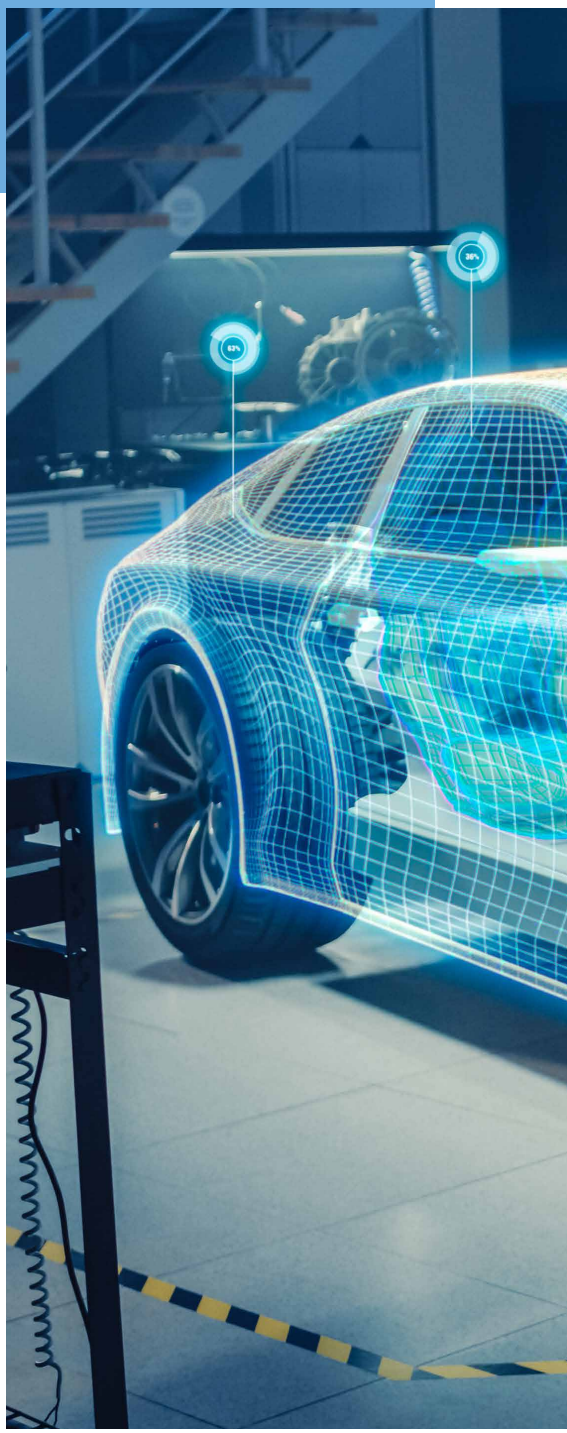
VEHICLE SECURITY ESSENTIALS

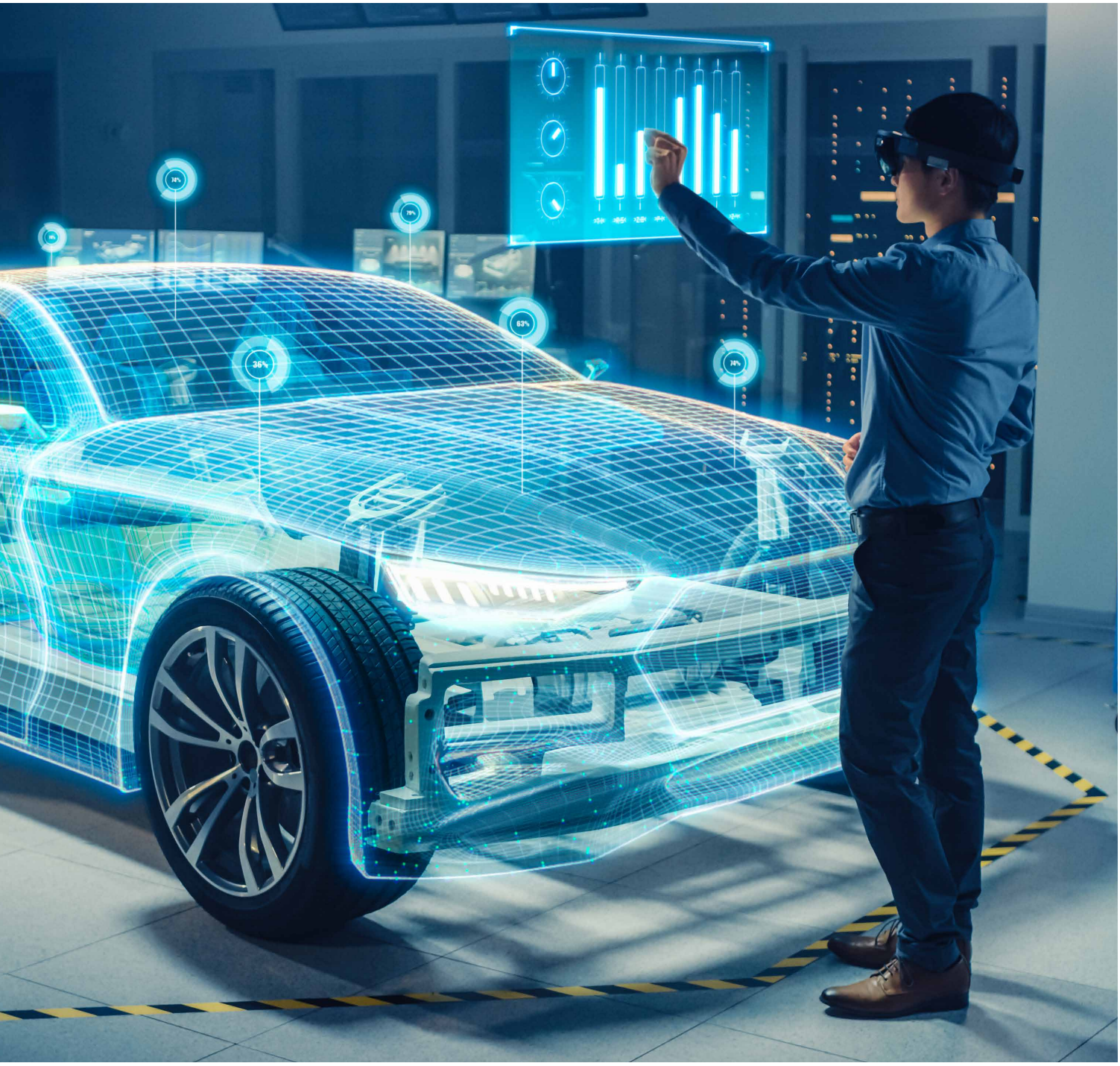
ACCELERATING THE SHIFT FROM SECURITY-THROUGH-OBSCURITY TO SECURITY-BY-DESIGN

NXP



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.

