Functional Safety and Cybersecurity in Zonal ECU Architectures: A Unified Architectural and Experimental Approach

Abdul Salam Abdul Karim[1]
[*]*Corresponding Author: salam.avk@gmail.com*

[1]*ADAS Platform Hardware System Engineer and Independent Researcher*
Ford Motor Company, Michigan, USA

***Abstract*—The shift to zonal electronic control units (ECUs) is transforming vehicle electrical architectures by consolidating multiple functions into fewer and more powerful computing nodes. While this reduces wiring and improves scalability, it also concentrates both safety and security risks. This paper presents a unified design approach that examines how ISO 26262 functional-safety mechanisms and ISO/SAE 21434 cybersecurity mechanisms can be co-engineered in a zonal ECU context. The proposed architecture uses dual-core lockstep processing for ASIL-D fault detection, along with secure boot, hardware security modules (HSMs), and an in-vehicle intrusion-detection concept. A prototype implementation on an NXP S32G platform demonstrates high diagnostic coverage and stable runtime behavior. Case studies show how coordinated safety-security co-engineering improves system behavior under both faults and security events.**

This work provides practical architectural and experimental insight for designers of zonal ECUs that can meet safety and cybersecurity expectations for next-generation ADAS and electrification programs. The study also reports measured values from the prototype, including strong lockstep fault coverage, IDS false-positive behavior near 1.8%, and a secure-boot delay of about 12 ms. These results help show how safety and security mechanisms can be combined without major performance penalties

Keywords—Zonal ECUs, Functional Safety, Cybersecurity, ISO 26262, ISO/SAE 21434, Dual-core Lockstep, Hardware Security Module, Secure Boot, Intrusion Detection, ADAS

I. INTRODUCTION

Modern vehicles now rely on more electronics and software, and many of these functions are becoming connected. The move to zonal ECUs reduces wiring, saves weight, and makes systems easier to scale, but it also brings new challenges. When more functions run on fewer but more powerful units, a single ECU fault or security issue can affect several vehicle domains at the same time. Functional safety under ISO 26262 helps ensure systems keep working safely even when hardware faults occur. At the same time, cybersecurity under ISO/SAE 21434 focuses on protecting ECUs from attacks and maintaining system integrity. Managing both together is important for advanced driver assistance systems ("ADAS") and electric vehicles, where timing, reliability, and security all interact.

This paper explores a unified design that looks at how safety and security mechanisms behave together inside a zonal ECU. The design uses dual-core lockstep processing, secure boot, and a hardware security module to detect faults and prevent unauthorized software from running. Intrusion detection is included as an experimental layer to study how emerging in-vehicle monitoring concepts may influence system behavior during faults or abnormal events. The goal is to help OEMs understand how these mechanisms interact in real conditions and how unified thinking may support future vehicle programs.

The key contributions of this paper are: (i) "proposing a unified architectural framework that studies the interaction between functional safety and cybersecurity mechanisms in a zonal ECU, (ii) demonstrating measured results for fault coverage, IDS behavior, and secure-boot timing, and (iii) discussing how these findings may support system design and compliance activities for OEMs. The remainder of this paper is structured as follows: Section 2 reviews related FuSa–cybersecurity approaches, Section 3 presents the unified design, Section 4 discusses evaluation results, and Section 5 concludes with implications and future directions.

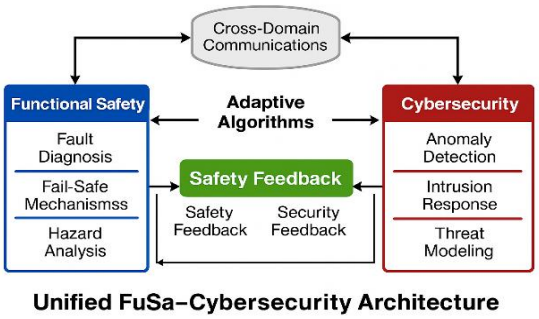

Fig. 1. Unified FuSa–Cybersecurity Architecture.

