Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Secure and Safety-Aware IST Architectures for Next-Gen Automotive Systems

Jayesh Kumar Pandey
Independent Researcher, USA
Corresponding Author: Jayesh Kumar Pandey, **E-mail**: jayeshk.pandey@gmail.com

| ABSTRACT

Contemporary automotive System-on-Chip architectures necessitate revolutionary transformations in In-System Test implementations to address the convergent requirements of functional safety and cybersecurity protection. Modern vehicle computational platforms integrate multiple subsystems within single-chip solutions while satisfying stringent ISO 26262 compliance standards and emerging cybersecurity regulations. Traditional testing methodologies demonstrate significant inadequacies in protecting against sophisticated cyber threats targeting low-level debug interfaces and test access mechanisms that historically lacked comprehensive security protocols. The evolution toward next-generation automotive systems presents unprecedented design challenges, particularly in implementing robust diagnostic capabilities that maintain operational reliability throughout vehicle lifecycles while preventing unauthorized access to proprietary system data. Secure and safety-aware IST architectures incorporate trusted test controllers, safety-certified Built-In Self-Test engines, hardware-level isolation mechanisms, and secure telemetry systems that collectively address both accidental failures and malicious attacks. Integration complexities arise from fundamental conflicts between safety and security domains, creating substantial barriers through latency considerations, certification gaps, and interoperability challenges across multiple automotive standards. The automotive industry requires comprehensive solutions that implement zero-trust access principles, redundant validation mechanisms, comprehensive audit trails, and cross-functional collaboration between security and functional safety teams. Future advancements encompass AI-driven security policy adaptation, hardware root of trust implementations, digital twin integration for real-time reliability modeling, and distributed validation architectures that enable continuous assessment of system health and safety margins across diverse operational scenarios.

| KEYWORDS

Secure IST, Functional Safety, Automotive SoCs, ISO 26262, JTAG Security, Runtime Test, Cybersecurity, Self-Test, Digital Diagnostics

| ARTICLE INFORMATION

ACCEPTED: 01 June 2025 **PUBLISHED:** 23 June 2025 **DOI:** 10.32996/jcsts.2025.7.106

1. Introduction

Modern automotive System-on-Chip (SoC) architectures represent a transformative shift in vehicle computational capabilities, fundamentally altering the landscape of automotive electronics. The evolution toward next-generation automotive systems presents unprecedented design challenges, particularly in the integration of multiple subsystems within single-chip solutions that must satisfy both performance and reliability requirements [1]. Contemporary automotive applications demand SoCs that operate reliably under extreme environmental conditions while meeting stringent functional safety standards defined by ISO 26262, encompassing Automotive Safety Integrity Levels (ASIL) ranging from A through D classifications. The integration complexity within automotive SoCs has increased exponentially, with modern implementations incorporating advanced processing architectures that combine high-performance computing cores, dedicated digital signal processors, and specialized hardware accelerators for artificial intelligence applications [2]. These sophisticated integrated circuits must simultaneously

address multiple operational domains, including powertrain control, advanced driver assistance systems, infotainment processing, and vehicle connectivity management, all while maintaining strict isolation between safety-critical and non-critical functions. Cybersecurity threats targeting automotive systems have emerged as a critical concern, particularly affecting low-level debug interfaces and test access mechanisms that traditionally lacked comprehensive protection protocols. The automotive industry faces increasing pressure to implement robust security measures that prevent unauthorized access to proprietary system data while maintaining essential diagnostic capabilities for field service operations [1]. Traditional In-System Test (IST) methodologies demonstrate significant limitations in addressing these dual requirements, often providing inadequate security protection mechanisms or insufficient diagnostic coverage for modern safety-critical applications. The convergence of safety and security requirements necessitates innovative IST architectures capable of supporting continuous self-diagnostic operations without compromising system performance or introducing vulnerabilities to potential cyber attacks. These advanced testing solutions must integrate seamlessly with existing automotive communication protocols while providing comprehensive protection against data leakage and unauthorized system access [2]. The automotive industry requires IST implementations that support real-time diagnostic operations, maintain high levels of fault coverage for safety-critical functions, and implement robust encryption mechanisms to protect sensitive test data and intellectual property from potential exploitation.

