thalesgroup.com

THALES
Building a future we can all trust



Building a connected car we can all trust

An overview of cybersecurity challenges, regulation and best practices

Executive Summary

The connected vehicle is at a complex crossroads today. As industry development continues, two items are of particular interest to car manufacturers (OEMs), equipment suppliers (Tier 1 and Tier 2) and drivers: connectivity and cybersecurity.

The development of the connected and, ultimately, autonomous vehicle requires all types of reliable, embedded connectivity capable of withstanding the rigors of urban environments while supporting both critical systems and infotainment applications. Connected vehicle technology is enabling access to a wide range of digital services including vehicle-to-vehicle and vehicle-to-roadside unit communications (V2X), intelligent transportation systems (ITS), virtual car keys, and more. However, to ensure that such connectivity will not be the gateway to cyber attacks, cybersecurity has become a priority for car manufacturers very early on to achieve the seamless security required of connected cars.

Cybersecurity is all the more relevant as it is now part of a European and international framework that is particularly decisive for the spread of connected and autonomous vehicles, especially in terms of vehicle approval and road safety. Accordingly, as a response to the growing concern about cyber threats in the automotive industry, cybersecurity is now part of the upcoming regulation of the UNECE's World Forum for Harmonization of Vehicle Regulations (WP.29).

Adopted in June 2020, the cybersecurity aspect of the UNECE WP.29 regulation dedicated to Cyber Security Management System (CSMS) and Software Update Management System (SUMS) came into effect in early 2021 and will be binding in the EU in summer 2022. These UN guidelines provide uniform provisions concerning the approval of vehicles with regards to cybersecurity and the deployment of a CSMS. The challenge for the automotive industry is to provide optimal security for the connected vehicle while complying with future regulations and standards.

Because achieving the connected and autonomous car is also a race for competitive positioning and brand image, OEMs and Tier 1 suppliers need to inspire confidence and trust in their connected car offerings if they are to penetrate this promising and growing market. They need to master available technologies to design connected cars leveraging advanced security systems and lifecycle management solutions that will enable them to meet the requirements of the future.

This whitepaper provides guidance to move towards the implementation of a robust automotive cybersecurity infrastructure, which is not only secure at the time of vehicle deployment but along the connected car´s long life.



1 The Connected Vehicle: Forerunner of Future Mobility

The automotive market is undergoing an unprecedented technological, societal and competitive revolution. The car is now a true connected object, gradually offering new functionalities such as alerting the driver to danger, detecting drowsiness or connecting a smartphone to the on-board computer.

In addition, the real-time exchange of data between the vehicle, the user and their environment opens up a whole new world of services, most of which are yet to be invented. As part of the wider ecosystem of the Internet of Things (IoT), the vehicle of tomorrow will be able to communicate and interact with household equipment, road infrastructure and even the city as a whole (car parks, petrol stations, shops, etc.).

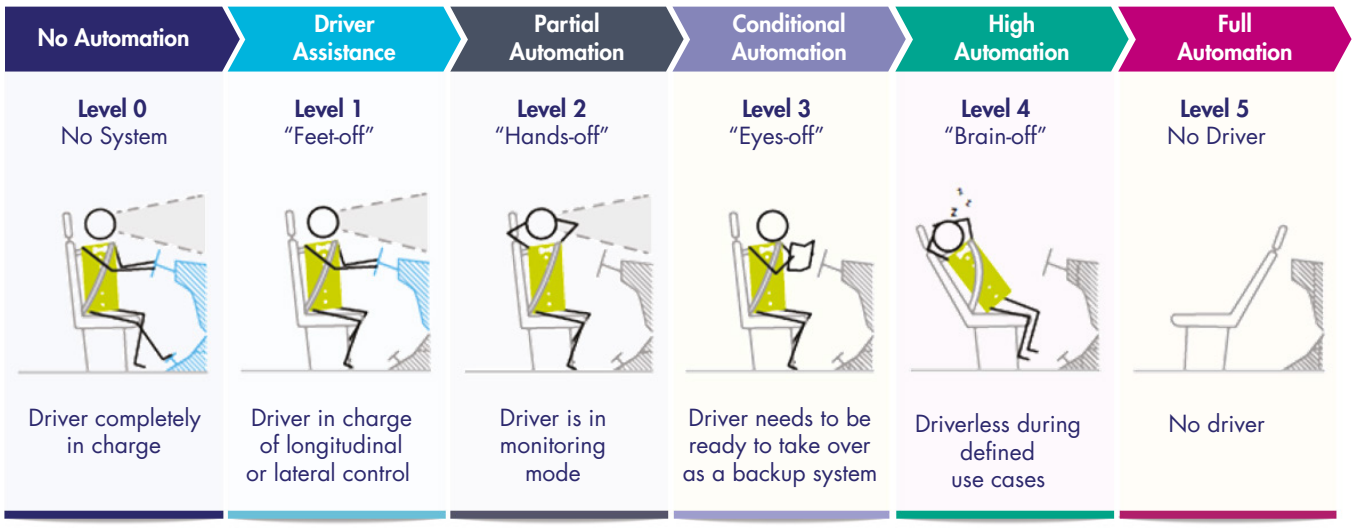
As we move from connectivity to autonomy, it is only natural that 2020 saw the marketing of the first autonomous vehicles. Although the technology already exists, we still have to overcome major challenges before we see large numbers of autonomous vehicles on our roads.

