Understand automotive cybersecurity

Training and certification for security professionals in automotive

Course overview

With the rising role of electronics in automobiles, cybersecurity has increasingly become a critical aspect of product design and development. To improve awareness of cybersecurity threats, this two-day course is designed to help engineers, developers, project leaders and quality managers gain a better understanding of security processes, related standards, and their impact on the automotive industry. During the training, UL's expert instructors will walk through exercises and examples to show attendees how requirements and concepts of various standards are applied, including SAE J3061, ISO/SAE 21434, and Automotive SPICE®.

Training topics

- Cybersecurity general concepts
  - Attack descriptions, from servers through embedded to automotive
  - Terminology
  - Risk assessment models
  - Type of attacks and countermeasures
  - Threat models – theory and exercise
- Cybersecurity countermeasures in the embedded ecosystem
  - Available countermeasures on the automotive domain
  - Cybersecurity assurance
    - Features analogies between the payments industry and connected technologies
- Regulations and standards
  - Introducing different organizations that regulate the automotive world (CC, SAE, ISO, UNECE)
  - Introducing the SAE J3061, ISO/SAE 21434, and Automotive SPICE® standards
- Cybersecurity in the automotive industry
  - Automotive attack surfaces and countermeasures
  - Supply chain cybersecurity
  - Risk and cyber threats in the automotive industry
  - Cybersecurity in automotive – theory and exercise

Optional UL Certified Cybersecurity Professional Exam

Participants who complete the two-day training are eligible to take a two-hour certification exam on the afternoon of the second day. Those who pass the exam are individually certified as a *UL Certified Cybersecurity Professional* in Automotive or *UL-CCSP*.

Upon the successful completion of the *UL-CCSP* exam, participants will receive a certificate and badge that they can use to demonstrate their competence in cybersecurity for automotive systems. The certification is good for three years, after which individuals may recertify.

Objectives

Upon completion of this workshop, you will be able to:

- Have an improved awareness of cyber threats and of the necessity to include cybersecurity in all stages of a product development
- Become familiar with real life attacks in the automotive domain
- Define the state of the art in terms of security in the embedded and automotive ecosystems, and the main cybersecurity concepts, e.g. assets, threats, threat agents, attacks, attack vectors, attack surface, vulnerabilities, risks, mitigations, etc.
- Gain an overview and understanding of existing threats, e.g. STRIDE, PASTA, etc. and risk assessment models, e.g. DREAD, CVSS, OWASP, etc.
- Establish a threat model (assets/process/threats/interactions identification)
- Understand the contents and purpose of the ISO/SAE 21434, SAE J3061, and Automotive SPICE® standards, and have a good overview on the regulatory ecosystem regarding cybersecurity in automotive
- Determine that augmentation of connectivity means wider attack surface, and that augmentation of a vehicle's autonomy means increased risk and worse consequences

Target audience

- Engineers of organizations involved in engineering design and development of automotive electrical and electronic systems and sub-systems
- Experienced developers, project leaders, quality managers, and testers who are developing secure components in automotive that will be based on the ISO/SAE 21434 standards
- Managers seeking a better understanding of the cybersecurity of automotive electronic systems and the SAE J3061, ISO/SAE 21434, and Automotive SPICE® standards
- Quality and safety professionals intended to be engaged in ISO/SAE 21434 compliance

Why choose UL?

From materials testing to supply chain management, new energy options to security and interoperability solutions, leverage our expertise and insights to navigate the global regulatory landscape and bring your products to market.

UL's global network of technical experts and state-of-the-art facilities, along with our longstanding relationships with regulatory authorities, partner laboratories and industry technical leaders, helps manufacturers gain the compliance credentials they need to compete in a more complex global supply chain.

Knowledge you can trust – Our experienced staff will support you from the initial design stage of product development through testing and production. Our experts can assist you in understanding the certification requirements for your specific markets.

Speed and efficiency – Our cost-effective systems and state-of-the-art facilities cut through the red tape and help accelerate your time to market.

Single-source provider – UL meets all of your compliance needs and, by bundling safety, performance and interoperability services, also helps save you valuable time and money.

Global reach and access – Our global network of expert engineers helps you understand the various national and global requirements for your specific market application.

For more information, call 1.864.630.5373, email: kvasales@UL.com or visit kvausa.com.

Empowering Trust™