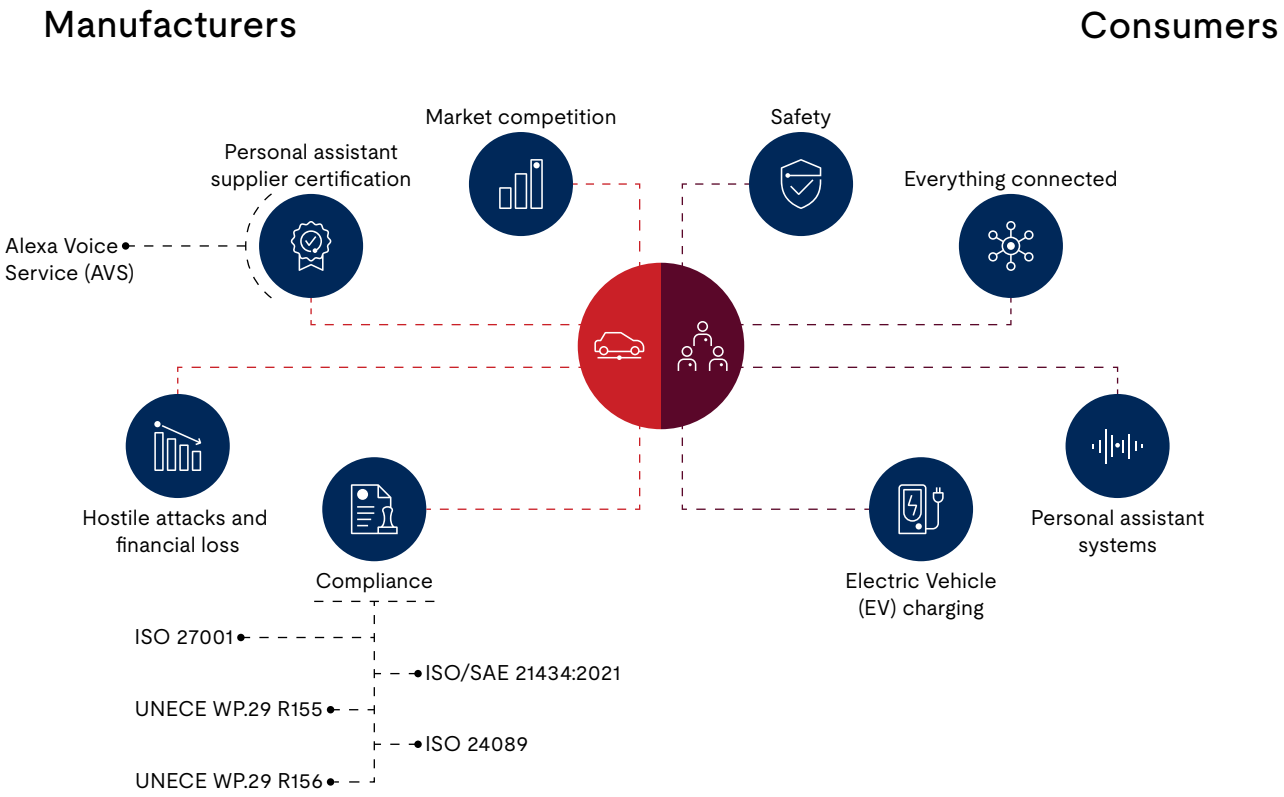
Automotive cybersecurity

Advances in automotive technology introduce increased cybersecurity risk

Automotive technology is evolving rapidly from infotainment systems and operational sensors to mobile app integrations and full driving automation. Modern vehicles have up to 150 electronic control units and 100 million lines of code. By the year 2030, many observers expect them to have roughly 300 million lines of software code. In comparison, mass-market personal computer software has close to 40 million. While each line of code and point of connectivity enhances functionality and usability, they also introduce the risk of breaches and cyberattacks.

Interconnected products and systems can be targeted by attackers who manipulate software vulnerabilities and weak links in ecosystems. In automotive, a cyberattack introduces additional risk to public safety, which is why building cybersecurity into connected products and systems is crucial to the safe adoption of modern automotive technologies.

