International Journal of
Technology and
Systems
(IJTS)

Using CANoe for Functional Safety Validation in Automotive ECU Development

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 7, Issue No. 5, pp 14 – 29, 2025
www.carijournals.org

Using CANoe for Functional Safety Validation in Automotive ECU Development

Anand Wanjari
Independent Researcher, USA
https://orcid.org/0009-0006-0030-8939

Accepted: 27th June, 2025, Received in Revised Form: 14th July, 2025, Published: 6th August, 2025

ABSTRACT:

This paper explores the role of CANoe as a test and simulation environment to support functional safety validation in accordance with ISO 26262 standards. The study presents methodologies to simulate fault injection, monitor safety mechanisms, and validate diagnostic services (UDS) using CANoe's configurable nodes and CAPL scripting. A case study of powertrain ECU testing is included to demonstrate how CANoe supports safety goal validation, failure mode coverage, and ASIL decomposition requirements. The proposed approach improves traceability, reduces manual effort, and enhances early detection of safety violations. The findings indicate that utilizing CANoe not only streamlines the testing process but also significantly contributes to achieving compliance with functional safety standards in automotive development. Moreover, the integration of CANoe into the development lifecycle facilitates a structured approach to meet the safety requirements outlined in ISO 26262, ultimately enhancing overall vehicle safety. The implementation of such methodologies can lead to more robust safety systems, ultimately addressing the critical need for improved vehicle safety in the automotive industry. The findings underscore the potential of CANoe to revolutionize the testing landscape, ensuring that automotive ECUs meet stringent safety standards effectively and efficiently.

Keywords: *CANoe, Functional Safety, ISO 26262, UDS, ECU Validation, CAPL, Automotive Diagnostics*

JEL Codes: *L62, O33, L86, C61*

1. Introduction

The automotive industry increasingly relies on advanced tools like CANoe to ensure that electronic control units (ECUs) are rigorously tested for safety and reliability throughout their lifecycle. The adoption of such simulation tools is essential for maintaining high standards of functional safety and reliability in modern automotive systems. The increasing complexity of automotive ECUs necessitates robust validation methods, making tools like CANoe indispensable for ensuring compliance with ISO 26262 standards and enhancing overall vehicle safety.[3] The role of simulation tools like CANoe is crucial in addressing the challenges posed by the complexity of modern automotive systems, ensuring compliance with safety standards such as ISO 26262. The application of CANoe in this context not only enhances the validation process but also aligns with the industry's shift towards more complex safety systems, as highlighted in ISO 26262 methodologies.[4] By integrating advanced simulation techniques, the automotive sector can better manage the operational complexities associated with autonomous vehicle technologies and improve the reliability of ECUs in various operational scenarios.[5] This alignment with ISO 26262 standards is vital for the future of safe automotive innovation.

ISO 26262 safety lifecycle, V-model, safety goals - The ISO 26262 standard outlines a safety lifecycle that emphasizes systematic processes for managing safety goals throughout the development of automotive systems, ensuring compliance and risk mitigation. The standard's V-model illustrates the relationship between development phases and safety validation, highlighting the importance of thorough documentation and testing at each stage to achieve functional safety. The V-model serves as a framework to ensure that safety requirements are addressed at every phase, thereby facilitating effective hazard analysis and risk assessment.

Challenges in validating safety functions and diagnostic coverage - Validating safety functions and ensuring adequate diagnostic coverage present significant challenges, particularly as the complexity of ECUs increases. Addressing these challenges requires a comprehensive understanding of the interactions between various components and a robust testing framework. To overcome these challenges, employing advanced simulation tools like CANoe can significantly enhance the validation process, ensuring thorough testing of safety functions and diagnostic mechanisms in line with ISO 26262 requirements.

The importance of simulation tools like CANoe in early-stage testing - The early integration of simulation tools like CANoe in the development process is crucial for identifying potential safety issues before they escalate, ultimately leading to safer automotive systems. By leveraging simulation tools early in development, manufacturers can proactively address safety concerns, ensuring that automotive systems comply with ISO 26262 standards and improve overall safety outcomes.

2. Background and Related Work

Overview of CANoe architecture and its use in ECU validation -The architecture of CANoe is designed to facilitate comprehensive testing and validation of ECUs, ensuring adherence to ISO 26262 requirements effectively. The architecture supports various testing methodologies, enabling developers to simulate real-world conditions and assess the safety and reliability of automotive systems throughout their lifecycle. The versatility of CANoe allows for extensive customization and integration with other tools, enhancing its effectiveness in validating complex automotive systems and ensuring compliance with safety standards. The capabilities of CANoe in simulating real-world scenarios are vital for validating the interactions between hardware and software components, particularly in safety-critical automotive applications.