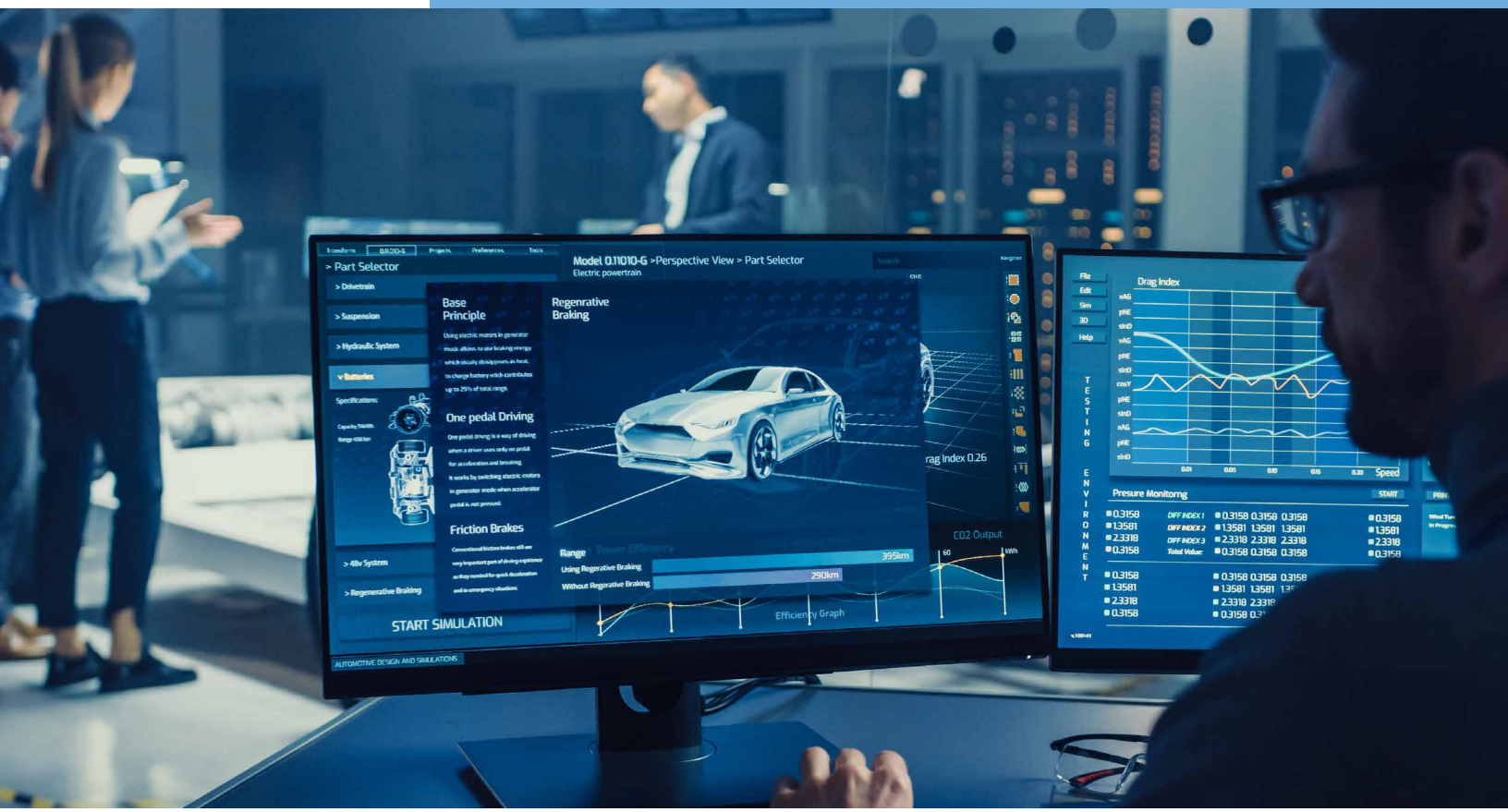
Another critical step in increased automotive cybersecurity took place in the form of two new automotive requirements, UN R155 for cybersecurity and UN R156 for software updates. The requirements were adopted in 2020 by the United Nations Economic Commission for Europe (UNECE) WP.29, also known as the 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.

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.

HOW HACKERS GET IN

Cyberattacks can be remote or local. Local attacks require the hacker to physically connect to the vehicle systems and components to hack them, while remote attacks can be orchestrated at short range a few steps away from the vehicle or long-range from anywhere in the world via the Internet.

Also the most common attack vectors today are cloud services, keyless entry systems, and mobile apps. Cloud attacks represent more than a quarter of attacks seen today, followed by keyless entry systems. Together, they represent at least half of all vulnerabilities, more than all others combined. Cloud attacks involve compromises to telematics command-and-control servers, database servers, web servers, and others to and from which data from the vehicle is sent for analysis.

Traditional keyless entry systems, which automatically unlock the vehicle when the key fob is in proximity can be another potential attack vector. The key fob is always broadcasting a very low power signal to tell the vehicle it is close by (or inside, for starting systems), while the car is always looking for that signal. Attackers in proximity could relay this signal to the real key fob, tricking the vehicle to think that it is within proximity. Newer vehicles are deploying Ultra-Wideband (UWB) for secure ranging, thereby effectively mitigating this risk.

Other recent attack vectors are mobile apps, which are increasingly used not just by individuals but also in over-the-road trucking. Approximately 90% of today's truck drivers have a mobile device with a tracking app; most large fleets have invested heavily in mobile apps to enhance their services. Mobile apps can be used as an attack vector to access the vehicle and the app's back-end servers. This can allow bad actors to obtain a vehicle's GPS coordinates, trace its route, open its doors, start its engine, turn on auxiliary devices, and many other functions.

The back-end servers of telematics service providers, fleet management systems and OEM-provided online services have also been subject to attacks. Such services often enable users to run, analyze and use vehicle-generated data — and even control vehicle systems, significantly increasing the potential damage of an exploited vulnerability.

But it's not only about attacks on cloud services, mobile apps and car access systems. There is also a growing interest from researchers and hackers in the security of electronics and software inside the vehicle. In the last five or more years, several vulnerabilities were found in infotainment systems, sensors, in-vehicle networks and OBD dongles. The real-life impact for end users has, so far, been relatively limited. But the industry has clearly recognized the need to step up here as well.

