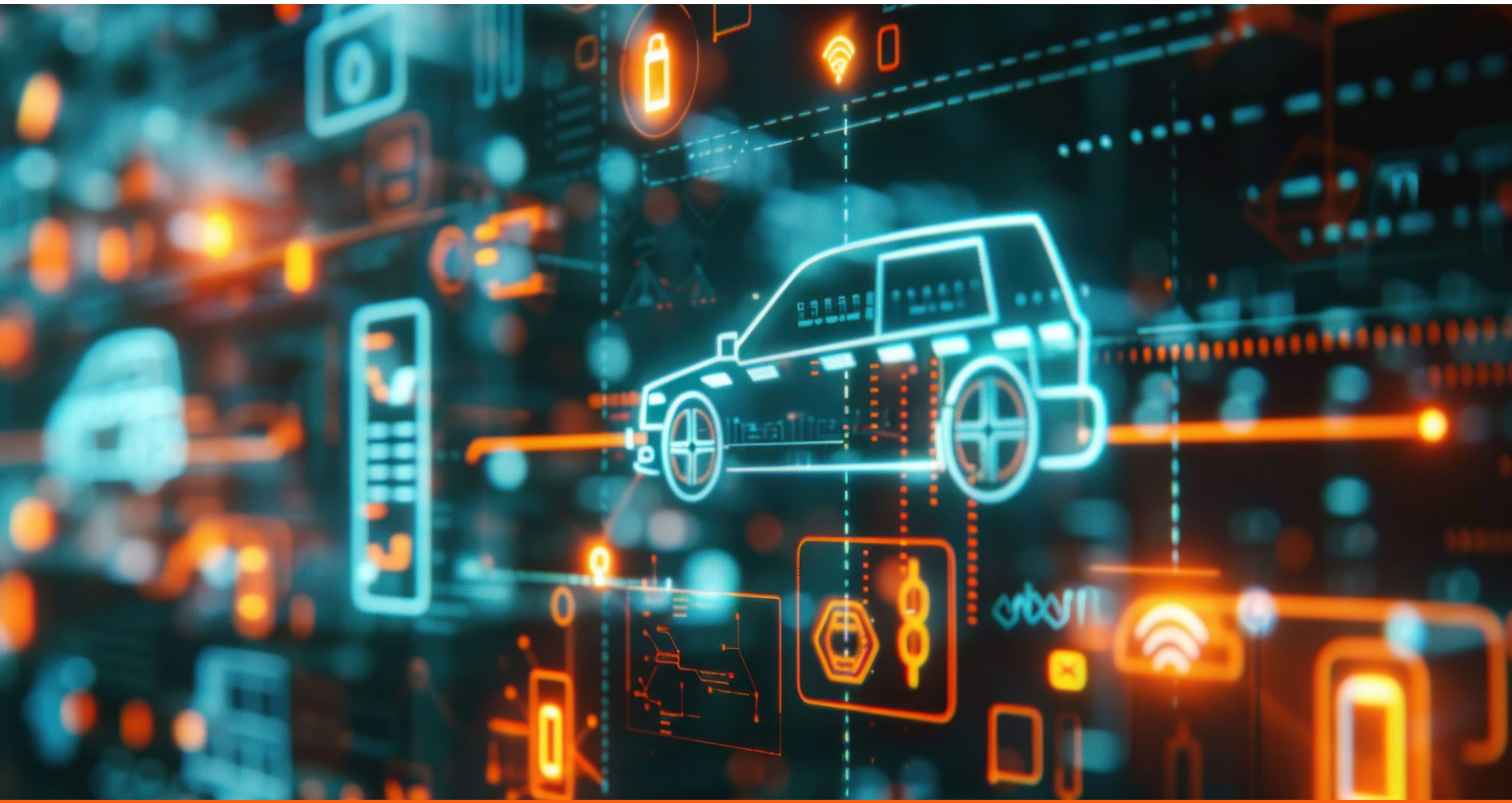
info@apriorit.com
www.apriorit.com



Case study

Auditing the Security of a Connected Vehicle Communication System

The client

Our client is a global provider of software solutions for connected vehicles. They specialize in delivering connected vehicle communication systems that enable data exchange between vehicles and vehicle infrastructure.

While working on a new advanced vehicle communication system (AVCS), they were looking for an experienced team to conduct an independent security analysis.