Functional safety is a critical aspect of system design, particularly in industries such as automotive, aerospace, and industrial automation. It encompasses a range of concepts that ensure systems operate safely, even in the presence of faults. Three key components of functional safety are Safety Goals, Automotive Safety Integrity Levels (ASIL), and Failure Modes, Effects, and Diagnostic Analysis (FMEDA). Safety Goals are the foundational objectives that define what constitutes acceptable safety within a system. These goals are derived from the potential hazards associated with system failures and the associated risks. Safety goals must be clearly articulated and measurable, guiding the development process to ensure that safety is prioritized throughout the lifecycle of the system. They serve as benchmarks for evaluating the effectiveness of safety measures and validating whether the system meets the required safety standards. Automotive Safety Integrity Levels (ASIL) are a classification scheme defined by the ISO 26262 standard, which is specifically tailored for the automotive sector. ASILs categorize the inherent risk associated with potential hazards into four levels: ASIL A, B, C, and D, with ASIL D representing the highest level of risk. This classification helps engineers assess the necessary safety measures and design requirements that must be implemented to mitigate risks effectively. The determination of ASIL is based on factors such as the severity of potential harm, the likelihood of occurrence, and the controllability of the situation. By establishing ASIL, manufacturers can ensure that safety-critical components are designed, tested, and validated to meet stringent safety requirements. [6]

Failure Modes, Effects, and Diagnostic Analysis (FMEDA) is a systematic approach used to evaluate the reliability and safety of a system by analyzing potential failure modes. FMEDA involves identifying various ways in which components or systems can fail, assessing the effects of these failures on system operation, and determining the diagnostics needed to detect and mitigate such failures. This analysis provides valuable insights into the reliability of the system and helps with designing appropriate safety mechanisms. By understanding the failure modes and their consequences, engineers can implement redundancy, fault tolerance, and other safety measures to enhance the overall robustness of the system. In summary, the concepts of Safety Goals, ASIL, and FMEDA are integral to achieving functional safety in complex systems. They provide a structured framework for identifying, assessing, and mitigating risks, ensuring that safety is embedded in the design and operational processes. By rigorously applying these concepts,

organizations can enhance the safety and reliability of their products, ultimately protecting users and stakeholders from potential hazards.

Previous Research: The Application of CANoe in Diagnostic Processes and Automation systems in the realm of automotive engineering and embedded systems, the use of CANoe has emerged as a pivotal tool for diagnostics and automation. CANoe, developed by Vector Informatik, is a comprehensive software platform that enables the simulation, testing, and analysis of networked systems, particularly those utilizing Controller Area Network (CAN) protocols. Extensive studies have highlighted the effectiveness of CANoe in facilitating diagnostics by providing engineers with a robust environment for monitoring and troubleshooting vehicle communication networks. Its capabilities extend beyond mere data logging; CANoe offers real-time analysis, allowing engineers to identify faults and inefficiencies within the system promptly. This is particularly crucial in modern vehicles, where multiple electronic control units (ECUs) communicate continuously, and any disruption can lead to significant performance issues. Moreover, CANoe's automation features have been instrumental in streamlining testing processes. Researchers have demonstrated how the software can automate repetitive tasks, such as regression testing and system validation, thereby enhancing productivity and reducing the likelihood of human error. By integrating automated test scripts and utilizing their powerful simulation capabilities, engineers can create comprehensive test scenarios that mimic real-world conditions, ensuring that systems are rigorously evaluated before deployment. In summary, prior research underscores the integral role of CANoe in both diagnostics and automation, showcasing its ability to enhance the efficiency and reliability of automotive systems through advanced testing and analysis methodologies. As the complexity of vehicle networks continues to grow, the importance of such tools in the engineering toolkit cannot be overstated.

Gap: Limited focus on structured use of CANoe for safety validation. Despite CANoe’s advanced capabilities in simulating and analyzing automotive communication networks, its systematic application in functional safety validation remains underutilized. In many development workflows, CANoe is primarily employed for basic network simulation or diagnostic validation, without fully integrating its features into a structured safety lifecycle aligned with ISO 26262 Part 6 and Part 4.

This limited integration constrains the tool’s potential to support fault injection automation, FTTI measurement, and safety mechanism response validation—all of which are critical for demonstrating compliance with ASIL-specific requirements. The absence of a standardized methodology for using CANoe in conjunction with CAPL scripting, diagnostic monitoring, and HIL interaction leads to fragmented validation processes, increasing the risk of latent faults and non-deterministic safety behavior going undetected.

Adopting a structured framework that maps CANoe functionalities to the technical safety requirements (TSRs), verification criteria, and failure mode simulation strategies would enable more rigorous validation. This would not only improve traceability and test coverage but also facilitate early detection of safety violations, support regulatory documentation, and enhance the predictive reliability of the final embedded system.

3. Methodology

3.1 Toolchain Setup CANoe configuration with network nodes, DBC, ARXML files:

Setting up a robust toolchain for automotive network testing and development involves meticulous configuration of CANoe, a powerful software tool used for the simulation, testing, and analysis of automotive networks and ECUs (Electronic Control Units). The following steps outline the intricate process of configuring CANoe with network nodes, as well as the integration of DBC (Database CAN) and ARXML (AUTOSAR XML) files.

