GUARDKNOX

AUTOMOTIVE CYBERSECURITY STANDARDS
ISO/SAE 21434 & UNECE R155

The shift to next-generation E/E architectures and the software-defined vehicle where vehicles offer drivers a new layer of personalization and connection is here. OEMs are providing drivers with added capabilities, altering their driving experience from simply getting from point A to point B to becoming part of a connected environment. These advanced features and access to OTA updates can cause a vulnerability threat to the internal systems in the car, ultimately harming the safety and security of drivers, passengers and others on the road.

An OEM's biggest challenge today is not only securing one domain or attack vector to prevent casualties, rather securing the entire software system to ensure safety and security for everyone on the road. In a future where software is the focus, cybersecurty needs to be built from the ground up.

AT GUARDKNOX

We are determined to meet the changing needs of software-defined vehicles and connected vehicles. To do that, security must be built from the ground up and not as an afterthought.

For the next generation of vehicles to provide high-performance, personalized, customizable functioning even in safety-critical systems, automotive cybersecurity must be at the forefront.

WE SEE A FUTURE OF VEHICLE CYBERSECURITY THAT WILL

- 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

quality@guardknox.com | www.guardknox.com

FREEDOM TO EVOLVE

FREEDOM TO EVOLVE

ISO/SAE 21434 OVERVIEW

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.

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.

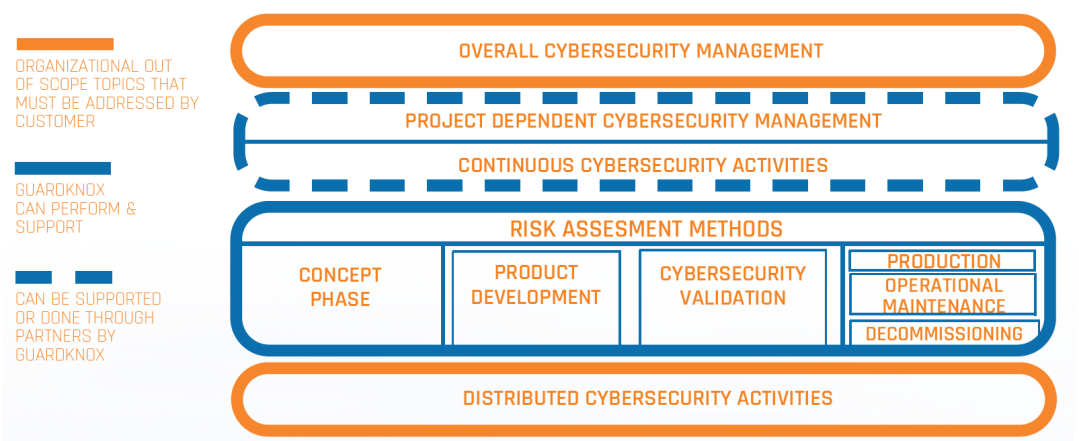
PROJECT CYBERSECURITY MANAGEMENT

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 suppliers 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.

ISO/SAE 21434 STANDARD OVERVIEW



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 subtier 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.

quality@guardknox.com | www.guardknox.com

FREEDOM TO EVOLVE

UNECE R155 OVERVIEW

The United Nations Economic Commission for Europe is a regulatory body that develops vehicle regulations that are applicable to the 62 member countries of the UNECE 1958 agreement.

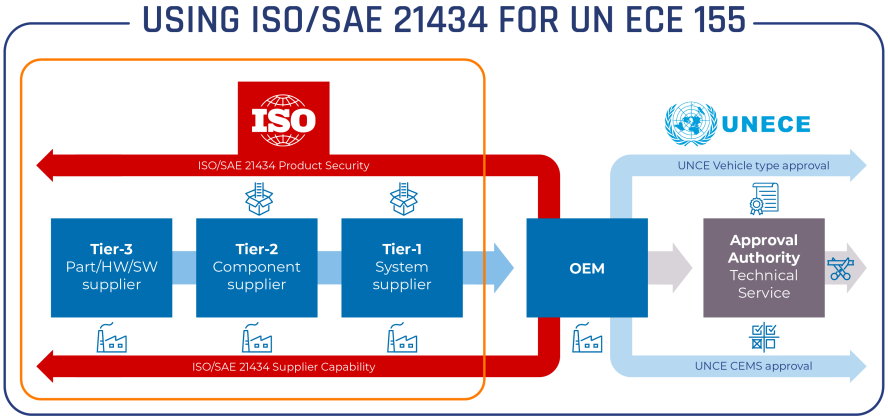
UNECE R155 introduces stricter cybersecurity requirements that each OEM must fulfill in making sure their own operations are fully compliant. While UNECE R155 only applies to OEMs, each one is fully responsible for collecting evidence from their suppliers to prove that they are fully compliant with the regulation.

UNECE R155 requires OEMs to implement a CSMS consistent of:

- SECURITY MANAGEMENT & GOVERNANCE
- RISK MANAGEMENT
- INCIDENTS & VULNERABILITIES
- SUPPLY CHAIN INTERACTION

ISO/SAE 21434 RELATION

One way to comply with UNECE R155 is to implement ISO/SAE 21434. Its scope allows OEMs to define Interfaces and security requirements for its suppliers (CID – Cybersecurity Interface Document) and ensure that every link in the supply chain is compliant. The cybersecurity standard was developed using the same structure and includes what OEMs need to fulfill the CSMS requirements of UNECE R155. If an OEM's supplier is already compliant with ISO/SAE 21434, the OEM will have an easier time adhering to UNECE R155 requirements.



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.

quality@guardknox.com | www.guardknox.com

FREEDOM TO EVOLVE

GUARDKNOX PRODUCT COMPLIANCE

GuardKnox is in-vehicle focused and is augmented for off-vehicle requirements by a large number of partnerships. GuardKnox can provide the customer with a complete and certified solution. All GuardKnox products employ security by design and therefore can be certified to the standard.

Every GuardKnox design is aimed at being semi-formal verifiable, the equivalent of Common Criteria EAL5 and the proposed ISO/SAE 21434 CAL4 rating (Annex E) which is the highest level. Be advised that unlike safety, security is not the sum of its parts, no work product can be certified on its own without context. No supplier can provide a certified product that does not require anything (verification or analysis) on the OEM side to ensure that after integration the system as a whole remain secure.

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. 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 is proud to be fully ISO/SAE 24134 certified, meeting the highest standards for automotive cybersecurity.

Contact us to learn how GuardKnox can help you secure the in-vehicle communication to adhere to UNECE R155 requirements before the regulation goes into effect in July 2024.

quality@guardknox.com | www.guardknox.com