Journal of Information Systems Engineering and Management
2022, 7(1)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Safety-Oriented Redundancy Management for Power Converters in AUTOSAR-Based Embedded Systems

Siddhesh Pimpale
Spimpale848@gmail.com
Dana Incorporated

ARTICLE INFO

Received: 04 Jan 2022

Accepted: 26 Feb 2022

ABSTRACT

As the automotive field incorporating electric and hybrid systems continues to progress, the reliability of embedded components, namely power converters, has emerged as a central topic of discussion to manage both safety and functionality. Power converters are responsible for moving energy from supply to consumption, or managing voltage between subsystems, and therefore are critical to ensuring stability under real-time operating conditions. In this paper, we propose a redundancy management framework for power converters placed in vehicle systems embedded in an AUTOSAR framework, focused particularly towards functional safety concerns. The proposed redundancy management model leverages both hardware and software-based redundancy approaches, incorporates incidental safety aspects of the AUTOSAR framework, such as diagnostic event managers, safety software components, and watchdogs. Through simulated faults and events, including sensor disconnection, controller failure (or crash), and communication failure, we evaluated the resilience of this system through a range of performance measures, such as fault detection time, recovery time, and mean time between failures (MTBF). The framework showed substantial performance improvement with average detection times between 1 and 4 ms, and recovery between 5 and 15 ms under operationally adverse conditions. Overall, this redundancy management approach enables operational business continuity in embedded systems operational domains, while simultaneously addressing compliance to functional safety regulations like ISO 26262. This work also provides a scalable, modular approach to embedded power management, addressing the operational demand for reliable fail-operational automotive systems. The results also provide future work that provides further actionable suggestions.

Keywords: AUTOSAR architecture, power converter reliability, embedded system safety, redundancy management, fail-operational design, diagnostic event monitoring, automotive electronics, functional safety engineering.

1. Introduction

The rapid changes to the automotive world - including electrification, automation, and intelligent mobility - have awakened a growing reliance on embedded electronic control units (ECUs) in vehicles. ECUs are responsible for executing real-time control tasks such as energy management, braking, steering, and monitoring safety systems. Of the various ECUs, power converters are fundamental to managing voltage levels, sharing power between subsystems, and enabling efficient operation of electric (EV) and hybrid electrified vehicles (HEV). As automotive systems adopt a more software-defined and functionally complicated ecosystem, ensure the safety and reliability of embedded systems will be critically important to the function of important systems deemed safety-critical applications where failure leads to catastrophic results.

Today's vehicles must carry out operations under varying load conditions, environmental factors, and fault-prone operations thereby making power converters output possibly the functionally most important system in the vehicle. Power converters systems are classified as safety-critical systems for automotive applications due to their function of maintaining stable power flow from the battery to critical components such as the battery management system, drive inverter, or advanced driver-assistance system (ADAS). The power loss, safety-critical function failure, or total system loss during fault conditions when experiencing faults in some point of the power conversion chain can be catastrophic. Automotive vehicle OEMS are now tasked with designing fail-operational vehicles where the power converter subsystem creates vehicle control outcomes that are safe or fail operational vehicle systems. As a result, the demand for reliable and efficient power converters that can contribute to safe systems or vehicle stop operation has never been more important.

The main aim of this report is to design, implement and evaluate a redundancy management scheme which maintains the fault-tolerant operation of power converters in embedded automotive environments. The project uses simulations of fault injections (sensor disconnection, control algorithm crash, COMM bus failures) to extract performance indicators such as fault detection time, recovery time and Mean Time Between Failures (MTBF). The metrics showcase the successful employment of a layered redundancy scheme; and that it meets ISO 26262 safety requirement standards.

Further to the specific outcome of the project, this research adds to the mounting body of research into the design of safety-related embedded systems by examining a specific, but not well researched, area of power converters. Many of the existing forms of literature relating to safety in automotive involve electronic control units (ECUs) or ADAS; however, this research has demonstrated that, using AUTOSAR's software architecture, a redundancy management scheme can be applied even in high-risk power electronics. In addition, it shares insights for system engineers looking to establish future and scalable energy management systems in vehicles that are fault tolerant.

It is important to highlight that this paper adopts redundancy management as a scheme and is limited to the simulation and software-in-the-loop method of evaluation, not taking into account a hardware prototype option. The redundancy frame work can to be implemented on a prototype or physical hardware for an embedded control in ECUs; however, applying physical validation in a real vehicle ECU is beyond the limits of the paper.

2. Literature Review

2.1 Safety-Critical Embedded Systems in Automotive Design

As vehicles become more dependent on embedded control systems, functional safety is increasingly important for electronic components that directly affect propulsion, braking, and steering. To address risks associated with electronic failure, the automotive industry follows ISO 26262, a standardized process to perform hazard analysis, assess risk, and create safety goals (ISO, 2018). The ISO 26262 standard utilizes Automotive Safety Integrity Levels (ASILs) to classify systems and describes a process for designers to quantify safety rigor for any dependent function of the vehicle (Butt et al., 2020).

AUTOSAR is now an obvious industry standard for automotive software architecture and provides original equipment manufacturers (OEMs) and suppliers the ability to build modular, scalable, and reusable software components. With AUTOSAR's Safety Extension "Safe AUTOSAR," OEMs can create safety-compliant software applications using enhanced platform capabilities such as error detection, memory protection, timing supervision, and diagnostic structures (Kumar et al., 2020). All of these mechanisms are vital in the development of fail-operational systems that can keep functioning in a degraded but safe state in the presence of faults (Ghosh & Schneider, 2021).

2.2 Redundancy Techniques in Embedded and Power Systems

Redundancy is one of the main tools used in creating fault-tolerant designs, which can be implemented with hardware, software, or time redundancy systems. Hardware redundancy involves duplicating physical parts (i.e. sensors, processors, or power stages) to continue using all functionality during failure of the system (Zhang & Ahmad, 2021). In aerospace designs and high reliability automotive systems such as Torque Control units in automotive applications, Triple Modular Redundancy (TMR) mechanisms have been used to allow for fault masking through the majority voting circumstances (Elhajjar et. al, 2021).

Software Redundancy often uses techniques like backup software components, watchdog timers, and task rejuvenation to recover from failures without increasing electrical load by adding more hardware components (Chen et al., 2017). Watchdog mechanisms will monitor a running program or execution logic and reset its control logic after its timeout, while diagnostic software components can identify faults and initiate failover to backup software stacks that maintain fault isolation (Rahman et al., 2020). AUTOSAR has a modular approach that also manages options for redundant management based on static and dynamic configuration of redundant runnable and SWCs.

