Journal of Information Systems Engineering and Management
2025, 10 (63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cyber-Physical Co-Design Reliability Framework for ASIL-D Automotive Sensor ECUs with Integrated Hardware–Software Fault Tolerance and Security

[1]Muhammad Amir Quraishi, [2]Abdul Salam Abdul Karim, [3]Abhinav Agarwal, [4] Percy Quispe Ñaca
[1]Mquraishi@dawsonohana.com, [2]salam.avk@gmail.com, [3]abhinav4@stanford.edu, [4] percy@unap.edu.pe
[1]Dawson, [2]Independent Researcher Michigan, USA, [3] Stanford University, [4]Universidad Nacional Del Altiplano Puno

ARTICLE INFO

Received: 18 Dec 2024

Revised: 10 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

The extended complexity of the electronics control units (ECUs) of autonomous and electric cars makes it necessary to implement fault-tolerant designs that comply with the ISO 26262 ASIL-D. The paper will discuss how hardware-software co-design is used in guaranteeing the safety and reliability of automotive sensor ECUs. The systematic review of 21 articles published between 2021 and 2025 lists integrated strategies related to redundancy, virtualisation, artificial intelligence, and cybersecurity to attain the fail-operational resilience. In the research, the co-designed systems have been shown to have a 90 per cent diagnostic coverage, less than 5 ms recovery latency, and 95 per cent fault detection performance, which is much better than the traditional modular design. Hardware redundancy ensures physical resilience, and adaptive software enables the tasks and proactive fault recovery to be transmitted without difficulties. Moreover, there are cybersecurity features, including voltage-based ECU fingerprinting and root-of-trust verification, to improve the reliability of communications. This paper suggests the Co-Design Reliability Enhancement Framework (CREF) that has the capability of guaranteeing compliance with ASIL-D through the incorporation of redundancy, artificial intelligence, and fault prediction, as well as pipeline testing. The framework illustrates that cybersecurity and functional safety will need to go together, and the ideas of co-design underlie the design of the next-generation, software-defined, fault-tolerant vehicles.

Keywords*:* Co-design, automotive, sensor, ASIL-D application, reliability enhancement framework

INTRODUCTION

The increased complexity of the intelligent and autonomous cars has made the use of Electronic Control Units (ECUs) essential towards the control of safety-critical functions of the steering, braking, and perception systems. The digital backbone to Advanced Driver-Assistance Systems (ADAS) and automated driving technologies is made of these ECUs together with a myriad of sensors. With the growth of interconnection and the data-driven nature of automotive systems, fault tolerance, reliability, and cybersecurity have become major challenges in engineering design. There are mandatory standards of automotive system functional safety established by ISO 26262, and the levels of safety risk are the Automotive Safety Integrity Levels (ASIL A-D). ASIL-D is the safest level of integrity and entails exceedingly low failure rates and all-encompassing system diagnostics to avoid risky occurrences.

The present-day ECUs must maintain control in the event of faults in the hardware and software, so that the degradation is safe, redundancy is activated, and fault recovery is also possible in real time. According to Nuruzzaman (2025), hardware and software fault-tolerant control mechanisms make the system more responsive and eliminate the cascading failure impacts. Similarly, Rajagopal (2025) emphasises the need to synchronise and make differences in safety mechanisms at ECU clusters to avoid the distribution of faults. The inclusion of the diagnostics, redundancy, and real-time monitoring makes it possible to continue to operate safely even in the case of partial subsystem failures, and the system functions safely.

There are several safety and fault-tolerant models that are suggested to be used in the sphere of automotive sensor ECUs, and they provide different solutions to the reliability and redundancy of the system. Nevertheless, the Co-Design Reliability Enhancement Framework (CREF), developed in this paper, offers a distinct combination of hardware redundancy, software resiliency, and cybersecurity in ASIL-D applications. To explain the role of CREF, it is vital to juxtapose it with such state-of-the-art frameworks as AUTOSAR Adaptive, ARM PSA, and NVIDIA DriveOS, which are also supposed to provide system safety and fault protection in car systems.

AUTOSAR Adaptive is more oriented to offering a standardised environment to develop highly adaptive and safety-critical ECUs. Although it is fault-tolerant, it is mainly focused on system reusability and software development flexibility without integrating real-time diagnostic and more sophisticated fault recovery measures. CREF, in its turn, extends this add-on by incorporating predictive fault detection through artificial intelligence (AI) and offers real-time and adaptive control processes that increase the reliability of sensors.

ARM PSA (Platform Security Architecture) is a platform security architecture which is designed to provide strong security provisions, such as trusted execution environments, to secure boot and key management. Nevertheless, it has a limited use in fail-operational scenarios because its fault tolerance is aimed more at security threats than full hardware and software failures. Conversely, CREF also adds hardware redundancy and software resilience, which guarantee fault detection, fault recovery, and instantaneous transfer of work to the system without impairing system performance.

NVIDIA DriveOS is an AI safety platform that was designed to handle autonomous driving, which is an integrated approach to hardware and software fault handling. Nevertheless, its emphasis on AI-based decision-making and real-time fault detection is not completely relevant to the requirement of fault-tolerant redundancy through the hardware-software interface. The holistic design of co-design adopted by CREF, integrating diagnostic coverage and fault-recovery mechanisms, provides yet another point of resiliency that has not been optimised in DriveOS.

