PARASOFT®

WHITEPAPER

How to Accelerate ISO/SAE 21434 Compliance With Automated Software Testing

Overview

The automotive industry is rapidly morphing into a complex smart mobility ecosystem, introducing new levels of software sophistication and potential vulnerabilities. The increasing use of software and data-sharing features in road vehicles are notable growth drivers in the automotive sector, however, reports show that new attack vectors capable of large-scale disruptions could bring the industry to its knees if appropriate mitigating factors are not put in place. Cyberattacks on vehicles can compromise the safety, privacy, and performance of the drivers, passengers, and other road users.

One of the key initiatives to address this need is the development of ISO/SAE 21434, an international standard for cybersecurity engineering in road vehicles. The primary purpose of ISO/SAE 21434 is to ensure that vehicle manufacturers loop in cybersecurity measures from the start to the decommissioning of road vehicles.

ISO/SAE 21434 compliance requirements involve the implementation of a cybersecurity management system that covers all stages of product development life cycle. The requirements also include the need for software systems powering road vehicles to undergo rigorous testing rounds, risk assessment, monitoring and review and more.

In this whitepaper, we will discuss the common challenges and solutions for implementing ISO/SAE 21434, and how automated testing solutions can support and ease the compliance process.

ISO/SAE 21434: Understanding the Framework

ISO/SAE 21434 is a standard for cybersecurity engineering in road vehicles that was published in September 2021. The standard was developed by the International Organization for Standardization (ISO) in collaboration with experts from the automotive industry, academia, and government agencies. It's based on the best practices and experiences from various domains, such as information technology, aerospace, and defense.

The primary objective of ISO/SAE 21434 is to provide a comprehensive and consistent framework for managing cybersecurity activities throughout the life cycle of road vehicles and covers all types of road vehicles, like passenger cars, trucks, buses, motorcycles, and trailers, as well as their components, systems, software, and services. The standard also applies to all stakeholders involved in the development, production, operation, maintenance, and disposal of road vehicles, such as manufacturers, suppliers, service providers, operators, and users.

The key goals of ISO/SAE 21434 are as follows:

- Define cybersecurity best practices throughout the automotive supply chain, including during design, development, production, operation, maintenance, and decommissioning.
- Establish a structured process and consistent framework for implementing cybersecurity in vehicle design globally.
- Complement ISO 26262 and UNECE WP.29.
- Provide a threat-informed approach to guide security controls.
- Adopt and apply a risk-based approach.
- Provide guidance for developing a cybersecurity management system (CSMS) for vehicles.
- Identify guidelines for cybersecurity across the vehicle life cycle, which includes design and engineering, production, operations, maintenance, and decommissioning.

Why Is ISO/SAE 21434 Crucial for the Automotive Industry?

The automotive industry faces mounting cybersecurity threats as vehicles become increasingly connected. Manufacturers have struggled to implement sufficient safeguards, leaving modern vehicles susceptible to attacks. For example, Fiat Chrysler once recalled 1.4 million vehicles after hackers demonstrated they could access critical driving systems.

As cars increasingly rely on software, the risks of vehicle cyberattacks and data breaches expand exponentially. A report published by Fortra shows that attack vectors on road vehicles have widened. The report also notes that threat actors can remotely access automotive electronics to disable safety features, manipulate acceleration and steering, and ultimately put lives at risk.

Without a mandatory industry-wide vehicle cybersecurity standard like ISO/SAE 21434, automotive manufacturers may lack proper incentives to treat protection as an integral requirement. Typical corporate cost calculations result in inadequate investment. Yet the consequences of cyber incidents include not just costly recalls, but significant brand damage and legal liability given the safety repercussions.

Therefore, it's no longer safe for automotive companies to voluntarily address these inherent and increasing risks. With lives on the line, nothing less than a comprehensive and binding cybersecurity framework can turn the tide. The ISO/SAE 21434 standard lays the precise groundwork automakers need to secure vehicles throughout manufacturing processes and across their lifespan.