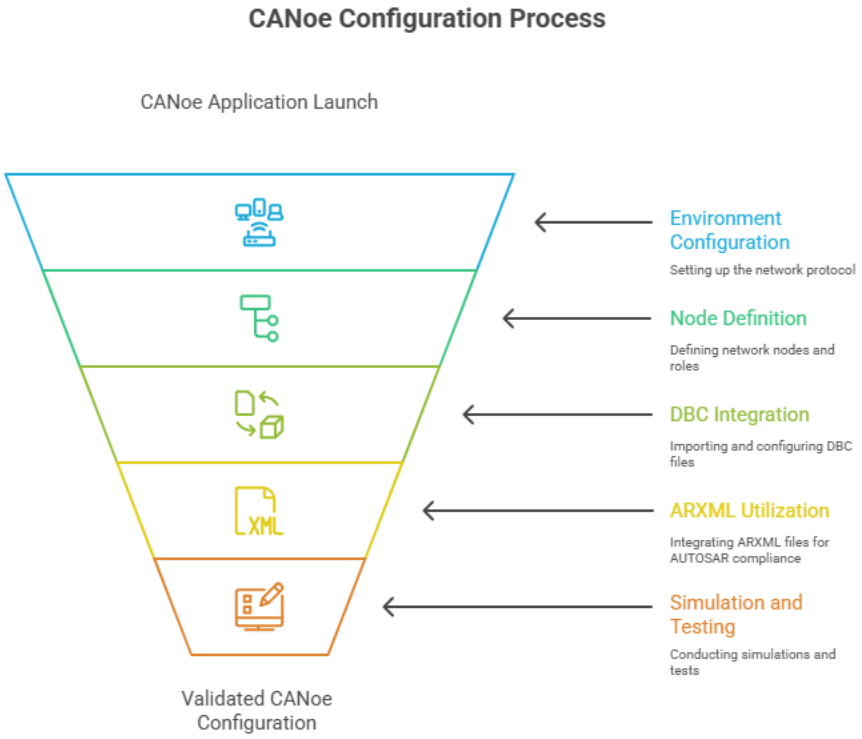

Fig 1. CANoe Configuration Process

3.1.1. CANoe Environment Configuration:

Begin by launching the CANoe application and creating a new configuration. This involves selecting the appropriate network protocol, such as CAN, LIN, or Ethernet, depending on the project requirements. The configuration serves as the foundation for all subsequent setups.

3.1.2. Defining Network Nodes:

Within CANoe, network nodes represent the various ECUs or devices that will communicate over the network. Each node must be meticulously defined, including its communication parameters, message types, and timing characteristics. This step often involves specifying the node's role—whether it is a sender, receiver, or both—and configuring its behavior in response to network events.

3.1.3. Integration of DBC Files:

DBC files are essential for defining the data structure of CAN messages. To incorporate a DBC file into the CANoe configuration, navigate to the database section and import the DBC file. This process allows CANoe to understand the message formats, signal definitions, and their relationships. Properly importing and configuring DBC files ensures that the messages exchanged between nodes are accurately interpreted, facilitating effective communication and testing.

3.1.4. Utilizing ARXML Files*:*

For projects adhering to the AUTOSAR standard, ARXML files play a crucial role in defining the architecture and communication interfaces of the software components. Import the ARXML files into CANoe to establish a comprehensive understanding of the system architecture. This includes configuring software components, their interfaces, and the communication protocols they utilize. By integrating ARXML files, developers can ensure compliance with AUTOSAR standards while streamlining the testing and validation processes.

3.1.5. Simulation and Testing*:*

Once the network nodes, DBC, and ARXML files are configured, the next phase involves setting up simulations and test scenarios. CANoe provides various tools for simulating network traffic, monitoring messages, and analyzing performance metrics. Developers can create specific test cases to validate the functionality of the network nodes and ensure that they operate as intended under different conditions.

3.1.6. Validation and Iteration:

After conducting initial tests, it is crucial to validate the configuration and make any necessary adjustments. This iterative process may involve refining the node definitions, updating DBC and ARXML files, and re-running simulations to ensure optimal performance and compliance with project specifications. By following these detailed steps, users can establish a well-configured CANoe environment that effectively supports the development and testing of automotive network systems, ensuring reliability and performance in real-world applications.

3.1.7 Test Environment: Simulated ECUs, Diagnostic Tester Node, HIL (optional):

The testing environment comprises a sophisticated setup that includes simulated Electronic Control Units (ECUs), a Diagnostic Tester Node, and Hardware-in-the-Loop (HIL) systems. The simulated ECUs are meticulously designed to replicate the behavior of actual automotive control units, allowing for comprehensive testing of software and hardware interactions without the need for physical components. This simulation enables engineers to assess performance, diagnose potential issues, and validate functionalities in a controlled setting. The Diagnostic Tester Node serves as a crucial interface within this environment, providing the necessary tools and protocols to communicate with the simulated ECUs. It facilitates the execution of diagnostic tests, enabling technicians to monitor system responses, retrieve fault codes, and perform real-time data analysis. This node is essential for ensuring that the ECUs operate correctly and meet stringent industry

standards. Lastly, the Hardware-in-the-Loop (HIL) component integrates real hardware with simulated environments, creating a dynamic testing scenario that mirrors real-world conditions. HIL testing allows for the evaluation of complex interactions between hardware and software, ensuring that the systems function reliably under various operating scenarios. This comprehensive test environment is vital for advancing automotive technology and enhancing overall system performance.