The challenge

The client’s system enables real-time communication by leveraging 5G and Wi-Fi connectivity along with vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), and vehicle-to-everything (V2X) protocols.

To ensure that their new system would be resilient against potential cyber threats, our client was looking for an experienced security auditing team. The complexity of their system required experts with:

- A deep understanding of security specifics of 5G and Wi-Fi networks
- Expertise in real-time data exchange mechanisms
- Knowledge of security requirements from major industry standards like MISRA C, ISO/SAE 21434, and NIST recommendations

Additionally, the client needed assistance building a proper registry of all software components within their AVCS.

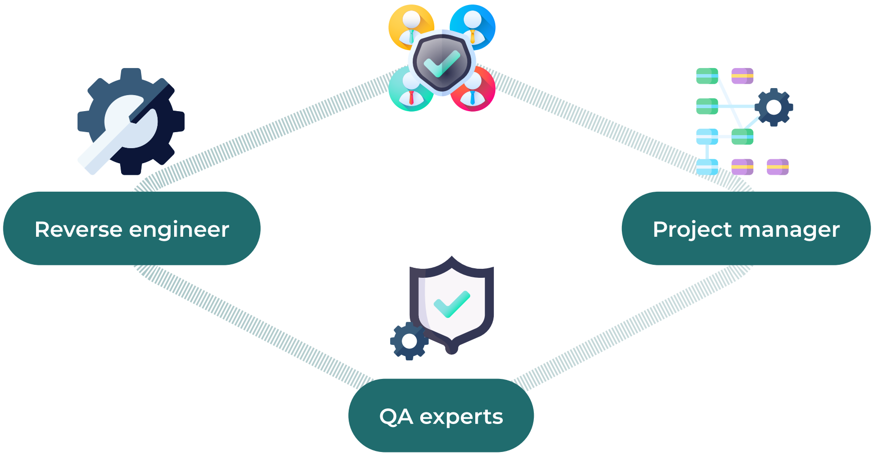
As Apriorit is a TISAX-certified company with an understanding of automotive software development specifics and deep cybersecurity expertise, the client entrusted us with this security audit.

The solution

To assess the security of our client’s system, we assembled a specialized team that included:

- A reverse engineer for deep security analysis and work with poorly documented features
- Quality assurance **(QA) experts** for static analysis, penetration testing, and stress testing of the system
- A project manager for improved team efficiency and seamless communication between the team and project stakeholders

