Can we trust our cars?

By Balázs Simacsek, NXP Semiconductors

When we talk about automotive security, most people think about protecting cars from thieves. But with the emergence of automated driving, fast expanding connectivity options and ever-increasing complexity, vehicles are vulnerable to new kinds of cyberattacks. In this new environment vehicles need more protection than ever before.

Table of Contents

What makes our cars vulnerable?

Every day we rely on services and data from the cloud to keep us connected. We want to have the same convenience on the road, so our cars are becoming more connected too. This increases the attack surface (the sum of attack vectors, that represent potential paths for hackers and attackers to exploit vulnerabilities). Every connectivity option represents a potential entry point.

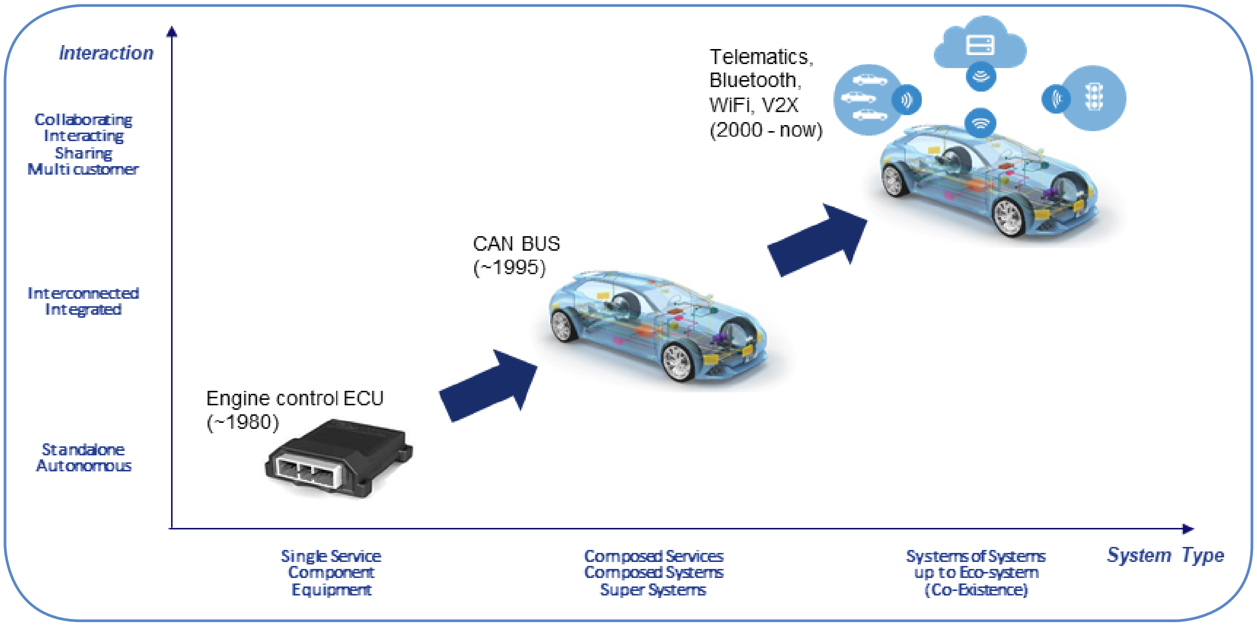
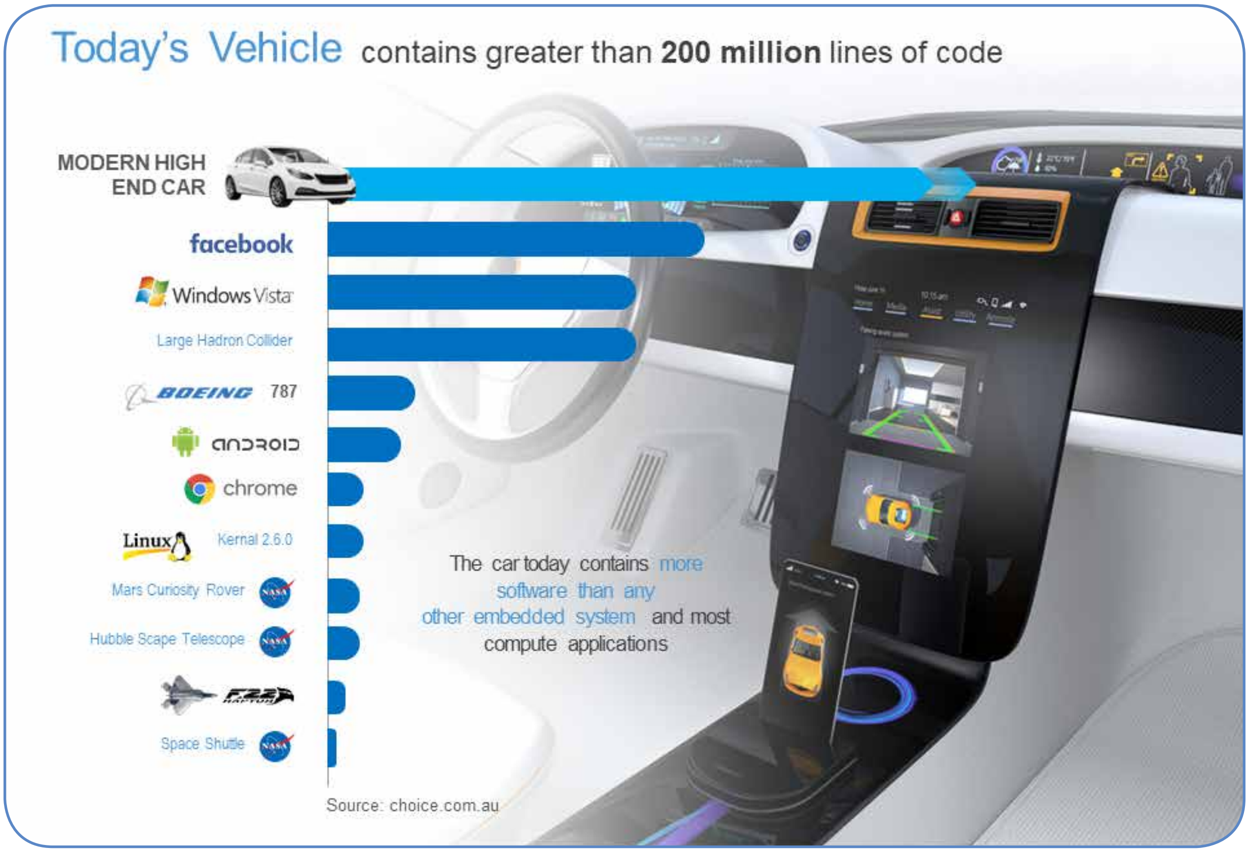