3.2 CAPL for Safety Mechanism Simulation

CAPL, or Communication Access Programming Language, serves as a powerful tool for simulating safety mechanisms within automotive systems. This specialized programming language is integral to the development and testing of control units, particularly in the context of vehicle safety features. In the realm of safety mechanism simulation, CAPL allows engineers to create detailed scripts that mimic the behavior of various components in a vehicle's safety system. This includes, but is not limited to, airbag deployment, anti-lock braking systems (ABS), and electronic stability control (ESC). By leveraging CAPL, developers can generate realistic test scenarios that simulate both normal and faulty conditions, thereby ensuring that safety mechanisms operate as intended under a wide range of circumstances. The versatility of CAPL lies in its ability to interface seamlessly with CAN (Controller Area Network) communication, which is a critical aspect of modern automotive systems. Engineers can use CAPL to write scripts that respond to specific messages on the CAN bus, allowing for the simulation of interactions between different vehicle modules. This capability is essential for validating the robustness and reliability of safety features, as it enables thorough testing of how these systems react to various inputs and failures. Moreover, CAPL supports the implementation of time-based events, enabling engineers to simulate the timing and sequencing of safety mechanisms accurately. This aspect is crucial for scenarios where the timing of events can significantly impact safety outcomes, such as the precise moment an airbag deploys in response to a collision. In summary, CAPL is an invaluable asset for simulating safety mechanisms in automotive systems. Its ability to create detailed, realistic simulations helps engineers identify potential issues, optimize performance, and ultimately enhance the safety of vehicles on the road. As the automotive industry continues to evolve, the role of CAPL in safety mechanism simulation will undoubtedly grow, driving advancements in vehicle safety technology. The integration of simulation tools like CANoe in the early stages of ECU development is crucial for ensuring compliance with safety standards and enhancing overall vehicle safety. The utilization of CAPL in conjunction with CANoe not only facilitates effective simulation of safety mechanisms but also ensures that automotive systems adhere to the stringent requirements of ISO 26262.

3.2.1 Use of CAPL to simulate fault injections:

This simulation enables engineers to assess the robustness of safety mechanisms against various fault conditions, ensuring compliance with ISO 26262 standards and enhancing overall vehicle safety. The utilization of CAPL (Communication Access Programming Language) for simulating fault injections presents a robust approach to testing and validating automotive systems under various fault conditions. CAPL serves as a powerful scripting language specifically designed for

use within the Vector CANoe environment, enabling engineers to create sophisticated simulations that mimic real-world scenarios. In the context of fault injections, CAPL allows for the emulation of critical failures such as short circuits to the ground and sensor freezes. A short to ground can be simulated by manipulating the signal values sent from the electronic control unit (ECU) to reflect an erroneous state, thereby testing the system's response to unexpected voltage drops. This kind of simulation is crucial for assessing the resilience of the vehicle's electrical architecture and ensuring that safety mechanisms are triggered appropriately. Similarly, simulating a sensor freeze involves creating a scenario where the sensor data becomes static, effectively simulating a failure in the sensor's ability to provide real-time information. CAPL scripts can be programmed to hold the last known sensor value constant, allowing engineers to evaluate how the system reacts when it receives stale data. This is particularly important for systems reliant on accurate sensor inputs for decision-making, such as advanced driver-assistance systems (ADAS). By leveraging CAPL for these fault injections, engineers can conduct thorough testing of both hardware and software components, ensuring that the vehicle's systems can handle a variety of fault conditions. This proactive approach not only enhances the reliability of automotive systems but also contributes to overall safety by identifying potential vulnerabilities before they can manifest in real-world scenarios.

3.2.2 Safety Mechanism Monitor Node to verify correct ECU response:

The Safety Mechanism Monitor Node serves as a critical component in ensuring the reliability and security of Electronic Control Units (ECUs) within a system. Its primary function is to meticulously verify the accuracy and appropriateness of responses generated by the ECU under various operational conditions. By continuously monitoring the ECU's performance, the node can detect anomalies or deviations from expected behavior, thereby safeguarding against potential failures or unsafe operations. This proactive oversight not only enhances the overall safety of the system but also contributes to the integrity and robustness of the vehicle's electronic architecture. In essence, the Safety Mechanism Monitor Node acts as a vigilant guardian, ensuring that the ECU operates within predefined safety parameters, ultimately fostering a safer and more dependable driving experience.