Parameter	**Traditional Systems**	**Next-Generation SoCs**
Processing Domains	Single Domain	Multiple Integrated Domains
Safety Requirements	Basic Standards	ISO 26262 ASIL A-D
Integration Level	Discrete Components	System-on-Chip
Security Considerations	Minimal	Comprehensive Protection

Table 1: Automotive SoC Integration Complexity Metrics [1,2]

2. Role of IST in Functional Safety and Security

In-System Test (IST) architectures serve critical dual functions within automotive SoC environments by addressing both functional safety compliance and cybersecurity protection through integrated diagnostic and access control mechanisms. The functional safety domain necessitates comprehensive analysis methodologies that combine traditional safety assessment techniques with modern cybersecurity evaluation frameworks to address the interconnected nature of safety and security risks in automotive systems [3]. Integrated functional safety and cyber security analysis approaches recognize that security vulnerabilities can directly compromise safety functions, requiring holistic evaluation strategies that assess both domains simultaneously rather than treating them as independent concerns. The importance of functional safety in automotive applications extends beyond regulatory compliance, encompassing fundamental system reliability requirements that ensure proper operation under all anticipated operating conditions and failure scenarios [4]. Functional safety methodologies must address systematic failures arising from inadequate design processes, random hardware failures occurring during normal operation, and increasingly, security-related failures that could result from malicious attacks targeting safety-critical functions. Modern automotive systems require sophisticated diagnostic capabilities that can distinguish between random failures, systematic faults, and security-induced malfunctions while maintaining appropriate response strategies for each failure category. Runtime diagnostic operations within IST architectures must provide continuous monitoring of safety-critical functions while simultaneously protecting against unauthorized access to diagnostic interfaces and sensitive system information [3]. The integration of safety and security analysis frameworks enables the identification of potential attack vectors that could exploit diagnostic pathways to compromise vehicle safety, including scenarios where malicious actors might manipulate test interfaces to disable safety functions or inject false diagnostic data. These integrated approaches require comprehensive risk assessment methodologies that evaluate both the likelihood of security breaches and their potential impact on functional safety performance. Cybersecurity considerations within automotive IST implementations focus on protecting diagnostic interfaces from unauthorized access while maintaining necessary functionality for legitimate maintenance and diagnostic operations [4]. The functional safety imperative demands that security measures themselves do not introduce additional failure modes or compromise the ability to detect and respond to safety-critical faults. Security implementations must therefore balance access protection with diagnostic accessibility, ensuring that authentication mechanisms do not prevent rapid fault detection or emergency diagnostic procedures during safety-critical situations. The convergence of functional safety and cybersecurity requirements in automotive IST architectures necessitates the development of comprehensive testing strategies that validate both safety compliance and security robustness through integrated verification processes [3]. These approaches must demonstrate that security measures enhance rather than compromise functional safety performance, while ensuring that safety mechanisms do not inadvertently create security

vulnerabilities that could be exploited to undermine system integrity or availability.

Security Feature	Specification Level	Implementation Value
AES Encryption (bits)	Standard	256
RSA Authentication (bits)	Minimum	2048
Security Token ID (bits)	Required	128
Session Timeout (minutes)	Maximum	15-30
JTAG Clock Frequency (MHz)	Typical	10-50
Hash Algorithm Strength	Standard	SHA-256

Table 2: IST Security Implementation Specifications [3,4]