Figure 1 Vehicle Electronics and Security

We also want more safety, comfort and convenience, which increases the complexity of automotive solutions. Most functions of a modern vehicle are controlled by electronic systems. Modern high-end cars have 200+ ECUs (Electronic Control Units) and 200M+ lines of code, making them one of the most complex systems used every day.

Widespread use of fully automated vehicles may seem like distant future, but the threat of taking over the control of our cars is closer than most people think. The famous **Jeep hack** (when researchers took control of a production vehicle remotely from their basement) was three years ago (in 2015) and multiple hacks have been published since then.



The car today contains more software than any other embedded system and most compute applications

Source: choice.com.au

Figure 2 Comparisons of average lines of code

Security is important for more than personal safety

Security concerns are most obvious for self-driving cars, but all vehicles must be protected. Not only do we want to stop hackers from controlling our cars (especially when we sit in them), we also want our cars to be safe from criminals who are looking for ways to take our money (e.g. by installing ransomware).

Privacy is a growing concern, as more and more sensitive information is stored either in the car itself or in the cloud, connected to the car. We use online services, communicate with each other and pay using our credit cards. Cars have access to information about our location, our driving habits and other sensitive information that must be protected. Governments are already taking actions to protect our privacy – for example, GDPR (General Data Protection Regulation) in the EU, CCPA (California Consumer Privacy Act) in California or the SPY Car Act (Security and Privacy in Your Car Act) – but our cars must be smart and secure enough to protect us.

Vehicles are more than just smartphones on wheels. Tons of steel in the wrong hands could be dangerous, and strong security measures must be in place to stop terrorists from taking over the control of our cars and weaponizing it. Transportation is part of our key infrastructure and protecting it must be part of the national security strategy of every country.

Security is a race between attack and protection methods

There is no perfect security, everything can be broken if you have enough resources (time, money, equipment, etc.). In practice protection must be strong enough to convince attackers that it is not worth trying to gain access to the protected asset.

Attackers analyze the cost (money and time spent, required know-how and equipment, risk of being caught, etc.) versus the benefit (stolen goods or data, publicity, etc.) and when the balance is right, they will strike. If an attack can be executed remotely or if it can be scaled easily to a fleet of vehicles, then there is a more attractive return on investment.

Attack methods are improving over time and becoming cheaper, making them more affordable and potentially profitable for criminals and terrorists. Automotive security must continuously evolve as well. This means that car makers must support updateable and upgradeable future-proof security (e.g. Firmware/Software Over-The-Air updates (FOTA/SOTA)) across the vehicle and beyond, together with their suppliers. New vulnerabilities may be found in the field because the race continues long after the car leaves the production line. It must be possible to apply security fixes during the lifetime of the vehicle, which is longer than the lifetime of most other consumer goods.

Many consider security a topic for researchers, which can delay action

The previously mentioned Jeep hack was quickly forgotten (studies show that only half of the people who heard about it, remembered it one year later).

On technology forums, new hacks (and solutions) are being published continuously, but it is still not common for consumers to demand information about the security of their cars at the dealerships. A commonly agreed upon framework to classify the level of security independently and objectively – as it is done for safety – doesn't exist today.

Governments are actively raising awareness, as with the **FBI's public warning on car hacking**, but reaching the right level of consumer awareness for the existing threats and solutions will still take time.

Until now, successful hacks were mostly executed by researchers and industry players themselves, not by criminals or terrorists. But we – the consumers, the industry and society in general – must act now. As we pack future cars with more features and connectivity options for convenience, we must implement the matching measures to ensure security and safety in this more complex, dangerous environment.

Governments and industry players are already working solutions

Car OEMs and their suppliers are defining the security architecture of future vehicle systems and the necessary infrastructure for features like V2X (Vehicle-to-everything communication), cloud services and over-the-air updates. Security is integral part of new designs.

Government initiatives play an important role in assuring the safety of autonomous vehicles, for example, **US DoT, Automated Vehicles 3.0** that focuses on a wide range of automated vehicles from SAE automation level 1 (driver assistance) to level 5 (full automation).