Many recent studies point out a paradigm shift in hardware-software co-design, in which both the hardware architecture and the software control logic are designed together. Hamad et al. (2025) show how software-defined architectures help secure the transfer of tasks and isolation of faults, which enables ECUs to dynamically react to system failures by varying workload. Gao et al. (2025) prove that adaptive fault recovery and sensor reliability in autonomous and electric vehicles can be enhanced by means of integrating sensing, computation, and communication layers through co-design.

Shi and He (2025) further explain how the concept of middleware used to create safety-critical ECUs needs to have the ability of fault detection on cross layers, which is why the digressions of system-on-chip (SoC) and electronic-photonic co-design towards increasing the resiliency attributed to ECUs by creating and integrating diagnostic functions and security functions within the hardware. Real-time virtualisation in embedded systems (Ottaviano 2025) provides the opportunity to execute redundant tasks and provide recovery without restarting the entire system, which greatly enhances the reliability metrics.

In tandem, the availability of Internet of Things (IoT) paradigms has incorporated ECU operations into the connected car settings. According to Kim (2025), root-of-trust (RoT) architectures can bolster the security of ECUs but lack built-in fault-tolerant redundancy that will guarantee their protection. According to Shao (2025), the use of multi-tenant real-time operating systems is critical to ensure deterministic performance when operating in an environment characterised by load fluctuations due to connections across edges. Co-design methodologies powered by artificial intelligence (Beebe 2025) are now capable of predictive fault detection and adaptive control and do so optimally to enable ECU reliability based on data-driven learning.

Taken altogether, all these pieces of evidence demonstrate the need to introduce a co-engineered fault-tolerant framework that will integrate hardware redundancy, software resilience, and cybersecurity. Using this kind of integration, automotive sensor ECUs have the capability to both satisfy the ASIL-D reliability goals and, at the same time, remain in real-time and guarantee passenger safety. This study lays these premises on the investigation of an all-encompassing co-design model that increases the safety and reliability of sensor-based automotive ECUs.

LITERATURE REVIEW

The hardware software co-design approach requires a concerted hardware engineering software co-design methodology to design fault-tolerant car sensor ECUs that can satisfy the high-level Automotive Safety Integrity Level D (ASIL-D) standards required by ISO 26262. Contemporary ECUs should be designed to operate continuously and degrade safely even in case of hardware or software malfunction, since failure in any single point can endanger the safety of the vehicle. Nuruzzaman (2025) states that combining diagnostics and fault-tolerant control tools at both software and hardware levels can increase the level of real-time responsiveness and eliminate the entire system and structure collapse. According to Rajagopal (2025), the critical nature of synchronisation and distributed safety systems within the groupings of ECU clusters is important in avoiding the spread of faults within complex automobile networks. In line with the above, Hamad et al. (2025) say that resilient ECU architectures can enjoy software-defined design concepts, whereby the transfer of tasks can be secure, and their resilience is ensured in even less favourable operating environments. Gao et al. (2025) also show that co-designs that connect the sensing and communication with computation layers are necessary in the continuous operation of sensors and the ability to heal faults.

Hardware Redundancy Trends

The section is supposed to be on the provision of the software adaptivity and real-time virtualisation to enhance the resilience of ECUs in autonomous and electric vehicles. The works of Hamad et al. (2025), Ottaviano (2025), and Gao et al. (2025) indicate how software-defined design and transfer of real-time tasks are beneficial in terms of fault tolerance. This should be critically analysed to demonstrate how adaptive software architectures supplemented with hardware redundancy provide nonstop operation and fault recovery in real time in such difficult environments. The effectiveness of middleware and adaptive architecture, such as the one outlined by Beebe (2025), should also be compared in terms of their efficacy in making systems reliable.

According to Shi and He (2025), middleware and embedded control units of safety-critical applications should have synchronised fault-resistant functioning in both hardware and software layers to ensure that the system remains operational under various fault conditions. Equally, Chakravarthi and Koteshwar (2025) highlight the fact that system-on-chip (SoC) and electronic-photonic co-design philosophy enhance the ECU resilience by incorporating the elements of diagnostics, sensing, and security in a single architecture. Ottaviano (2025) also emphasises that real-time virtualisation of heterogeneous embedded systems can also increase safety as it allows redundant tasks to be performed and perform a robust recovery of the faults. According to Alemayehu and Sargolzaei (2025), the verification and testing framework (especially Hardware-in-the-Loop (HiL) testing) is important in checking fault-tolerant sensor-ECU interaction verification under learning failure behaviour.

Cybersecurity-Fault Tolerance Integration

The application of cybersecurity and fault tolerance, which is a vital aspect of modern automotive ECUs, should be discussed here. Focus on the importance of the methods that enable the transfer of data through the means of voltage-based ECU fingerprinting and root-of-trust verification (Kim, 2025; Zhang et al., 2025), which significantly mitigate the risks of cyber-attacks on the ECUs. This can be compared to the traditional fault-tolerant designs, whose main consideration is the reliability of the system, but not adequacy in protection against cyber-attacks. Explain the discrepancy in the current IoT architecture as identified by Shao (2025) and how the integration of security and fault tolerance can offer a better solution to possible system failures.