Furthermore, compliance with ISO/SAE 21434 is important for organizations in the automotive sector, as it will help them achieve the following:

- Enhance the security and trustworthiness of road vehicles and their elements and protect them from cyberattacks that could compromise the safety, privacy, and performance of the drivers, passengers, and other road users.
- Meet the regulatory and legal obligations related to cybersecurity, such as the UNECE WP.29 vehicle regulations.
- Enable the innovation and competitiveness of the automotive sector by facilitating the development and deployment of reliable software systems.
- Reduce the costs and risks associated with cybersecurity incidents and vulnerabilities, such as recalls, lawsuits, fines, reputational damage, and customer dissatisfaction.

Software Complexity: A Key Hurdle in Satisfying ISO/SAE 21434

Implementing ISO/SAE 21434 is not an easy task. It involves a number of challenges. While some of the known issues include the diversity and heterogeneity of road vehicles and the ever-evolving nature of cyber threats, the complexity of the software required to power modern road vehicles is also a key factor that's often swept under the rug.

According to McKinsey, the growing complexity of automotive software applications is a critical issue for many organizations. This is evidenced in a report by the National Center for Manufacturing Sciences (NCMS) that showed that advanced vehicles can contain between 1,000 and 3,000 microchips and as many as 150 electronic control units (ECUs) that are operated by software code consisting of up to 150 million lines. This goes to show the level of complexity of modern vehicles.

The complexity of integrating massive lines of code, intricate electronic systems, artificial intelligence (AI) algorithms and external data links in modern vehicles provides attackers with countless entry points to exploit. These threats gain greater urgency as more autonomous and connected vehicles enter the market.

Managing the cybersecurity of these massive systems requires a holistic and systematic approach that considers the interactions, dependencies, and interdependencies among the various elements that make up the software that power these vehicles.

Therefore, satisfying the rigor of the ISO/SAE 21434 protocols in such complex systems will require extensive testing of the software underpinning modern vehicles. With the software building blocks of automotive applications running in millions of codes, automakers must implement robust testing procedures to identify vulnerabilities across the entire attack surface, segment critical driving systems, conduct regular cybersecurity audits and scans, and evaluate threat detection capabilities.

Comprehensive software testing also entails extensive penetration testing, code reviews, static and dynamic analysis of source code, fuzz testing, and other methodologies to validate the standards of security controls. Test procedures should also account for potential risks from third-party software components and connected vehicle services. Only through these thorough and proactive measures can automakers harden their vehicle software against escalating cyber threats targeting safety-critical systems and sensitive driver data.

Therefore, a path toward achieving ISO/SAE 21434 compliance will start with decluttering this level of complexity baked into vehicle software.

Cutting Complexity Through Software Testing: A Path to ISO/SAE 21434 Compliance

Within ISO/SAE 21434, software testing is addressed as part of the overall cybersecurity engineering process. Beyond the cybersecurity viewpoint, software testing of this scale helps engineers pick apart and further understand the labyrinth of complexity that make up automotive software systems.

These tests often rely on the power of test automation solutions, such as Parasoft C/C++test, Jtest, and SOAtest. Automated software testing solutions can help auto manufacturers achieve test compliance within ISO/SAE 21434, by providing the following features and functionalities.

Static analysis. This type of test analyzes the source code without executing it and identifies and reports issues like coding errors, security vulnerabilities, and compliance deviations that may compromise the quality, reliability, or security of the software. Static analysis helps organizations in the automotive sector to improve the quality and security of their software and to adhere to the coding standards related to ISO/SAE 21434, such as MISRA, CERT, and CWE.

Unit testing. Unit testing of C and C++ applications helps verify and validate the functionality, performance, and security of the individual components of the software. With Unit testing, organizations in the automotive sector can ensure the correctness and robustness of their software. By doing so, they're on a path to attaining the testing requirements and criteria of ISO/SAE 21434.

Integration testing. Integration testing can help auto manufacturers ensure the compatibility and interoperability of their software. Software testing solutions can perform integration testing on the interactions and interfaces between the units or modules of software applications, and verify and validate their functionality, performance, and security.

Requirements-based testing. In requirements-based testing, test cases are created by focusing on the goals and conditions outlined in the requirements that were decomposed or flushed out during the development phases in the SDLC. These tests aim to cover specific functions or aspects like security, safety, reliability, and usability. So basically, you design test cases according to what the requirements state, ensuring that the software meets those specified criteria as called by ISO/SAE 21434.