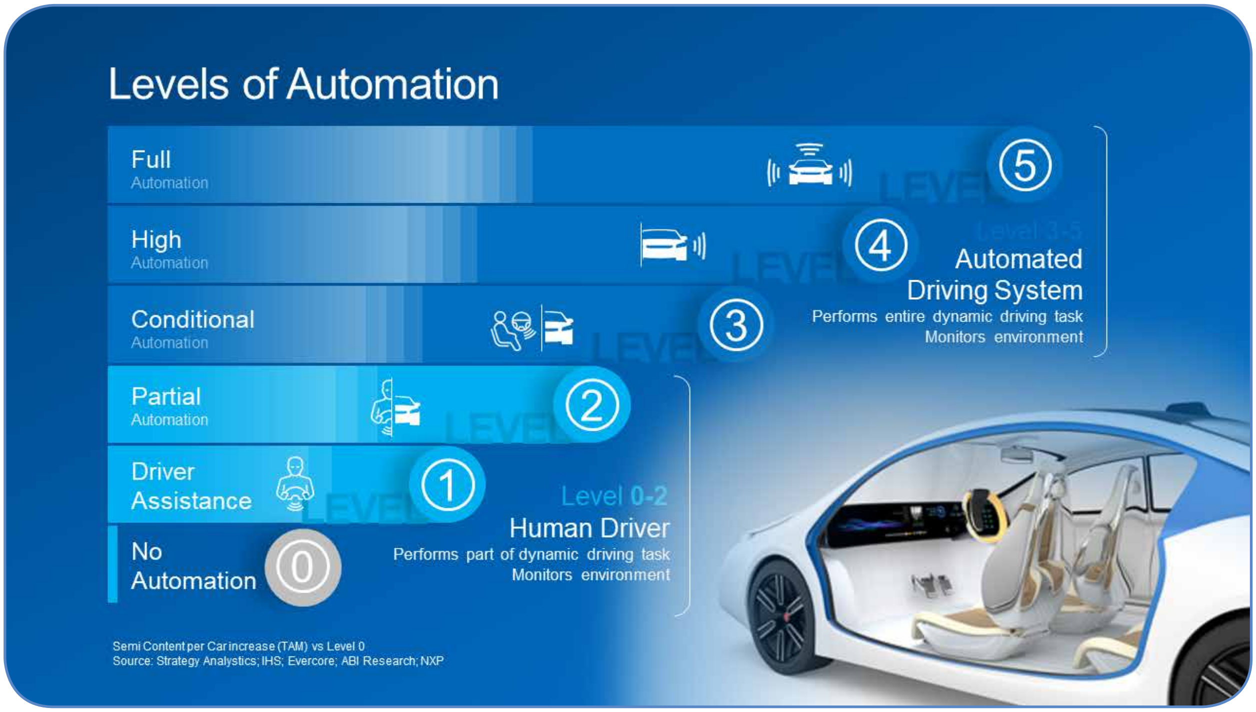


Figure 3 Levels of Automation

Standards are currently being developed. SAE J3061 (Cybersecurity Guidebook for Cyber-Physical Vehicle Systems), published in 2016 describes a process framework that can be used to build cybersecurity into vehicle systems. SAE's Vehicle Electrical System Security Committee is working on SAE J3101 (Requirements for Hardware-Protected Security for Ground Vehicle Applications) to define a common set of requirements. The emerging standard ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering) defines a framework to ensure a consistent, well defined and robust approach to foster a cybersecurity culture, to manage cybersecurity risks across the complete vehicle lifecycle, to allow adaptation to a continually changing threat landscape and to institute a cybersecurity management system. It will thus address security in product engineering, similarly to how ISO 26262 addresses functional safety. ISO/SAE 21434 is scheduled for publication in 2020 and it will likely replace SAE J3061.

