Cycuity

SIMPLIFYING AUTOMOTIVE SEMICONDUCTOR CYBERSECURITY

Cycuity streamlines compliance efforts by introducing scalability and traceability to hardware security verification

Overview

Modern vehicles depend on an array of electronics, sensors, and computer systems. These expanding attack surfaces require strong cybersecurity measures to ensure automotive components and systems work as intended and are built to mitigate safety and security risks.

New regulations and standards aim to define such measures to enable and ensure robust vehicle cybersecurity throughout the automotive supply chain. UN Regulation #155 covers uniform provisions for the approval of vehicles with regards to cybersecurity and requires that manufacturers have a cybersecurity management system in place. And recent industry standard ISO/SAE 21434 "Road vehicles – Cybersecurity engineering" focuses on the cybersecurity risks associated with the design and development of automotive electronics and provides guidelines and requirements for cybersecurity policies, processes and threat assessment.

Automotive OEMs and manufacturers must ensure they can demonstrate compliance with these regulations and standards for cybersecurity across the entire system — including those relevant to hardware security. Chip design plays an important role in the standard. Chips can be seen as components in the larger vehicle ecosystem and chip designers need to ensure that their components are not the weak link in the chain.

Additionally, while critical to demonstrate security rigor, manually gathering, compiling, and presenting supporting certification documentation can take significant time and effort, all while pressures to meet product release timelines remain persistent.

Common Compliance Roadblocks

- Lack of resources to drive the compliance requirements and necessary documentation
- Insufficient security compliance and verification processes, which tend to be ad-hoc and focused on functional compliance
- Poor security specification and scope - leading to incomplete or unverifiable security requirements
- Issues with traceability that can introduce information gaps in documentation
- Efficiently creating detailed and objective documentation
- Meeting hardware security verification deadlines with new security compliance requirements
- Translating and managing security compliance requirements and approvals across multiple stakeholders and global design and security teams
- Providing compliance evidence
- Non-certified tools create management and documentation overhead

Cycuity Delivers Compliance Process and Documentation Efficiency

Radix technology from Cycuity enables semiconductor suppliers in the automotive supply chain to efficiently comply with ISO/SAE 21434, and other standards, by introducing repeatability, scalability, and traceability to hardware security verification.

Radix aids compliance efforts by providing an *asset-based methodology* and information flow technology for a process of systematically detecting and evaluating emerging and known hardware security weaknesses across semiconductor design and development.

The technology complements existing semiconductor design tools, with a specific focus on security, so organizations and their global teams can perform comprehensive security verification and analysis before chips and components for connected cars go into production.

Define Verifiable, Asset-Based Security Requirements

Threat modeling and risk assessment are key steps when designing semiconductors, especially those that will handle sensitive data or critical vehicle functions. A threat model should be constructed to understand potential vulnerabilities, possible attack vectors, and risks. This involves assessing what could happen if the chip is compromised and designing safeguards to prevent or mitigate those threats as well as identifying security sensitive assets.

Radix helps:

- Develop and document verifiable security requirements based on the underlying asset you are trying to protect
- Gain comprehensive insight into locations and flows of security assets and architecture of security protection mechanisms
- Extend security beyond vulnerability and weakness-based requirements for the most comprehensive and measurable security program

Amplify Security Verification

Ensuring that a chip's design is secure requires rigorous verification and validation. This could mean exhaustive testing to ensure that security features work as intended and that the chip is resistant to known vulnerabilities or attack techniques. Verification of both functionality of security features and verification of security requirements, i.e., integrity and confidentiality of assets is required. While functional verification is covered by familiar techniques such as simulation, assertions and formal methods, a tool based on information flow tracking such as Cycuity's Radix is required for sufficient verification of security requirements.

Radix helps:

- Ensure security requirements are consistently met during implementation, integration, and configuration as designs progress
- Streamline security compliance validation by simultaneously checking for security violations during functional verification with existing EDA verification tools
- Provide an additional level of security by scanning the entire system for unexpected or unidentifiable information leakage

Easier ISO/SAE 21434 Tool Management

Requirement [RQ-05-14] of the ISO/SAE-21434 standard states: "Tools that can influence the cybersecurity of an item or component shall be managed." Managing tools in this context pertains to ensuring that the software tools used in the design, development, and verification processes related to automotive cybersecurity adhere to a set of defined criteria to ensure their integrity, reliability, and security. The goal is to ensure that the software tools themselves do not become a source of vulnerability or risk in the automotive cybersecurity lifecycle.

Radix is certified to comply with ISO/SAE-21434, eliminating the need to perform due diligence on tool suitability and security, and producing evidence there-of, requires a lot less resources than using a non-certified tool.

Achieve Certification with Confidence and Detailed Documentation

Cybersecurity verification is an integral part of the product development phase, described in section 10 of the ISO/SAE-21434 standard, ensuring that the designs and implementations meet the set cybersecurity requirements. For semiconductor components, compliance requirements include verifying conformance with security requirements, for instance:

- [RQ-10-09] Integration and verification activities shall verify that the implementation and integration of components fulfil the defined cybersecurity specifications.
- [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.
- [RQ-10-12] Testing should be performed in order to confirm that unidentified weaknesses and vulnerabilities remaining in the component are minimized.

Verifying security with Radix makes it easy to meet these compliance requirements and produce the required documentation:

- [WP-10-07] Integration and verification report, resulting from [RQ-10-09], [RQ-10-11] and [RQ-10-12].

The last two compliance requirements listed above are significantly more difficult to meet using standard functional verification tools without Radix.

Radix helps:

- Present evidence of rigorous testing and documentation that all security requirements and objectives were fulfilled
- Ensure stakeholders are aligned and collectively sign off on measurable success criteria
- Provide evidence of security rigor

Ready to Streamline Compliance with ISO/SAE 21434 and Other Standards?

Cycuity helps ensure tomorrow's vehicles are secure, by providing a systematic approach to the hardware security verification process and simplifying the data collection necessary to demonstrate cybersecurity compliance with evolving standards. Today, leading automotive suppliers are using Cycuity to streamline their ISO/SAE 21434 cybersecurity certification efforts at both the process and product levels.


CERTIFICATE
No. Z10 119002 0001 Rev. 00
Holder of Certificate: Cycuity, Inc.
Certification Mark:
Product: Software Tool for Safety Related Development Systematic Hardware Security Verification and Assurance
Model(s): Radix
Parameters:
Tested according to: ISO/SAE 21434:2021
Test report no.:
Valid until:
Date:

CERTIFIED
ISO/SAE 21434

Cycuity

Learn more. Request a demo.

www.cycuity.com