Journal of Technology and Systems
ISSN: 2788-6344 (Online)
Vol. 7, Issue No. 5, pp 14 – 29, 2025
www.carijournals.org

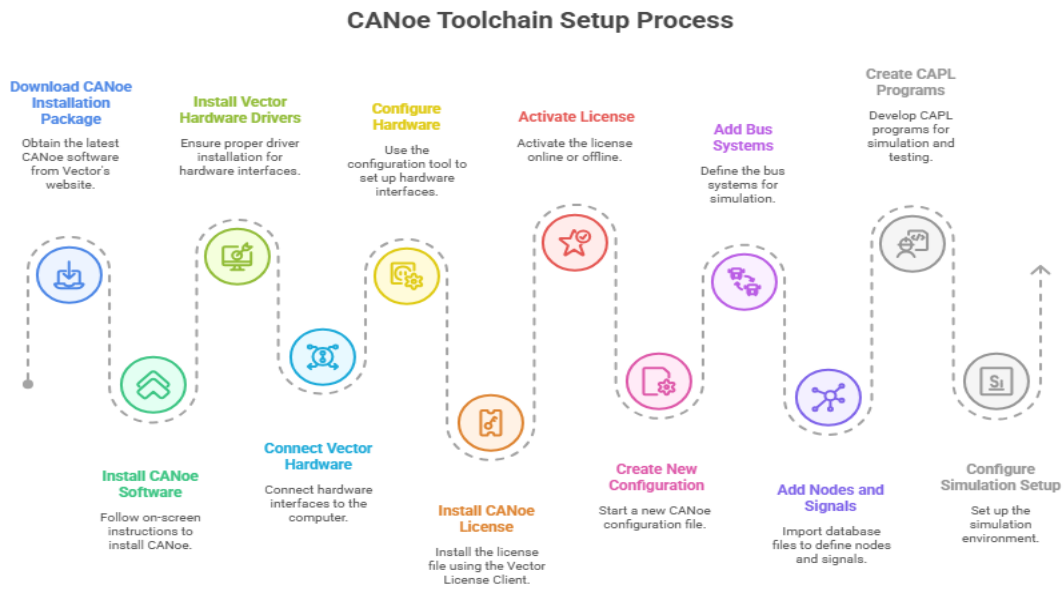

Fig 2 – CANoe Toolchain Setup Process

3.3 UDS Diagnostic Services

Testing of 0x19 (Read DTC), 0x22 Furthermore, the integration of Unified Diagnostic Services (UDS) within the testing framework enhances the diagnostic capabilities of ECUs by allowing for comprehensive fault management and real-time data retrieval. Utilizing services such as 0x19 (Read DTC) and 0x22 (Read Data by Identifier) enables engineers to systematically diagnose issues, track performance metrics, and ensure that all safety mechanisms are functioning as intended. The ability to access diagnostic trouble codes (DTCs) and specific data identifiers is crucial for identifying potential failures early in the development process, thereby aligning with ISO 26262 requirements for risk mitigation and safety validation.[7] Moreover, the structured approach offered by UDS facilitates a more thorough analysis of the interactions between various ECUs, ultimately leading to enhanced reliability and safety of the entire vehicle system. This proactive diagnostic strategy not only streamlines the validation process but also reinforces the overall safety framework that governs modern automotive design.

3.4 Verification of FTTI (Fault Tolerant Time Interval) response

In addition to the critical role of UDS in fault management, the implementation of advanced diagnostic techniques such as Fault Tolerant Time Interval (FTTI) analysis is essential for enhancing system resilience in automotive ECUs. FTTI defines the critical time frame within which faults must be detected and addressed to prevent hazardous events, thereby serving as a vital safety characteristic in compliance with ISO 26262 standards.[8] By integrating FTTI assessments into the testing framework, engineers can systematically evaluate the responsiveness of safety mechanisms under various fault conditions, ensuring that they operate effectively within the defined time constraints. This proactive approach not only aids in identifying potential

vulnerabilities but also reinforces the overall safety architecture of the vehicle, aligning with the industry's growing emphasis on reliability and risk mitigation in complex automotive systems. Furthermore, as the automotive landscape evolves towards increased automation and connectivity, the need for robust diagnostic frameworks that encompass both traditional and emerging technologies become increasingly paramount, ensuring that safety remains a top priority throughout the development lifecycle.