A growing market: from connected to autonomous vehicles

Although the fully autonomous vehicle is not a reality for consumers yet, the connected car is. The connected car market is the world's third largest market in terms of growth, behind the tablet and smartphone markets. The auto industry and consumers alike have embraced the promising future of both autonomous and connected cars. It is estimated that between 2015 and 2025, the connected vehicle market will have quadrupled and will reach more than €115.2 billion in sales worldwide. This will mainly benefit two technology segments: safety and driving assistance, which will reach €47.34 billion and €35.66 billion respectively by 2022 (1).

As for the autonomous vehicle, every effort is being made to accelerate its penetration into the market. IHS Markit expects global sales of vehicles with some level of autonomy to reach 76 million by 2035 (2).

The path to the fully autonomous car



Source : Deloitte Consulting

(1) Source: Strategy Analytics 2019 (2) Source: IHS Automotive Forecast 2019

Building trust in the connected vehicle

As more and more Electronic Control Units (ECUs) and new functionalities are embedded in vehicles, connectivity is becoming a key concern for OEMs and suppliers as it is the foundation for interaction and communication between the vehicle and its environment, infrastructure and the cloud. Optimal, uninterrupted connectivity in all circumstances determines driving quality and, even more importantly, safety related services like mandatory eCall.

However, the connectivity issue goes hand in hand with security concerns, in particular cybersecurity. As soon as connected vehicles become connectivity platforms, they become a potential gateway for cyber attacks. Controlled by on-board and interconnected systems, connected cars present manufacturers with cybersecurity issues that are unprecedented in the industry, leading to public scepticism, mistrust and lack of confidence in the autonomous connected vehicle as the car of the future.

2 The Automotive Cybersecurity Landscape: Keeping Connected Cars Secure and Protected

a. A new kind of threat for a new kind of vehicle

The scene goes back to June 2015. Quietly seated in front of their computer screens, two cybersecurity researchers, Charlie Miller and Chris Valasek, managed to take control of a Jeep Cherokee driven by a journalist via a simple IP address. The whole world was discovering the vulnerability of connected cars to possible cyber attacks. Since then, other models and makes of vehicles have undergone the same type of test attack. The worst-case scenario of the connected car, where remote hacking compromises a vital vehicle function and could potentially affect a fleet of vehicles, is no longer fiction but a real possibility. As the arrival of autonomous cars approaches, cybersecurity is now a central issue for today's connected vehicles.

Incorporating around 150 ECUs and about 100 million lines of software code (3) (for luxury models), the car today is a true computer on wheels. The technology enabling cars to become hyper connected objects is closely linked to the software and its ability to communicate with the immediate (sensors) and distant (telecommunications) environment. The vehicle is one of the connected objects of the IoT, but its interaction with its environment requires constantly switching from private to public data. Therefore, the communication vectors are numerous for a connected vehicle. In addition to internet connectivity for telemetry, software updates, fleet tracking and all imaginable value-added services, the connected car is likely to be also connected to a smartphone. There are also V2V (Vehicle-to-Vehicle) connections that allow driving information to be shared among vehicles located within the same perimeter and V2I (Vehicle-to-Infrastructure) connections that allow the vehicle to communicate with infrastructure elements, again forming temporary networks. The aim of forming so many temporary networks is to increase safety and convenience, through a better knowledge of the environment.