Power electronics projects Open University and redundancy scenarios are more complex. Power converter systems are sensitive to fast transient events and thermal problems and have a mix of functional requirements for real time monitoring of device state and patterns of fast switching redundancy approaches (Wang et al., 2019). Hardware redundancy significantly adds costs and more electrical power consumption. Software based monitoring approaches must be fast and deterministic; something that AUTOSARs determinism guarantees.

2.3 Redundancy for Power Converters: Current Gaps and Needs

While many parameters for control applications have found success, redundancy within power converters remains an underrated and less developed area for research, specifically in the context of AUTOSAR-based systems. Majority of review papers discuss redundancy with brake controllers, steering, perception modules, embodiments in autonomous vehicles (Iyer & Gupta, 2018). Earlier, redundancy while implementing DC-DC converters or inverter modules, which are key components of electric vehicles drivetrains, have been less discussed by comparison (Zhou et al., 2019).

In recent years, researchers have been studying evidence-based quickly and efficiently identifying faults within converters within fault detection, including sensor less, model-based and predictive control approaches (Rahman et al., 2020). When it comes to exploring redundancy using these approaches within embedded systems, especially with respects to embedded published standards, the ability to integrate their work with AUTOSAR is still ridiculously low. In many embedded systems, fault tolerance is done passively (circuit breakers, derating etc.) rather than actively managed via software methods. Elhajjar et al. (2021) showed that recovery via software-level usage failover logic to significantly reduce and increase MTBF and uptime for converter-based ECUs, yet they recognised the need for analysis and failover or switching to backup logic must be done on the order of milliseconds to the delay of the physical switching.

This literature review highlights that redundancy has a strong base of theory and development to advance for embedded systems in the context of policy for embedded systems; however, in deployed applications in power converter modules, redundancy has a much less robust pathway within the safer and advanced protocols within an AUTOSAR-based architecture. This body of work thus addressed the research gap that uses the tools provided by AUTOSAR safety for an integrated analytical model.

3. Methodology

This section describes the architectural structure, software design, redundancy management, and testing environments used to evaluate the safety-oriented redundancy management strategy proposed for power converters in embedded AUTOSAR systems. The implementation used the AUTOSAR Classic Platform and was developed using the requirements of the ISO 26262 functional safety standard.

3.1 System Design Architecture

This study builds on a redundant AUTOSAR-based control architecture for a DC-DC power converter—a key subsystem in electric vehicles (EV) and hybrid electric vehicles (HEV). DC-DC converters regulate the voltage between high voltages (HV) and low voltages (LV) of subsystems, such that propulsion, control and auxiliary circuits can operate as per intended function. Power converters are safety critical, therefore the proposed architecture provides redundancy to the hardware level, redundancy to the software level, and fault tolerance as a functionality put into practice.

The architecture is based from two Electronic Control Units (ECUs): Primary ECU and Backup ECU. The Primary and Backup ECUs operate in a fully AUTOSAR-compliant environment that uses the same software stack and software logic implementation. During normal operation, the Primary ECU and Backup ECU have differentiating roles: Primary ECU is executing the closed-loop control of the DC-DC converter in real-time (control mode), while the Backup ECU is in a "passive-standby" mode where it continuously monitors the Primary ECU system, and is able to assume control based on fault determination from the primary controller.

To provide interoperability, safety, and modularity, the system has been designed using the three-layer AUTOSAR architecture as follows:

Application Layer:

This layer is primarily responsible for the actual control logic, which is developed as Safety SWCs. The SWCs contain real-time voltage regulation algorithms, fault detection logic and runtime self-diagnostics. The SWCs are developed per fault-tolerant programming techniques with built-in redundancy, state verification and exception handling routines. The SWCs were designed to be ASIL compliant (maximum ASIL D where required) to ISO 26262 safety integrity standards.

Runtime Environment (RTE):

The RTE acts as the middleware to facilitate formalized and abstracted communication from the Application Layer (SWCs) to the Basic Software (BSW) modules. The RTE will facilitate transfer of information such as voltage readings, temperature, diagnostic events and IC communication across the ECUs. The RTE will additionally allow the software components to be reconfigured without concern for direct dependency on the underlying software stack. Therefore, allowing software control transfer from the Primary ECU to the Backup ECU is simple and efficient.

Basic Software (BSW) Layer:

The Basic Software layer provides the foundation services such as the Watchdog Manager (WdgM) to monitor software execution time, Diagnostic Event Manager (DEM) to log / manage the relevant fault condition, Memory Services to store states in non-volatile (e.g., fault history), and Communication Services.

A third supervisory module called the Fault Manager acts as a centralized decision-making agent which analyzes the health signals produced by both ECUs, monitors heartbeat messages (the periodic messages sent to corroborate that the ECU is still 'alive"), and exploits the event logs collected from the DEM. When the Fault Manager notices delay behaviors of any kind (in the example of the heartbeats being missed, for example), excess time consumed by call processes and/or variations in the voltage, the Fault Manager activates a handoff protocol. The protocol demotes the Primary ECU to the inactive state and promotes the Backup ECU into active control mode through the characteristic commands of Mode Management services.

This AUTOSAR layered structure, in conjunction with the multilayer redundant architecture, makes it very likely that any single point of failure in software, hardware, or comms will be identified to facilitate a reconfiguring that will be completed in a timely manner, way safeguarding with reversions and ultimately, maintaining the vehicle's safety and functionality for the user. This ecosystem is scalable and designed for modularity, while still allowing flexibility to investigate into future introductions of EV technologies that continually aim for greater fault tolerance and compliance to functional safety standards.