3. Design Components of Secure and Safety-Aware IST

The architecture of secure and safety-aware In-System Test (IST) implementations requires sophisticated design components that address the convergence of functional safety and cybersecurity requirements in modern automotive systems. Contemporary automotive applications demand comprehensive protection mechanisms that safeguard against both accidental failures and malicious attacks while maintaining operational reliability throughout the vehicle lifecycle [5]. Trusted Test Controller implementations manage access to IST resources through comprehensive authentication frameworks that enforce strict access control policies for diagnostic operations. These controllers implement secure boot sequences that validate system integrity before enabling test access, ensuring that only authorized personnel can initiate diagnostic procedures on safety-critical automotive systems [5]. The authentication process incorporates cryptographic handshakes that establish secure communication channels between external diagnostic tools and internal test infrastructure, preventing unauthorized access to proprietary system data and control algorithms. Safety-certified Built-In Self-Test engines represent critical components that implement comprehensive logic and memory validation procedures specifically designed for ISO 26262 compliance requirements. These engines execute systematic test patterns that verify the operational integrity of processing cores, memory subsystems, and peripheral interfaces without disrupting normal vehicle operations [5]. The certification process ensures that BIST implementations meet stringent automotive safety standards while providing continuous monitoring capabilities for detecting potential hardware degradation or malicious tampering attempts. Hardware-level isolation mechanisms utilize sophisticated privilege separation architectures that maintain strict boundaries between test execution contexts and runtime operations. These systems implement dedicated hardware firewalls that prevent unauthorized access to safety-critical system components during diagnostic operations, ensuring that test procedures cannot compromise vehicle safety functions [5]. The isolation framework provides temporal and spatial separation of test activities, preventing potential interference between diagnostic operations and real-time control systems essential for vehicle operation. Secure telemetry systems implement comprehensive encryption protocols for protecting test data transmitted through internal communication channels and external diagnostic interfaces. These implementations ensure data integrity through authenticated encryption algorithms that prevent unauthorized modification or interception of diagnostic information during transmission [5]. Logging mechanisms provide tamper-evident storage capabilities that maintain comprehensive audit trails of all diagnostic activities, enabling forensic analysis of potential security incidents while supporting regulatory compliance requirements. Policy-based orchestration frameworks define comprehensive rule sets that govern when, where, and how diagnostic tests execute within automotive systems. These frameworks balance performance optimization requirements with safety objectives by implementing dynamic scheduling algorithms that adapt test execution based on operational context and system state [5]. The orchestration system ensures that diagnostic activities do not interfere with safety-critical functions while maximizing test coverage and maintaining system reliability throughout the vehicle's operational lifetime.

4. Use Cases in Modern Automotive Systems

Modern automotive Electronic Control Units represent sophisticated computing platforms that integrate comprehensive In-System Test capabilities across multiple operational scenarios throughout the vehicle lifecycle. Contemporary automotive systems incorporate dozens of ECUs that manage everything from engine control and transmission systems to advanced driver assistance and infotainment functions, with each unit requiring specialized diagnostic and testing procedures to ensure reliable operation [6].

Power-On Self-Test procedures constitute fundamental initialization sequences that automotive ECUs execute during system startup to verify the operational integrity of safety-critical subsystems before enabling normal vehicle functions. These comprehensive diagnostic routines validate processor core functionality, memory subsystem integrity, and peripheral interface operation through systematic test patterns that ensure all critical components meet operational specifications [7]. The POST sequence establishes baseline system health metrics that serve as reference points for subsequent runtime diagnostic operations, enabling early detection of potential hardware degradation or malicious tampering attempts that could compromise vehicle safety or security. Periodic runtime diagnostic operations execute during system idle states to provide continuous monitoring of ECU health without interfering with real-time control functions essential for vehicle operation. These non-intrusive test procedures utilize available computational resources during periods when primary control algorithms are not actively processing sensor data or executing actuator commands [6]. Runtime diagnostics implement sophisticated scheduling algorithms that balance diagnostic coverage requirements with performance constraints, ensuring that safety-critical functions maintain deterministic response characteristics while providing comprehensive system health monitoring throughout the operational lifecycle. Error escalation mechanisms trigger automated response sequences when diagnostic procedures detect anomalous conditions that exceed predefined threshold parameters for system operation. These escalation paths implement hierarchical alert protocols that range from simple warning notifications for minor deviations to immediate system shutdown procedures for catastrophic failure conditions that could compromise vehicle safety [7]. The error management framework incorporates sophisticated decision algorithms that evaluate fault severity, system criticality, and operational context to determine appropriate response actions while maintaining compliance with automotive safety standards and regulatory requirements. Customer return analysis capabilities enable automotive manufacturers and service organizations to retrieve comprehensive diagnostic data from failed field units while implementing robust intellectual property protection mechanisms. These field diagnostic systems maintain detailed operational logs and fault histories that support root cause analysis and reliability improvement initiatives without compromising proprietary control algorithms or calibration parameters [6]. The secure data extraction process enables authorized service personnel to access relevant diagnostic information for warranty analysis and failure investigation while protecting sensitive design details from unauthorized disclosure through advanced encryption and access control mechanisms [7].