Automotive system security assessment team



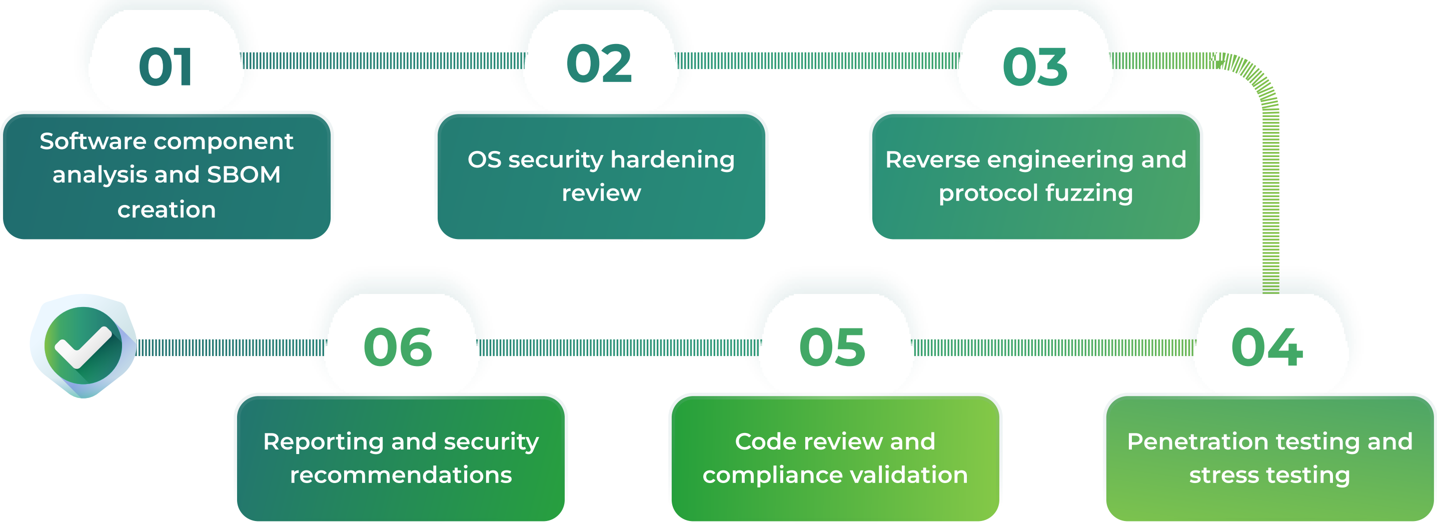
Reverse engineer

Project manager

QA experts

After analyzing the client’s request, we decided to execute this assessment in six steps:

6 steps of the automotive system security assessment



01 Software component analysis and SBOM creation

02 OS security hardening review

03 Reverse engineering and protocol fuzzing

04 Penetration testing and stress testing

05 Code review and compliance validation

06 Reporting and security recommendations

Step 1: Software component analysis and SBOM creation

Our first step was to run a fundamental analysis of the client’s connected vehicle communication system and its components.

First, we performed automated vulnerability scanning of the system. This allowed us to identify outdated and unpatched components in the client’s AVCS.

Then, our specialists designed a comprehensive software bill of materials (SBOM) for the system. Having an SBOM will provide our client with better visibility into all components, libraries, and dependencies that comprise their product and streamline future assessments.

Step 2: OS security hardening review

The client’s platform had several operating system hardening features that required a separate in-depth audit. Our quality assurance experts checked that essential security mitigations were enabled properly, which is crucial to prevent unauthorized system access and reduce the attack surface yet keep the overall performance of the system at an acceptable level.

Step 3: Reverse engineering and protocol fuzzing

The client’s system also had an integrated custom feature with poor documentation, which made traditional testing methods not efficient enough. Leveraging our reverse engineering expertise, we analyzed this feature’s functionality and uncovered potential security flaws that standard testing methods would have missed.

Our team also fuzz-tested critical business logic and communication protocols to identify cases that could lead to unpredictable behavior or system crashes.

Step 4: Penetration testing and stress testing

To evaluate the ability of the client’s AVCS to withstand potential cyber threats, we conducted penetration testing that simulated various attack scenarios.

For pentesting, Apriorit experts used the STRIDE model. Focusing on the threats most relevant and critical for our client, we composed a precise list of test case scenarios, approved it with the client, and only then proceeded with testing the system.

Additionally, we tested the product for resilience against DDoS attacks and stress-tested network nodes to assess their ability to handle high traffic loads and denial-of-service attacks.

Step 5: Code review and compliance validation

As part of our security audit, the Apriorit team conducted a code review for MISRA C compliance, helping the client detect and address issues that could impact the reliability and security of their codebase. We also performed an automated scan for CWE Top-25 vulnerabilities across both source code and compiled binaries to identify high-risk security weaknesses.

Additionally, Apriorit experts examined system configurations and data exchange operations for compliance with ISO/SAE 21434 and NIST security requirements.

Step 6: Reporting and security recommendations

Once all assessment operations were finished, the Apriorit team composed a detailed security audit report, providing the client with:

- A comprehensive overview of all detected vulnerabilities
- Prioritization of detected security risks along with an evaluation of their potential impact
- Guidance for mitigating each identified issue
- Additional suggestions for further improving system security

The recommendations provided as part of the security audit can serve as guidelines for future improvements, helping the client improve code quality, enhance firmware security, and maintain their platform’s regulatory compliance.

We also included all information about the applied testing and analysis methodologies and our risk rating approaches in the report.

The impact

As a result of our work, the client received two detailed documents:

- **An SBOM** to easily track and manage software dependencies, thus reducing the risk of unpatched vulnerabilities in future updates to their AVCS.
- **A security assessment report** to get a clear picture of current system vulnerabilities, their potential impact, and optimal mitigation strategies and prioritize further cybersecurity efforts accordingly.

Satisfied with the quality of our services and impressed by our ability to analyze even poorly documented features, the client decided to continue working with Apriorit and tasked us with implementing suggested security improvements within their vehicle communication system.

Need expert security audit or penetration testing of your automotive software?

Apriorit's quality assurance and security professionals will help you detect and mitigate cybersecurity risks, ensuring strong data protection, seamless system performance, and compliance with industry security standards.