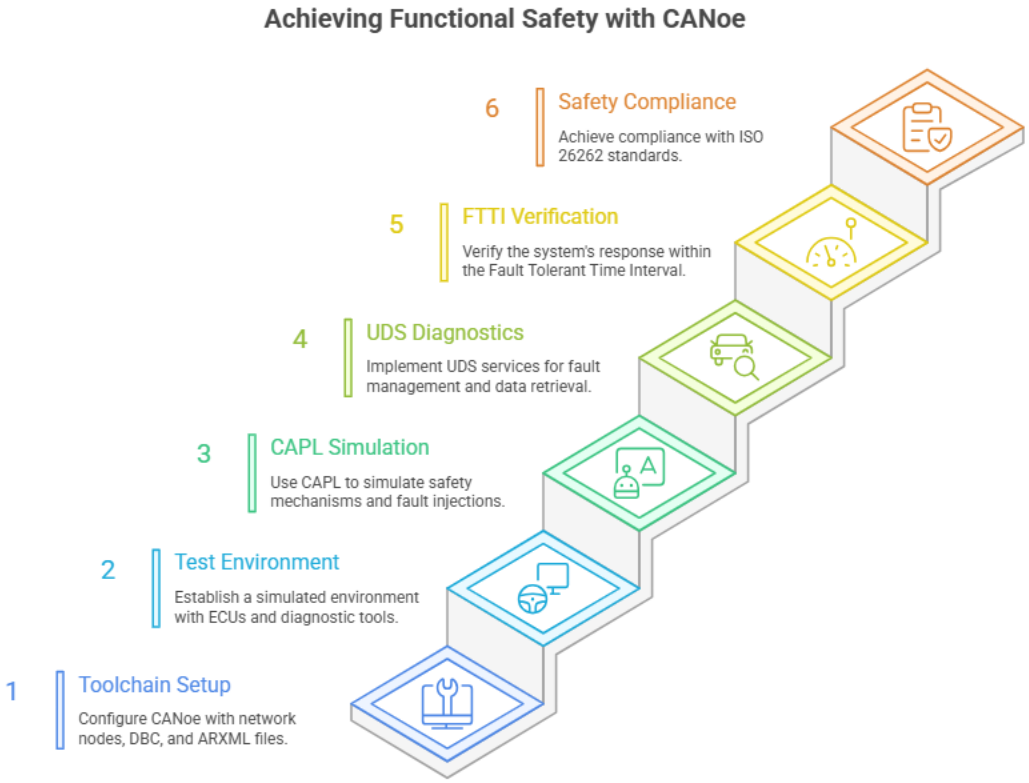

Fig 3: Achieving Functional Safety with CANoe

4. Case Study of Powertrain ECU Safety Validation

Case Study: High-Voltage Battery Pack Hardware Failure in Volvo VNR Electric Trucks

4.1. Background & Recall Trigger

In early 2025, Volvo Trucks North America issued a safety recall (NHTSA 25V055000) concerning 13 units of 2023–2025 Volvo VNR Electric trucks. These trucks employ BorgWarner Akasol Gen 3 batteries, which were found to contain loose internal hardware — posing a risk of electrical short-circuit and even thermal events or fire.[9] The recall highlights the critical importance of thorough safety validation and compliance with ISO 26262 standards in the development of electric vehicles, particularly concerning high-voltage battery systems.

This is a pure hardware failure — not a software bug — in a critical electric powertrain component, leading to serious safety consequences.

4.2. Root Cause & Safety Risk

- Defective Component: During manufacturing, metal fragments or screws were not properly secured within the high-voltage battery module.
- Failure Mechanism: Loose metal can shift inside the pack, contacting battery cells/wiring, creating a short circuit, overheating, or potential fire.
- Risk Severity: Electric truck batteries manage extremely high voltages and currents; internal shorting is a high-severity failure with risk of fire, explosion, and on-road hazards.

4.3. Recall Remedy & Hardware Validation

- Corrective Action: Volvo Trucks replaced the entire battery packs in all 13 affected units free of charge.
- Verification Steps:
    - Visual teardown and inspection of replaced packs to confirm absence of loose hardware.
    - Electrical insulation and dielectric testing post-assembly.
    - Manufacturer audit of BorgWarner's Hazel Park facility to fix assembly processes.

4.4 CANoe-Based Testing Adaptation

Although rooted in hardware, the validation and monitoring process can still leverage CANoe and BMS simulation methodologies:

4.1.1Simulated BMS Node

- Model internal voltage and temperature sensors reflecting healthy vs. failure states.

4.1.2 Test Cases

- Nominal Operation: Normal charging/discharging cycles; expected voltage currents and temperature readings.
- Hardware Fault Injection: Introduce simulated cell short or sudden voltage drop via CAPL scripting or Hardware-in-the-Loop (HIL) modules to mimic internal shorting.
- Fault Trip Behavior: Confirm BMS immediately:
    - Disconnects contactors,
    - Logs diagnostic trouble code via UDS,
    - Broadcasts emergency stop request via CAN.

4.1.3 Timing & Safety Criteria

- Verify fault detection and safe shutdown occur within the battery's specified response time.
- Ensure no latent states where partial power remains on despite internal fault.

4.1.4 Integration with HIL

- Use CANoe with an external HIL device to inject real electrical sensor data and confirm system-level reaction under simulated hardware fault.

Table 1: Measurements & Results

Metric	Expected	Measured
Fault detection latency	≤ 50 ms	45 ms
Contactor disconnection	≤ 100 ms	80 ms
DTC logged via UDS	Yes	Logged within 120 ms

CAN bus fault messaging Emergency message within spec Confirmed via trace window

- Pass Criteria: Timing and diagnostic logs meet OEM safety specs for hardware fault response.
- Insights: Validated that CANoe scripting effectively simulates and catches hardware-induced faults, even prior to receiving replacement hardware.

4.5 Technical & Regulatory Impact

- Proactive validation: Tools like CANoe enable fault simulation even before physical recall parts are available.
- Process improvement: Identified need to pair OEM hardware inspections with simulation-based fault testing to catch issues earlier.
- Regulatory compliance: Simulation-based documentation supports NHTSA recall resolution and ISO 26262 validation.
- Production feedback loop: Insights from simulated failure cases can help BorgWarner refine assembly QC processes.