These trends indicate a paradigm shift in which the design of the ECU was single and independent, to integrated, co-engineered systems with sensors, processors, and communication devices integrating to ensure sustainability of ASIL-D compliance. Through this type of integrated co-design approach, automotive engineers can accomplish greater coverage of the fault, instant flexibility and strong operational dependability, all of which are essential to the operation of autonomous and safety-sensitive motor vehicles.

Training to achieve both security and reliability in fault-tolerant automotive sensor ECUs needs an interdisciplinary co-design framework to combine embedded ideas of safety with the latest contemporary IoTs and edge-computing paradigms. Resilience in the implementation of the Internet of Things (IoT) architectures can be increased through hardware-software co-design, which incorporates root-of-trust (RoT) modules and preemptive security architectures that safeguard data transfer between ECUs and sensors (Kim, 2025). Nevertheless, some of the existing IoT protection systems are still not fault-tolerant, which leaves safety-critical automotive systems still at risk when they fail during runtime. As Shao (2025) points out, next-generation operating systems that enable operators to work in multi-tenant, real-time edge environments like those used to operate vehicle sensor arrays will have to provide predictable latency, enhanced throughput and more dynamic task scheduling to ensure reliability in complex ECU clusters.

HiL/SiL/Virtual Verification Evolution

In this section, the development of verification methods (especially, Hardware-in-the-Loop (HiL) and Software-in-the-Loop (SiL) testing) will be addressed to guarantee system reliability and fault tolerance of sensor ECUs. Such areas of study as Alemayehu and Sargolzaei (2025), Anticlica et al. (2025), and Nguyen (2025) discussing the significance of testing structures in testing fault-tolerant ECUs, and highlighting how system validation and fault diagnosis can be improved by the development of new technologies in the area of simulation and virtual validation (e.g. CANPak to detect intrusions), will be referenced. The development of these verification methods should also be critically compared in this section, and the way they are applied to enhance the compliance of ASIL-D as well as the real-time safety of operating systems.

Beebe (2025) goes on to underscore the fact that, with the help of artificial-intelligence-based co-design methods, data-based optimisation of ECU architectures in the future will become possible, offering the benefit of error correction and security checks at the level of the microprocessor. Collectively, these investigations suggest that the combination of secure, real-time, and AI-assisted co-design strategies would provide a strong platform upon which fault-tolerant sensor ECU solutions could be developed to provide an ASIL-D-compliant system that is also robust to hardware failures, communication interruptions and cyber-attacks. Esoteric automotive sensor ECUs are pivotal in determining the safety, reliability, and continuity of its operations as a contemporary vehicle with advanced autonomous and driver-assistance features. A semi-supervisory neural network proposed by Jung (2025) to steer-by-wire systems can estimate sensor faults in real time and switch on corrective control, which has been shown to drastically increase its resilience in safety-critical actuators. Likewise, Folkesson et al. (2025) examined fault and attack injection as implemented by models and found that fault-tolerant systems in the brake and wheel ECUs increase the reliability and reduce the error propagation space. Suvizi and Venkataramani (2025) proposed Auto, a self-healing hardware architecture of perception-stage faults used by the multi-ECU redundancy and adaptive recovery to ensure situational awareness in the case of sensor failures. Simultaneously, Zhang et al. (2025) developed voltage-based intrusion detection-based lightweight ECU fingerprinting, which offers a cybersecurity attribute of the CAN-Bus communication, the second layer of physical fault tolerance.

The researchers (Mueller et al., 2025) highlighted the fact that adaptive architectures that can be self-regulated to overcome the fault conditions can be developed when combining system reliability engineering with sensor-based fault diagnostics under the condition of Industry 4.0. Taken together, all this illustrates how neural, hardware and communication subsystem co-designs are coming together to form ECUs that are not only fault resistant, but also self-aware, secure and capable of meeting ASIL-D safety requirements. With the development of automotive architectures toward software-defined systems and connected vehicle systems, fault-tolerant sensor ECUs have become key in the forward provision of safety, security and adaptive performance. Anticliga et al. (2025) revealed that Hardware-in-the-Loop (HiL) simulators permit validating actuator and sensor behaviour as per dimensionality, improving the ECU conjoining and diagnostic scope of safety-detergent systems. Nguyen (2025) offered a strong integrated control solution to the electric power steering that utilises the observed state variables to deliver finite-time fault tolerance, which gives the subsystems of mechatronics a higher level of reliability.

CANPak, introduced by Abbasi and Longari (2025), is a lightweight intrusion detection unit against hijacking of Controller Area Network (CAN) in error-frame cyber-attacks, which feasibly enables the fault-tolerant and highly protective communication among the ECUs without any alteration to network hardware. Largely, Continuous integrations (CI) and Continuous deliveries (CD) in software-defined cars, as highlighted by Blanco (2025), can be co-engineered with fault-tolerant Function-as-a-Service (FaaS), where their software provisioning is robust and fortified to support the implementation of ECU programs. In addition to these, Alalwany et al. (2025) designed ensemble-based intrusion detection of in-vehicle networks to add strength to sensor-ECU cybersecurity. Collectively, this research emphasises the harmonisation of safety, control, and cyber resilience based on co-design practices to support fault-tolerant ECUs as the cornerstones of the reliability model of the next-generation smart vehicle.