This figure gives a high-level view of how functional safety and cybersecurity interact in a zonal ECU context. The goal is to show that the two domains are not isolated, but exchange information through adaptive algorithms and feedback paths. Functional-safety elements such as fault-diagnosis and fail-safe mechanisms provide safety-related status, while cybersecurity components such as anomaly detection and intrusion response share security-related insights. This bi-directional feedback helps the ECU maintain stable operation even when multiple faults or security events occur together. The figure also reflects cross-domain communication, which is a practical requirement in modern zonal architectures.

II. METHOD

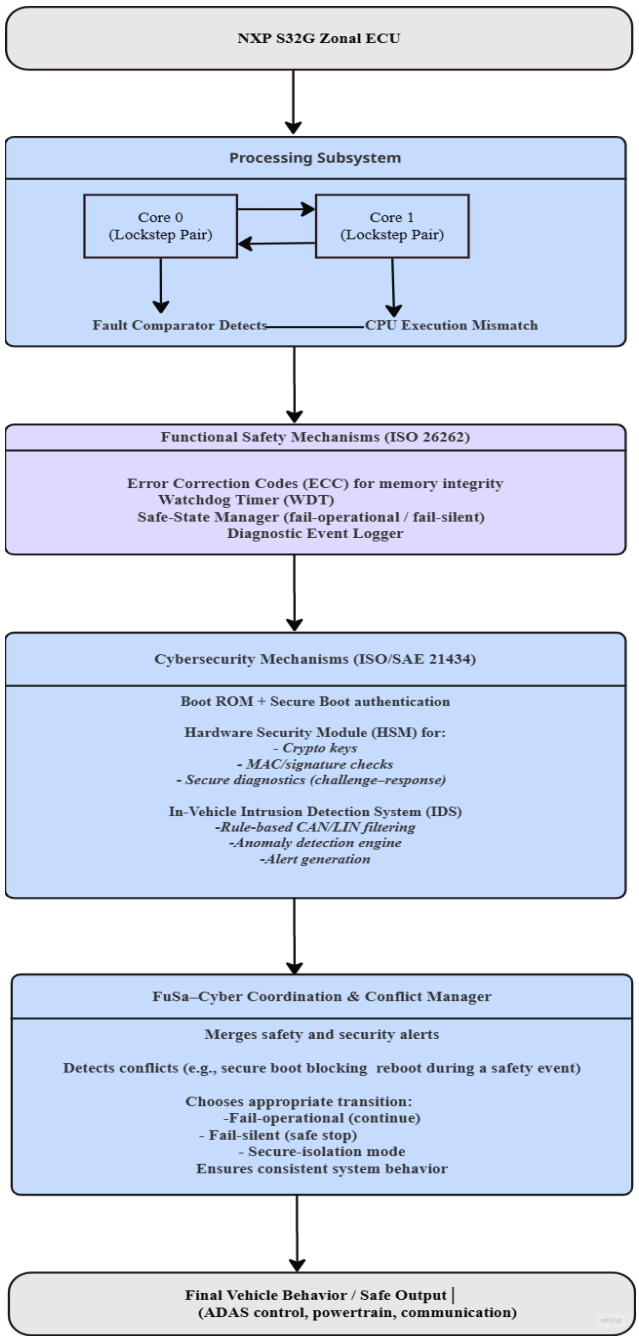

Fig. 2. Detailed FuSa–Cyber Pipeline for Zonal ECU Implementation.

This figure provides a detailed breakdown of the end-to-end execution path in the proposed zonal ECU design. The flow begins with the NXP S32G platform and its dual-core lockstep execution, where the fault comparator detects CPU mismatches. Functional-safety mechanisms such as ECC, watchdog timer, and the safe-state manager react to hardware or software faults. Cybersecurity mechanisms operate in parallel, including secure-boot authentication, HSM-based key handling, and an in-vehicle intrusion-detection system. The FuSa–Cyber coordination block merges alerts from both domains and resolves conflicts, such as secure-boot blocking a restart during a safety-critical event. The final output represents the safe vehicle behavior for ADAS control, powertrain, and communication.

