ROKE

RICARDO

Digital resilience

a partnership between Ricardo and Roke

Digital Resilience Vehicle Assessment and Benchmarking

Helping our clients to understand and resolve potential vulnerabilities in their products ensuring the physical safety of end users and their data protection and making vehicles fit for the challenges of connected and autonomous mobility

Legislation is on its way

International regulations and legislation for vehicle cybersecurity are currently under development by the United Nations Economic Commission for Europe (UNECE). This is expected to include:

- the mandatory audit of a vehicle manufacturer's cybersecurity management system
- verification that a new vehicle has been appropriately engineered with relevant risks identified, analysed and mitigated

In future, these are likely to be required before a vehicle manufacturer is able to gain type approval for a new vehicle.

An OEM now needs to be able to demonstrate that it has considered the risks of, and taken measures to prevent, accidents or theft of personal data in the event of a cybersecurity breach. This is a board level responsibly.

Digital Resilience Vehicle Assessment and Benchmarking at our testing facility in Shoreham-by-Sea

Digital Resilience Vehicle Assessment and Benchmarking

✓ Independent assessment which draws on the recommendations of the 5StarS vehicle assurance framework and the unique methodology developed by the Digital Resilience partnership

✓ Identifies potential vulnerabilities which may be exploited by a threat agent, now and in the future, and provides an indication of the implications for driver safety and personal data protection

✓ Indicates how vulnerabilities can be addressed with immediate and cost-effective remedial action

✓ Provides recommendations of how vulnerabilities can be addressed through improved design practices

✓ Gives valuable early insight to OEMs of how secure their product is and how it compares within the market against a stable benchmark test criteria

✓ Gives an early indication of where the vehicle might sit in future insurance-led assessment criteria

For further information:

E: enquiries@digitalresilience.info **W:** https://digitalresilience.info/ **Tel:** +44 (0) 1794 833 100

Digital Resilience Vehicle Assessment and Benchmarking Process

✓ Test and fix
✓ Secure by design
✓ Assurance and functionality

The Digital Resilience Vehicle Assessment process is a tiered approach, addressing a variety of test categories (described bottom right) and providing increasing levels of sophistication tailored to meet the needs of our clients. During the assessment, we help clients understand the risks of any potential vulnerabilities identified and offer further support to address them. We use our benchmarking database to provide an objective assessment of where clients stand with respect to competitors.

Vehicle Assessment Tiers

Baseline Assessment

We identify and categorise potential vulnerabilities that may be exploited and provide indication of their implications for driver safety and personal data protection. The Digital Resilience level is ranked with respect to competitors' data and a cost-effective fix is recommended.

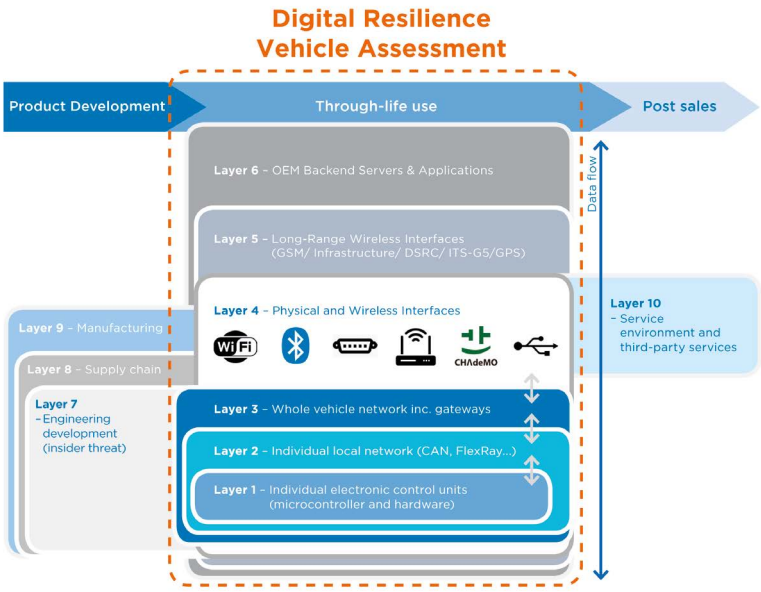
Enhanced Assessment

In addition to the baseline assessment, we conduct penetration testing to exploit identified vulnerabilities to assess potential impact of a successful breach. The testing boundary is the same as the baseline but more physically intrusive and may include the analysis of OEM backend servers and applications.

Bespoke Assessment

A fully bespoke level of analysis tailored to the client's requirements.

Testing tailored to suit our clients' requirements



The 'attack surface' of a modern car

Digital Resilience Vehicle Assessment Test Categories

ECU Analysis

Attack surface layer 1

Analysing the resilience of embedded software systems to malicious manipulation

Subnetwork Analysis

Attack surface layer 2

Analysing the resilience of subnetwork communications to malicious manipulation

Vehicle Network Architecture Analysis

Attack surface layer 3

Assessing the resilience of vehicle network architecture design

Physical and Wireless Interface Analysis

Attack surface layer 4

Assessing the implementation of local communication interfaces

Long-Range Interface Analysis

Attack surface layer 5

Assessing the implementation of long-range wireless communication interfaces

OEM Servers and Applications Analysis

Attack surface layer 6

Investigation of accessibility from OEM servers and mobile applications