Automotive cybersecurity trends and challenges



Collaborate with UL Solutions

Your cybersecurity journey along the automotive product development life cycle

01 Advisory

- Understanding the automotive cybersecurity landscape

02 Training

- Understanding regulatory and standard requirements

03 Gap analysis

- Identifying cybersecurity risks and gaps
- Mitigating risks and gaps by strengthening cybersecurity posture

04 Certification

- Achieving regulatory approval and market access
- AVS

05 Lifecycle management

- Maintaining secure operations during the entire life cycle

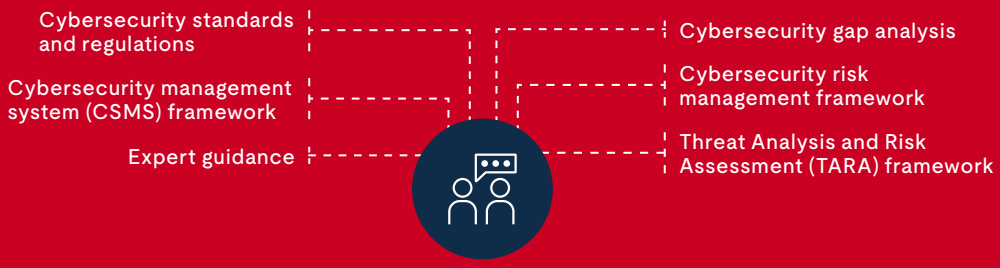
Time to market | **Benchmarking** | **Brand protection** | **Risk and cost control**

Automotive cybersecurity solutions

- Provide guidance and support to original equipment manufacturers (OEMs) and automotive component and system manufacturers
- Navigate complexity and develop a framework for automotive cybersecurity standards and best practices
- Help you identify and manage software vulnerabilities and cyber risk

I need to understand and implement automotive cybersecurity standards and best practices.

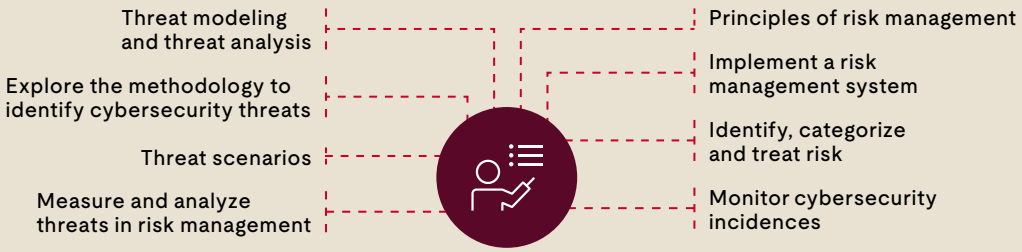
Automotive Cybersecurity Services – Analyze risk, mitigate threats, maintain compliance and train your team to address cybersecurity for your modern automotive innovations.



Automotive Cybersecurity Services
UNECE WP.29 | ISO/SAE 21434

I need to level up my automotive cybersecurity knowledge.

Automotive Cybersecurity Training – Apply cybersecurity principles, processes, the necessary standards and requirements to reduce the cyberthreats risk to automotive products and systems.



Automotive Cybersecurity Training
ISO/SAE 21434 | UL Certified Cybersecurity Professional in Automotive or UL-CCSP

How mature is our cybersecurity? How to succeed?

Automotive Cybersecurity Auditing and Testing – Uncover product and software exploitation risk and validate that security measures align with industry requirements, including ISO/SAE 21434 and WP.29.

Automotive Cybersecurity Auditing and Testing
ISO/SAE 21434 | UNECE WP.29

Why UL Solutions for cybersecurity?

- Independent, trusted third party
- Full life cycle solutions
- Hardware- and software-based security evaluations
- Assessment of security development practices
- Cybersecurity expertise
- Industry knowledge
- Cybersecurity and safety
- Global teams and local support

Cybersecurity foundation

- Expertise in global standards and frameworks
- Extensive knowledge of best practices
- Growing list of Internet of Things (IoT) security solutions

Learn more and speak to one of our experts today at UL.com/automotive-cybersecurity.

UL Solutions

UL.com/Solutions

IMS23CS705800
057.01.0323.EN.CYB