All these means of communication have one thing in common: they are wireless. Wireless networks are, by nature, more vulnerable to attack and interference than their wired counterparts. Our worldwide mobile networks are dependent upon highly mobile human beings with humans increasingly dependent upon their ever-present wireless communications tools. The embedded connectivity of the connected vehicles is poised to become just as critical to everyday life, which makes them a prime target for cyber attacks.

(3) Source: https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf

Connected Cars Security Incidents - Examples over the last few years

2017:
Jason Hughes, a whitehat hacker, managed to hack his own Tesla and further gained access to Tesla´s entire vehicles fleet through their internal servers.
Source: Electrek

2017:
TrendMicro exploited a vulnerability in Controller Area Network (CAN) protocols to reprogram a car´s infotainment system, disable airbags, tamper with locking systems and steal the vehicle.
Source: ZDNet

2017:
A Hyundai Blue Link app contained a vulnerability where hackers could enter via insecure Wifi and obtain private user information and start cars remotely.
Source: Forbes

2018:
Calamp released a misconfigured server that provided open access to 1.5 million connected devices, allowing unwanted location of vehicles, password resets, door unlocks, alarm disables, engine starts and vehicle thefts for multiple car brands.
Source: Forbes

2018:
A security researcher, at Belgian university KU Leuven, managed to break into a Tesla Model X in minutes, through a Bluetooth attack, and drive away.
Source: Wired

2020:
The Sky-Go car security research team found more than a dozen vulnerabilities in a Mercedes-Benz E-Class car that allowed them to remotely open its doors and start the engine.
Source: TechCrunch

2020:
The consumer group "Which?" exposed security flaws that ranged from remotely exposing private, customer information (e.g. location history, contact info) to disabling the traction control system on Ford and Volkswagen popular models.
Source: edinburghnews.scotsman.com

2020:
Parts of Honda global operations halted by a ransomware attack (file-encrypting malware), causing production, customer and financial services issues.
Source: TechCrunch

2020:
Split-second phantom attacks causing advanced driver-assistance systems (ADAs), Tesla Model X and Mobileye 630, to issue false notification and stop a car in the middle of a road.
Source: Schneier

2020:
Daimler onboard logic unit (OLU) source code leaked online, giving access to passwords and access tokens, and allowing anyone to register on one of its on-premise GitLab servers.
Source: ZDNet

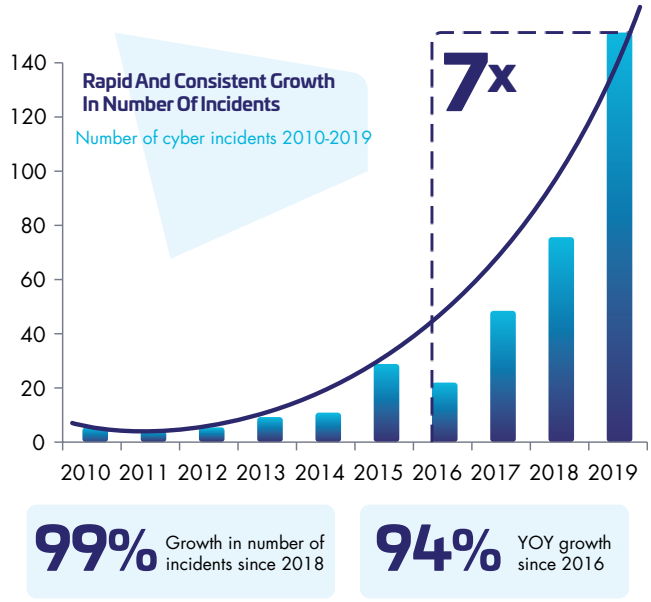
b. The challenge of cybersecurity

Diagnostic, open internet protocols, entertainment systems, ECUs for vital functions, remote warning systems, connected surveillance systems and poorly protected keys are all particularly sensitive points. The issues of security and data protection are both inevitable and vital.

The challenge is simple but all encompassing: ensure the security of all critical digital systems and infrastructures against intrusions.

Another security hotspot is web applications that allow the exchange of information between the vehicle and/or driver and the manufacturer's IT system. If the authentication process is not secure, an attacker can enter the driver's account and take control of the vehicle. Additionally, there is the risk that drivers' personal driving data may be collected, used, sold or communicated.