AUTONOMY UPS THE ANTE

With the increasing levels of autonomy in modern and future vehicles, achieving cybersecurity becomes orders of magnitude more complex, as they wirelessly communicate among themselves and to roadside sensors and wireless networks. The advanced driver assistance systems with their many sensors and advanced algorithms inside the vehicle imply a steep increase in complexity. And also, the infrastructure required to support them is complex, connecting everything from surveillance cameras to street signs, streetlights and traffic signals. An entire city could be hacked from a great distance, with large social and economic impact and potentially harming people.

In short, as vehicles become more automated, they will present cybersecurity challenges that dwarf other types of attacks because of the sheer magnitude of the accidents and harm they can cause even in a small area. The problem is compounded by the fact that once people become confident in letting the vehicle control everything, they will pay little or no attention to driving. If cybersecurity threats become numerous, owners will be much less likely to want partial or fully autonomous vehicles, potentially stalling the intelligent transportation revolution in its tracks.

THE WEB UNLOCKS ECONOMY OF SCALE

The so-called dark web has been a treasure trove of information for years, and today more attention is being paid to tools for automotive cyberattacks. It includes guides for infotainment hacking, CAN-bus reverse engineering, chip tuning and software hacks or illegal upgrades. OEM-related information and credentials stolen in data breaches are also available for a fee on the Dark Web, as are tools for vehicle theft or modification — including key signal grabbers, key-fob programmers and GPS jammers. The market for this adverse hardware and software is growing, and it is available to anyone who knows or can quickly learn how to navigate the dark web.

While criminals prefer using the dark web, others with presumably good intentions are making more and more information publicly available on the internet. It is nowadays relatively easy to find descriptions of proprietary automotive protocols, APIs and more on the web. For example, security researchers and white hat hackers analyze the implementation and security of automotive systems and components and share their findings in conference papers and blogs. Consequently, the collective intelligence is rapidly growing, unlocking economy of scale for hackers. No longer do they need to reverse engineer all of the bits and pieces of a vehicle themselves; instead, they can build on work done by others and focus their own time and efforts on finding weak spots inside these systems. **This also means the industry has to accelerate the shift from security-through-obscurity, to security-by-design.**

PUTTING THE BRAKES ON CAR HACKS

These vulnerabilities have one thing in common: they can exist because vehicles increasingly rely on complex electronics and software. An average connected vehicle is made up of thousands of electronic components. Incidents may happen when there are insecure components within a product's supply chain, as vulnerabilities in such components could be exploited by cybercriminals to hack the vehicle or part thereof. Vehicles have complex supply chains involving devices in multiple tiers; a vehicle contains Tier-1 components (such as ECUs and the infotainment system) that contain Tier-2 components (such as chips and software libraries), and so on.

