AUTOMOTIVE CYBERSECURITY STANDARDS
ISO/SAE 21434 & UNECE WP.29

OVERVIEW

It is well known that the modern connected vehicle is already heavily connected and therefore vulnerable to cyber threats. As we look towards the future, the automotive industry is driving with the pedal to the metal toward Advanced Driver Assisted Systems (ADAS) and fully autonomous vehicles. Connected and autonomous vehicles promise safer and less expensive travel for billions of people the world over. OEMs, dealerships, aftermarket parts and service providers, application developers, insurance companies, fleet operators, governments and a multitude of other players are focused on the direction of this market that is developing faster than an Indy car in the straightaway. The road ahead is not entirely clear, but the industry is accelerating toward an exciting future of both connected and autonomous mobility.

GuardKnox’s solutions empower the auto industry with the FREEDOM TO EVOLVE to meet the changing needs of connected vehicles safely and securely

At GuardKnox, we have determined that the key enabler for securing not only the vehicles of today, but also the vehicles of the future is automotive cyber security. Without it, the next generation of vehicles will not be safe enough, nor our personal information protected enough, to make it to the next intersection.

We see a future of vehicle cyber security standards that will at once:

• Protect our personal information
• Improve the safety of our vehicle and our driving
• Enable plug-and-play capabilities between a wealth of new products and services
• Cut the costs of vehicle and fleet ownership, use, and maintenance
• Make our road-travel experience more convenient and enjoyable

We see the standardization committees and the standards which they publish as key partners as we push towards a safer, more connected, innovative, and personalized tomorrow.

We, at GuardKnox, have outlined the key takeaways in both the ISO/SAE 21434 and UNECE WP.29 below, in order to better understand the current state of automotive cybersecurity standards.

For further questions please visit www.guardknox.com or email us at Quality@guardknox.com
The ISO/SAE 21434 standard is a joint working group between ISO and SAE to create a comprehensive and robust worldwide standard for automotive cybersecurity. It addresses the entire vehicles lifecycle from concept to decommissioning and also lays out requirements and activities on an organizational level.

**Overview**

ISO/SAE 21434

**Organization Cybersecurity Management**

Requirements and definitions which are organizational (OEM and Tier 1) and lays out roles and processes. These requirements cannot and should not be outsourced as it may have significant financial and business implications in case of an incident.

**Project Cybersecurity Management**

Portrays activities & guidelines to be implemented & observed on a per-project basis. Many of these can be supported by external contracts (such as security engineering), collaborations (pre-dev projects) and support. These requirements extend to Tier supplier as the OEM alone does not have full visibility and ownership of deliverables.

**Product Cybersecurity Activities**

Lays out & defines work products, activities & relations between them. These address full product lifecycle from concept to decommissioning as well as all aspects of the vehicle from E/E design to component level. It must be incorporated into the existing development cycle & cannot be done in retrospect. deliverables.

**Compliance**

Certification is done on a per-project basis. The standard effectively mandates security by design, meaning, it covers every aspect from the E/E to component level. It also means that all the tier and sub-tier suppliers work products must comply with the standard requirements. It must be stressed that compliance with the standard is an engineering effort intertwined with existing product activities and cannot be achieved through traditional outsourced consulting work.

**ISO/SAE 21434 Standard Overview**

- **Overall Cybersecurity Management**
- **Project Dependent Cybersecurity Management**
- **Continuous Cybersecurity Activities**
- **Risk Assessment Methods**
  - Concept Phase
  - Product Development
  - Cybersecurity Validation
- **Production**
- **Operational Maintenance**
- **Decommissioning**

**Distributed Cybersecurity Activities**
UNECE WP.29
OVERVIEW

The UNECE WP.29 is a baseline for automotive cybersecurity and mandates the necessities for having a secure connected vehicle. Although not as broad or comprehensive as ISO/SAE 21434, it is expected to be mandated by regulation in all major markets much sooner.

WP.29 refers mainly to the following topics:

- **GOVERNANCE**
- **SECURITY BY DESIGN**
- **SOFTWARE UPDATES**
- **MONITORING**

**ISO/SAE 21434 RELATION**
UNECE WP.29 addresses several specific cybersecurity topics and is inclusive to ISO/SAE21434. If a system is compliant with ISO/SAE 21434 it is highly likely to be compliant with UNECE WP.29 as well requiring only the submission of evidence.

**COMPLIANCE**
For in-vehicle components the standard specifically mentions topics to be taken into consideration on Annex 5, which is a comprehensive but not a complete list of threats to be assessed. Governance and organizational requirements are largely the responsibility of the customer much like it is in ISO/SAE 21434.

All GuardKnox products are secure by design and therefore are compliant with the regulation (ISO 21434 and the UNECE WP.29). Topics which are not in-vehicle related (such as monitoring) are achieved through partnerships to provide the customer with a complete solution.
GUARDKNOX INVOLVEMENT: ISO/SAE JOINT WORKING GROUP

It took 20 years for seat belts to become common in vehicles, but we don’t have 20 years for cybersecurity standards to evolve.

GuardKnox was and still is an active member of the ISO/SAE joint working group, ISO-TC22-SC32-WG11, the working group tasked with creating ISO-SAE 21434: Road vehicles – Cybersecurity Engineering.

SAFETY IS A TOP PRIORITY

Whenever they are connected to the outside world, vehicles require cyber security. Connected vehicles resemble IT networks and, as such, are open systems, i.e., open to communications from the outside anytime. However, safety-critical functions in the same vehicles must be treated like closed systems, just like fighter jets and other military-grade systems. While open systems must be updated constantly with the latest threat intelligence and rules, closed systems must be impervious to attack at all times. They are air-gapped and protocol- and technology-agnostic. They do not rely on threat intelligence updates or after-the-event incident response.

GuardKnox’s Communication Lockdown™ methodology eliminates risks to the safety of the vehicle, enforcing a formally verified and deterministic configuration of communication among the various networks within the vehicle.

GUARDKNOX

GuardKnox is the first Cybertech Tier supplier of secure, high-performance computing platforms for the software-defined and service-oriented vehicle. The company’s pioneering approach to automotive innovation is inspired by technology from the missile defense systems and aviation industry. The leadership team at GuardKnox have vast knowledge and experience in both Military and high-tech industry fields, with multiple degrees in the Electrical/Electronic/Software Engineering and Computer Sciences. The experience of the GuardKnox team in developing and testing cybersecurity for military systems places them in a unique position to now apply these solutions to address similar challenges for ground vehicles.

GuardKnox is based in Israel, with subsidiary locations in Stuttgart, Germany, and Detroit, Michigan.