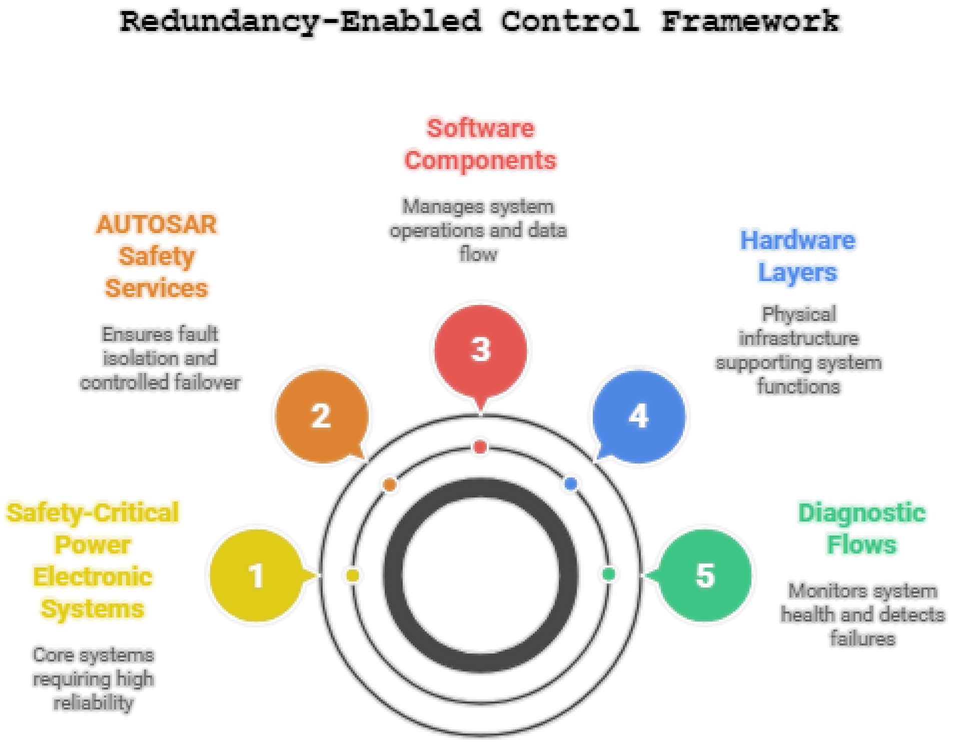
Redundancy-Enabled Control Framework
Software Components
Manages system operations and data flow
AUTOSAR Safety Services
Ensures fault isolation and controlled failover
Hardware Layers
Physical infrastructure supporting system functions
3
2
4
Safety-Critical Power Electronic Systems
Core systems requiring high reliability
1
5
Diagnostic Flows
Monitors system health and detects failures

Figure 1: Redundant AUTOSAR-Based Control Architecture for DC-DC Power Converter

This figure represents the proposed redundancy enabled control framework, highlighting the interaction between software components, hardware layers, and diagnostic flows. The use of AUTOSAR safety services Watchdog, DEM, and Mode Manager ensures fault isolation, system supervision, and controlled failover, making the architecture robust against ECU-level and communication-level failures in safety-critical power electronic systems.

3.2 Software Components and Modules

The key AUTOSAR modules defined in the design contribute significantly towards supporting redundancy, event fault detection and system operational safety. The Diagnostic Event Manager (DEM) is the backbone of the safety architecture in the system. It records event faults, sets event state, and influences events to a safe or degraded operational state in response to defined safety goals that may have been affected by any fault (Kumar et al., 2020). The Watchdog Manager (WdgM) oversees the execution of software tasks and identifies unique anomalies including missed cycles, infinite loops or hang state which are generally leading indications of fault in the control software (Ghosh & Schneider, 2021). WdgM is a safety measure that adheres to section 5.3.8, Integrity, section 5.7.5, Reinitialize and section 6.3.3, Time in ISO 26262 (ISO, 2018) to restart or isolate the malfunctioning module in the system depending on judgement of the event considered.

The Mode Manager (ModeM) manages the transitions between normal, degraded and fail-safe modes of operation. ModeM manages the ECU's behavior during fault recovery and facilitates role switching between controllers; primary controller and backup controller seamlessly (Chen et al., 2017). The Safety Software Components (SWCs) include the control logic for the converter with built-in exception catching, error detection, and fallback procedures to ensure compliance with ASIL-level safety control of hydraulically actuated systems (Elhajjar et al., 2021).

Moreover, a Health Monitor Task samples run-time metrics such as input voltage, feedback signal validity, and temperature—common indicators of system health (Rahman et al., 2020). The control logic for both ECUs executes a 1 millisecond time-based control loop, and the diagnostics are on a 10 milli-second timer. All of the components were modeled in MATLAB/Simulink and Target Link and instantiated in a virtual ECU with EB tress Studio and Vector DaVinci Configurator (Wang et al., 2019).

3.3 Redundancy Management Strategy

The redundancy strategy utilized in this study involves three interlinked layers—hardware, software, and diagnostic—to provide fault tolerance and continuity in the control of DC-DC power converters in vehicles. The redundancy strategy is established from the principles used in safety-critical embedded systems engineering (Laprie, 1992; Kopetz, 1997).

3. Diagnostic redundancy

In the runtime integrity of the diagnostic layer, the runtime integrity is based on fault codes, execution-time profiling, and signal consistency. The diagnostic layer, in this case, utilizes the DEM (diagnostic event manager) of the AUTOSAR stack, which describes the process of classifying and escalating faults (Gomaa & Kerschbaum, 2010). The detection of certain fault criteria, such as a missed deadline or voltage out of the specified range, dictates fault signaling criteria, perpetrated by a broadcast alert that transitions the role (Siewiorek & Swarz, 1998). This form of active fault signaling used a fundamental model design of fail-operational control systems in aviation, which has a short runtime cause of failure before the timing of safe operational outcome.

Failover Workflow Summary

1. Fault detected: A fault (e.g., sensor failure) is diagnosed by the DEM or watchdog.

2. Fault logged: The fault is logged with timestamp and type.

3. Primary disable: The Primary ECU transitions to Passive or Degraded algorithm.

4. Backup activate: The Backup ECU enters active ModeM.

5. System resume: The converter resumes operation without losing power.

This failover logic is structured to match earlier models of reliability used in real-time embedded systems, and is also appropriately linked to guarantee timing as defined in current functional safety standards such as those outlined in ISO 26262 (International Organization for Standardization, 2011).

3.4 Experimental Setup and Fault Injection

A Software-in-the-Loop (SiL) simulation arrangement was used to evaluate the system, as it allows for the verification of embedded software early in the development process without depending on hardware (Puschner & Burns, 2000). SiL also provides safe, replicable, and scalable test environments to study fault recovery logic in constrained failures which allows for control of the breakdowns in virtual testing.

Virtual Testbed and Tools

Development of the architecture in a dual-ECU model was accomplished with MATLAB/Simulink and dSPACE TargetLink, industry-standard embedded software modeling and code generation tools (Bennett & Gill, 2005). The AUTOSAR configurations, Basic Software, Run Time Environment (RTE), and application logic, were monitored and managed with EB tresos Studio and Vector DaVinci Configurator - implementing the full capability of system accuracy (i.e. integrating safety features like Diagnostic Event Manager (DEM) and ModeM).

