Security by design - establishing a cybersecurity framework for a new vehicle

Case study overview

A major off-highway machine OEM approached HORIBA MIRA for support in establishing a cybersecurity framework for a concept machine. Connectivity lay at the heart of this new technology demonstrator, along with the latest advanced driver assistance and safety features. It therefore needed to be designed from the outset to provide a secure architecture that would be futureproof in a rapidly evolving market.

This project represented a step change in the level of connectivity offered by the manufacturer. HORIBA MIRA's expertise minimised the risks associated with this transition and helped to establish self-sufficiency for future projects.

Engineering team deployed: Project lead plus three other consultants based in Nuneaton, UK.

Cybersecurity and vehicle electrical architecture

Off-highway machines

UK

This is a rapidly evolving field, so being able to tap straight into an experienced team who could turn it around in a short space of time was hugely beneficial for the client.

Paul Wooderson, Chief Engineer for Cybersecurity
HORIBA MIRA

Approach

After discussions with HORIBA MIRA, the decision was taken to align the manufacturer's existing cybersecurity framework with the ISO/SAE 21434 standard used for road vehicles. The work began in the concept phase by analysing the system architecture and its functionality, identifying the assets that needed to be protected. Next, the team worked through identifying potential damage scenarios, threat scenarios and the potential entry points.

Armed with this knowledge, a risk assessment was performed, looking at both the likelihood of the various attack scenarios and the severity of their consequences. Combined, this process is known as TARA (Threat Analysis and Risk Assessment). Based on the TARA, cybersecurity goals and requirements were specified and documented in a cybersecurity concept.

Having worked with a broad range of different cybersecurity projects over more than 15 years, HORIBA MIRA already had extensive knowledge of relevant threat scenarios that it was able to include in the analysis. The team also brought a tried and tested approach that iteratively manages cybersecurity risk of the product throughout the project. Based on the success of the first project, work has continued into a second phase that spans cybersecurity specification, vulnerability analysis and a cybersecurity verification plan for future testing.

Successes and benefits

The first part of the project has seen the cybersecurity architecture pass through the concept phase and into initial development. Notable successes so far include:

- ✓ **Strategic planning** and architecture definition based on ISO/SAE 21434
- ✓ **Comprehensive** threat analysis and **risk assessment**
- ✓ Definition of **high-level cybersecurity** goals for the vehicle, based on that analysis, to minimise security risks
- ✓ **Definition** of the **cybersecurity requirements** that will need to be met by suppliers

Deliverables

- ✓ Item definition
- ✓ Threat analysis and risk assessment
- ✓ Cybersecurity concept
- ✓ Cybersecurity specification
- ✓ Vulnerability analysis
- ✓ Cybersecurity verification plan for future testing

HORIBA MIRA Ltd. Watling Street, Nuneaton, Warwickshire, CV10 0TU, UK
+44 (0)24 7635 5000 I www.horiba-mira.com/enquiries