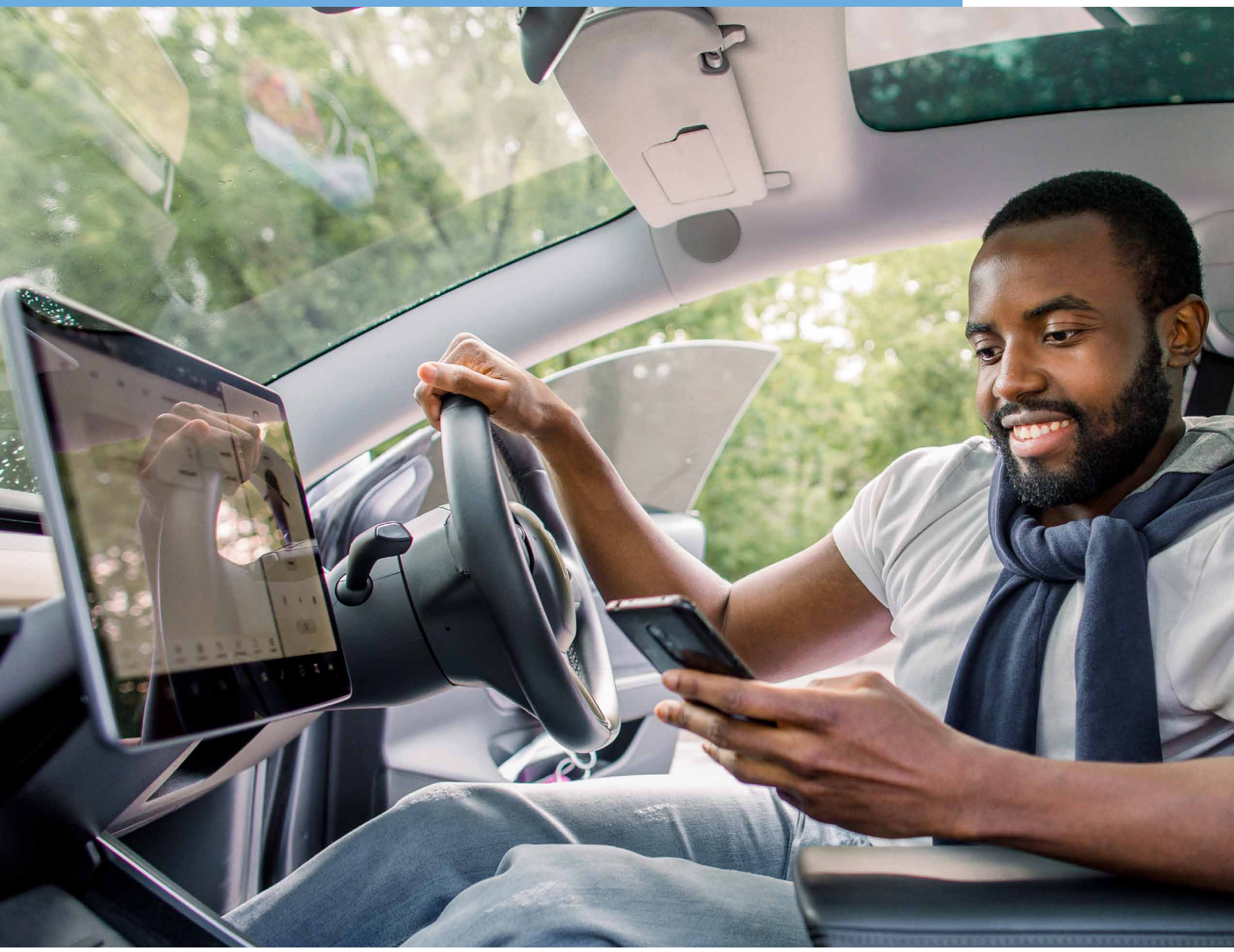
A single vulnerability in any one component in the supply chain can potentially endanger the security of the vehicle. And this is not just theoretical. For example, in 2020, more than 300 vulnerabilities were found in 40 ECUs developed by 10 different companies, while information disclosure and remote code execution vulnerabilities were revealed in a version of software that is widely used for in-vehicle infotainment systems.

The UNECE WP.29 regulation (UN R155) therefore demands that automakers ensure the entire automotive supply chain is secure. It is the automaker's responsibility to manage all risks associated with contracted Tier-1 and Tier-2 suppliers, service providers and other related sub-organizations. This new regulation will be adopted in various regions, starting in Europe, Japan and Korea, together representing more than a third of global vehicle production. Europe is planning to require compliance from July 2022 onward for the approval of new vehicle types and two years later also for existing ones; Japan and Korea plan to follow a similar timeline.

The related ISO/SAE 21434 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. As such, the standard can be very supportive in implementing the requirements of UN R155 in organizations along the supply chain.

In the next few years, as cybersecurity regulations and standards become globally implemented and enforced, OEMs, suppliers and mobility service providers will need to make comprehensive efforts to ensure safe and secure automotive products and services that meet regulators' expectations.

in 2020 more than 300 vulnerabilities were found in 40 ECUs developed by 10 different companies



NXP'S DRIVE FOR VEHICLE SECURITY

NXP has a rich heritage in security. The company's approach to product security is built on these pillars: technology, process, compliance, certification, support and partners.

The company takes a holistic approach to security, across all parts of its organization, based on proven security processes and policies. For example, NXP's IT cybersecurity team works diligently to secure the IT environment in which NXP develops, manufactures and supports its products. Physical site security teams assure the security at NXP's premises, which includes ensuring there is adequate access control and monitoring in place. The approach to IT and site security has been confirmed by independent assessment, and all NXP sites are ISO 27001 certified — and approximately half of those are also Common Criteria certified. This provides the foundation of NXP's product security approach.

Working with experts in the product lines, security teams in the NXP Competence Center for Crypto and Security ensure NXP products have adequate security for their intended applications and systems. The company's vulnerability analysis lab validates the resistance of products, and employees involved in product security participate in NXP's Security School, which provides technical training. NXP also established one of the industry's first Product Security Incident Response Teams (PSIRT).

In the last decade, NXP has adapted its long-standing expertise in security to address the specific needs of the auto industry and has worked with partners in the Automotive Information Sharing & Analysis Center (Auto-ISAC) to align on best practices. More recently, the NXP organization and processes were validated to comply with the new standard ISO/SAE 21434 through an audit by third-party TÜV SÜD. To achieve this, existing policies and extended processes were refined to address the requirements for this new automotive security standard. We also created templates for additional product documentation required by the standard.