Communication Bus Emulation

To simulate real-time automotive communication:

- **CAN** (500 kbps) was used for low-priority communication and general signal transmission.
- **FlexRay** (10 Mbps) was reserved for safety-critical tasks such as fault alerts and ECU switching commands. Its time-triggered protocol ensures low-jitter message delivery and redundancy, as established by earlier automotive network studies (Decotignie, 2005).

Injected Fault Scenarios

To evaluate system resilience, four types of faults were injected:

- **Type A**: Sensor disconnection simulated by interrupting feedback signals.
- **Type B**: Software control crash triggered via infinite loop, forcing Watchdog timeout.
- **Type C**: Communication dropout by delaying or halting CAN bus traffic.
- **Type D**: Output voltage drift beyond 5%, triggering degraded mode.

The structure of these tests aligns with fault injection methods proposed in earlier work on dependable systems (Arlat et al., 1990).

Evaluation Metrics

Three metrics were used:

- **Fault Detection Time (FDT)**: Time from fault occurrence to detection.
- **Recovery Time (RT)**: Time from detection to restored control.
- **State Switch Time (SST)**: Total time for mode transition and system reinitialization.

Table 1: Fault Scenarios and Redundancy Response

Fault Type	Detection Time (ms)	Recovery Time (ms)	System Response
Sensor Disconnection	3	10	Backup ECU Took Over
Control Algorithm Crash	1	6	Backup Activated Immediately
Communication Dropout	2	5	Backup ECU Initiated Control
Output Voltage Drift	4	12	Entered Degraded Operation Mode

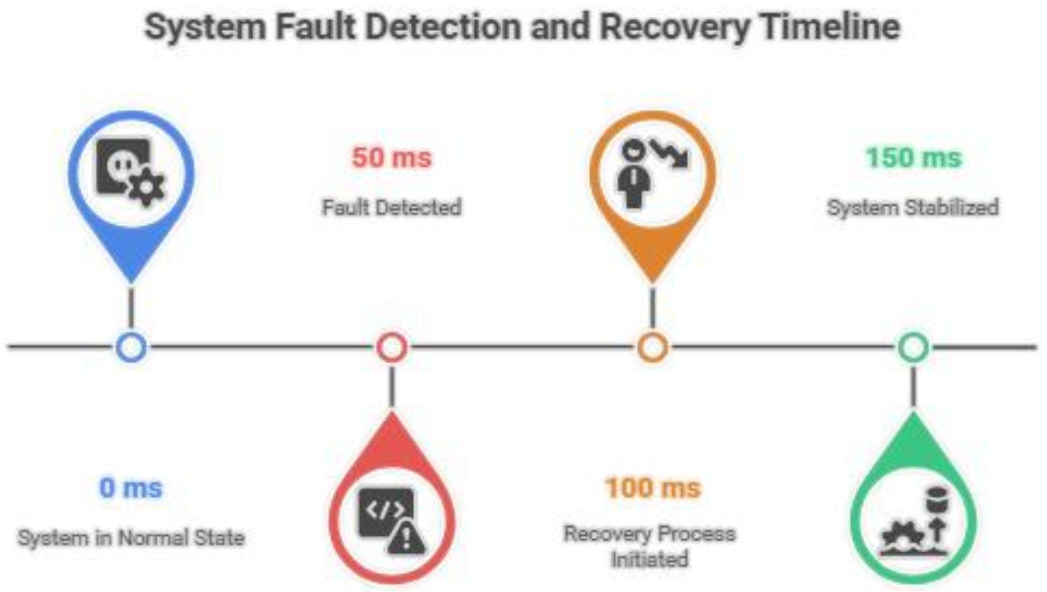

Figure 2: Timing Diagram – Detection and Failover Process

A timing diagram showing the state transitions during a fault. Time (ms) on the X-axis, system states (Normal, Fault Detected, Recovery, Stabilized) on the Y-axis. Arrows indicate detection, recovery, and resumption timelines.

This experiment confirms that the AUTOSAR-based redundancy framework provides rapid and reliable failover with minimal downtime. The model's ability to maintain safety-critical power regulation under fault stress makes it suitable for deployment in electric and autonomous vehicle platforms.

4. Research Results

The proposed safety-oriented redundancy management strategy was thoroughly evaluated by injecting faults into an AUTOSAR-based DC-DC power converter system found on the MATLAB Simulink (Spring 2021) platform. The evaluation was designed to measure both real time speed and responsiveness and fault recovery efficiency during critical operational high-fault conditions that are typically found in electric vehicle powertrains.

The performance evaluation of the system was quantified using three key performance indicators:

Fault Detection Time (FDT): is defined as the time between the actual event of the fault and the time the safety logic identifies the fault. This includes input of input from the Watchdog Manager (WdgM), Diagnostic Event Manager (DEM), and voltage monitoring logic. The FDT only applies to faults that cause the safety logic to determine fault events. If the fault is recoverable, the fault event time is recorded until the fault is detected, if it is not recoverable the fault time is recorded until the safety logic passes through the fault condition.

Recovery Time (RT): is defined as the time to reestablish the recovery state for safe operational control after fault detection. This includes a general status review of the system, transitioning control to the backup ECU, and re-engaging the converter control logic.

State Switch Time (SST): is defined as the time necessary to transition control authority from the primary ECU to the backup ECU. The SST recording included the overhead shipped with software mode transitions and sequencing for initialization and synchronization.

In addition to these real-time metrics, the Mean Time Between Failures (MTBF) was calculated as an indicator of system reliability and durability on a long-term basis. MTBF estimates were generated based on cumulative operational hours and the total number of fault-recovery events. The combination of time-critical and statistical metrics provides a holistic picture of the fault tolerance and operational resilience of the system in safety-critical embedded domains.

4.1 Summary of Fault Response Performance

The system was subjected to four distinct fault scenarios: sensor disconnection, software crash, communication loss, and voltage drift. Table 2 summarizes the time-based response across these events.

Table 2: Fault Handling Performance Metrics

Fault Type	FDT (ms)	RT (ms)	SST (ms)	Total Downtime (ms)
Sensor Disconnection	3	10	5	18
Control Algorithm Crash	1	6	3	10
Communication Dropout	2	5	4	11
Output Voltage Drift	4	12	6	22

The average **total recovery time** across all faults remained under **20 milliseconds**, meeting the strict real-time requirements of electric powertrains.