Operation Type	**Primary Function**	**Execution Context**	**Data Protection Level**
Power-On Testing	System Validation	Startup Sequence	Hardware-Level
Runtime Monitoring	Continuous Health Check	Idle State Operations	Software-Protected
Error Processing	Fault Response Management	Real-Time Operations	Encrypted Storage
Field Analysis	Failure Investigation	Service Operations	IP-Protected Access

Table 3: Automotive ECU Diagnostic Operation Classification and Protection Mechanisms [6]

5. Integration Challenges

The integration of secure and safety-aware In-System Test architectures in automotive systems presents multifaceted challenges that arise from the fundamental need to reconcile conflicting requirements between safety and security domains. Modern automotive systems face unprecedented complexity in balancing functional safety compliance with cybersecurity protection while maintaining operational performance standards required for real-time vehicle control applications [8]. Latency and intrusiveness considerations constitute primary obstacles for IST implementation in safety-critical automotive environments where diagnostic operations must execute without compromising deterministic response characteristics essential for vehicle safety functions. The challenge emerges from the inherent conflict between comprehensive diagnostic coverage requirements and strict timing constraints imposed by real-time control systems that govern critical vehicle operations such as engine management, braking systems, and steering control [8]. Safety-critical automotive applications demand predictable system behavior with minimal jitter and guaranteed response times, while comprehensive IST implementations require additional computational resources and memory bandwidth that can potentially interfere with primary control functions. Tool and certification gaps in existing development environments create substantial barriers to implementing integrated safety and security testing methodologies that simultaneously address both functional safety requirements and cybersecurity protection mechanisms. Current Electronic Design Automation toolchains typically address safety and security concerns through separate, often incompatible approaches that lack comprehensive integration capabilities for automotive applications [8]. The certification process becomes particularly complex when safety and security requirements must be validated concurrently, as traditional validation methodologies were developed to address these domains independently rather than as integrated system requirements.

Interoperability challenges encompass the complex alignment requirements across multiple automotive standards and protocols that govern different aspects of vehicle system operation, including functional safety, cybersecurity management, and diagnostic communication interfaces. The automotive industry relies on diverse standards frameworks, including AUTOSAR for software architecture, ISO 26262 for functional safety, ISO 21434 for cybersecurity management, and various diagnostic protocols such as Unified Diagnostic Services that must operate cohesively within integrated vehicle systems [8]. These standards were developed independently with different underlying assumptions about system architecture, threat models, and operational requirements, creating substantial integration challenges when implementing comprehensive IST solutions that must comply with multiple overlapping and sometimes conflicting requirements. The convergence of safety and security requirements in automotive IST implementations demands innovative approaches that transcend traditional domain boundaries while maintaining compliance with established automotive standards and certification requirements. Integration challenges are further complicated by the need to support legacy vehicle architectures while enabling next-generation connected and autonomous vehicle capabilities that introduce additional complexity through expanded attack surfaces and more sophisticated safety requirements [8]. The resolution of these integration challenges requires coordinated efforts across multiple stakeholders, including automotive manufacturers, semiconductor suppliers, tool vendors, and standards organizations, to develop comprehensive solutions that address the converged safety and security requirements of modern automotive systems.

6. Recommendations and Best Practices

Adopting a zero-trust approach for all test access paths becomes essential in automotive software testing environments where stringent security requirements must be maintained throughout the development lifecycle [9]. Modern automotive systems require comprehensive verification protocols that ensure every component interaction undergoes continuous authentication validation, particularly when dealing with safety-critical functions such as braking, steering, and engine management systems. The zero-trust architecture ensures that no system component or testing interface receives implicit trust, thereby reducing potential attack vectors that could compromise vehicle safety or security during testing phases [9]. Implementation of zero-trust principles in automotive testing environments necessitates the establishment of micro-segmented network architectures where each test harness, simulation tool, and diagnostic interface operates within defined security boundaries [9]. The approach requires continuous monitoring of test data flows, ensuring that authentication credentials undergo regular validation cycles throughout extended testing sessions that may span multiple days or weeks during comprehensive vehicle validation programs. Validating test logic integrity through redundancy and voting mechanisms proves particularly crucial in automotive software testing, where single points of failure can lead to catastrophic safety consequences [9]. Automotive testing frameworks must employ multiple independent validation paths to ensure that test results accurately reflect actual system behavior, especially when validating safety-critical functions that directly impact vehicle occupant protection and operational safety. The implementation of diverse testing methodologies provides enhanced confidence in test outcomes while reducing the probability of undetected faults that could propagate into production vehicles [9].