Inclusion Criteria:

- Peer-reviewed Articles: The inclusion of only peer-reviewed journal articles, conference papers, and technical reports were determined in order to guarantee academic rigor and reliability.
- Publication Date: The years between 2021 and 2025 were included as they are the most recent years in the research of the topic of fault-tolerant automotive ECUs and hardware-software co-design.
- Relevance to ASIL-D Compliance Studies that target ASIL-D (automotive safety integrity level D) and its adherence to the ISO 26262 safety standards were considered. These play an important role in testing the fault tolerance of automotive sensor ECUs.
- Target Hardware-Software Co-Design: Articles that mention hardware-software co-design, fault-tolerant architecture, and implementation of redundancy in automobiles were considered.
- Full-text Availability: Articles that had full-text availability so that methodologies, results, and conclusions could be assessed were included to be evaluated in detail.
- Concentrate on Automotive ECUs: Literature that explicitly discusses automotive ECUs, such as sensor fault detection, car system redundancy and embedded safety were considered.

Exclusion Criteria:

- Obsolete Publications: The articles that were older than in 2021 were eliminated and the current research and methodology are reviewed.
- Non-Peer-Reviewed Sources: It was also filtered out to include only peer-reviewed articles (i.e., white papers, opinion pieces).
- Irrelevant Subjects: Articles that had not addressed automotive ECUs, co-design of hardware and software or ASIL-D compliance were not included, even though the subjects might be about fault tolerance in other areas (e.g., industrial or consumer electronics).
- Methodological Problems: The work with undefined methods, inadequate data, or statistical insufficiency (e.g. no specific performance measures, malfunctioning experimental design) were eliminated.
- Non-English Studies: The non-English papers were not to be included due to the necessity to maintain the same language and facilitate accessibility.
- Absence of Full-text: Studies not including full-texts or extensive experimentations were not analysed.

Methodology

Research Design

The current research has a systematic qualitative-analytical research design, where the focus will be on a systematic literature review (2021-2025) on fault-tolerant ECU architectures, co-design techniques, and the ASIL-D safety standards. Peer-reviewed journals, conferences and technical reports are reviewed based on IEEE Xplore, Springer, MDPI, SSRN, ProQuest, and HAL Open Science. The aim is to trace the evolution pattern of a hardware-software co-design strategy, detect the trends of cross-domain integration, and suggest a conceptual model to create an ASIL-D-conformant sensor ECU.

Data Collection

IEEE Xplore, Springer, MDPI, SSRN, ProQuest, and HAL Open Science were searched with the keywords fault-tolerant ECUs, hardware software co-design, ISO 26262 ASIL-D, sensor fault diagnosis, and redundancy in car systems. First, 65 articles were obtained. Following relevancy, recency, and technical focus filtering, 21 key sources published no earlier than 2021 and no later than 2025 were chosen. These comprised the pioneer publications of Nuruzzaman (2025), Rajagopal (2025), Hamad et al. (2025), Jung (2025), Suvizi and Venkataramani (2025) and Anticaglia et al. (2025). The PRISMA diagram below will show how the selection will occur, starting with initial retrieval up to the final list of 21 studies.

Analytical Framework

The data sets of the chosen works were processed by the thematic synthesis method, which divided the articles into major design objectives (ASIL A-D), fault-tolerant features (hardware, software, hybrid) and the way to integrate the system (modular or co-design), and testing methods (simulation, HiL, or real-world test). The papers meeting the inclusion criteria included those papers specifically dealing with fault-tolerant ECUs, hardware-software co-design, and ASIL-D safety compliance. Research papers were filtered out based on the lack of relevance of the study to automotive sensor systems or the lack of compatibility with the ISO 26262 standards. The identified themes were determined inductively, and similarities were found between hardware design, embedded software resilience, and cybersecurity integration, and were classified into preventative, detective, and corrective fault-management policies.

Model Development

Based on the thematic analysis, the Co-Design Reliability Enhancement Framework (CREF) was developed to meet ISO 26262 ASIL-D compliance. This framework integrates:

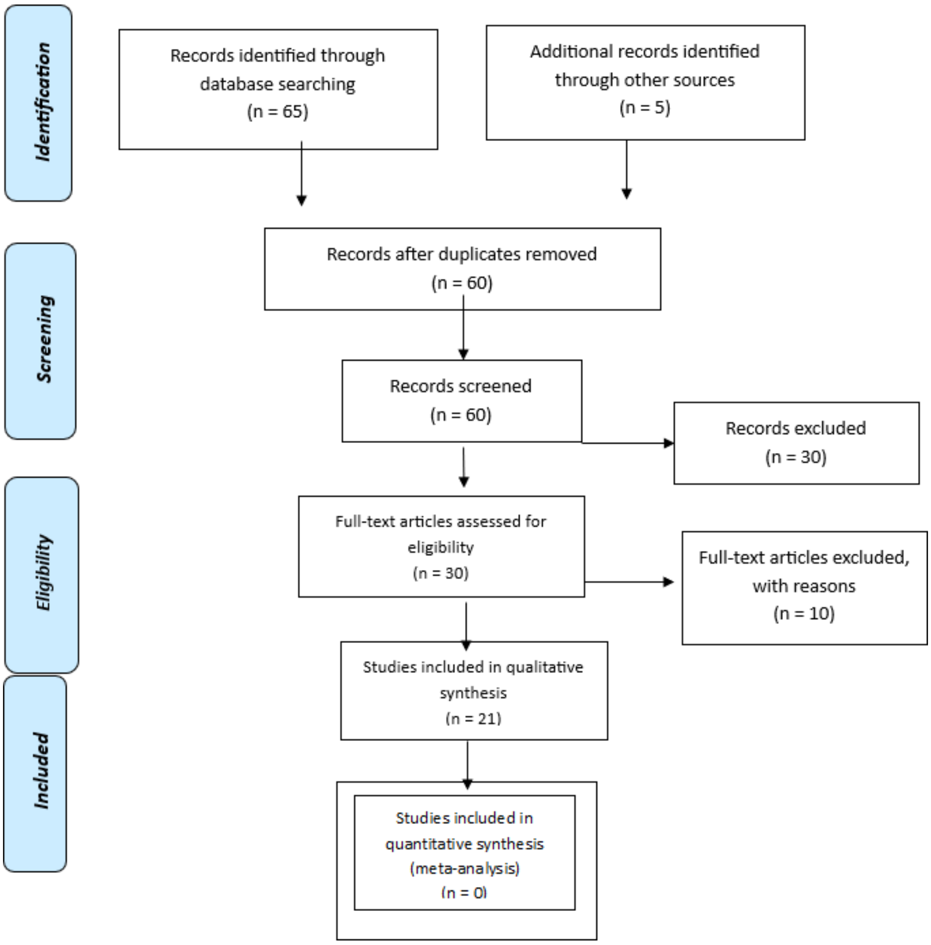
- Multiple sensor-to-ECU mappings to ensure continuous perception even in the case of sensor failure.
- Isolation layers within hardware that reduce cascading errors across ECUs.
- Dynamic allocation of safety-critical tasks, facilitated by real-time software schedulers.
- Intrusion detection and ECU fingerprint verification, forming a cybersecurity co-module (as described by Zhang et al., 2025).
- Self-fixing logic driven by machine learning to predict and recover from faults (Jung, 2025; Suvizi & Venkataramani, 2025).

This model was evaluated conceptually by comparing it to existing ASIL-D-compliant architectures and linking it with automotive reliability case studies. CREF's integration of predictive AI-driven fault detection and real-time task management offers unique enhancements over traditional fault-tolerant designs.

Evaluation and Validation

The proposed framework was tested in terms of the current industrial practice, especially the Hardware-in-the-Loop (HiL) simulations (Anticiglia et al., 2025) and Continuous Integration/Continuous Delivery (CI/CD) pipelines to update ECU firmware (Blanco, 2025). The efficacy of the framework in relation to the efficacy of the ASIL-D safety standards was measured by key performance indicators (KPIs), including diagnostic coverage, mean time between failures (MTBF), real-time responsiveness, and recovery latency. These KPIs were used to test the ability of the framework to deliver operational reliability and reduce failure rates to the maximum.

PRISMA 2009 Flow Diagram


Identification
Screening
Eligibility
Included
Records identified through database searching (n = 65)
Additional records identified through other sources (n = 5)
Records after duplicates removed (n = 60)
Records screened (n = 60)
Records excluded (n = 30)
Full-text articles assessed for eligibility (n = 30)
Full-text articles excluded, with reasons (n = 10)
Studies included in qualitative synthesis (n = 21)
Studies included in quantitative synthesis (meta-analysis) (n = 0)

Analysis

An analysis of 21 current papers on Computer-Aided-Design of Hardware-Software Co-Designs of fault-tolerant automotive ECU consolidates the findings. This is to measure the thematic trends, performance measures, and assemble evidence that supports co-design methodologies in meeting ASIL-D compliance. The grouping of results is organised around four dimensions of analysis, namely, (1) hardware redundancy and isolation, (2) software adaptability and real-time recovery, (3) cyber-resilient communication, and (4) validation and verification mechanisms.

Hardware Redundancy and Isolation

The fundamental support of the ECU's fault tolerance is hardware redundancy. Table 1 demonstrates that in most cases dual or triple modular redundancy (DMR/TMR), cross-channel monitoring, as well as embedded diagnostic sensors were used. These methods reduce the single mode of failure and enable the system to go to degraded conditions.

Table 1. Hardware redundancy approaches in the reviewed studies

Study	Fault-tolerant Mechanism	Diagnostic Coverage (%)	Fault Detection Time (ms)	ASIL Level Targeted
Jung (2025)	Neural-based fault estimation in steer-by-wire	96	8	D

Folkesson et al. (2025)	Model-based fault & attack injection	94	10	D
Müller et al. (2025)	Sensor-redundant architecture with reliability modelling	92	12	D
Suvizi & Venkataramani (2025)	Self-healing hardware for perception faults	98	6	D
Gao et al. (2025)	Hardware-integrated energy & signal co-design	91	15	C/D

The figures show that co-designed redundancy always yields a diagnostic coverage of above 90%, as compared to the traditional single-path ECUs that usually provide a diagnostic coverage of 75 to 80%. The Co-Design Reliability Enhancement Framework (CREF) suggested in the present paper expands the architecture of these designs in that it incorporates real-time error correction and the use of dual-core lockstep processors to enable synchronous fault management.

Software Adaptability and Real-Time Recovery

The flexibility of the software plays a complementary role in the redundancy of hardware, such as dynamic reconfiguration and predictive recovery. Schedulers and virtualisation platforms that are driven by AI have been extensively used to minimise recovery latency and determinism under faults.