Code coverage. Automakers can also measure and report the code coverage of the software testing activities and indicate the percentage of the source code that has been tested or analyzed with a quality software testing solution. Code coverage ensures the completeness and comprehensiveness of software testing, which is one of the critical criteria for having quality software. To be more specific to ISO/SAE 21434, code coverage is used to ensure that every branch and MC/DC path of a security requirement or functional capability is fully tested.

Broader Automotive Industry Compliance Landscape

ISO/SAE 21434 is not the only standard or regulation that affects the automotive industry and its cybersecurity engineering practices. There are standards and regulations that are specific to autonomous driving and safety. Others are applicable to the general software development and production processes. Understanding these standards also paves the way for ISO/SAE 21434 compliance.

Below are some of these standards and regulations and how they relate to ISO/SAE 21434.

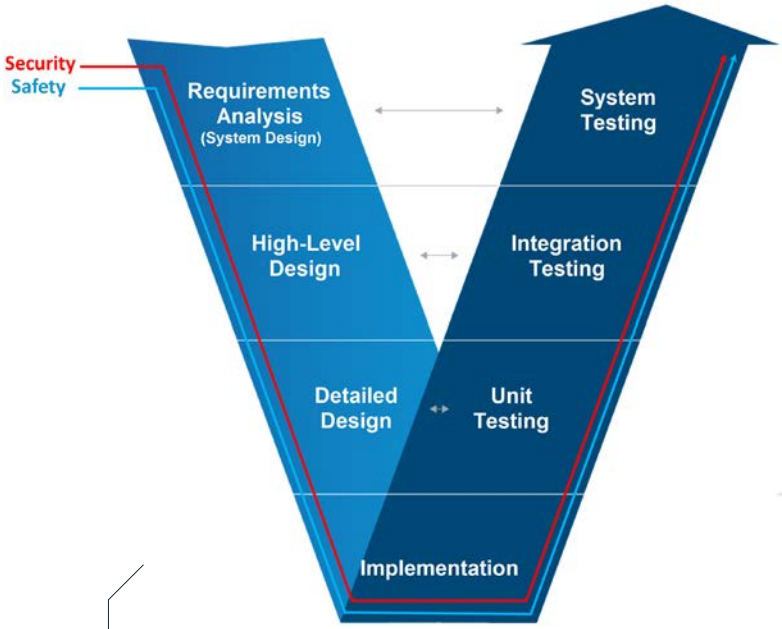


Figure 1: Safety and security integrated at every phase of the SDLC.

ISO 26262. This is an international standard for functional safety of electrical and electronic systems in road vehicles. The standard defines the process, requirements, and activities for ensuring the functional safety of road vehicles and their elements, such as hardware, software, and systems, throughout their life cycle, from concept to decommissioning.

ISO 26262 covers all types and levels of automation of road vehicles, including autonomous driving, and provides guidance and methods for performing hazard analysis and risk assessment, safety goals, safety design, safety validation and testing, and safety management.

Although ISO 26262 focuses on the functional safety of road vehicles and their elements, it complements ISO 21434. As such, they should be applied together to achieve comprehensive and consistent safety and security engineering of road vehicles and their elements.

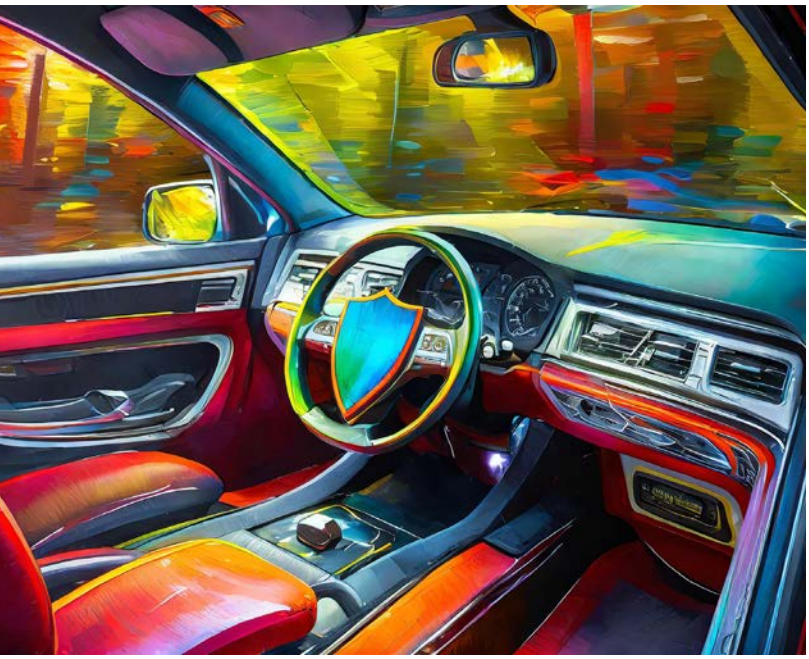
ISO 21448. Known as Safety of the Intended Functionality (SOTIF), this standard outlines measures to ensure the safety of road vehicles' intended functionality. It's particularly relevant for systems requiring high levels of situational awareness for safety, such as emergency intervention systems and driving automation systems ranging from levels 1 to 5. ISO 21448 and ISO/SAE 21434 are both automotive standards, each addressing a unique aspect of vehicle safety and overall security.

