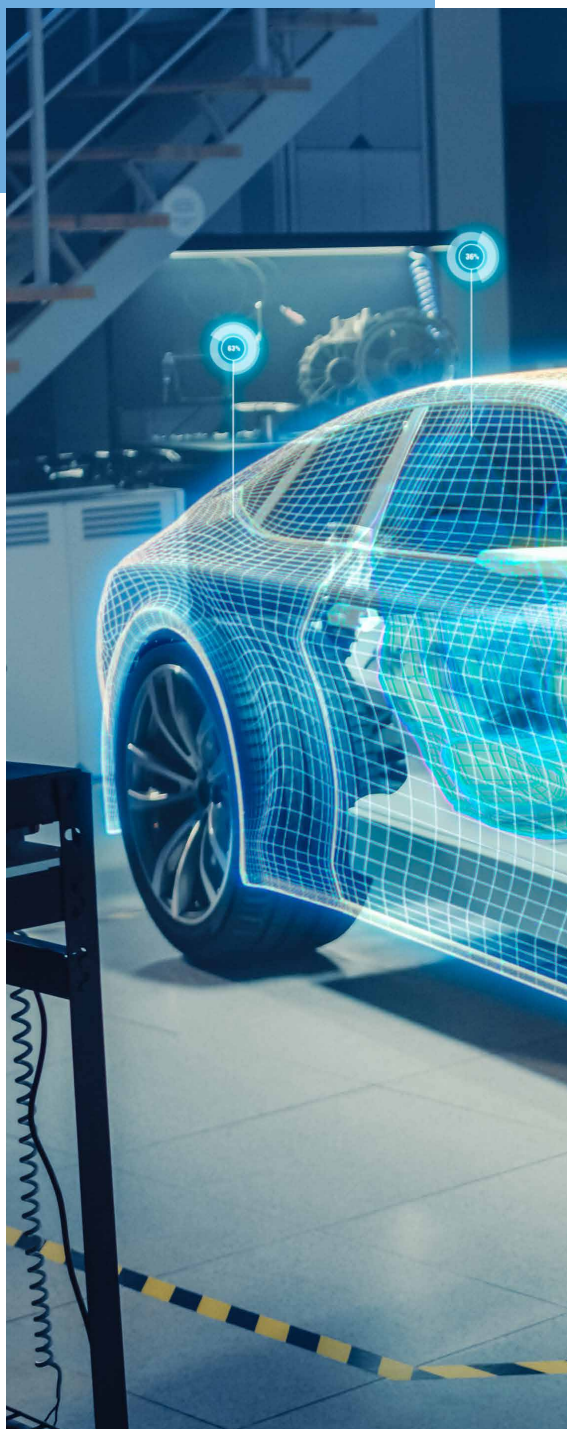
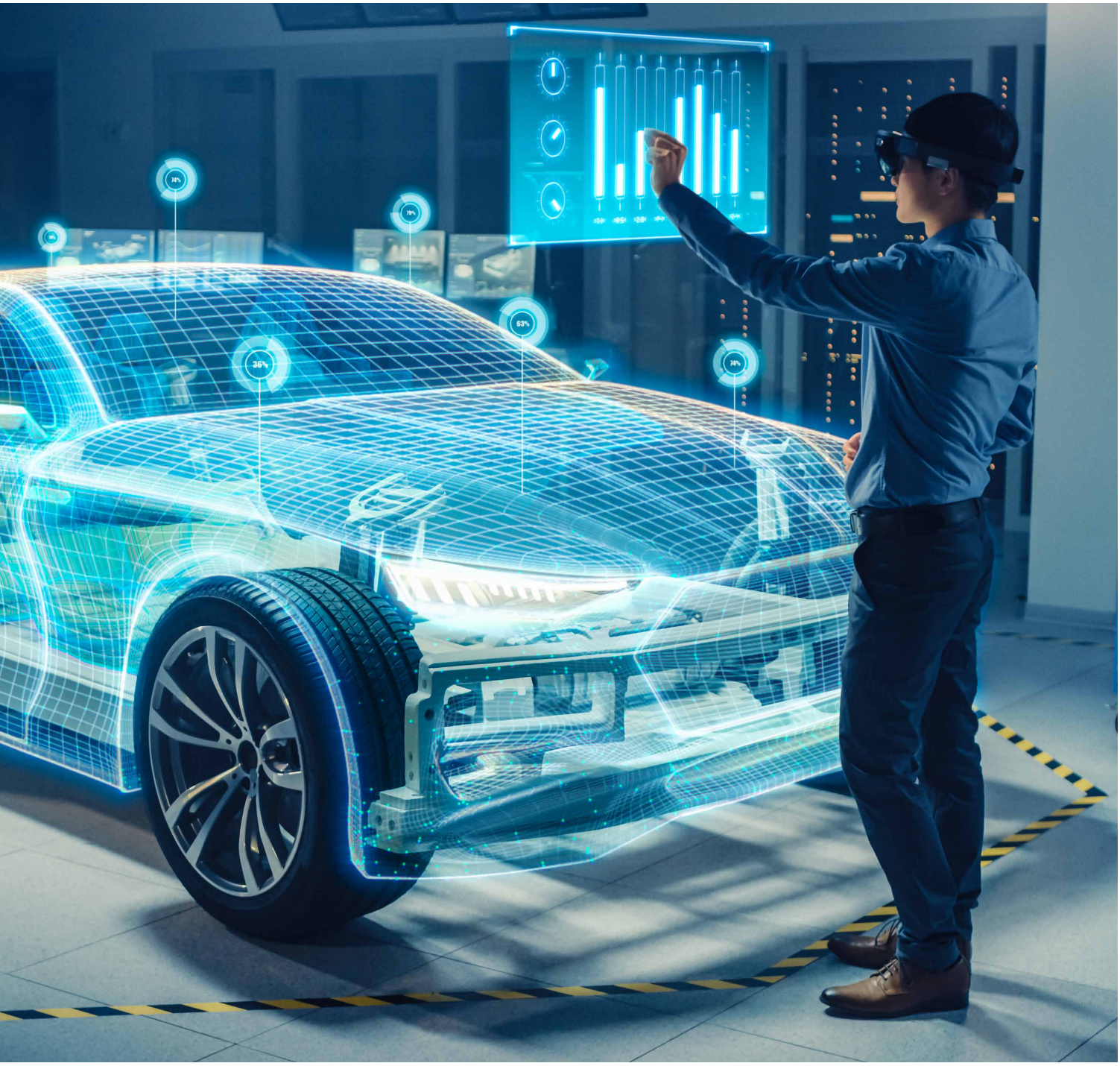
VEHICLE SECURITY ESSENTIALS