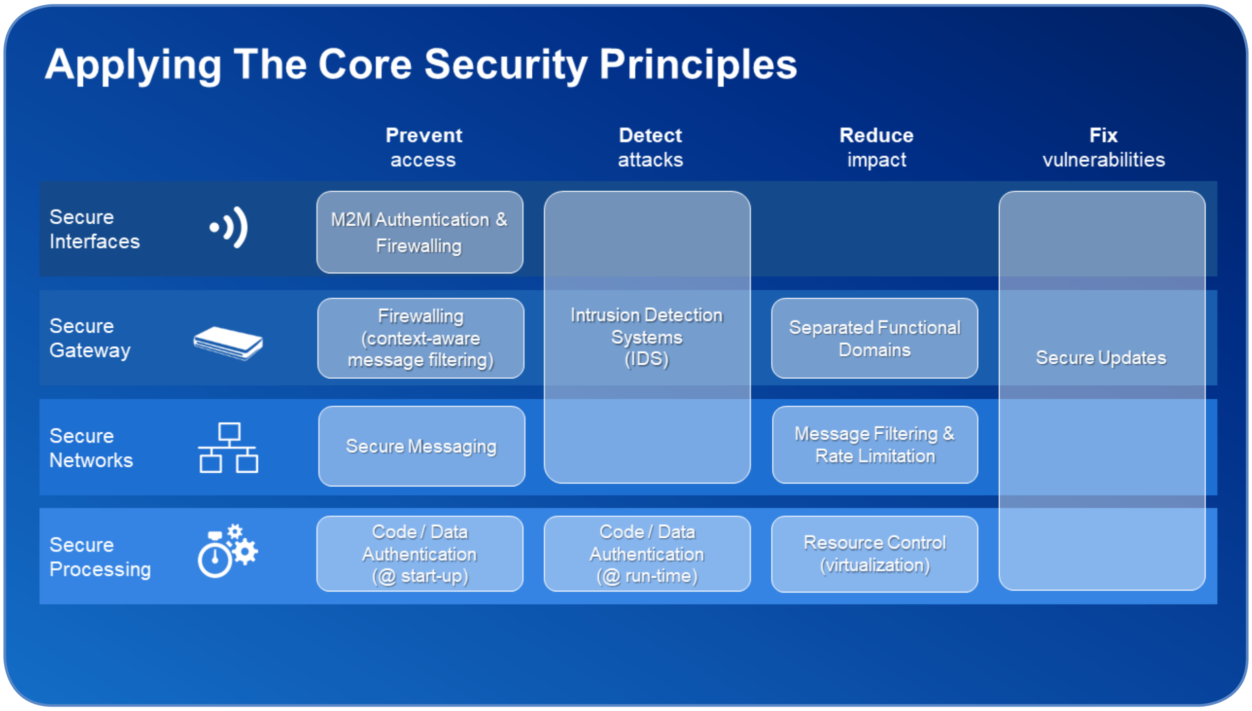
Alliances are formed among vehicle manufacturers and suppliers, providing platforms for developments that require industry-wide co-operation. From the many important forums, one to highlight is **Auto-ISAC**, which is one of the important global cybersecurity-focused communities (sharing intelligence and providing best practice guides) and **C2C-CC** (Car 2 Car Communication Consortium) that focuses on the deployment of Cooperative Intelligent Transport Systems and Services (C-ITS).

Key principles to implement reliable and future-proof automotive security solutions

The industry addresses these security challenges by applying state-of-the-art security principles to automotive design.

Car makers must design and develop end-to-end solutions focusing on the complete system, including also how the cars interact with their environment and other vehicles. A proper security-by-design approach ensures that security is not an afterthought but is designed into every component from day one. The OEM-defined system security concept integrates elements from multiple suppliers, so efficiently driving this system security concept through a complex supply chain is an important element of success.

Another principle that must be applied to all systems is defense-in-depth or multi-layer-security because security in general is only as strong as the weakest link. This means that if one layer of security is breached, the next layer must continue to protect the system. An example: if the infotainment unit is hacked, then the internal firewall will still protect safety-relevant systems like steering controls and brakes from unauthorized access.



Applying The Core Security Principles

	Prevent access	Detect attacks	Reduce impact	Fix vulnerabilities
Secure Interfaces	M2M Authentication & Firewalling	Intrusion Detection Systems (IDS)		Secure Updates
Secure Gateway	Firewalling (context-aware message filtering)		Separated Functional Domains	
Secure Networks	Secure Messaging		Message Filtering & Rate Limitation	
Secure Processing	Code / Data Authentication (@ start-up)	Code / Data Authentication (@ run-time)	Resource Control (virtualization)	

Figure 4 Core Security Principles

As mentioned before, it is important to ensure that the security solutions of a car remain effective during the whole lifetime of a vehicle. Components must have inherent upgrade paths in place to keep the security solutions state-of-the-art and to address potential vulnerabilities that may be found in the future. These upgrades can be applied, for example, at the local dealership or with over-the-air updates.