Recent automotive product developments already followed a mature security product development process; with the latest improvements, new developments will also fully comply with the new ISO/SAE 21434 standard. For customers, this means they can trust that NXP fulfills the requirements of the standard. This also means its products have been designed with security in mind and have been thoroughly reviewed. It further means that its products achieve an adequate level of security for their intended applications, and supporting evidence is available.

NXP'S SECURITY SOLUTIONS LEAD THE WAY

NXP has decades of experience in automotive security. As early as the mid-1990s, NXP helped reduce vehicle theft by introduction of electronic immobilizers. In 2010, NXP released an automotive MCU that was compliant with the Secure Hardware Extension (SHE) specification. In 2015, NXP began focusing on security for its automotive processors and, among other efforts, released a dedicated automotive hardware security module (HSM). The HSM provides on-chip security for automotive applications to protect software from being manipulated and support secure software updates and data protection.

Automotive processors

NXP's S32 automotive processing platform of MCUs and MPUs provide an architecture that balances performance and power efficiency, as well as addresses current and future connectivity, security and safety challenges. As part of this portfolio, NXP has created vehicle network processors in its S32G family that combine a hardware security subsystem, ASIL-D functional safety, real-time application processing and network acceleration for service-oriented gateways, domain controllers and safety coprocessors. The S32 platform also includes S32R45 radar processors, S32S safe vehicle dynamics microcontrollers and S32K3 microcontrollers for body electronics, battery management and other general purpose applications. Additionally, NXP i.MX 8 processors used for infotainment, instrument cluster, eCockpit and telematics applications feature on-chip security capabilities, including encrypted secure boot, high performance symmetric and public-key cryptography, secure key storage and support for SHE, EVITA and other automotive security specifications.

Today, new automotive processors and microcontrollers that we make include a dedicated hardware security module that is isolated from the rest of the chip. This module, or engine, provides a rich set of security services and platform security functions which it manages independently without impacting the function of the processor or controller. Secure boot and real-time integrity checking schemes verify that the software is authentic, trusted and unaltered. These modules also add more flexibility to how automakers can fix security vulnerabilities, as they enable secure over-the-air updates that let automakers update software after the car hits the road — without a costly recall.

Furthermore, life cycle management mechanisms allow controlled lockdown of some of the controller and processor features. For example, debug and serial download are essential features during vehicle development and manufacturing — but they'd be invaluable tools for hackers if they were accessible on production vehicles. Lastly, our products feature hardware-enforced resource isolation and the latest products furthermore add built-in hardware protection against tampering of clock signals, supply voltage, temperature and power.

Secure CAN transceivers

In addition, as the CAN bus is used universally by all automakers and will continue to be for years, NXP introduced secure CAN transceivers: the TJA115x CAN/CAN FD transceiver family. They provide a cost-effective solution for securing classic CAN and CAN FD communication, offering message filtering capabilities to protect against message spoofing, message tampering and bus flooding. The transceivers also facilitate logging and reporting security incidents on the bus and to the local host.

Secure Ethernet switch

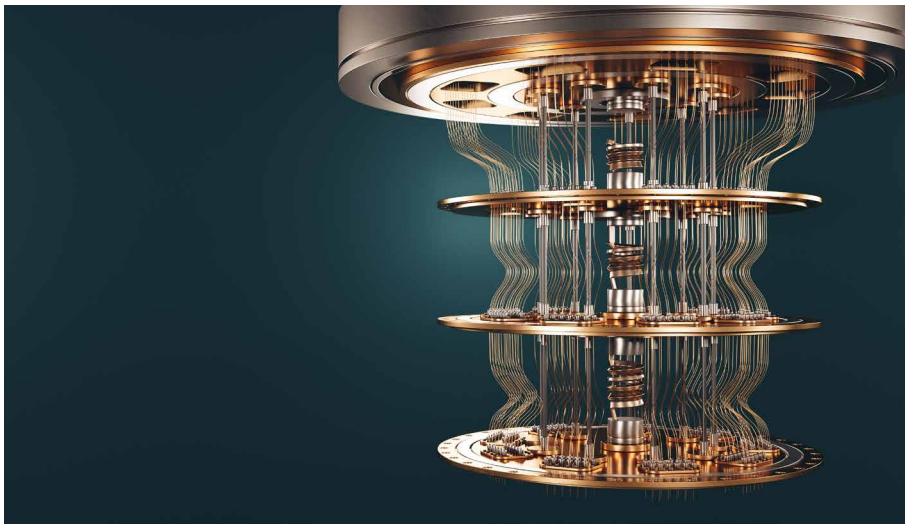
The SJA1110 multi-gig TSN Ethernet switch SoC comes with hardware-assisted security and safety capabilities. The SJA1110 is further optimized to work with our vehicle networking processor to enable distributed firewall and intrusion detection/prevention systems (IDPS) reaching high levels of scalability and performance.