UNECE WP.29. The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) sets global standards for vehicle safety and environmental impact. It complements ISO/SAE 21434 by requiring manufacturers to demonstrate an appropriate cybersecurity management system (CSMS) in line with the ISO/SAE 21434 standard.

All four standards and regulations are complementary, compatible, and should be applied together for achieving comprehensive and consistent safety and security engineering of road vehicles and their elements.

Related Coding Standards for ISO/SAE 21434

In addition to the above regulatory requirements, it's crucial for organizations to understand certain coding standards relevant to the automotive sector. These programming conventions provide a roadmap for ensuring the quality, reliability, and security of software, regardless of the domain, application, or technology. Some of these coding standards include:



CERT provides secure coding guidelines for languages like C, C++, Java, and Python. It offers recommendations, best practices, tools, and resources to improve the secure coding of software.

MISRA provides coding standards for developing reliable and safe C and C++ code in automotive systems. Given its over two decades of existence, it has gained wide adoption by the embedded systems community and has become one of the dominant, international coding guidelines. Just like the coding standards above, MISRA C/C++ has relevance in satisfying standards like ISO 26262, ISO/SAE 21434, and ISO 21448 as it promotes secure coding in system-level requirements.

AUTOSAR C++14 refers to the C++14 coding language standard defined by the AUTOSAR consortium. AUTOSAR C++14 helps various industries, and not limited to the automotive sector develop high-quality, scalable, and interoperable software, ultimately contributing to safer, more efficient, and technologically advanced applications.

OWASP is a security framework that provides guidance, tools, and resources for improving the security of web applications and APIs. Its recommendations help developers build secure code and test for vulnerabilities like injection attacks and broken authentication.

How Organizations Can Simplify This Broader Compliance Spectrum

While the standards discussed above are crucial for building cyber resilient automotive software systems, we cannot deny that it takes a lot to satisfy them. Over the years, software testing companies like Parasoft have simplified the process of meeting this spectrum of compliance by baking these into their software testing solution. Below are some of the capabilities.

Automation. Parasoft's software testing solutions automate software testing workflows and tasks like the following to reduce the manual effort and intervention required for software testing.

- Code analysis
- Test case generation
- Test execution
- Test result analysis
- Report generation

Automation helps organizations in the automotive sector improve the efficiency and effectiveness of their software testing, saving time, money, and resources.

Optimization. This is another key ingredient in automotive software testing. Automotive software testing tools are ingrained with advanced techniques and algorithms, such as AI, machine learning (ML), and heuristics, to prioritize, select, and execute the most relevant and important software tests and to provide the most accurate and actionable software testing results and feedback. With this feature, software engineers can improve the quality and accuracy of their software testing, as well as reduce the cost, effort, and duration of software testing.

Integration. Some software testing solutions geared towards meeting coding standards integrate with existing software development and production tools and environments including:

- IDEs
- Compilers
- Debuggers
- Version control systems
- Build systems
- Deployment systems

They also provide seamless and consistent software testing capabilities and functionalities across the different elements and stakeholders involved in software development. This integration helps organizations in the automotive sector improve the consistency and coherence of their software testing and align their software testing with their software development and production workflow.