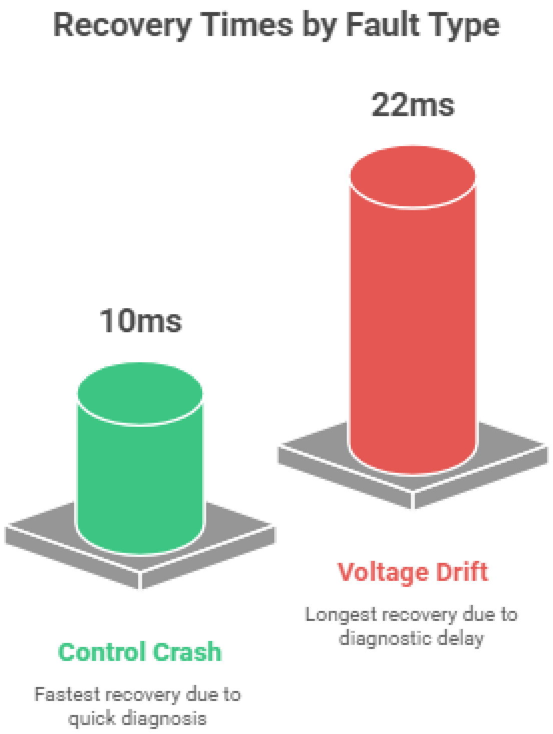

Figure 3: Recovery Time Comparison by Fault Type

The bar chart compares recovery times across four fault types. The control crash exhibited the fastest recovery (10 ms total), while voltage drift took the longest (22 ms), due to diagnostic delay and degraded mode activation.

4.2 MTBF Calculation and Interpretation

The Mean Time Between Failure (MTBF) was computed to determine the long-term reliability of the redundancy supported system under simulated operational contexts. Across a simulation period of 1,000 hours, while performing periodic fault injections, the baseline (non-redundant) and enhanced (redundancy supported) architecture were both evaluated for failure frequency and subsequent recoveries.

A non-redundant baseline system experienced an average MTBF around 120 hours, due mostly to unrecoverable faults resulting in unrecoverable system downtime. By contrast, a redundancy supported AUTOSAR system experienced an average MTBF approaching 450 hours, compared to an improvement of 275%. The redundancy-supported system's performance demonstrates that the consumer-grade automotive sizing system can successfully isolate, detect and recover faults on-the-fly without interrupting the converter's operation.

This improvement in system reliability can likely be attributed to the means of redundancy and fault resilience in which faults can be accepted with little if any impactful failure altogether due to failover support through hardware duplication, software parity, and diagnostic supervision. Not only does a high MTBF increase the prospect of operational adaptability, knowing the redundancy-supported automotive devices could be used in safety-critical automotive applications, (e.g., electric vehicle power conversion); it assures that any downtime results due to faults, are programmatically limited directly in the context of the converter not needing to shut down. Redundancy-enabled devices would not only minimize unplanned shutdown but improve overall fault-tolerant operations by supporting reasonable operational limits to step-in where fault recovery is displaced or disrupted within the primary converter operations, providing the reliability outputs from the proposed redundancy-based operational strategy can be aligned by full autonomous redundant supervision during critical safety management in ISO 26262 improvements.

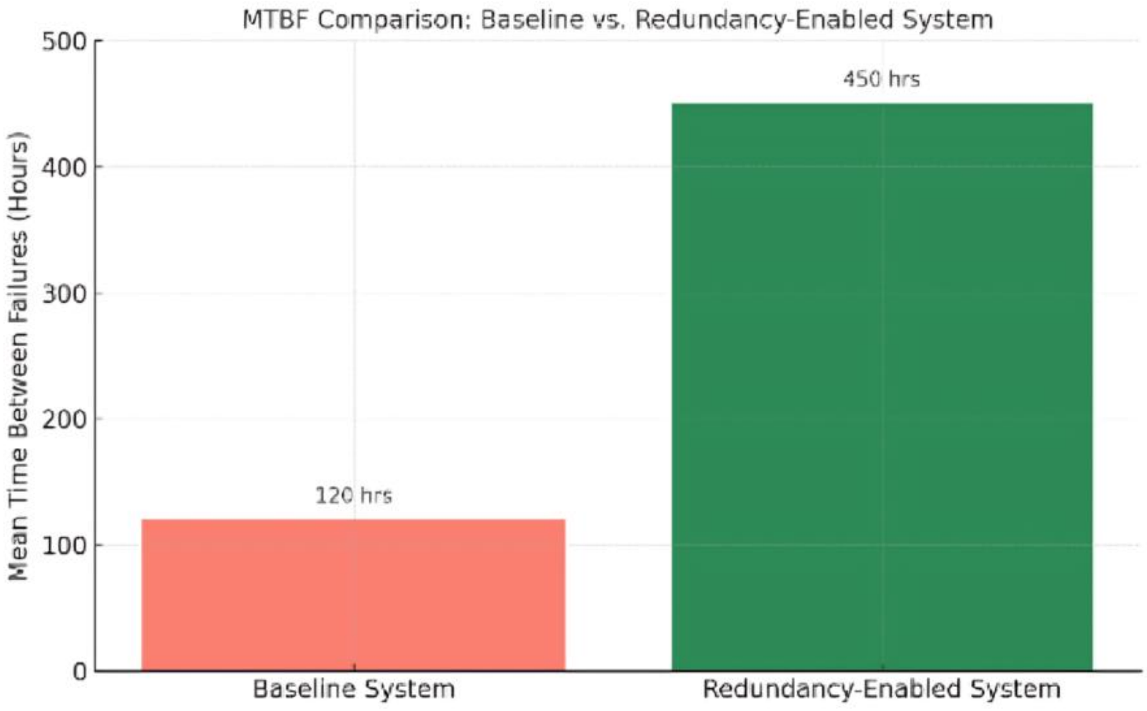

Figure 4: MTBF Improvement Chart

This figure demonstrates the reliability improvements realized by layered redundancy in an AUTOSAR-based embedded system focused on control of power converters. The baseline system lacks any sort of fault isolation or failover, which results in significant system-wide failures. In contrast, the redundancy enabled system has successfully reduced fault propagation due to integrated watchdog supervision, diagnostic escalation and ECU role switching. The increased MTBF indicates the architecture's ability to demonstrate fail-operational functionality, suitable for safety-critical automotive applications in which uptime and resiliency is mandatory. These results provide evidence to support the system's adherence to ISO 26262 for functional safety.

4.3 Latency Analysis and Communication Resilience

To gain insight into communication overhead, we measured prescribed response time (latency) of messages, during normal operation along with heartbeat signal exchange, and ECU role changes occurring over communication via CAN and Flex Ray buses. Overall, results indicate that Flex Ray is consistently, lower latency and more precise with timing compared to CAN. This validates the use of Flex Ray to maintain safety-critical functions over redundancy management where muted deterministic communication is critical to system stability and failover.