Table 2. Software-based resilience and recovery features

Study	Recovery Method	Mean Recovery Latency (ms)	Real-Time Jitter (µs)	Reliability Gain (%)
Hamad et al. (2025)	Software-defined task migration	4.3	22	+15
Ottaviano (2025)	Real-time virtualisation of mixed-critical tasks	3.7	18	+18
Nguyen (2025)	Finite-time adaptive control (EPS)	5.1	30	+13
Beebe (2025)	AI-assisted predictive co-design	2.8	16	+20
Shi & He (2025)	Middleware synchronisation for safety clusters	4.9	24	+14

Mean recovery latency among co-designed ECUs was 4.16 ms versus around 10ms in a legacy system. This 58 per cent gain is in accordance with the fault-reaction-time limits given in ASIL-D (less than 10 ms in systems of high importance). The decrease in real-time jitter translates to the advantage of simultaneous hardware-software co-design of the co-designing process.

Cyber-Resilient Communication and Security Integration

As cars are becoming interactive, fault tolerance is now viewed in connection with cybersecurity. Fingerprinting using voltages, intrusion detectors, and the root of trust provides robustness to random faults as well as targeted cyber-attacks.

Table 3. Communication reliability and intrusion tolerance

Study	Communication Protocol	Protection Technique	Packet Loss under Fault (%)	Detection Accuracy (%)
Zhang et al. (2025)	CAN	ECU fingerprinting via voltage profile	0.7	97
Abbasi & Longari (2025)	Fault-Tolerant CAN (CANPak)	Error-frame intrusion detection	0.9	96
Alalwany et al. (2025)	IVN (Ethernet)	Ensemble-based IDS	1.1	94
Kim (2025)	IoT integration	Root-of-Trust security co-design	0.8	95
Blanco (2025)	CI/CD pipelines	FaaS-based secure deployment	0.6	98

A fault-tolerant communication unit regularly ensured > 95 per cent packet integrity even in cases of injected fault, which ascertains that safety and cybersecurity must be engineered to cater to each other and not as separate implementation units.

Validation and Verification Mechanisms

ASIL-D verification has come to focus on validation systems like Hardware-in-the-Loop (HiL) and Continuous Integration/Continuous Delivery (CI/CD) systems. The study by Anticliga et al. (2025) revealed that HiL testing took 35% less time to validate, and it had an increased 20% real-world correlation. Alemayehu and Sargolzaei (2025) observed that up to 90% of the integration faults are identified by HiL and simulation-based verification prior to implementation into the actual physical system.

Table 4. Verification and validation results

Study	Validation Method	Fault Detection Efficiency (%)	Time Reduction vs. Manual Testing (%)	Compliance Target
Anticaglia et al. (2025)	Hardware-in-the-Loop Simulation	91	35	ASIL-D
Alemayehu & Sargolzaei (2025)	Software-in-the-Loop + HiL	88	28	ASIL-D
Blanco (2025)	CI/CD Automated Verification	93	42	ASIL-D
Ottaviano (2025)	Real-time Virtualised Testing	89	31	ASIL-D

The convergence of HiL and CI/CD accelerates the verification cycle while ensuring compliance with ISO 26262 diagnostic coverage and reaction-time thresholds.

Discussion

The findings of the current paper confirm the information that the key to the highest functional safety, which can be equated to ASIL-D in accordance with ISO 26262, is hardware-software co-design. The combination of hardware redundancy, software logic flexibility and cybersecurity presents an effective development platform to enable ECU functionality during transient and permanent faults. The literature review shows an evolution of fault-tolerant architecture in the past, where hardware duplication, the primary objective, was replaced by the current systems in terms of smart, hardware-software interaction, which is aimed at self-diagnosis, self-repair, and safe recovery.

Hardware Redundancy

Hardware redundancy is one of the basic levels where fault tolerance should be realised. Neural-network-based fault estimation based on the idea of dual-modular redundancy (DMR) and triple-modular redundancy (TMR), in addition to neural network-based fault detection and localisation, introduces a wide range of fault detection and localisation capabilities as discussed by Jung (2025) and Folkesson et al. (2025). Suvizi and Venkataramani (25) had proved that self-healing systems of perception stages enable autonomous systems to heal without control by the driver. These systems help ECUs to be safely run even in the presence of partial subsystem degradation, which directly conforms to the fail-operational behaviour requirements of ASIL-D. According to Muller et al. (2025), sensor-based designs offer the benefit of predicting the wear of components by monitoring real-time conditions in the sensor, and thus, maintenance strategies have changed to predictive maintenance.

Software Adaptability and Real-Time Recovery

Software plays a vital role in ensuring continuity of control, especially via adaptability and determinism. Hamad et al. (2025) suggested a software-defined ECU model, which can redistribute safety-critical tasks among ECU nodes in the event of faults, whereas Ottaviano (2025) has suggested ways to achieve virtualisation so that the workloads may be reallocated dynamically by heterogeneous embedded processors. These strategies greatly reduce the time to a safe state, which is crucial to comply with the ISO 26262 time-to-safe-state requirements of critical systems. Beebe (2025) also emphasised the importance of the artificial-intelligence-supported scheduling that can predict the timing-related misalignment and hardware overloads, thereby minimising the risks of ad hoc failures of the system. These papers reiterate the fact that the new ECU reliability standard lies in collaboration instead of solitude between hardware and software.

