Connected automobiles require trust

We help you innovate secure vehicles.

Trusted guidance in navigating automotive cybersecurity compliance

Today, automobiles, trucks and vehicles do much more than their intended use of transportation. From infotainment systems to operational sensors to mobile app integrations, the automobile has become a modern technology hub. But with each connected innovation, the risk of breaches and cyberattacks increases.

Cars 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.[1]

That's where UL helps original equipment manufacturers (OEMs) and automotive component and system manufacturers test and verify security certification compliance. Through expert gap analysis, advisory services, cybersecurity and interoperability testing, and more, we aid in building trustworthy connectivity and achieving faster approvals, which can lead to improved market access across the globe.

Cybersecurity across automobile connectivity

We work with OEMs and component manufacturers across a myriad of connectivity compliance areas.

- Dual-band Wi-Fi
- GPS/Global Navigation Satellite System/BeiDou
- 4G/5G cellular connectivity
- Infotainment center
- Cameras
- Subscription-based communications
- Vehicle to everything (V2X)
- Maintenance cellular radio system
- Tire pressure monitoring
- Remote keyless entry and ignition
- Onboard diagnostics
- Light detection and radar
- Bluetooth

CONNECTED VEHICLE MARKET is expected **to grow** **14%** **to $122.5B** (U.S.) by 2023[2]

Expert understanding cybersecurity requirements

With over 500 security experts located internationally, UL services customers globally with our industry-leading, working knowledge of automotive regulations and compliance. We serve as task force participants and advisors on several standards groups and industry consortiums, such as the International Organization for Standardization, the UN Automotive Harmonization Forum and more. Our insights with these groups allow us to efficiently and proactively work with you to help plan, test, verify and modify components to gain authority approvals necessary for vehicles to be on the road.

Automotive cybersecurity regulations and standards we service:

- UNECE WP.29
- ISO/SAE 21434
- Singapore Standards Council Technical Reference 68 for Autonomous Vehicle

VEHICLE SOFTWARE is expected **to grow 7%** to $469B (U.S.) by 2030[2]

Our comprehensive automobile cybersecurity solutions can help improve market access and build trust in your brand

Training
We offer courses to help engineers and developers gain a better understanding of security processes, related standards and the impact on the automotive industry.

- Automotive cybersecurity best practices
- Principles of risk management
- Threat modeling and analysis

Verification and validation
Our security experts perform invasive and noninvasive penetration tests of components and systems based on vulnerability analysis and management.

- Cybersecurity audit
- System testing
- Component testing

Advisory
Our advisory and gap analysis looks at cybersecurity management systems against WP29 regulations and ISO/SAE 21434 requirements. We then provide detailed documentation to assess and design road maps and frameworks to work toward compliance.

- Gap analysis
- Cybersecurity management systems framework
- Software update management systems framework
- Risk management framework
- Threat analysis and risk assessment framework
- Cybersecurity incidence monitoring and evaluation
- Supply chain management

Regulatory compliance
We look at overall digital homologation and offer guidance on market regulations and compliance requirements for target markets. We also provide up-to-date access to evolving regulatory information.

- Cybersecurity management systems audit and assessment
- Software update management system audit and assessment

Ready to innovate secure, trustworthy automotive components?
Start a gap analysis today or learn more at ul.com/automotive-cybersecurity.

Empowering Trust®

[1] *Source: McKinsey, "The race for cybersecurity: Protecting the connected car in the era of new regulation," October 2019.*
[2] *Counterpoint Research*
[3] *Source: McKinsey, "Mapping the automotive software-and-electronics landscape through 2030," July 2019.*