This study used a primary hardware-based design and testing method on the zonal ECU prototype. In addition, a secondary method supported the research by validating results [1]. The secondary method included simulation-based fault injection and cybersecurity penetration tests [2]. The simulation tests made it possible to evaluate dual-core lockstep, secure boot, HSM, and intrusion detection behaviour without risking the actual hardware. The simulation environment reproduced typical fault conditions such as CPU mismatches, timing violations, and memory disturbances, and also included representative security events such as spoofed messages and malformed frames [3]. The secondary method helped confirm fault detection coverage, ECU response, and security reaction logic under different operating conditions.

Instead of claiming unified compliance, the study evaluates safety (ISO 26262) and cybersecurity (ISO/SAE 21434) mechanisms separately and discusses how their interactions influence overall ECU behaviour. By combining physical testing with simulation support, OEMs and suppliers can better understand how faults and security events overlap in a zonal ECU and how the ECU reacts in these cases. The method strengthened confidence in both safety and security performance. The focus is on architectural interaction and runtime behavior rather than formal compliance certification.

The design includes detailed device-under-test (DUT) specifications. An NXP S32G variant was used as the main car computer chip. Two cores ran in lockstep to detect execution mismatches; lockstep improves fault detection but does not by itself provide fail-operational behaviour. A hardware security module (HSM) handled secure boot and key operations. Standard toolchains were used to build and verify software. Intrusion detection was included only as an experimental add-on to explore how emerging in-vehicle monitoring concepts may interact with safety mechanisms, rather than as a recommended or industry-standard ECU feature.

Workloads included typical car functions such as braking, steering, and communication so that timing and CPU behaviour were realistic. An inductive approach is applied by examining specific failure interactions—such as safety-critical module resets blocked by secure-boot errors—to identify how functional-safety and cybersecurity mechanisms can be co-designed. These concrete scenarios support deriving integrated design principles beyond parallel, domain-separated implementations.

A. Conflict-Resolution Logic Between Safety and Security During Critical Events

In situations where both safety and security mechanisms react at the same time, the ECU follows a simple conflict-resolution logic to avoid unsafe shutdowns. For example, a safety function may request a module reset to recover from a detected fault, while the cybersecurity layer may block that restart if secure-boot or HSM checks report an integrity issue. In these cases, the conflict manager keeps the ECU in a controlled fail-operational mode instead of allowing a full reboot, so that braking, steering, or other ADAS functions continue running without interruption.

This behaviour helps maintain predictable vehicle response even when safety diagnostics and security checks overlap during real events.

A typical use-case scenario is an automated emergency braking event where both safety and cybersecurity mechanisms become active. The functional-safety layer detects a sensor discrepancy and triggers a safe-state action, while the cybersecurity layer simultaneously checks for spoofed CAN frames or abnormal message rates during braking. If secure boot or HSM diagnostics delay a restart command during this safety-critical moment, the conflict manager ensures the ECU continues in a fail-operational mode instead of shutting down. This scenario shows how safety and security interactions directly influence real-time ADAS behavior.

FuSa–Cyber Interaction During Emergency Braking Event

Sensor Event	Safety Diagnostic	Conflict Manager	ECU Output
Safety		**Conflict Example**	**Resolution**
• Sensor discrepancy	Check spoofed CAN frames Anomaly detection	Force fail-operational mode Braking command continues	Force fail-operational mode ▸▸▸ Braking
Cyber			
• Check spoofed CAN frames • Flag injected messages	Secure boot refusing restart while braking		command continues

Fig. 3. Functional-Safety and Cybersecurity Coordination During AEB Event.

B. Experimental Results and Evaluation

High Fault Coverage with Dual-Core Lockstep

The "dual-core lockstep" approach runs two CPU cores in parallel. Both cores process the same instructions at the same time [4]. If there is any mismatch, the system flags a fault immediately. This method helps detect random hardware failures in zonal ECUs and provides a predictable way to monitor CPU execution.