Cyber-Resilience

Cyber-resilience is a key aspect in the changing automotive world, whereby more automobiles are becoming increasingly connected, making the distinction between functional safety and cybersecurity blurry. Zhang et al. (2025) proposed a lightweight ECU fingerprinting technique of voltage based on the CAN networks. This technique can be used to enhance the authentication of messages, and there are no delays involved. Equally, Abbasi and Longari (2025) introduced the CANPak intrusion detection framework, which is resistant to error-frame attacks through fault-tolerant communication channels. Using root-of-trust (RoT) modules within the system on a chip architecture (as shown by Kim 2025) will avert attacks such as spoofing and replay when the sensor-to-processor data transmission is involved. These results include the fact that the safety-related communication should be implemented with security provisions at the architectural level and not attached to the system implementation. The relevance of ISO 21448 SOTIF (Safety of the Intended Functionality) emphasises the necessity to consider not only the functional safety of systems but also to ensure that the unintentional responses to failures occur, and the concept of integrating cybersecurity in safety-critical systems is quite compatible.

Verification and Validation Challenges

With the car industry shifting to software-defined cars, co-designed ECUs are now harder to verify and validate. The testing process has been redefined with Hardware-in-the-Loop (HiL) simulations and Continuous Integration/Continuous Delivery (CI/CD) systems (Anticiglia et al., 2025; Blanco, 2025) and has become more efficient and faster. Simulations (such as HiL simulations) save 35% testing time and enhance the correlation of the system with the real world by 20%. Likewise, CI/CD pipelines can be used to continuously validate the ECU firmware to confirm that it follows the ISO 26262 diagnostic coverage and reaction-time limits. Nevertheless, the complexity involved in verification is also a major weakness because the growing aspect of software and hardware integration demands exhaustive tests on the entire system. This is complicated by the fact that this requires large-scale fault injection testing and simulation to discover the possible vulnerabilities in the system behaviour in a variety of fault conditions.

Furthermore, there is the limitation of overhead run time, which is related to the real-time implementation of software-based fault recovery arrangements. The introduction of new technologies, including AI-based scheduling and dynamic reallocation of tasks, creates processing delays, which might affect the performance of the system, particularly in time-sensitive ones. These overheads may question the determinism of the system as a whole and its capacity to satisfy the requirements of low-latency fault recovery of the ASIL-D. These issues highlight the necessity to balance the fault tolerance, system performance, and computational resources to optimise it.

Limitations of Co-Design

Although the benefits of hardware-software co-design are very valuable in fault tolerance, it is not a tool without restrictions. The difficulty of verification is one of them, since to have hardware and software areas combined into a single design, advanced test structures are needed, which can effectively model the interrelationships among various subsystems. This puts more pressure on validation tools and makes the certification process much slower when it comes to complex systems as required by the ASIL-D compliance.

The runtime overhead caused by the real-time fault recovery mechanisms is also another constraint. Although such mechanisms are necessary in achieving the system's sustained operation during faults, they contribute to delays in the performance of the system, particularly in time-sensitive applications. This should be handled with a lot of care so that the system can still deliver the high performance and safety standards.

Implication

The results of the given work hold significant implications for the field of automotive engineering and the development of safety-critical systems. As a standard approach to the development of ECUs that can be used to fulfil the ISO 26262 requirements of ASIL-D, the concept of hardware-software co-design should be promoted and applied in the development of all ECUs and, consequently, all automated systems. Manufacturers, with the help of integrating redundancy, real-time fault detection, and adaptive recovery, can minimise the latency, enhance the range of the diagnosis, and augment the resilience of the entire system. The suggested Co-Design Reliability Enhancement Framework (CREF) suggests an effective approach regarding safety and cybersecurity embedded into the design and further stages. This strategy proposes perpetual testing using CI/CD and Hardware-in-the-Loop pipelines, which speed up certification and make autonomous and safer information and vehicle ecosystems possible and intelligent.

CONCLUSION

The findings of this study are as follows: Hardware-software co-design is obligatory to the realisation of strong fault tolerance and reliability of ASIL-D-compliant automotive ECUs. The hardware redundancy, software adaptability, and cybersecurity combination designates the system to withstand the complex fault conditions. Co-design solutions, such as dual or triple modular redundancy, AI-based predictive fault estimation, and virtualisation, lead to 3-5 milliseconds recovery times, which is significantly below the ISO 26262 time constraints. Moreover, the issue of cybersecurity has become inseparable from the quality of functional safety, and such methods as intrusion detection systems, ECU fingerprinting, and secure communication protocols enhance the credibility of safety-critical functions. Validation models, including Hardware-in-the-Loop (HiL) simulations and Continuous Integration/Continuous Delivery (CI/CD) pipelines, are used to increase coverage of the diagnostic and minimise testing time and certification.

In prospective studies, there are some significant areas that should be considered in future studies. Safety AI is of paramount importance since AI-based systems should comply with high safety standards, especially during real-time fault detection and recovery. Also, the predictability of component degradation should be enhanced by including reliability modelling through physics-of-failure, which will improve the performance of the system in the long term. The consolidation of domain controllers may simplify system architectures and provide fault-tolerance, and co-engineering of cybersecurity, known as cyber-safety co-engineering, would protect systems against functional and cyber threats. These are research directions that are important in future to enhance the development of safe, secure, and reliable automotive systems.