ACCELERATING THE SHIFT FROM SECURITY-THROUGH-OBSCURITY TO SECURITY-BY-DESIGN



The introduction of a new security regulation and standard is the latest step to accelerate the shift from security-through-obscurity to security-by-design. Until recently, vehicles had limited or no means to connect with the outside world other than with key fobs for doors, audio streaming with mobile devices or communication with the manufacturer for emergency services. They have been an island unto themselves, mostly isolated from their environments and the internet, but this is changing fast. Vehicles of all kinds are becoming more connected with cellular networks, as well as Wi-Fi®, V2X and other networks to improve user experience, enable services and increase road safety.

This presents immense cybersecurity challenges because the vehicle and the supporting infrastructure offer broad attack surfaces with appealing targets for all types of threats. Mitigation begins with electronic components in the vehicle and extends to wireless networks and cloud-based data centers. NXP leverages more than a decade of security experience for carmakers to have confidence that our building blocks help ensure safe and secure vehicles of the future. This white paper discusses various cyberthreats to vehicles, emerging standards and NXP's approach to automotive security.



PUTTING TEETH INTO VEHICLE CYBERSECURITY: ISO 21434

The threat from cybercriminals makes traditional ways of protecting vehicles inadequate. Although extremely effective in what they were designed for, best practices leave it to automakers to achieve them any way they see fit rather than based on defined, mandatory rules. Examples of best practices include NHTSA's Cybersecurity Best Practices for Modern Vehicles and Auto-ISAC's Automotive ISAC Best Practices.

Efforts to create an automotive security standard began in 2016 when SAE International and ISO started a joint initiative to create an industry standard for automotive cybersecurity. Both organizations had individually worked on automotive safety and security-related standards in the past. For example, ISO 26262 sets functional safety standards, and SAE J3061, "Cybersecurity Guidebook for Cyber Physical Vehicle Systems," sets the foundation for cybersecurity standards. The two organizations ultimately joined efforts and reached out to automakers, component and subsystem suppliers, cybersecurity vendors, governing organizations and more than 100 experts from more than 82 companies in 16 countries.

The result was ISO/SAE 21434. It provides a well-defined cybersecurity framework and establishes cybersecurity as an integral element of engineering throughout the life of a vehicle from concept through decommissioning. The standard lays out clear organizational and procedural requirements throughout the entire vehicle lifecycle, from concept and development to production, operations and maintenance and finally decommissioning. It calls for effective methods for fostering a cybersecurity culture, including cybersecurity awareness management, competence management and continuous improvement, as well as close collaboration throughout the supply chain. It also specifies a threat analysis and risk assessment (TARA) methodology to identify and determine potential threats, feasibility and impact.