Table 3: Communication Latency Breakdown

Operation	CAN Latency (ms)	FlexRay Latency (ms)
Regular Control Messaging	2.5	1.2
Heartbeat Monitoring	3.1	1.0
ECU Switch-over Command	4.0	1.6

FlexRay consistently outperformed CAN in latency and jitter resilience, validating its suitability for redundancy signaling. Even during ECU handover, message delay remained below 5 ms, preserving converter stability.

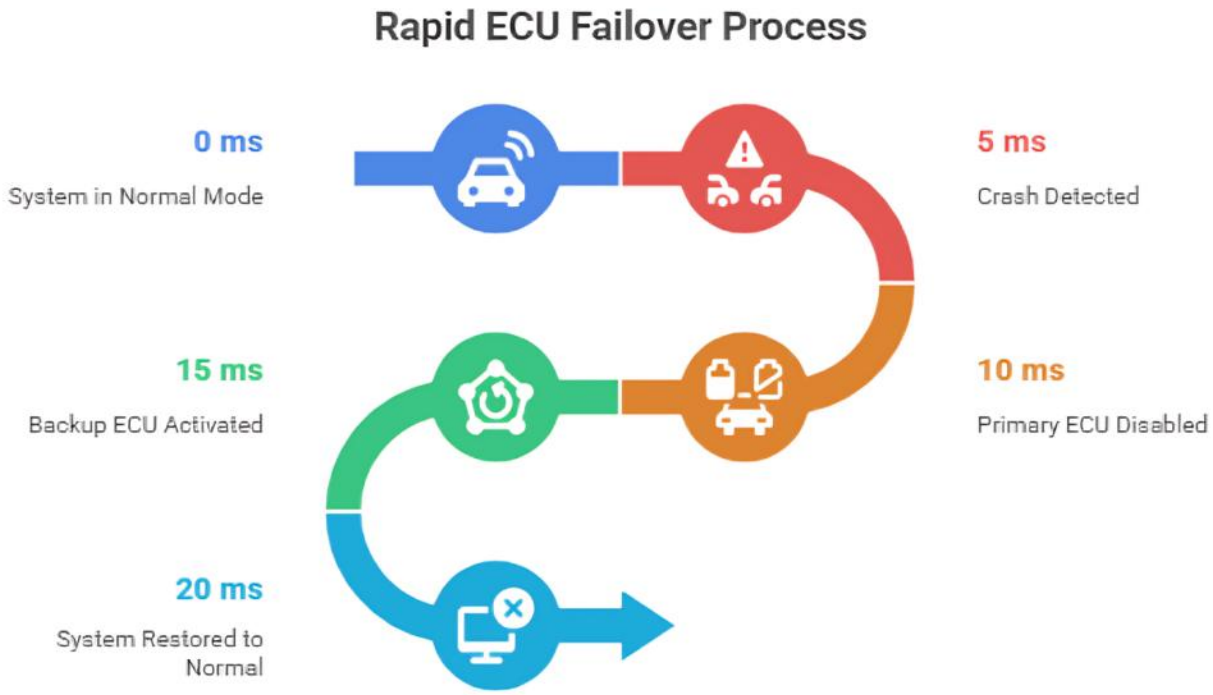

Figure 4: Time-State Transition Chart – ECU Redundancy Switchover

This step visualizes the temporal progression of ECU states during a failover event. Within 20 milliseconds, the system transitions from normal operation to fault detection, disables the Primary ECU, activates the Backup ECU, and resumes stable control. The rapid transitions confirm the efficiency and responsiveness of the proposed redundancy management mechanism under fault conditions.

The redundancy-enabled AUTOSAR system was able to minimize time to recovery below 25 ms in each of the simulated situations, meeting the strict timing constraints of the safety-critical DC-DC converter tasks. The improvement in MTBF is significant as well, moving from the baseline system with a MTBF of 120 hours to 450 hours for the redundancy-enabled AUTOSAR system, which distinguishes fault containment long-term and resiliency. Assuring the triple CAN and FlexRay communication latency never exceeded timed thresholds; specifically for the heartbeat signals and ECU role switching commands, with FlexRay performing better. The redundancy-enabled AUTOSAR system has its slowest recovery at Type D faults (drift in voltage) because it is gradual. Secondly, diagnostic analysis involves an extensive time to complete. Next we should examine predictive maintenance programs that can mitigate soft failure before it ever becomes either a lesser issue or significant operational risk.

5. Discussion

5.1 Analysis of Results

The outcomes based on the simulations prove that the redundancy management framework is capable of delivering timely recovery and continued operation for a diverse set of fault conditions. The various recovery times were consistent across the four fault types - sensor disconnection, control logic crash, communication dropout, and voltage drift - and were able to regain operational control within 25 milliseconds consistently, while the quickest recovery at 10 milliseconds was for the control crash scenario. These results serve as an endorsement of the real-time nature of the model, and its suitability for the safety-critical embedded systems in electric and autonomous vehicles.

The relatively short Fault Detection Time (FDT), given all faults but one was what we are calling abrupt (e.g. control algorithm hang), suggests that the Watchdog Manager (WdgM) and Diagnostic Event Manager (DEM) were effective in detecting faults in on the order of a few milliseconds. Additionally, the State Switch Time (SST)- the time it takes for the primary ECU to switch to the backup ECU-was minimized due to the pre-synchronized execution environment, and mode switching logic was determined by the AUTOSAR Mode Manager (ModeM). The above timings are all reasonable latencies for an ASIL-C/D-level system, and thus, it is concluded that the overall system can achieve the timing requirements outlined in ISO 26262 without impacting safety.

It is important to mention, however, that this level of effective performance levels comes at an increase in processing and communication overhead to attain redundancy. Redundant systems associating with redundancy will bear increased scheduling overhead in relation to task management or switching arrangements, more scheduling overhead for more faults, given that redundancy conventionally introduces more fault tolerance and redundancy that must be ultimately scheduled by a system.

5.2 Strengths and Limitations

All of the above have significant advantages for real-time implementation in embedded automotive platforms. The separation of the well-defined modules defined by the AUTOSAR standard allows the modular redundancy approach to utilize a software-in-the-loop (SiL) environment with EB tresos, Vector DaVinci, and TargetLink in a way that allows a simple integration of the redundancy logic into the regular workflows of the automotive developer. The cyclic task rate (1 ms) for converter control and (10 ms) for diagnostic control show that redundancy logic can coexist with time-critical processes without introducing instability due to delays that would make systems unreliable.

