ISO/SAE 21434

Setting the Standard for Connected Cars' Cybersecurity

The expectations of the functions and usage of today's automobiles are changing as connectivity drives the demand for more modern features. In response, the automotive industry is quickly churning out more connected cars, adjusting their development and production cycles to accommodate the market. Unfortunately, the speed of adoption has put a significant amount of stress on the cars' development phases, with an increased dependence on software that affects users' cybersecurity and safety.

IN BRIEF

Recognizing this growing need, more than 80 enterprises and organizations related to the automotive industry participated in drafting **ISO/SAE 21434 "Road vehicles – Cybersecurity engineering."** The standard describes how a culture of cybersecurity can be established to keep up with the technological changes and attack techniques deployed by malicious actors. In the heels of the standard's implementation, the industry recognizes that this could result in legislative changes that would force industry players to keep up.

The document highlights the need for the industry to establish an environment that consciously implements cybersecurity practices across all its phases through governance, policies, tools, and procedures to address expected and unknown threats. Companies are expected to intentionally plan their subsequent vehicle designs and features around this standard. While making no specific recommendations for compliance, the standard, which applies to road vehicles, presents the following benchmark principles for all vendors in the automotive industry:

- Ensure system security for cars that are released to the market
- Ensure that automakers and suppliers can perform due diligence
- Focus on cybersecurity engineering based on current technologies and methodologies
- Adopt a risk-oriented approach
- Use the standard as a basis for management activities for cybersecurity
- Identify guidelines for cybersecurity activities and/or processes for all phases of the vehicle's life cycle

OUR RECOMMENDATIONS

The tools and methods applied by the cybersecurity industry today can be contextualized for the automotive industry's use. Continuously assessing, managing, monitoring, sourcing, and analyzing known and unknown threats and vulnerabilities from the current automotive ecosystem are just some of the techniques that can reinforce a secure environment. We recommend using a layered approach able to provide comprehensive contexts for events from each system as they happen; securing connected vehicles to reduce the probability of successful attacks and intrusions; and mitigate any impact of successful attacks. By holistically enhancing the security of connected cars from conceptualization to decommissioning, the automotive industry can empower users and their products with comprehensive protection through proven solutions that support connected car management, execute uniform control throughout the systems' phases, and defend against attacks that target the vehicle, the networks, and the backend.

Read "ISO/SAE 21434: Setting the Standard for Connected Cars' Cybersecurity" for more information and highlights of the standard's guidelines, as well as our recommendations.

TREND MICRO | research