Redundant testing architectures in automotive environments typically involve parallel execution of identical test scenarios across different hardware platforms, simulation environments, and real-world testing conditions [9]. Voting algorithms compare results

from multiple test instances to identify discrepancies that might indicate hardware failures, software bugs, or environmental factors that could affect test validity. This approach becomes particularly important when validating complex driver assistance systems, autonomous driving functions, and vehicle-to-everything communication protocols, where test accuracy directly correlates with public safety outcomes [9]. Maintaining comprehensive test activity audit trails supports forensics and compliance requirements that automotive manufacturers must satisfy to meet regulatory standards across different global markets [9]. Automotive testing environments generate substantial volumes of test data, diagnostic information, and validation results that must be preserved for regulatory review, safety investigations, and quality assurance processes that may extend years beyond initial vehicle production. The audit trail must capture not only test results but also environmental conditions, hardware configurations, software versions, and personnel involved in testing activities [9]. Collaboration with security and functional safety teams from the design phase onwards ensures that testing strategies align with both cybersecurity requirements and functional safety standards such as ISO 26262 [9]. Early integration of security and safety perspectives into testing frameworks reduces the likelihood of discovering critical vulnerabilities late in the development process when remediation costs and schedule impacts become significant. Cross-functional collaboration facilitates the development of comprehensive testing scenarios that address both intentional attacks and unintentional failures, ensuring that automotive systems maintain robust operation under diverse threat conditions [9].

7. Future Outlook

Secure and safety-aware In-System Test (IST) architectures will become indispensable in meeting the dual demands of functional safety and cybersecurity in automotive System-on-Chip implementations. The automotive industry faces unprecedented challenges as vehicle complexity increases exponentially, with modern vehicles containing over 100 Electronic Control Units that must operate cohesively while maintaining strict safety and security requirements [10]. Traditional testing methodologies prove insufficient for validating the intricate interactions between safety-critical systems, cybersecurity measures, and emerging technologies such as artificial intelligence and machine learning algorithms integrated into automotive platforms.

The evolution of automotive testing demands comprehensive approaches that address both hardware-level vulnerabilities and software-based security threats throughout the vehicle lifecycle [10]. In-system testing architectures must accommodate the growing complexity of automotive semiconductors while ensuring compliance with ISO 26262 functional safety standards and emerging cybersecurity regulations. The integration of multiple testing methodologies within unified frameworks enables simultaneous validation of safety mechanisms, security controls, and functional performance across diverse operational scenarios.

Future advancements will include AI-driven security policy adaptation that leverages machine learning algorithms to continuously optimize testing parameters based on real-world operational data and emerging threat patterns [10]. These adaptive systems will analyze vehicle behavior, environmental conditions, and usage patterns to automatically adjust security configurations and testing protocols without human intervention. The implementation of artificial intelligence in automotive testing requires sophisticated algorithms capable of making autonomous decisions while maintaining the deterministic behavior essential for safety-critical applications. Hardware root of trust implementations for test access will establish cryptographically secured foundations that ensure only authorized personnel can access vehicle diagnostic and testing interfaces [10]. These hardware security modules provide immutable identity verification and tamper-resistant storage for cryptographic keys, creating comprehensive audit trails for all testing activities. The integration of hardware-based security anchors into automotive silicon enables the creation of trusted execution environments where safety-critical testing operations can proceed without exposure to potential cybersecurity threats from adjacent system components. Full integration with vehicle digital twins for real-time reliability modeling represents a fundamental transformation in automotive validation methodologies [10]. Digital twin implementations create comprehensive virtual representations of physical vehicles that incorporate real-time sensor data, historical performance metrics, and predictive analytics to enable continuous assessment of system health and safety margins. These virtual replicas support advanced testing scenarios, including accelerated lifecycle simulations, comprehensive fault injection studies, and extensive security penetration testing without compromising the integrity of physical vehicle systems or endangering operational safety. The convergence of edge computing capabilities with automotive testing infrastructure enables distributed validation architectures where vehicle-mounted processing resources collaborate with cloud-based analytics platforms [10]. This distributed approach facilitates real-time analysis of complex system interactions, multi-vehicle coordination scenarios, and comprehensive fleet-wide validation studies that would be impractical using conventional centralized testing methodologies. Advanced simulation technologies, including high-fidelity environmental modeling and neural network-based behavior prediction, enable comprehensive validation of autonomous driving functions and advanced driver assistance systems across diverse operational conditions.