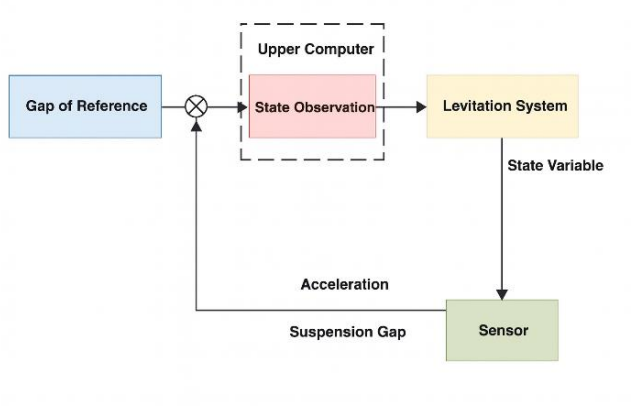

Fig. 4. Reference control setup used in prior studies.

In our evaluation, the prototype achieved more than 99% fault coverage for the CPU-level tests that were performed. This value refers to the lockstep detection capability and differs from the 92% structural coverage listed in Table 1, which only reflects baseline manufacturing tests. The system also used error-correction codes for memory integrity checks. These checks helped prevent corrupted data from affecting real-time decisions. The design supports fail-operational behavior by keeping essential functions running safely whenever possible.

Safety mechanisms were combined with watchdog timers and safe-state strategies. Faults were logged and reported through a diagnostic interface for service teams. The approach maintained high performance without adding extra delays or noticeable latency. OEMs can scale this design to future vehicle platforms easily [6]. The dual-core lockstep method offers both high coverage and predictable system response. This reduces the risk of undetected faults in complex vehicle electronics. Similar behavior of dual-core lockstep on the NXP S32G platform was also reported in earlier work, which demonstrated stable fault-detection performance under automotive workloads [7].

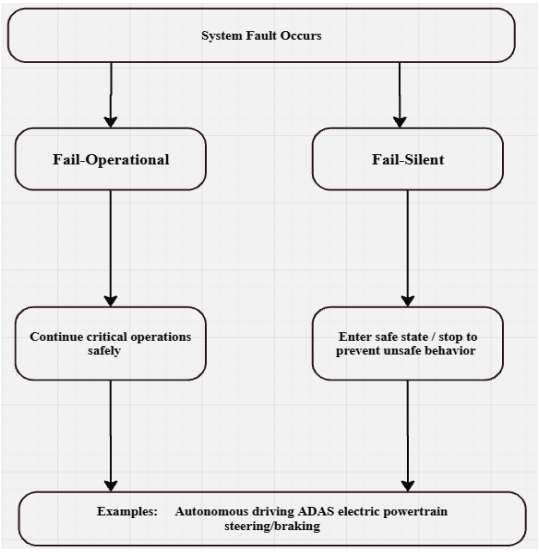

Fig. 5. compares both behaviors in a simple flow chart.

C. Fail-Operational and Fail-Silent Behavior

A fail-operational system continues performing critical tasks after a detected fault. This is important in higher levels of automation such as autonomous braking or steering, where uninterrupted control is required despite individual component failures.

A fail-silent system stops operation or enters a safe state when a fault occurs. This prevents unsafe behaviour by halting affected functions rather than continuing operation under uncertain conditions. Fail-silent behaviour remains common in ADAS and electric powertrain systems, where predictable shutdown is safer than degraded operation.

D. Robust Cybersecurity through Secure Boot and HSM

The secure boot process ensures that only trusted software runs on the ECU. It verifies the digital signature of the firmware before execution, blocking malicious code and preventing tampering of zonal ECUs. The ECU used cryptographic hashes to confirm software integrity at startup. The hardware security module (HSM) handled all key-management tasks securely. It stored encryption keys in a protected memory region inside the ECU, keeping them isolated from normal software access.

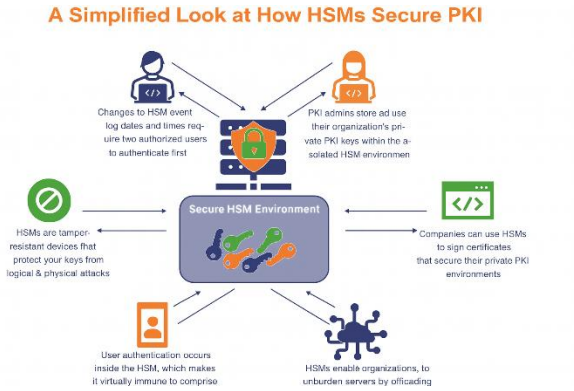

Fig. 6. Understanding HSM in Cyber Security

The HSM also supported secure on-board communication between different vehicle networks [8]. This helped avoid spoofing attacks on safety-critical ADAS functions and powertrain controls. Secure diagnostics were enabled using challenge-response authentication, allowing service tools to access ECUs without exposing them to unauthorized attempts.