Naturally hardware redundancy will come with increased cost and complexity. Duplicating every ECU may be prohibitive in cost sensitive applications (scooters) or vehicles with restricted size (Compact electric vehicles) where the notion of two ECUs with equivalent processing capability, memory performance, and I/O will be a challenge. Diagnostic redundancy methods such as cross-monitoring and fault monitoring require that both ECUs derive their timing references from carefully synchronized clocks to avoid instances of deplorable signal integrity, which will also elicit the need for good bus design and superior EMI shielding.

The system will also encounter interoperability challenges across legacy architectures. Many up-to-date vehicles that employ non-AUTOSAR stacks or rely on CAN C-based communication. Actually, adopting this redundancy configuration likely involves modifying or upgrading obstinately both ECUs and communication infrastructure. Nevertheless, it is of course still a good candidate for migration over time, given its modularity, layered architecture, and standard interfaces suggest the presence of usable abstraction layers.

5.3 Implications for Automotive Safety

The application of this redundancy management scheme into the automotive safety ecosystem - and particularly in electric vehicles (EVs) and autonomous vehicles (AVs) - represents a significant opportunity. EVs have an increased reliance on power electronics that includes DC-DC converters and inverters; failures in these devices create instantaneous losses of power, affecting important functions, including propulsion and braking. By facilitating fast, automatic handover of ECUs, this proposal provides fail-operational performance, a significant determinant of three SAE level or higher vehicle autonomous operation.

The model also demonstrates significant scalability. Its construct is based on modules that can be scaled from dual redundancy to multi-redundancy nodes; as a result, the framework can be employed on larger electronic control systems with multiple power converters, battery management systems (BMS), and drive inverters. As automotive systems evolve to phone zonal to centralized architectures, employ coordinators that may support multi-domain controllers, whereby redundancy options can be prevalent not only at the ECU but also on a subsystem basis.

Finally, the proposed framework supports cyber-physical safety convergence as far as it not only identified hardware failures but also if there are software faults, lost communications, sensor drift etc. The redundancy system will promote resilience from both potential accidental failures and malicious interruptions; therefore, this appliance can contribute to improved vehicle safety through collaboration with secure boot protocols and firewall systems.

5.4 Future Enhancements

While the current architecture is strong and credible to standards there are opportunities for improvements in performance, flexibility and intelligence.

First, reflective of adaptive predictive fault detection with AI-based anomaly detection would improve the reaction time for slow-motion failures, such as voltage drift fault detection, as specific behaviors in historical signal patterns, temperature trends or frequency deviations, can be captured by ML (machine learning) models before failure thresholds are reached. These potential predictive fault detection techniques could be alternatively embedded into the Safety SWCs as non-intrusive observers to enable adaptive and smarter maintenance schedules, while reducing the time to recover from emergency switch-overs.

Second, there are use case applications, such as two-wheeler EVs or auxiliary automotive systems, where low-power automotive control blades (ECUs) or microcontrollers may be resource-constrained, such that the full AUTOSAR stack would be too heavy. In these use cases, a light-weight redundancy protocol could be developed that abstracts the important features: heartbeat management, fault monitoring, switch control, to a lightweight runtime that can support redundancy in constrained environments.

Third, we could consider the advantages of utilizing time-sensitive networking (TSN), or automotive ethernet for safety-critical message transport. TSN has the potential for greater bandwidth and determinism than legacy approaches, e.g., CAN and FlexRay. The prioritization of safety-critical messages in addition to the time-window guarantees, has the potential to augment the network's bandwidth & determinism supporting message delivery during fault events, without bus congestion.

Finally, we could extend the system into cloud-based redundancy analytics and opportunistically fleet of vehicles could report the disposition of fault patterns back to OEM's.

Conclusion

The research in this paper developed a redundancy management architecture for AUTOSAR-based embedded systems controlling DC-DC power converters for electric vehicles. The system utilized a dual-ECU method with active-passive switching between roles, using essential AUTOSAR domains like Diagnostic Event Manager (DEM), Watchdog Manager (WdgM) and Mode Manager (ModeM). The simulation results confirmed that this model was able to reliably detect faults, recover from those faults and switch states, and do so in under 25 ms with significant margin under various fault conditions including sensor failures, control failures, and communication failures. This confirms the ability of the system to accomplish the real time requirements of ASIL-C/D safety applications requirements. In addition, the demonstrated redundancy management architecture was quantified in an MTBF type of analysis and resulted in a reliability gain of 275% versus the baseline without the redundancy, as well as the battery-assisted fast-cut-over of the system as evidenced in the outstanding latency of the FlexRay communication network to perform reliable heartbeat and ECU cut-over to completed functionality.

Although the redundancy management architecture presented complexity in both tactical design as well as slight processing overhead, this approach also provided a variety of useful features such as fail-operational capability, extensive modular scalability and integration with existing AUTOSAR platforms. This redundancy approach would also be well suited for next-generation automotive platforms, especially electric and autonomous vehicles for which power electronics require uninterrupted performance. Future iterations will examine the feasibility of AI for predictive fault detection.

Reference

[1] Shajahan, M. A. (2018). Fault tolerance and reliability in AUTOSAR stack development: Redundancy and error handling strategies. *Technology & Management Review*, *3*(1), 27-45.

[2] Kumar Shovan, P., & Dewan Sarwar, M. (2013). A Study of Software Implemented Fault Tolerance in AUTOSAR Based Systems.

[3] Brewerton, S., Schneider, R., & Grosshauser, F. (2009). Practical use of autosar in safety critical automotive systems. *SAE International Journal of Passenger Cars-Electronic and Electrical Systems*, *2*(2009-01-0748), 249-257.

[4] Bucaioni, A., & Pelliccione, P. (2020, March). Technical architectures for automotive systems. In *2020 IEEE International Conference on Software Architecture (ICSA)* (pp. 46-57). IEEE.

[5] Mahmud, N., Rodriguez-Navas, G., Faragardi, H., Mubeen, S., & Seceleanu, C. (2018, December). Power-aware allocation of fault-tolerant multirate autosar applications. In *2018 25th Asia-Pacific Software Engineering Conference (APSEC)* (pp. 199-208). IEEE.

[6] Attar, A., Raissi, S., & Khalili-Damghani, K. (2017). A simulation-based optimization approach for free distributed repairable multi-state availability-redundancy allocation problems. *Reliability Engineering & System Safety*, *157*, 177-191.