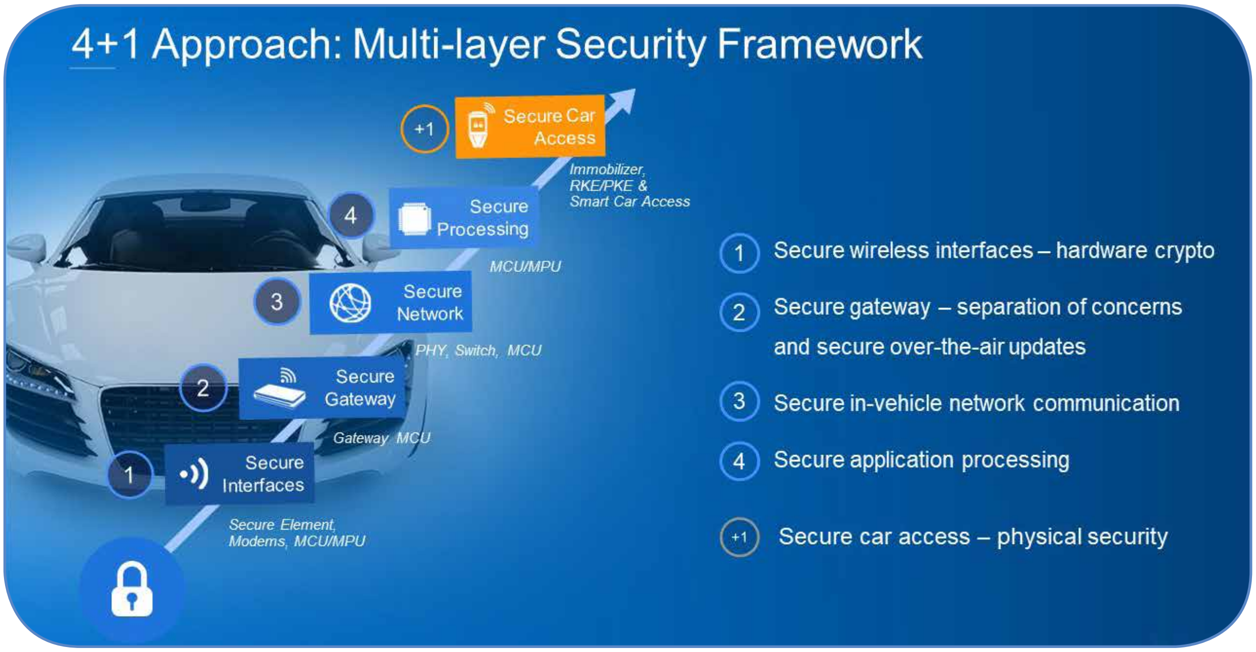
The level and nature of protection must be in line with the threats in the different functional domains, applications and components in the vehicle. The protection level of an ECU depends on multiple parameters, including the attack surface, the criticality of the functions implemented on it and the protected asset. Components with external connectivity capabilities – e.g. the infotainment system, or the gateway – require a higher level of protection than most of the body control modules.

Potentially vulnerable components should be isolated from safety-critical functions, so the impact from a successful attack can be limited and contained. If a successful attack is detected, core functionality must be maintained and safeguarded to ensure that the car remains functional and safe, but additional functionality (e.g. live video streaming) may be disabled to reduce the potential impact.