ISO/SAE 21434 establishes cybersecurity engineering baselines for connected vehicles and addresses the engineering of electrical and electronic systems. By ensuring appropriate consideration of cybersecurity, the standard aims to enable the engineering of these systems to keep up with evolving technologies and attack methods. Similarly, ISO 24089 establishes baselines and requirements for software update engineering.

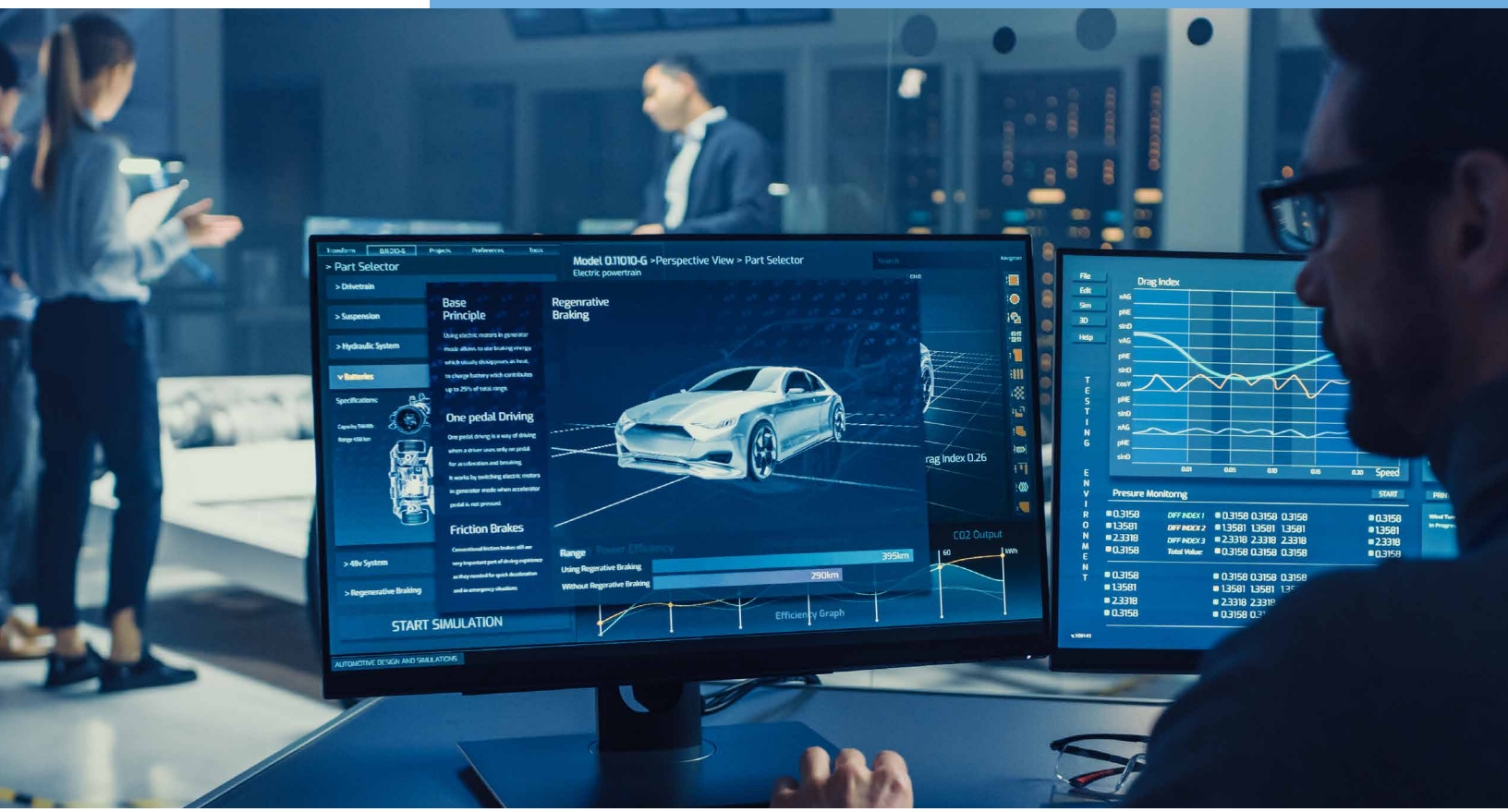
Another critical step in increased automotive cybersecurity took place in the form of two new automotive requirements, UN R155 for cybersecurity and UN R156 for software updates. The requirements were adopted in 2020 by the United Nations Economic Commission for Europe (UNECE) WP.29, also known as the World Forum for Harmonization of Vehicle Regulations. These regulations require OEMs to have Cybersecurity Management (CSMS) and Software Update Management (SUMS) systems in place. They require measures to be implemented for managing vehicle cyber risks; for securing vehicles by design to mitigate risks throughout the value chain; for detecting and responding to security incidents; and for providing secure software updates over the air. It is generally recognized that ISO/SAE 21434 and ISO 24089 can be very supportive in implementing the requirements on the CSMS and SUMS to the organizations along the supply chain.