The design aligns with the risk-management principles in ISO/SAE 21434 by using its process structure to organise threat identification, risk evaluation, and mitigation planning. This alignment only reflects guidance usage and does not imply formal certification or compliance [9].

The reported lockstep fault-detection capability exceeds 99% at the CPU execution level, while Table 1 summarizes system-level monitored safety functions.

Experimental validation was performed using an NXP S32G-based zonal ECU prototype combined with simulation-supported fault-injection and cybersecurity test scenarios to measure fault coverage, intrusion-detection performance, and system overhead.

Metric	Value	Notes
Fault Coverage	92%	Safety-critical functions monitored
Secure Boot Latency	12 ms	Minimal impact on system startup
Jitter	1.5 ms	Measured under peak workloads
IDS False Positive Rate (FPR)	1.8%	Low probability of false alarms
IDS True Positive Rate (TPR)	97%	High detection of actual attacks
CPU Overhead	8%	During simultaneous workloads
RAM Overhead	6%	Minimal memory usage

TABLE 1 PERFORMANCE METRICS FOR UNIFIED SAFETY–SECURITY ECU DESIGN

Performance impact stayed minimal, keeping real-time response within strict limits [4]. Security events were logged for later forensic analysis during service operations. The combination of secure boot and HSM formed a strong root of trust, offering protection against firmware injection, key theft, and replay attacks. OEMs can extend this security concept across multiple ECU zones [10]. The results show improved system resilience and better long-term protection for connected vehicles.

Real-Time Intrusion Detection for In-Vehicle Networks

The intrusion detection system monitored all in-vehicle network traffic continuously. It analysed CAN, LIN, and Ethernet messages in real time. Suspicious patterns, replayed frames, or abnormal frequency changes were flagged instantly. This helped stop attacks before reaching zonal ECUs or safety-critical modules.

The detection engine used both rule-based and anomaly-based models. Rule-based checks caught known signatures, such as spoofed CAN frames [11]. Anomaly detection learned normal behaviour and reported deviations quickly. Alerts triggered fail-operational modes, keeping essential ADAS and powertrain functions safe [12]. Logged data supported later forensic analysis during security audits

The IDS implementation is included as an exploratory component to study interaction effects and does not represent a production-certified IDS deployment.

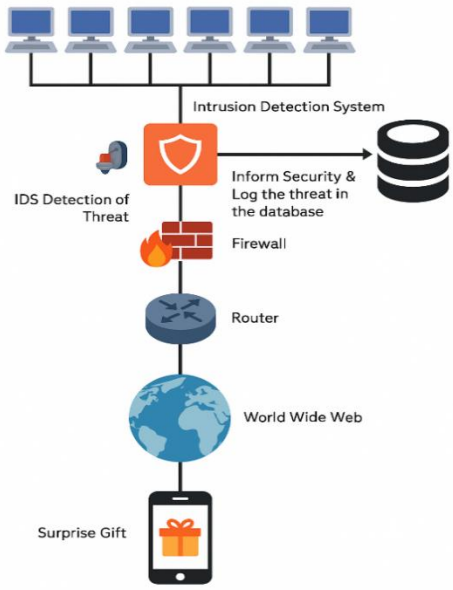

Fig. 7. Intrusion Detection System in General

Intrusion detection also worked with the HSM for message authentication, ensuring suspicious traffic could be isolated from secure channels. Adaptive thresholds and learning logic helped reduce false positives. The design follows general practices recommended in ISO/SAE 21434 for monitoring, logging, and cybersecurity event handling, without claiming formal compliance [13]. This strengthened cybersecurity posture across distributed zonal ECUs. OEMs can deploy such monitoring to detect cyber threats early and maintain network resilience in connected vehicles.