Solutions for safe and secure mobility around the globe

All companies in the automotive supply chain must be prepared to continuously invest into cybersecurity solutions to stay ahead of the threats that evolve over time. This requires maintaining a comprehensive and holistic automotive cybersecurity program that includes: products with built-in security capabilities, secure product engineering processes integrated into the normal development flow, internal/external security evaluation and certification, a product security incident response team and a systematic way to share threat intelligence. Building and maintaining a security aware organization is essential as security is becoming integral part of product design.

NXP's **S32 Processing Platform** offers one of the strongest security solutions available today based on the **4+1 Automotive Security Framework**. The 4-layer cybersecurity solution offers a secure interface to the outside world for M2M (Machine-to-Machine) communication, secure gateway for domain isolation, secure network for messaging both internally and externally, and secure processing on ECUs. Together with secure car access systems, it enables defense-in-depth protection across the vehicle.


4+1 Approach: Multi-layer Security Framework

1 Secure wireless interfaces – hardware crypto

2 Secure gateway – separation of concerns and secure over-the-air updates

3 Secure in-vehicle network communication

4 Secure application processing

+1 Secure car access – physical security

Figure 5 Multi-layer security framework

Security by design is critical, which is why all products developed as part of the S32 platform offer a comprehensive range of security capabilities, implemented in a dedicated security sub-system called HSE (Hardware Security Engine): secure boot, symmetric and asymmetric cryptographic services (encryption, decryption, signing and verification), hashing, high-quality random number generation, key management services, side channel protection and fault resistance. Hardware acceleration is in place to fulfill the real-time requirements of the safety-critical automotive systems.

To serve a wide range of applications (body, comfort, powertrain, vehicle dynamics, safety, driver assistance and driver replacement, gateways, domain controllers, etc.) while ensuring that the products are easy-to-use, easy-to-reuse and easy-to-integrate, security services across the complete S32 portfolio can be accessed through a compatible Security API. All products are AUTOSAR-compliant and fully meet the functional goals and objectives of the 'SHE' and 'EVITA Full' specifications.

Because any solutions coming to the market today must offer a way to keep security solutions up-to-date over the extended lifetime of a vehicle, it is important that offline and over-the-air firmware and software updates are supported through secure (encrypted and authenticated) channels. Updateable, upgradeable and therefore future-proof security must be available across all domains to support the vehicles from design to end-of-life.

What can car owners do to reduce the risk of being hacked?

The industry is working hard to design and maintain security systems in cars in a way that owners won't have to do more than follow good security practices, such using strong passwords and reporting suspicious malfunctions they observe.

Cars and their security systems are very complex with multiple access points. They require deep security expertise to decide the best way to protect sensitive data and ensure the safe and secure operation of the vehicle.

The automotive industry must provide sufficient security solutions to current and future car owners. Governments can also play a role, for example, by defining a legal framework for independent evaluation of the security capabilities of our vehicles.

Car owners can and should demand proven high-security solutions, together with comfort and safety. Increased consumer awareness and demand helps accelerate the required steps, so security implementations can fulfill the fast-increasing security requirements of assisted or automated driving in highly connected vehicles.

The future of automotive security

Everything considered: Can we trust our vehicles, especially as we see more and more 'self-driving robots'? The answer is that we can, if we consider security as integral part of the overall vehicle design and are prepared to stay ahead of the developing attack techniques with updateable and upgradeable future-proof security.

It is important that we all do our part: governments, industry players and car owners. Requesting information about the security capabilities of our cars should become routine, in the same way as we learn about safety, driving parameters and convenience features today. Providers must support this goal with the most advanced technology, so we can all be safe and secure.

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

USA/Europe or Locations Not Listed:
NXP Semiconductors USA, Inc.
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXP Semiconductors Germany GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Japan Ltd.
Yebisu Garden Place Tower 24F,
4-20-3, Ebisu, Shibuya-ku,
Tokyo 150-6024, Japan
0120 950 032 (Domestic Toll Free)
www.nxp.com/jp/support/

Asia/Pacific:
NXP Semiconductors Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

www.nxp.com