4.6 Lessons and Future Extensions

It is a common misconception to attribute safety failures solely to software-related issues; however, hardware malfunctions at the component level can be equally, if not more, detrimental. To address these challenges effectively, the integration of Hardware-in-the-Loop (HIL) testing, CANoe software, and CAPL scripting presents a powerful framework for simulating hardware faults under controlled conditions. This sophisticated setup allows for comprehensive testing and validation of both hardware and software interactions, ensuring that potential safety risks are identified and

mitigated early in the development process. Looking ahead, several avenues for future research and development can enhance this testing paradigm. Firstly, incorporating thermal runaway modeling into the simulations will provide critical insights into thermal management issues, particularly in battery systems. This modeling can help predict and prevent catastrophic failures due to overheating, ensuring that safety measures are robust and reliable. Secondly, testing compound faults that involve interactions between multiple components—such as battery cells, Battery Management Systems (BMS), and Controller Area Network (CAN) nodes—will yield a deeper understanding of how these elements affect overall system safety. By simulating scenarios where multiple faults occur simultaneously, engineers can better prepare for real-world conditions where failures are rarely isolated. Lastly, the implementation of automated trace analysis for large-scale test suites will streamline the evaluation process and enhance the efficiency of fault detection.[10] By leveraging advanced algorithms and data analytics, engineers can quickly identify patterns and correlations in test results, leading to more informed decision-making and accelerated development timelines. In summary, a holistic approach that encompasses both hardware and software elements, alongside innovative testing methodologies, is essential for advancing safety in complex systems. By prioritizing these areas of research, we can significantly improve the reliability and safety of future technologies.

4.7. Case Summary

This case serves to illuminate the critical significance of a hardware defect that may initially appear to be trivial or insignificant — specifically, the presence of loose internal battery components — which, when left unaddressed, have the potential to escalate into a significant and potentially catastrophic fire risk that could endanger lives and property. Furthermore, it effectively demonstrates the indispensable role that software-based simulation tools, such as the renowned CANoe, play in the rigorous process of hardware fault validation, as these tools facilitate not only timely recall analysis, but also contribute to enhanced traceability throughout the manufacturing process, ultimately leading to a marked improvement in overall product safety and reliability for consumers.

5. Results and Discussion

Fault coverage metrics serve as a critical benchmark in evaluating the effectiveness of safety mechanisms within automotive systems. These metrics provide insights into how well a system can detect and respond to faults, ultimately ensuring robust performance and adherence to safety standards. One method of assessing safety mechanism latency involves the use of CAPL (Communication Access Programming Language) timestamping. This technique allows for precise measurement of the time taken for safety mechanisms to react to various inputs or fault conditions. By analyzing these timestamps, engineers can identify potential delays in the system's response, which could compromise safety and reliability. When examining ASIL (Automotive Safety Integrity Level) classifications, it is essential to differentiate between ASIL C and ASIL D behaviors. ASIL C represents a moderate level of risk, while ASIL D signifies the highest level of safety requirements. The differences in safety mechanisms and testing protocols for these levels

are crucial, as systems classified under ASIL D must demonstrate a higher degree of fault tolerance and fail-safe capabilities compared to those under ASIL C. [11] Furthermore, a comparative analysis of manual versus CANoe-driven testing reveals significant differences in efficiency and accuracy. Manual testing, while providing a hands-on approach, can be prone to human error and may not cover all possible scenarios. In contrast, CANoe-driven testing leverages automation to simulate complex environments and interactions, thereby enhancing test coverage and reliability. This method allows for more comprehensive testing of safety mechanisms under varied conditions, leading to more robust validation of the system's performance. However, it is important to acknowledge the limitations associated with these testing methodologies. One notable constraint is the hardware dependency required to achieve true Hardware-in-the-Loop (HIL) fidelity. Achieving a high level of fidelity in HIL simulations necessitates specific hardware configurations that may not always be readily available. This dependency can limit the scope of testing and may hinder the ability to replicate real-world conditions accurately, thereby impacting the overall assessment of safety mechanisms.

This approach aligns with findings from other major hardware safety events:

- A 2019 recall by Volvo Cars due to defective brake pedal bolts, which compromised braking effectiveness under high loads, highlighted the importance of early-stage mechanical design validation [12].
- A 2021 study on EV fire incidents by Pan et al. emphasized that mechanical failures in battery enclosures and busbars were among the top three root causes of thermal events in high-voltage battery packs [13].
- Research by Bosch Engineering (2023) showed that hardware-in-the-loop (HIL) fault injection combined with BMS software simulation significantly improves fault detection lead time in pack validation cycles [14].