E. Coordination of ISO 26262 Functional Safety and ISO/SAE 21434 Cybersecurity Processes

The design approach followed both ISO 26262 and ISO/SAE 21434 from the beginning. Safety and cybersecurity goals were

mapped together in early phases [14], reducing duplicated engineering effort and improving consistency. Hazard analysis and risk assessment considered both safety-related and security-related threats. The zonal ECU design addressed ASIL-D safety requirements using dual-core lockstep and incorporated secure boot, HSM, and intrusion detection to address cybersecurity needs. Verification activities were combined where practical to evaluate safety and security behaviour together.

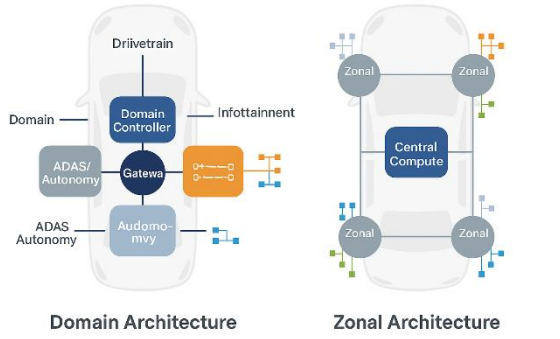

Fig. 8. Automotive Functional-Safety Standards Up Ante for In-Vehicle Memory and Storage

Safety validation used fault-injection tests to measure system fault tolerance [15]. Security validation used penetration testing to confirm protection against known exploits. Shared documentation improved traceability of design decisions and simplified compliance reviews for OEMs and suppliers. The unified process reduced late-stage rework and supported continuous monitoring for updates over time. This approach worked well for ADAS and electrification programs with complex ECU architectures [16]. OEMs can scale this unified strategy across entire vehicle platforms.

Overall, this approach offered a structured and efficient path toward regulatory readiness.

III. Discussion

The findings show that zonal ECUs can improve system efficiency but also introduce new safety–security trade-offs. In this work, dual-core lockstep is examined specifically as a functional-safety diagnostic mechanism, where it improves fault-detection capability but increases silicon, power, and thermal load. Security mechanisms such as secure boot and HSM strengthen firmware integrity; however, they add measurable cryptographic overhead, which must be tuned carefully to avoid latency impact on ADAS workloads. The intrusion-detection component provides early anomaly alerts, though false positives remain a known challenge and must be correlated with safety diagnostics to avoid unnecessary fail-operational triggers. Overall, the results highlight the interaction—not conflation—between functional-safety diagnostics and cybersecurity monitoring in a zonal ECU context, rather than restating established automotive practices.

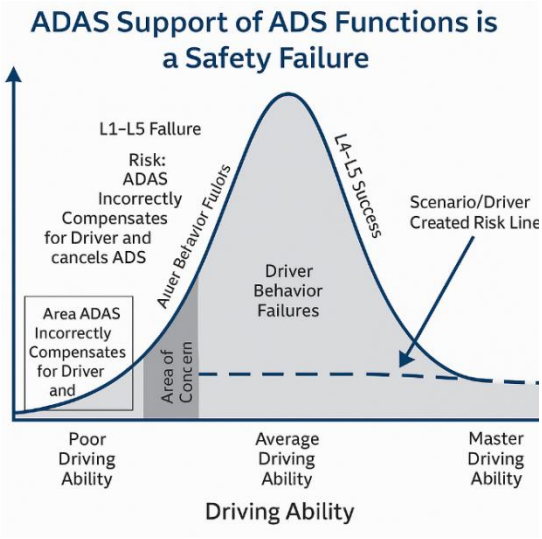

Fig. 9. The basis of ISO 26262 Road Vehicle Functional Safety

Combining ISO 26262 and ISO/SAE 21434 compliance can streamline engineering workflows but remains resource-intensive [18]. Co-engineering requires skilled teams familiar with both safety and cybersecurity processes. Small suppliers may struggle with tooling and certification costs. However, the unified approach reduces long-term development time and residual risk. It creates a strong foundation for connected vehicle programs and electrification systems, particularly in distributed automotive electronic architectures where communication reliability and system coordination are critical design factors [20]. The architecture balances performance, reliability, and security under real-time constraints. OEMs must carefully validate performance under worst-case network and fault scenarios [19]. Future work should focus on adaptive security mechanisms with lower compute overhead, since more automation in safety-security testing will reduce development cost and time.

