/profile/Antonio_Mondragon-Torres/publication/236844584_Hard_Core_vs_Soft_Core_A_Debate.
16. MOYER, W.; ROCHFORD, M.; SANTO, D.: Error detection and communication of an error location in multi-processor data processing system having processors operating in Lockstep. US Patent 8,090,984 (2012).
17. MUKHERJEE, S. S.; KONTZ, M.; REINHARDT, S. K.: Detailed design and evaluation of redundant multi-threading alternatives. Proceedings 29th Annual International Symposium on Computer Architecture (2002).