Collaboration. Collaboration is one of the hallmarks of modern software development. Quality software testing solutions facilitate collaboration and communication between the different elements and stakeholders involved in software development. Collaboration brings about transparency and accountability in software testing and ensures the alignment and integration of software testing with software requirements and expectations. Many organizations have adopted Agile methods to deploy and automate collaboration.

Best Practices for Satisfying ISO 21434

Compliance with ISO/SAE 21434 is not just about following the requirements and activities specified by the standard, but also a matter of adopting and applying the best practices that can support and enhance cybersecurity for the automotive industry.

Below are some of the best practices for meeting ISO/SAE 21434 and how they can help organizations improve the quality, reliability, and security of their software and other embedded systems.

Continuous Code Review

Code review is the process of examining and evaluating the source code of software and providing feedback and suggestions for improvement. Code review helps software engineers detect and correct any issues that may affect the quality, reliability, or security of their software, including the following:

- Coding errors
- Style violations
- Security vulnerabilities
- Compliance deviations

Code reviews can be challenging and time-consuming, especially when the software is complex, large, or frequently updated like what is obtainable in the automotive industry. As such, organizations should develop a culture of continuous code review, which is the practice of conducting code review on a regular and consistent basis, throughout the software development life cycle (SDLC).

Set Coding Standards From the Outset

One of the best coding standard practices for meeting ISO/SAE 21434 is to set coding standards like CERT and/or MISRA from the outset. Organizations can leverage automated software testing solutions like Parasoft C/C++test to support and simplify the coding standards definition and tasks, like coding standards selection, customization, and documentation, and reduce the manual effort, which reduces costs.

Follow Secure Supply Chain Practices for Third-Party Software

To mitigate supply chain cybersecurity risks associated with third-party software, automotive companies should institute strict secure code development, delivery, and integrity validation requirements for vendors.

Suppliers should securely develop code using best practices like threat modeling, static analysis, and safe languages to minimize vulnerabilities, then digitally sign off on the software. Robust encryption and access controls should be applied to secure distribution channels against tampering.

Once received, OEMs need to authenticate signatures, run checksums to validate correctness, and scan for any flaws or malware prior to integration. It's also important that vendors maintain transparency about their security controls and processes through audits and reports for continual oversight. Additionally, they need to promptly address any identified vulnerabilities per OEM disclosure policies.

Perform Continuous Testing

Continuous testing is another best practice for meeting ISO/SAE 21434. It is the practice of conducting testing on a regular and consistent basis, throughout the SDLC.

Continuous testing makes it easier to identify and resolve any defects, errors, or vulnerabilities in software as soon as possible. It also helps avoid the accumulation and propagation of defects, errors, or vulnerabilities that may become more difficult and costly to fix later. Timeliness enables organizations in the automotive sector to improve the efficiency and effectiveness of their software development and production processes and reduce the time, effort, and resources required for software testing and debugging.

Require Suppliers to Show Documentation of Their Own Cybersecurity Policies

Automotive organizations should mandate that component suppliers provide detailed documentation of their internal cybersecurity policies, programs, and practices. This documentation should be thoroughly reviewed to confirm alignment with the OEM's security checklist. Any gaps or deviations should be addressed.

Use TARA Strategy

Threat Analysis and Risk Assessment (TARA) is another key part of meeting the ISO/SAE 21434 standard for automotive cybersecurity. TARA provides a systematic way to identify, analyze, and evaluate cybersecurity risks to vehicles and automotive systems.

1. Define the asset. Which vehicles, systems, and data will be assessed?
2. Conduct threat analysis to identify potential attack vectors, entry points, vulnerabilities, and adversaries that could exploit them. Develop threat scenarios to describe how attacks could occur.
3. Evaluate each threat scenario's likelihood and potential impact to determine the overall risk level.

Executing the TARA strategy provides crucial input into the automotive cybersecurity activities described in ISO/SAE 21434, like the following:

- Define security requirements
- Implement countermeasures.
- Test and monitor continuously.
- Design a response plan.

Automated Testing for ISO/SAE 21434 Compliance

Parasoft C/C++test provides automated software testing solutions to help organizations meet ISO/SAE 21434 compliance.