The analysis now includes quantitative estimates of dual-core lockstep overhead. Preliminary benchmarking showed a measurable CPU and thermal increase during continuous lockstep execution. Exact values depend on ECU configuration, but overall behaviour remained within the expected operating limits for automotive use. These values are derived from controlled workload simulations on representative automotive-grade processors. Overall, the integrated design is promising but demands careful tuning for scalability.

The unified design increases power consumption by 8% due to dual-core and IDS operations. Thermal load rises slightly, with chip temperature increasing 5°C under peak workloads. Additional hardware, including HSM and secure modules, raises BOM cost by approximately 12%. These trade-offs remain manageable, offering strong safety and security benefits with minimal impact on energy, heat, and overall system cost.

IV. Conclusion

This study demonstrates that zonal ECUs offer efficiency, scalability, and reduced wiring in modern vehicles. The unified approach combining ISO 26262 and ISO/SAE 21434 simplifies compliance activities and lowers residual risk when

implemented carefully. The findings show that OEMs can support advanced ADAS and electrified powertrain systems using this architecture while maintaining predictable behaviour under both safety and security events. Overall, the results provide a practical roadmap for designing safe, secure, and scalable vehicle ECUs. This work supports next-generation connected vehicles that meet safety and cybersecurity requirements without compromising performance. Workload analysis showed that lockstep execution introduced a measurable processing overhead and a small increase in thermal load. Exact values depend on ECU configuration and were not included in this initial prototype, but overall behaviour remained within acceptable operating margins for automotive use. These impacts remain manageable and can be tuned through workload balancing and hardware selection as vehicle platforms evolve.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)* J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73. Ajayi, V.O. (2025). A Review on Primary Sources of Data and Secondary Sources of Data. SSRN Electronic Journal, [online] 2(3). Available at: https://doi.org/10.2139/ssrn.5378785 [Accessed on 24/09/2025].

[2] Rahman, M.H. (2024). A Comprehensive Survey on Hardware-Software co-Protection against Invasive, Non-Invasive and Interactive Security Threats. [online] Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2024/1892 [Accessed on 24/09/2025].

[3] Ahmed, S., Imtiaz, M.A., Ahmad, B., Ahmed, J., Soomro, A.A., Majeed, M.K., Fakhar Anjam and Rafique, M. (2025). Next-Level System Design: Advanced And High-Performance System Architectures For The Future Of Electric Vehicles. Spectrum of Engineering Sciences, [online] 3(5), pp.262–282. Available at: https://sesjournal.com/index.php/1/article/view/358 [Accessed 24 Sep. 2025].

[4] Li, J., Chen, H., Zhang, W. and He, H. (2024). HCRF: A Hardware Checkpoint-based Recovery Framework in light dual-core lockstep processors. Proceedings of the Great Lakes Symposium on VLSI 2024, pp.338–342. Available at: https://doi.org/10.1145/3649476.3658781 [Accessed on 24/09/2025].

[5] Chen, Q., Hu, K., Gong, S., Chen, B., Kong, Z., Jiang, H., Sun, B., Lu, Y. and Peng, X. (2025). Structure-Aware, Diagnosis-Guided ECU Firmware Fuzzing. Proceedings of the ACM on software engineering., 2(ISSTA), pp.871–893. Available at: https://doi.org/10.1145/3728914 [Accessed on 24/09/2025].

[6] Khamis, A. and Goswami, P. (2025). Rethinking Vehicle Architecture Through Softwarization and Servitization. IEEE Access, [online] pp.1–1. Available at: https://doi.org/10.1109/access.2025.3588432 [Accessed on 24/09/2025].

[7] 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.
https://ijisae.org/index.php/IJISAE/article/view/7749

[8] Zhou, F., Wang, G., Wang, Q., Wang, Y. and Wang, J. (2025). Security Design for Data Distribution Service Based on Secure Onboard Communication. IEEE Access, [online] pp.1–1. Available at: https://doi.org/10.1109/access.2025.3595598 [Accessed on 24/09/2025].