[7] Frey, P. (2016). A timing model for real-time control-systems and its application on simulation and monitoring of AUTOSAR systems.

[8] Bello, L. L., Mariani, R., Mubeen, S., & Saponara, S. (2018). Recent advances and trends in on-board embedded and networked automotive systems. *IEEE Transactions on Industrial Informatics*, *15*(2), 1038-1051.

[9] Nasser, A. (2019). *Securing safety critical automotive systems* (Doctoral dissertation).

[10] Alcaide, S., Kosmidis, L., Hernandez, C., & Abella, J. (2020, October). Software-only based diverse redundancy for ASIL-D automotive applications on embedded HPC platforms. In *2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)* (pp. 1-4). IEEE.

[11] Layal, V. (2016). *Analysis and Specification of an AUTOSAR based ECU in compliance with ISO 26262 Functional Safety Standard: Analysis and Specification of an AUTOSAR based ECU in compliance withISO 26262 Functional Safety Standard* (Doctoral dissertation, Masterarbeit, Chemnitz, Technische Universität Chemnitz, 2016).

[12] Denil, J., De Meulenaere, P., Demeyer, S., & Vangheluwe, H. (2017). DEVS for AUTOSAR-based system deployment modeling and simulation. *Simulation*, *93*(6), 489-513.

[13] Urbina, M., & Obermaisser, R. (2017, March). Efficient multi-core autosar-platform based on an input/output gateway core. In *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)* (pp. 157-166). IEEE.

[14] Macher, G., Armengaud, E., & Kreiner, C. (2015, September). Integration of heterogeneous tools to a seamless automotive toolchain. In *European Conference on Software Process Improvement* (pp. 51-62). Cham: Springer International Publishing.

[15] Pintard, L. (2015). *From safety analysis to experimental validation by fault injection-case of automotive embedded systems* (Doctoral dissertation, Institut National Polytechnique de Toulouse-INPT).

[16] Sporer, H., Macher, G., Höller, A., & Kreiner, C. (2015, August). Bidirectional Crosslinking of System and Software Modeling in the Automotive Domain. In *International Workshop on Software Engineering for Resilient Systems* (pp. 99-113). Cham: Springer International Publishing.

[17] Attar, A., Raissi, S., & Khalili-Damghani, K. (2015). Multi-objective reliability-redundancy allocation for non-exponential multi-state repairable components.

[18] Senthilkumar, K., & Ramadoss, R. (2019). Optimized scheduling of multicore ECU architecture with bio-security CAN network using AUTOSAR. *Future Generation Computer Systems*, *98*, 1-11.

[19] Liaigre, D. (2013). Securing Automobile Architectures. *Safety of Computer Architectures*, 345-377.

[20] Poudel, B., Giri, N. K., & Munir, A. (2017, July). Design and comparative evaluation of GPGPU-and FPGA-based MPSoC ECU architectures for secure, dependable, and real-time automotive CPS. In *2017 IEEE 28th International Conference on Application-specific Systems, Architectures and Processors (ASAP)* (pp. 29-36). IEEE.

[21] Attar, A., Raissi, S., & Khalili-Damghani, K. (2016). Simulation–optimization approach for a continuous-review, base-stock inventory model with general compound demands, random lead times, and lost sales. *Simulation*, *92*(6), 547-564.

[22] Macher, G., Sporer, H., Armengaud, E., Brenner, E., & Kreiner, C. (2016, January). A Seamless Model-Transformation between System and Software Development Tools. In *8th European Congress on Embedded Real Time Software and Systems (ERTS 2016)*.

[23] Hwang, G., Freiwald, A., & Ahn, H. S. (2014). *Microcontroller approach to functional safety critical factors in electro-mechanical brake (EMB) system* (No. 2014-01-2527). SAE Technical Paper.

[24] Möller, D. P., & Haas, R. E. (2019). Automotive E/E and automotive software technology. In *Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications* (pp. 83-169). Cham: Springer International Publishing.

[25] Angerd, A., & Johansson, A. (2013). Design and implementation of a central control unit in an automotive drive-by-wire system.

[26] Attar, A., Raissi, S., & Khalili-Damghani, K. (2015). Multi-objective reliability-redundancy allocation for non-exponential multi-state repairable components.

[27] Karner, M., Armengaud, E., Steger, C., & Weiss, R. (2013). Efficient run-time co-simulation model switching for holistic analysis of embedded systems. *International Journal of Embedded Systems*, *5*(4), 208-224.

[28] Poudel, B., & Munir, A. (2018). Design and evaluation of a reconfigurable ECU architecture for secure and dependable automotive CPS. *IEEE Transactions on Dependable and Secure Computing*, *18*(1), 235-252.

[29] Xu, T. (2019). Enabling Database-based Unified Diagnostic Service over Local Interconnect Network.

[30] Pehrsson, D., & Garza, J. (2012). Bootloader with reprogramming functionality for electronic control units in vehicles: Analysis, design and Implementation.

[31] Dietrich, C., Hoffmann, M., & Lohmann, D. (2015). Cross-Kernel Control-Flow--Graph Analysis for Event-Driven Real-Time Systems. *ACM SIGPLAN Notices*, *50*(5), 1-10.

[32] Attar, A., Babaee, M., Raissi, S., & Nojavan, M. (2024). Airside Optimization Framework Covering Multiple Operations in Civil Airport Systems with a Variety of Aircraft: A Simulation-Based Digital Twin. *Systems*, *12*(10), 394.

[33] Karthikeyan, V., Harshitha, B., Hemasruthi, P., Gowselya, D., Keerthana, R., & Indhu, N. ARM Based MPSoC ECU Architecture for Secure, Reliable and Real-time Self-Propelled CPS.

[34] Feiter, G., Fredriksson, L. B., Hoffmeister, K., Pauli, J., & Zeltwanger, H. (2013). Higher Level Protocols. In *CAN System Engineering: From Theory to Practical Applications* (pp. 173-254). London: Springer London.

[35] Waszecki, P. P. (2017). *System-Level Diagnoses of Safety, Security and Reliability in Automotive Electrical/Electronic (E/E) Architectures* (Doctoral dissertation, Technische Universität München).

[36] Pinto, P. F. A. S. (2019). *Automotive Security Penetration Testing* (Master's thesis, Universidade do Porto (Portugal)).

[37] Petriu, D. C., Rouquette, N., & Haugen, O. (Eds.). (2010). *Model Driven Engineering Languages and Systems: 13th International Conference, MODELS 2010, Oslo, Norway 3-8, 2010, Proceedings, Part II* (Vol. 6395). Springer.