1. **Comprehensive support for automotive standards** like MISRA, CERT, and AUTOSAR C++14. The packaged ruleset of automotive and security coding standards checkers, along with dedicated compliance reporting, helps automotive organizations achieve the required levels of safety and security in their systems.
2. **Customized compliance reporting and advanced analytics** with Parasoft DTP (Development Testing Platform), which centralizes, processes, and presents data related to software quality. It compiles results from diverse testing methods, enabling continuous oversight of testing results. DTP provides a consolidated dashboard to view outcomes from static analysis, unit testing, manual testing, code coverage, requirements traceability and more. It also includes ready-to-use analytics widgets for understanding risks and enhancing productivity. To meet compliance needs, DTP automates the gathering of quality data across all testing methods.
3. **Continuous software testing** to reduce the time, effort, and cost of delivering secure, safe, reliable, and compliant software. C/C++test's automated software testing capabilities are made for today's modern Agile DevOps environments and integrate into the developer's IDE, CI/CD pipeline, and containerized deployments to detect defects earlier in the SDLC and automatically enforce compliance with industry standards.

4. **Automated verification of internal coding standards** with Parasoft's specialized rules editor. Teams can create custom checkers to extend or customize built-in rules. This replaces the manual process of compliance verification, automating the verification of internal coding standards.

5. **AI and ML for better code analysis** and to assist organizations with adopting static analysis solutions successfully. A common roadblock that teams encounter is managing a large number of warnings and handling perceived false positives. Whatever the compliance requirements—MISRA, CWE, OWASP, and more—Parasoft's automated static analysis solution flags and prioritizes the rule violations that the team needs to fix first.

   The AI and ML-enhanced solution reviews new static analysis findings in the context of both historical interactions with the code base and prior static analysis findings to predict relevance and prioritize the new findings. A hotspot detection engine works with an advanced AI-based model to assign violations to developers matching their best skills and experience—learning from violations they fixed in the past.

6. **Automated unit test creation** enables the generation of unit tests applicable to project-wide testing and file-specific testing. The procedure includes the establishment of test infrastructure and the creation of test suites. Unit tests help ensure the safety, security, and reliability of code by testing small sections of it independently. To do this, developers and testers use a technique called stubbing, where they help isolate specific parts of the code referred to as a unit or function. These stubs mimic the behavior of other parts of the code or serve as temporary replacements for sections that haven't been developed yet.

Summary

The automotive industry needs to ensure the cybersecurity of road vehicles as they become more dependent on software and more exposed to cyberattacks. Cybersecurity affects the safety, privacy, and performance of drivers, passengers, and other road users, as well as the innovation, competitiveness, and compliance of the automotive sector.

Satisfying the standards stipulated within ISO/SAE 21434 is one of the ways software powering road vehicles is protected against cyberattacks. In addition to meeting ISO/SAE 21434, organizations need to pay attention to satisfying related standards like ISO 26262, ISO 21448, UNECE WP.29, CERT, MISRA, and OWASP.

Compliance with ISO/SAE 21434 and these other standards comes with challenges ranging from complexity, diversity, and dynamics to resources used in coupling automotive software systems. The automotive industry can overcome these challenges by adopting best coding practices and automating software testing with solutions like Parasoft C/C++test to experience the following benefits:

- Support and simplify the software testing processes needed for automotive software systems.
- Meet the regulatory and legal obligations related to cybersecurity.
- Reduce the costs and risks associated with cybersecurity incidents and vulnerabilities.

TAKE THE NEXT STEP

Talk to a compliance expert to learn how your embedded software development team can accelerate ISO/SAE 21434 compliance with automated software testing.

About Parasoft

Parasoft helps organizations continuously deliver high-quality software with its AI-powered software testing platform and automated test solutions. Supporting the embedded, enterprise, and IoT markets, Parasoft's proven technologies reduce the time, effort, and cost of delivering secure, reliable, and compliant software by integrating everything from deep code analysis and unit testing to web UI and API testing, plus service virtualization and complete code coverage, into the delivery pipeline. Bringing all this together, Parasoft's award-winning reporting and analytics dashboard provides a centralized view of quality, enabling organizations to deliver with confidence and succeed in today's most strategic ecosystems and development initiatives—security, safety-critical, Agile, DevOps, and continuous testing.