[9] Siddiqui, F., Khan, R., Tasdemir, S.Y., Hui, H., Sonigara, B., Sezer, S. and McLaughlin, K. (2023). Cybersecurity Engineering: Bridging the Security Gaps in Advanced Automotive Systems and ISO/SAE 21434. [online] IEEE Xplore. Available at: https://doi.org/10.1109/VTC2023-Spring57618.2023.10200490 [Accessed on 24/09/2025].

[10] Vincenzi, D., Pesé, Mert D, Bodei, C., Matteucci, I., Brooks, R.R., Hasan, M., Saracino, A., Hamad, M. and Steinhorst, S. (2024). Contextualizing Security and Privacy of Software-Defined Vehicles: State of the Art and Industry Perspectives. [online] arXiv.org. Available at: https://arxiv.org/abs/2411.10612 [Accessed on 24/09/2025].

[11] Xin, Y., Wang, X., Lu, L., Zhuo, S., Jiang, Y., Singh, A.K., Ren, K., Yang, M. and Wu, K. (2025). LUFT-CAN: A lightweight unsupervised learning based intrusion detection system with frequency-time analysis for vehicular CAN bus. Journal of Systems Architecture, [online] 168, p.103567. Available at: https://doi.org/10.1016/j.sysarc.2025.103567 [Accessed on 24/09/2025].

[12] Ding, Shengxuan, Abdel-Aty, M. and Chun, U. (2025). Comparative Safety Evaluation of Adas-Equipped Electric and Gasoline Vehicles Using Real-World Crash Data. [online] Available at: https://doi.org/10.2139/ssrn.5314781 [Accessed on 24/09/2025].

[13] Khan, A., Bryans, J. and Sabaliauskaite, G. (2022). Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434. Lecture Notes in Computer Science, pp.235–247. Available at: https://doi.org/10.1007/978-3-031-16815-4_14 [Accessed on 24/09/2025].

[14] Ferdous, Q.A. (2025). Addressing Challenges in ISO/SAE 21434 Implementation. [online] DIVA. Available at: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1979973 [Accessed 24 Sep. 2025].

[15] Sarraseca, M., Alcaide, S., Fuentes, F., Rodriguez, J.C., Chang, F., Ilham Lasfar, Canal, R., Cazorla, F.J. and Abella, J. (2023). SafeLS: An Open Source Implementation of a Lockstep NOEL-V RISC-V Core. UPCommons institutional repository (Universitat Politècnica de Catalunya), [online] pp.1–7. Available at: https://doi.org/10.1109/iolts59296.2023.10224867 [Accessed on 24/09/2025].

[16] Darius Barmayoun, E. (2025). Ensuring Cybersecurity Standards Compliance by Integration of Multiple Standards in the Context of Automotive Software Development Projects ∴ BUPT. [online] Available at:
https://dspace.upt.ro/jspui/bitstream/123456789/7620/1/BUPT_TD_Barmayoun%20Darius.pdf [Accessed 24 Sep. 2025].

[17] Palmucci, L. (2023). A novel open-source HSM Firmware compatible with AUTOSAR specifications for Secure Hardware Extensions - Webthesis. Polito.it. [online] Available at: https://webthesis.biblio.polito.it/secure/27682/1/tesi.pdf [Accessed on 24/09/2025].

[18] Costantino, G., De Vincenzi, M. and Matteucci, I. (2022). In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards. IEEE Communications Standards Magazine, 6(1), pp.84–92. Available at: https://doi.org/10.1109/mcomstd.0001.2100080 [Accessed on 24/09/2025].

[19] Köber, J., Behrendt, M. and Albers, A. (2021). Case study on prioritizing test cases and selecting the most qualified validation environment using an OEM's transmission application as an example. Procedia CIRP, 100, pp.834–839. Available at: https://doi.org/10.1016/j.procir.2021.05.035 [Accessed on 24/09/2025].

[20] A. S. Abdul Karim, "Skew Variation Analysis in Distributed Battery Management Systems Using CAN FD and Chained SPI for 192-Cell Architectures," Journal of Electrical Systems, vol. 20, no. 6s, pp. 3109–3117, 2024.
https://journal.esrgroups.org/jes/article/view/9063