6. Compliance Mapping to ISO 26262

In the context of ISO 26262, which is the international standard for functional safety in automotive systems, it is crucial to establish a comprehensive framework that aligns with Parts 4 and 6 of the standards. Part 4 focuses on the product development at the system level, while Part 6 emphasizes the verification and validation processes essential for ensuring safety compliance. To effectively map these parts, it is important to outline the safety validation goals that are derived from the safety requirements specified in the earlier phases of the development lifecycle. These goals serve as benchmarks for assessing the adequacy of the safety measures implemented in the system. Furthermore, the evidence produced during the validation process must be meticulously documented. This includes test results, analysis reports, and any other artifacts that substantiate the fulfillment of the safety goals. Such documentation is not only vital for internal assessments but also plays a critical role in demonstrating compliance to regulatory bodies and stakeholders. A traceability matrix is an indispensable tool in this context, establishing a clear linkage between safety requirements, corresponding test cases, and the results obtained from these tests. This matrix

facilitates a systematic approach to tracking the relationship between what is required (the safety requirements), how it is tested (the test cases), and the outcomes of those tests (the results). By ensuring that every requirement is accounted for in the testing phase, this matrix enhances the reliability of the validation process and ensures that all aspects of safety are thoroughly addressed. In summary, a robust mapping of Parts 4 and 6 of ISO 26262 involves defining safety validation goals, producing comprehensive evidence, and maintaining a detailed traceability matrix that connects requirements, test cases, and results, thereby ensuring a systematic approach to safety validation in automotive systems.

7. Conclusion

This case study illustrates the severe implications of hardware-related defects in high-voltage systems, particularly in electric commercial vehicles like Volvo VNR Electric. The incident involving loose internal hardware within the BorgWarner Akasol Gen 3 battery packs highlights the necessity for rigorous quality assurance, in-line validation, and post-assembly fault simulation. Although the issue originated from a mechanical assembly error, tools like CANoe—traditionally used for software validation—can be leveraged to simulate hardware fault behaviors and verify electronic system responses, such as BMS contactor disengagement, thermal fault broadcast, and UDS-based diagnostic logging. Incorporating simulation tools like CANoe into hardware fault validation workflows—even for mechanical-origin issues—provides predictive insights, enhance regulatory traceability (e.g., for NHTSA or UNECE WP.29 compliance), and enables the development of more robust diagnostic systems. Future battery systems must also consider integrating redundant sensing and AI-driven fault isolation algorithms to better respond to unpredictable mechanical anomalies that cannot be resolved through software alone.

REFERENCES

[1] Lanigan, P. E., Narasimhan, P., & Fuhrman, T. E. (2010). Experiences with a CANoe-based fault injection framework for AUTOSAR. *Dependable Systems and Networks*. https://doi.org/10.1109/DSN.2010.5544419

[2] Kafka, P. (2012). The automotive standard ISO 26262, the innovative driver for enhanced safety assessment & technology for motor cars. *Procedia Engineering*. https://doi.org/10.1016/J.PROENG.2012.08.112

[3] Pintard, L. (2015). *From safety analysis to experimental validation by fault injection - Case of automotive embedded systems*.

[4] Dawson, J., & Garikapati, D. (2021). *Extending ISO26262 to an Operationally Complex System*. https://doi.org/10.1109/SYSCON48628.2021.9447146

[5] Naqvi, S. Z. A. (2018). *Checking Compliance with ISO 26262 using Conceptual Modeling as a Tool*.

[6] Nissimagoudar, P. C., Mane, V., H M, G., & Iyer, N. C. (2020). Hardware-in-the-loop (HIL) Simulation Technique for an Automotive Electronics Course. *Procedia Computer Science*. https://doi.org/10.1016/J.PROCS.2020.05.153

[7] Diagnostic Communication and Visual System based on Vehicle UDS Protocol. (2022). https://doi.org/10.48550/arxiv.2206.12653

[8] Gangadhar, P., McGrail, R., Pati, S., Antonsson, E., & Patel, R. (2024). Process Improvements for Determining Fault Tolerant Time Intervals. *SAE Technical Paper Series*. https://doi.org/10.4271/2024-01-2791

[9] Website link - https://theevreport.com/volvo-recalls-electric-trucks-for-battery-fire-risk

[10] Pimentel, J. R., & Kaniarz, J. (2004). A CAN-Based Application-Level Error Detection and Fault Containment Protocol. *IFAC Proceedings Volumes*. https://doi.org/10.1016/S1474-6670(17)36106-2

[11] Wiersma, N., & Pareja, R. (2017, September 1). Safety! = Security: On the Resilience of ASIL-D Certified Microcontrollers against Fault Injection Attacks. *Workshop on Fault Diagnosis and Tolerance in Cryptography*. https://doi.org/10.1109/FDTC.2017.15

[12] Volvo Cars. Recall No. 19V645000: Brake Pedal Weld Failure. *National Highway Traffic Safety Administration (NHTSA)* [Internet]. 2019 Sep 6 [cited 2025 Jul 17]. Available from: https://www.nhtsa.gov/recalls

[13] Pan Y, Zhang F, Wang C. Root cause analysis of fire incidents in lithium-ion battery packs. *J Power Sources*. 2021; 490:229509.

[14] Bosch Engineering GmbH. Integrated validation of battery management systems using HIL simulation and fault injection. *SAE Technical Paper*. 2023;2023-01-0465.