Over the past decade, the number of automotive cybersecurity incidents has increased dramatically. Between 2016 and 2019 alone, the number of incidents grew sevenfold. As more connected vehicles hit the road, the potential damage of each incident rises exponentially, placing companies, infrastructure and consumers at risk.

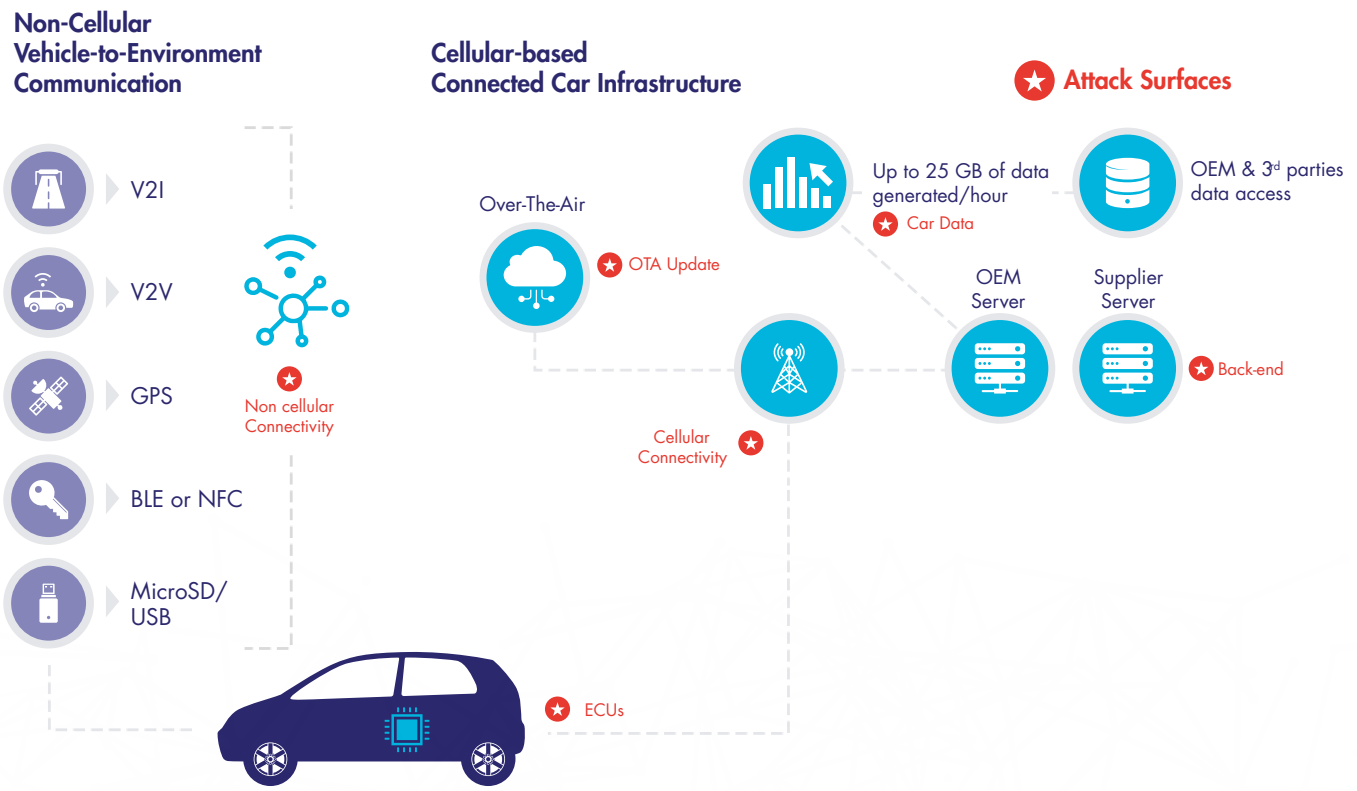


Source : Upstream Security Global Automotive Cybersecurity Report 2020

c. A variety of threats

The incredible possibilities provided by connected and autonomous cars also adds to their vulnerabilities. Malfunctioning features, temporary engine failure, ransomware, and spyware are just some of the havoc hackers could wreak on drivers and cars in the future. Losing a Wi-Fi connection can be very inconvenient in an office, but a lost connection in a connected car can render navigation and the entire entertainment system temporarily useless, or even the engine. An attack targeting the cellular network can lead to major malfunctions on thousands of vehicles simultaneously. A ransomware attack could prevent the car from operating until payment is made or spyware could monitor drivers' whereabouts for burglars or possibly gain access to banking login information.