Secure element for V2X communications

Safety is one of the most important goals of V2X communications, and the security of the V2X system plays a significant role in helping to achieve it. Carmakers need to ensure that fake messages sent by malicious actors do not go undetected and that the authenticity of the sender can be verified while preserving privacy. NXP addresses these security demands by leveraging its heritage in secure elements for chip cards and e-passports. NXP's SXF1800 secure element IC for V2X communication is based on a highly secure microcontroller and uses the same security technology that NXP uses to protect mobile payments and also protect ECC private keys used to secure V2X communication. The SXF1800 was the first standalone V2X secure element to receive Common Criteria EAL4+ certification, a prerequisite for participation in a common European V2X system.

UWB technology

NXP is also bringing forward Ultra-Wideband (UWB) technology for use in secure keyless entry systems and other applications. Instead of operating at high power spectral density in a narrow frequency range around a carrier frequency, UWB radio technology transmits at very low power over a wide frequency spectrum. UWB technology enables measuring the time-of-flight of signals propagating between the initiator and the responder. Each range measurement is protected by a set of unique pseudo-random pulse sequences.



One of UWB's distinct benefits is real-time localization capabilities that can be applied in vehicle handsfree smart access systems. When combined with highly secure, unique identifiers, it can protect vehicles from unauthorized access via two-factor authentication. A UWB-enabled vehicle can detect the presence of the owner's key fob or phone, verify their identity and ensure that access is granted if the distance between them is within a pre-defined threshold. This protects the vehicle from a relay attack, making it extremely difficult, if not impossible, to relay the signal to gain access the vehicle.

Secure element for car access

Smartphone-based car access solutions expand the convenience of car access by providing the secure basis required to enable new features like key sharing, multi-car access and configurable driving rights. NXP offers several smart card and secure element solutions for car access. Part of the solution portfolio includes the automotive-qualified NCJ38A secure element (SE), a dedicated hardware and software security architecture implemented with high resistance against physical attacks, which is ideal for securely storing the digital keys needed to unlock and start a car with a smart device.

The NCJ37A secure element for smart fobs stores and manages the digital key and provides the necessary cryptographic functionality to BLE and UWB ICs integrated in the future key fob. In addition, NXP offers an NFC-based smart card digital key solution that can be used as a backup for the car owner when a smartphone-based key is not available, and also serves as a primary car key trusted by the carmaker.

The secure elements together with NFC and UWB solutions enable carmakers to meet the Car Connectivity Consortium's Digital Key Specification, an architecture that is endorsed by the world's leading carmakers, smartphone manufacturers and electronics suppliers.

