Using Mayhem to Achieve ISO 21434 Compliance

Mayhem

ISO 21434 is a critical cybersecurity standard created to mitigate risks that have come about with the increasing connectivity and software complexities of modern vehicles. ISO 21434, along with current trends in automotive security, call for a proactive and comprehensive approach to address cybersecurity challenges.

What ISO 21434?

The growing connectivity and software complexity of modern vehicles have led to growing cybersecurity challenges in the automotive industry. ISO 21434, titled "Road vehicles - Cybersecurity engineering", is an international standard collaboratively developed by the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) to serve as a crucial framework to address these challenges. Building on the foundation laid by its predecessor, ISO 26262, which primarily focuses on functional safety, ISO 21434 specifically targets cybersecurity risks associated with the design and development of electronic systems in road vehicles.

In a nutshell, ISO 21434:

- Provides comprehensive cybersecurity guidelines and requirements for organizations, including Original Equipment Manufacturers (OEMs) and suppliers
- Encourages a "security by design" approach
- Outlines cybersecurity engineering requirements for the entire lifecycle of electrical and electronic systems in road vehicles
- Provides a framework for processes and a standardized language to manage and communicate cybersecurity risks
- Applies to series production road vehicle systems developed or modified after its publication in August 2021

The Impact of ISO 21434 on Cybersecurity Practices and Trends

ISO 21434 has had a profound impact on automotive development teams by shaping the way they approach cybersecurity, risk management, and the overall development lifecycle of connected vehicles. Compliance with ISO 21434 is essential for development teams to enhance the cybersecurity posture of their products and navigate the evolving landscape of connected and autonomous vehicles. Recent trends in automotive security have seen:

- An increase in remote CVEs compared to physical CVEs
- A predominant focus on peripheral vehicle components over the CAN Bus
- One-third of the most common CWEs are on the SANS Top 25 list
- Two-thirds of the most common CWEs are on the most recent OWASP Top 10
- Buffer overflows, replay, and Man-in-the-middle are the most common software attacks

In other words, most software vulnerabilities in the automotive space aren't automotive-specific issues. The best approach to automotive security encompasses the entire automotive supply chain and the associated service ecosystem. To mitigate risk, organizations in the automotive sector should shift their focus from automotive-specific cybersecurity practices, such as CAN Bus fuzzing, to prioritizing the security of all software within and around vehicles.

Using Mayhem to Address Key Areas of ISO 21434

Mayhem is an essential part of a successful ISO 21434 compliance program. By intelligently automating software test creation and execution, Mayhem helps teams identify and manage vulnerabilities as required in ISO 21434.

Mayhem helps teams deliver on ISO 21434 compliance in the following areas:

5.4 Tool Management
8.5 Vulnerability Analysis
8.6 Vulnerability Management
10.4 Product Development
15.7 Attack Path Analysis

5.4 Tool Management

Control Number	Control Description	How Mayhem Helps
RC-05-15	An appropriate environment to support remediation actions for the cybersecurity incident response (see 13.3) should be reproducible until the end of support for the product.	Mayhem provides a copy/paste reproduction and automatically created regression test for every issue found. With these, developers can replay any defect to support information gathering for remediation.

8.5 Vulnerability Analysis

Control Number	Control Description	How Mayhem Helps
RQ-08-05	Weaknesses and/or cybersecurity events shall be analyzed to identify vulnerabilities.	Mayhem identifies software bugs and attack risks in software and matches these to CWEs where indicated to identify application vulnerabilities.
RQ-08-06	A rationale shall be provided for a weakness that is not identified as a vulnerability.	Mayhem's dynamic SBOM (currently in limited beta) can verify whether components with weaknesses are present on the application attack surface, providing evidence for justifying weaknesses that are not vulnerabilities.

8.6 Vulnerability Management

Control Number	Control Description	How Mayhem Helps
RQ-08-07	Vulnerabilities shall be managed such that for each vulnerability: a) the corresponding cybersecurity risks are assessed and treated in accordance with 15.9 such that no unreasonable risks remain; or b) the vulnerability is eliminated by applying an available remediation independent of a TARA.	Mayhem provides a severity score for each identified vulnerability to allow management of remediation and mitigation efforts based on corresponding risk. Mayhem also determines whether mitigating factors will make exploitation harder or easier. Every vulnerability discovered by Mayhem is tested on all subsequent analysis runs to ensure that remediation is successful.

10.4 Product Development

Control Number	Control Description	How Mayhem Helps
RC-05-15	Criteria (see [RQ-10-04]) for suitable design, modeling, or programming languages for cybersecurity that are not addressed by the language itself shall be covered by design, modeling and coding guidelines, or by the development environment.	Mayhem checks applications for language-specific exploitability factors. These provide guidance for hardening applications when the language itself does not provide built-in hardening.
RQ-10-10	The integration and verification activities of [RQ-10-09] shall be specified considering: a) the defined cybersecurity specifications; b) configurations intended for series production, if applicable; c) sufficient capability to support the functionality specified in the defined cybersecurity specifications; and d) conformity with the modeling, design and coding guidelines of [RQ-10-05], if applicable.	Mayhem performs dynamic-analysis and can test interfaces between components, as specified in NOTE 2 of RQ-10-10.
RQ-10-11	If verification by testing is adopted, test coverage shall be evaluated using defined test coverage metrics to determine sufficiency of the test activities.	Mayhem measures test coverage of all applications analyzed.
RC-10-12	Testing should be performed in order to confirm that unidentified weaknesses and vulnerabilities remaining in the component are minimized: functional testing; vulnerability scanning; fuzz testing; and/or penetration testing.	Mayhem performs fuzz testing as part of its analysis to identify unidentified weaknesses and vulnerabilities.
RQ-10-13	If testing in accordance with [RC-10-12] is not performed, then a rationale shall be provided.	Mayhem's Dynamic SBOM (currently in limited beta) monitors the application attack surface to verify whether components are present and reachable. It can be used to assess the "feasibility to access the attack surface of the component".

15.7 Attack Path Analysis

Control Number	Control Description	How Mayhem Helps
RC-15-11	The attack feasibility rating method should be defined based on one of the following approaches: a) attack potential-based approach; b) CVSS-based approach; or c) attack vector-based approach	Mayhem uses historical exploit and CVE data to generate a CVSS for all vulnerabilities found.