Main attack surfaces in connected cars



Main motivations and attack modes

An attack on the most vulnerable system

Not all on-board systems and networks are made the same way. Attackers will attempt to identify vulnerabilities in the least protected systems or services, such as the entertainment systems, and then penetrate the on-board communication network and access more sensitive systems. For example, the engine management system communicates with the entertainment system to display alerts ("engine fault!" or "cruise control active"). These communications can be subject to attack.

System stability and predictability

The new generation of autonomous connected vehicles is likely to use software, including open source software, provided by different vendors. Unlike the industrial control systems that equip conventional cars, IT suffers from unpredictability: computer systems can break down without warning. This is less critical when a web server is inaccessible due to the rebooting of the servers that host it. On the other hand, the consequences can be much more unfortunate when the failure of a Wi-Fi or on-board entertainment system leads to a malfunction of the navigation system.

Ransomware

Ransomware is a threat that is proliferating on computers and smartphones. However, an autonomous car is an equally ideal target. Let's imagine the following scenario: a hacker hacks into the on-board display system to inform an owner that the vehicle is immobilized until a ransom is paid. In the case of a PC or tablet, restoration is relatively simple, assuming of course that data and settings have been backed-up. The case of a standalone car is quite different. The owner may be on the road, and the ransomware is programmed to run only when the vehicle is at a predetermined distance from their home. Dealerships and garages will not necessarily know how to handle such a logical failure, and will have to call upon expert skills to restore failed components and systems. The ransom amount is likely to be higher than the amounts typically requested in the case of ransomware attacks on conventional PCs, but most probably lower than the cost of repair as an incentive for the owner to pay the ransom. This is not to mention other direct or indirect costs of the attack, like the towing of the vehicle.

Spyware

Hackers will be tempted to collect personal data via a connected car. Driverless vehicles collect large volumes of data that can provide a lot of information about the owner: favourite destinations, routes, home address, buying behaviour and even travel companions. A hacker, who knows you are on holiday and away from home, can resell this information to burglars. There is also the risk to use hijacked login credentials to break into your bank account.

3 Standards and Regulations: Providing a Framework for Automotive Cybersecurity Implementation

As cybersecurity concerns rise, a new wave of global guidelines, regulations and standards are being created to prevent cyber threats and ensure the safety and security of automotive customers in the near to long term. These upcoming regulations like the cybersecurity aspect of the United Nation UNECE WP.29 regulation (CSMS and SUMS) adopted in June 2020, require automotive OEMs to integrate cybersecurity activities along the entire value chain. In other words, OEMs must adopt a security-by-design approach.

a. What is UNECE WP.29?

UNECE stands for United Nations Economic Commission for Europe. Despite its name, the organisation does not look to establish rules and requirements for European countries only, but it ensures the cooperation and integration of rules for its 56 member states.

The UNECE´s World Forum for Harmonization of Vehicle Regulations (WP.29) established six permanent working parties to look at defining requirements in terms of safety and environmental performance for a variety of vehicles: cars, trucks, buses, powered two wheelers, agricultural vehicles and non-road mobile machineries, such as cranes or locomotives. The forum enables open discussions on automotive regulation worldwide.

In June 2018, a new working party, called Automated/ Autonomous and Connected Vehicles (GRVA), was established to focus on the specific challenges and requirements of safety and security for these vehicles. In this context, questions raised on cybersecurity and software updates for connected vehicles led to the Cybersecurity Management System (CSMS) and Software Update Management System (SUMS) requirements with specific measures to be taken in four areas:

1. **Management of cyber risks for vehicles**
2. **Implementation of a "security by design" architecture during vehicle development to minimize risks along the value chain**
3. **Detection of intrusions and protection of vehicle fleets**
4. **Development of secure software updates and legal groundwork for "Over-the-Air" (OTA) updates**

b. A framework guiding OEMs towards cybersecurity implementation

The UNECE WP.29 regulation provides a framework for car makers with minimum requirements to implement. It insists on key elements to consider and a detailed list of connected vehicles´ security threats and vulnerabilities as well as mitigation opportunities.