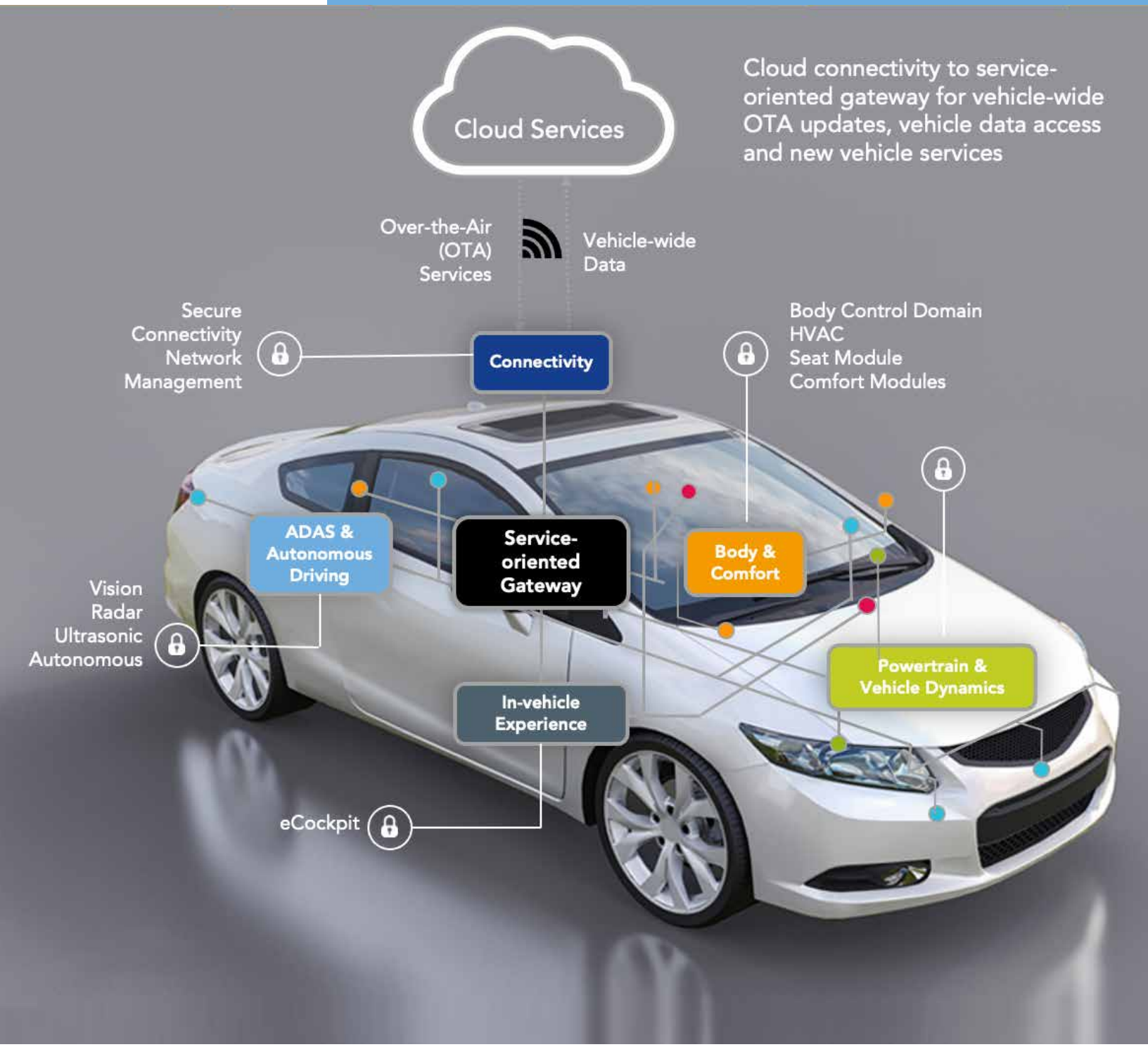
An Eye to the future

NXP has one of the most robust programs for delivering cybersecurity of any semiconductor manufacturer, serving the automotive market and is continually investing in the people, processes, and technology it applies to this challenge — now and in the future.

NXP is exploring emerging technologies such as post-quantum cryptography. Based on quantum-mechanical principles, when combined with unique algorithms, it can solve the mathematically complex problems used in all public-key cryptographic techniques, including RSA and elliptic curve cryptography. A competition for replacing cryptographic standards initiated by NIST in 2016 resulted in four finalists, two of which were designed in partnership with NXP.

Additionally, NXP has prototyped a recovery and damage control system that actively senses and recovers from attacks using machine learning processing at the edge.

As vehicles and smart mobility solutions further evolve with expanding connectivity options and ever-increasing electronics, security innovations must keep pace. In this new environment, our vehicles need more protection than ever before. NXP continues its investment to help carmakers and Tier 1s build security-conscious vehicle architectures.


Cloud Services
Cloud connectivity to service-oriented gateway for vehicle-wide OTA updates, vehicle data access and new vehicle services
Over-the-Air (OTA) Services
Vehicle-wide Data
Secure Connectivity Network Management
Connectivity
Body Control Domain
HVAC
Seat Module
Comfort Modules
ADAS & Autonomous Driving
Service-oriented Gateway
Body & Comfort
Vision
Radar
Ultrasonic
Autonomous
Powertrain & Vehicle Dynamics
In-vehicle Experience
eCockpit

Sources:

"2021 Global Automotive Cybersecurity Report," Upstream Security, 2020

"Global Automotive Cybersecurity Report. Research into Cyberattack Trends in Light of Cybersecurity Standards and Regulations," Upstream Security, 2020.

"How Apps are Changing the Driving Experience," Automotive IQ, 2018

www.nxp.com

Document Number: AUTOCYBERSECWP REV 0