HANECS

DRIVING CYBERSECURITY: PROTECTING THE FUTURE OF CONNECTED VEHICLES

Project Description

We specialize in securing connected vehicles, employing cutting-edge security protocols. Our efforts target vulnerabilities across communication networks, firmware, and software. Our comprehensive approach encompasses threat modeling, secure communication, and reprogramming—all while adhering to the ISO-21434 standard. A pivotal aspect of our role involves providing extensive assistance in automotive cybersecurity, tailored to meet the unique specifications of individual Original Equipment Manufacturers (OEMs). Our unwavering commitment remains: safeguarding vehicles and ensuring a secure mobility future.

Industry
Automotive

Customer
Global leading company for automotive and aerospace

Keywords
Software Development, Cyber Security, Automotive, SecOC

Solutions

At HANECS GmbH, we bring a profound understanding of embedded software development to the table. Our track record speaks for itself: we've seamlessly integrated numerous features, including enabling internal Hardware Security Modules (HSMs), implementing essential Security Access features, and ensuring robust Secure On Board Communication (SecOC) and Secure Reprogramming capabilities in our clients' projects.

But that's not all. We go beyond the code. Our commitment extends to supporting our clients by automating Cybersecurity tests for their project's current features. We tailor our solutions to meet the unique requirements of Original Equipment Manufacturers (OEMs), ensuring a secure and efficient development process.

Tools

- Renesas MCU
- PTC Integrity
- ETAS ISOLAR-AB
- Eclipse/VS-Code
- dSpace SystemDesk
- Lauterbach Trace32
- Vector CANoe
- Confluence
- MISRA