A key highlighted element is that cybersecurity should be implemented over the complete lifecycle of the vehicle to ensure vehicle systems are secure over their lifetime. This means that Tier 1 and 2 suppliers need to be deeply involved in the process and be able to prove the integrity of the components they supply to OEMs. It also means that OEMs need to consider systems that are evolutive and can be updated remotely in a secure manner.

c. The limits of UNECE WP.29

Although the regulation explains what needs to be achieved, it does not extensively explain how to reach the announced goals nor does it specify technologies to leverage. But the responsibility in implementing a solid cybersecurity infrastructure clearly falls to carmakers that need to be able to provide evidence that they have implemented systems to protect their vehicles.

This is why cybersecurity expert companies can support OEM and Tier 1 suppliers in their thorough implementation of the regulations.



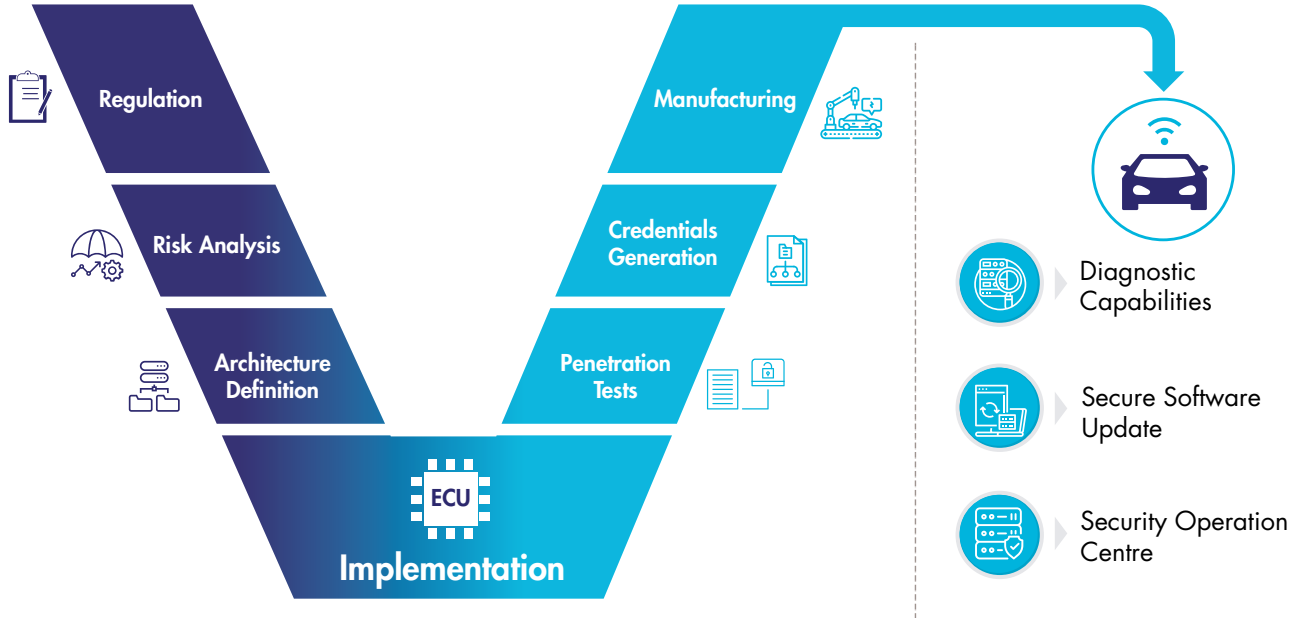
4 Thales vision, technologies & expertise in cybersecurity

Since 2013, Thales has been providing support to car manufacturers and equipment suppliers in the area of automotive cybersecurity. Following the development of the UN regulations and other automotive security standards, such as the new ISO/SAE 21434, to consider and ensure cybersecurity at all phases of a car lifecycle – from its conception, development and design, through the component and system testing, and up to the vehicle in operation (V-model) – Thales has been an integral partner.

Thales is committed to providing the most innovative cybersecurity solutions to protect connected vehicles against cyber threats by having different levels of sensitivity and exposure to threats coexisting inside the vehicle.

We are working with car manufacturers and equipment suppliers on deploying auto architectures that integrate the concept of "security by design" right from the design stage, which is not always the case today. We help to maintain cybersecurity at its highest level during the long lifecycle of the car, to keep adapting to new threats and react accordingly.