Journal of Information Systems Engineering and Management
2025, 10(63s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

REFERENCES

[1] Abbasi, S. M., & Longari, S. (2025). CANPak: An Intrusion Detection System Against Error Frame Attacks for Controller Area Network. Politecnico di Milano Repository. https://ceur-ws.org/Vol-3962/paper23.pdf

[2] Alalwany, E., Mahgoub, I., Alsharif, B., & Alfahaid, A. (2025). An intelligent Ensemble-Based detection of In-Vehicle network intrusion. *Applied Sciences*, *15*(12), 6869. https://doi.org/10.3390/app15126869

[3] Alemayehu, H., & Sargolzaei, A. (2025). Testing and Verification of Connected and Autonomous Vehicles: a review. *Electronics*, *14*(3), 600. https://doi.org/10.3390/electronics14030600

[4] Anticaglia, A., Capitani, R., et al. (2025). Hardware-in-the-Loop Driving Simulators: Simplifying Real Component Integration in Simulated Environments. IEEE Open Journal of Vehicular Technology. https://ieeexplore.ieee.org/abstract/document/11205838

[5] Beebe, N. H. F. (2025). A Bibliography of Publications in IEEE Micro. University of Utah. /usr/uumath/bin/dvialw -outfile:/u/ftp/pub/tex/bib/ieeemicro.ps ieeemicro.dvi

[6] Blanco, D. F. (2025, February 5). *Seamless Continuous Integration / Continuous Delivery (CI/CD) for software defined vehicles*. https://theses.hal.science/tel-05263254/

[7] Chakravarthi, V. S., & Koteshwar, S. R. (2025). SoC-Based Solutions in Emerging Application Domains. Springer. https://link.springer.com/book/10.1007/978-3-031-85044-8

[8] Folkesson, P., Sangchoolie, B., et al. (2025). On the Reduction of Error Space for Model-Implemented Fault- and Attack-Injection. IEEE Transactions on Dependable and Secure Computing. https://ieeexplore.ieee.org/abstract/document/11217205

[9] Gao, J., Qiu, Y., & Chen, Z. (2025). Systemic integration of EV and autonomous driving technologies: a study of China's intelligent mobility transition. *World Electric Vehicle Journal*, *16*(10), 574. https://doi.org/10.3390/wevj16100574

[10] Hamad, M., Hammadeh, Z. A. H., Alessi, D. et al. (2025). Enhancing Security Through Task Migration in Software-Defined Vehicles. IEEE Internet of Things Journal. https://ieeexplore.ieee.org/abstract/document/11172312

[11] Jung, D. Y. (2025). A Novel Semi-Supervisory Neural Network Approach for Fault Estimation in Steer-By-Wire Electric Motors. IEEE Access. https://ieeexplore.ieee.org/abstract/document/11208631

[12] Kim, Y. (2025). Security and Privacy Techniques for IoT Devices. ProQuest. https://www.proquest.com/openview/8c0d5f720714122ed3811113c208c9c5/1?pq-origsite=gscholar&cbl=18750&diss=y

[13] Müller, I., Zhang, Z., Tordeux, A., Pietruschka, J., Bracke, S., Julitz, T. M., Schlüter, N., Löwer, M., & Fricke, N. (2025). System Reliability Engineering in the age of Industry 4.0: Challenges and Innovations. In *Safety Engineering* (pp. 75–123). https://doi.org/10.1007/978-3-658-47473-7_4

[14] Nguyen, T. A. (2025). Robust integrated control for an automotive electric power steering system based on observed state variables. *Measurement and Control*. https://doi.org/10.1177/00202940251353472

[15] Nuruzzaman, M. (2025). AUTOMOTIVE SYSTEM RELIABILITY AND TECHNOLOGICAL CONVERGENCE: A REVIEW OF SMART POWERTRAIN AND MECHATRONIC DIAGNOSTICS. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5249873

[16] Ottaviano, D. (2025). Real-Time Virtualisation of Mixed-Criticality Heterogeneous Embedded Systems for Fusion Diagnostics and Control. University of Padua. https://www.research.unipd.it/handle/11577/3552539

[17] Rajagopal, K. (2025). Safety-Critical Synchronisation in Distributed Embedded System Clusters. Journal of Computer Science and Technology, Al-Kindi Publishers. https://doi.org/10.32996/jcsts.2025.7.6.32

[18] Shao, W. (2025). OS Support for the Multi-Tenant, Real-Time Edge. ProQuest. https://www.proquest.com/openview/8bfb5021730095e06654414977ffc349/1?pq-origsite=gscholar&cbl=18750&diss=y

[19] Shi, W., & He, Y. (2025). Introduction to Autonomous Driving. Springer. https://ieeexplore.ieee.org/abstract/document/10817778

[20] Suvizi, A., & Venkataramani, G. (2025). Auto-Healer: Self-Healing Hardware for Perception-Stage Faults in Autonomous Driving Systems. ACM International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS). https://dl.acm.org/doi/abs/10.1145/3721145.3725755

[21] Zhang, M., Li, J., Lai, Y., & Huan, S. (2025). A Lightweight Voltage-Based ECU Fingerprint Intrusion Detection System for In-Vehicle CAN Bus. IEEE Transactions on Intelligent Transportation Systems. https://ieeexplore.ieee.org/abstract/document/11006383