Technology Component	Current Implementation Level	Future Maturity Level	Integration Complexity	Safety Impact Rating
AI-Driven Adaptation	Low	High	Very High	Critical
Hardware Root of Trust	Medium	Very High	High	Critical
Digital Twin Integration	Low	High	High	Important
Edge Computing	Medium	High	Medium	Important

Table 4: Automotive Testing Technology Evolution Timeline [10]

Conclusion

The integration of secure and safety-aware In-System Test architectures represents a fundamental paradigm shift in automotive electronic system design, addressing the critical convergence of functional safety requirements and cybersecurity protection mechanisms within increasingly complex vehicle computational platforms. Contemporary automotive systems demand sophisticated diagnostic capabilities that transcend traditional testing boundaries, implementing comprehensive protection strategies against both systematic failures and malicious cyber attacks while maintaining strict compliance with ISO 26262 functional safety standards. The implementation of trusted test controllers, hardware-level isolation mechanisms, and secure telemetry systems establishes robust foundations for protecting safety-critical vehicle functions throughout operational lifecycles. Integration challenges encompassing latency considerations, certification gaps, and interoperability requirements across multiple automotive standards necessitate coordinated efforts among automotive manufacturers, semiconductor suppliers, and standards organizations to develop comprehensive solutions. The adoption of zero-trust architectures, redundant validation mechanisms, and comprehensive audit trail systems provides essential frameworks for maintaining system integrity while enabling legitimate diagnostic operations. Future technological advancements, including AI-driven security policy adaptation, hardware root of trust implementations, and digital twin integrations, will fundamentally transform automotive validation methodologies, enabling continuous assessment of system health and predictive maintenance capabilities. The convergence of edge computing with distributed validation architectures facilitates real-time analysis of complex system interactions and fleet-wide validation studies that enhance both individual vehicle safety and overall automotive ecosystem security. The successful implementation of these advanced IST architectures requires sustained collaboration between security and functional safety domains, ensuring that protective mechanisms enhance rather than compromise vehicle operational reliability and passenger safety throughout diverse operational conditions and emerging automotive applications.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Benjamin Glas et al., "Automotive Safety and Security Integration Challenges," GI Digital Library, Available: https://dl.gi.de/server/api/core/bitstreams/8e507d50-d364-4f56-8577-3544f51f68d7/content
[2] Beth Martin, "The future of in-system testing for automotive safety," Siemens, 7 April 2023. Available:https://blogs.sw.siemens.com/tessent/2023/04/07/the-future-of-in-system-testing-for-automotive-safety/
[3] Embien, "A Comprehensive Guide on the Automotive Electronic Control Unit - ECU," Available: Available:https://www.embien.com/automotive-insights/automotive-electronic-control-unit-ecu
[4] Janine Love, "Basics of Automotive Electronic Control Units," Samtec, 29 January 2025. Available:https://blog.samtec.com/post/basics-of-automotive-electronic-control-units/
[5] Jatinder (JP) Singh, "The Importance of Functional Safety," Lattice Blog, 02/06/2018.Available: https://www.latticesemi.com/en/Blog/2018/02/02/00/07/ImportanceofFunctionalSafety
[6] Jitesh H. Panchal and Ziran Wang, "Design of Next Generation Automotive Systems: Challenges and Research Opportunities, " ResearchGate, July 2023. Available:https://www.researchgate.net/publication/372779585_Design_of_Next_Generation_Automotive_Systems_Challenges_and_Research_Opportunities

[7] Linear Micro Systems, "The Role of System-on-a-Chip (SoC) in Automotive Systems, "2 June 2023. Available:https://linearmicrosystems.com/system-on-a-chip-soc-in-automotive-systems/
[8] M. Śliwiński et al., "Integrated functional safety and cyber security analysis," Science Direct, 2018.Available: https://www.sciencedirect.com/science/article/pii/S240589631832264X
[9] Sebastian Polzin, "Automotive software testing: requirements and best practices," Quality Assurance, 10 November 2023. Available:https://www.qt.io/quality-assurance/blog/automotive-software-testing
[10] Secure-Ic, "Introduction to Security and Safety in Automotive," 4 March 2022. Available: https://www.secure-ic.com/blog/automotive/security-and-safety-in-automotive/