A NEW TAKE ON AN OLD PROBLEM

Susceptibility to security threats is not new for the auto industry. When the on-board diagnostics (OBD) port was added to vehicles in the 1990s, it provided access to the engine's management systems. Back then, hacking a vehicle required expensive hardware, physical access to the port, and proprietary software — but there were still those willing to attempt it. In contrast, the increasing susceptibility of vehicles to hacking has a potentially large impact. Cyberattacks are far more easily achievable today, less expensive and can potentially be carried out remotely on not just one vehicle but on an entire fleet at once, from almost anywhere.

The increasing susceptibility of vehicles to cyberthreats has not been lost on automakers and national governments. The adoption in 2020 of the new cybersecurity regulation (UN R155) by UNECE's World Forum for Harmonization of Vehicle Regulations and the publication of the final ISO/SAE 21434 standard in 2021 demonstrate this concern and provide a pathway for manufacturers to follow in the years ahead.

Automakers must build vehicles that satisfy regulatory requirements. And with this new security regulation, automakers will be required to demonstrate adequate cyber-risk management practices throughout vehicle development, production, operations and maintenance, including the ability to implement over-the-air software security patches while the cars are in use.



THE AUTOMOTIVE SECURITY LANDSCAPE

A vehicle can be considered "connected" when it shares data or when certain functions are controlled via remote servers, mobile apps, communications networks or cloud-based data centers. At first glance, it might seem that few vehicles today meet the requirements of this definition, but in reality, every new vehicle is connected in some way right now. A vehicle is considered "connected" when a driver uses a smartphone to operate features such as the ability to create Wi-Fi hotspots, open doors, start the vehicle remotely or perform other functions.

Electric vehicles also routinely connect to cellular networks to locate charging stations, perform billing and other activities, and are typically connected to the manufacturer's back-end data systems for over-the-air updates and additional services.

In short, today's vehicles easily meet the criteria for being connected, and this is just the beginning as autonomous vehicles are connected by definition and will remain continuously connected to cellular and other networks to provide new levels of safety. All these sources, and others, are potential entry points for hackers.

These entry points have certainly caught the attention of hackers and security researchers alike. The world has seen several presentations of hacks on vehicles and their components at security conferences in the past few years. Also, a dedicated "Car Hacking Village" was first launched at DEF CON® in 2015, to build a community around discovering weaknesses and exposing vulnerabilities in automotive systems. This initiative was quickly adopted by and replicated at several other security conferences.

Vehicles are also a potential goldmine for cybercriminals; they have already played havoc even before most vehicles were fully connected and before they become partially or fully autonomous. The risk is also recognized by government agencies. For example, the FBI issued a Public Service Announcement in 2016 indicating that motor vehicles are increasingly vulnerable to remote exploits. More recently, they reported that hackers have been able to successfully target and infiltrate the systems of some American automotive manufacturers and that technology-enabled vehicle theft continues to pose risks to automotive industry stakeholders.

Furthermore, the increasing amount of data vehicles generate and share is a growing privacy concern for regulators.

CONTINUE READING THIS FREE WHITEPAPER

Get free Whitepaper (16 pages, PDF)

HACKERS AT WORK IN 2020: THE TOP 12

4,118 vehicles were stolen using cheap devices that allowed the thieves to bypass the ECU, unlock the vehicle, start the engine, and access the vehicle's computers.

A hacker **fooled the ADAS and autopilot systems** of the Mobileye 630 Pro and Tesla Model X to trigger the brakes and steer into oncoming traffic.

Hackers **reverse-engineered a vehicle's TCU** and using its telematics connection to hack into an automaker's corporate network.

19 vulnerabilities were found in a Mercedes-Benz E-Class vehicle that let hackers control the vehicle remotely, including opening its doors and starting the engine.

Hackers located passwords and API tokens for Daimler's internal systems after the source code of a connected car were made publicly available.

Hackers offered to sell car rental data for 3.5 million Zoomcar users on the dark Web.

An Australian transportation fleet **was hit twice by ransomware attacks**, affecting 1,000 servers.

More than 300 vulnerabilities were found in more than 40 of an automaker's ECUs that were developed by major companies.

A hacker **gained control over all Tesla vehicles** by exploiting a vulnerability in the company's servers.

Cars worth more than $400,000 were stolen in Russia by hackers disabling alarms and imitating key fob signals.

In Poland, **34 vehicles worth more than $1.6 million were stolen** using keyless entry systems

More than 60 vehicles worth more than $1.2 million were stolen by hacking their computers to allow access, start the engine, drive away.