Thales cybersecurity – from car conception to complete lifecycle management



a. Many connections and security threats in connected cars

Communications within the vehicle: Connected vehicles have several intelligent on-board systems dedicated to vehicle control, entertainment, passenger networking and even third-party on-board systems at the request of owners. These systems will need to communicate with each other to establish new services. However, these communications must be closely monitored and managed by firewalls and intrusion prevention systems that are capable of distinguishing between legitimate and suspicious communications within the car's internal network.

External communications: Most on-board systems will need to communicate with internet services for a variety of reasons: maintenance by the manufacturer, software updates, passenger access to the internet, guidance and navigation, purchase of goods or services or data backup. External communications are likely to be of the push-and-pull type, initiated from inside the vehicle, or to the vehicle from the car manufacturer or the internet. This two-way traffic will therefore need to be analyzed for illegitimate threats or communications, using firewall and intrusion prevention features.

The connectivity infrastructure: Connected cars use cellular networks. These networks, which already interconnect billions of smartphones and devices, are deficient in terms of security. This presents a risk to connected vehicles that will soon be autonomous. An attack targeting the cellular network, or carried out via this network, can lead to major malfunctions on thousands of vehicles simultaneously.

Access control and identification systems: These systems, designed specifically for machines and not individuals, will need to be deployed so that vehicles can authenticate incoming connections to critical systems. Internet services must be able to authenticate with certainty cars and information sent to the cloud, or transaction requests made by owners, such as services needed or payment of fuel or tolls.

Therefore, cybersecurity in the connected vehicle is indissociable from the safety of the vehicle, the protection of the users and, ultimately, the trust people have in connected cars.

b. Implementing a security-by-design approach with Thales

Thales cybersecurity expertise promotes a security-by-design approach with an end-to-end vision as required by the new UNECE WP.29 regulation. We provide advanced cybersecurity consulting, dedicated car IDs generation and lifecycle management, as well as Security Operations Centres (SOC) for real-time detection and response to cyber attacks in the field or in OEM factories.

Thales provides the right combination of expertise, services and products to keep connected cars secure and running well into the future. Keeping all stakeholders abreast of the latest regulations worldwide requires excellent communication at every step of design, engineering, development and beyond.

Ongoing risk analysis, defining secure architecture to address the security threats, testing and assessing the architecture before deployment are crucial to the Thales cybersecurity solutions. Thales Trusted Key Manager ensures end-to-end security for the automotive infrastructure, designed to protect the integrity of large car fleet deployments throughout the lifecycle. And our five Security Operations Centres throughout the globe ensure real-time monitoring and response to cyber attacks anytime, anywhere.



Automotive Cybersecurity: Thales 6-step approach

1 REGULATION COMPLIANCE

Providing consulting and support to build cyber regulations compliant policies

- Elaboration of a specific cybersecurity policy for connected vechicles and embedded architectures within the IT/IS perimeter
- Implementation of a cyber policy that will facilitate the alignment of the cyber strategy among the diffierent stake holders and communicate cybersecurity objectives and expectations to the different teams (conception, engineering, development...)

2 RISK ANALYSIS

Assessing the risks related to the introduction of connected functions within the vehicle

Performing a business risk analysis on the different ECUs and functions to be deployed in the vechicle to define the threat model, the attacker profile, the attack scenario and the global exposition/risk of the perimeter.

3 SECURITY ARCHITECTURE

Defining secure architectures and specifying cyber security measures

Based on the conclusions of the risk analysis and in accordance with the threat model, we define an architecture and specify technical security measures to be implemented in the global architecture.

4 PENETRATION TESTING

Assessing the real security level of architectures, ECUs and off board services

Using dedicated methodology and penetration testing approaches to find potential exploitable breaches on different exposed surfaces, interfaces and components.

5 CREDENTIAL LIFECYCLE MANAGEMENT

Ensuring end-to-end security for automotive infrastructures thanks to Thales Trusted Key Manager

Encompassing the world-leading Safenet Hardware Security Module (HSM), a dedicated Key Management System (KMS) and best-in-class Public Key Infrastructure (PKI), Thales Trusted Key Manager is an advanced cybersecurity solution designed to protect large IoT device deployments and to ensure their integrity and reliability during their entire lifecycle.

6 SECURITY OPERATION CENTRES (SOC)

Ensuring real time detection and response to potential cyber attacks thanks to our Security Operation Centres (SOC)

At Thales, our expertise in cybersecurity go throughout the connected car entire lifecycle. We have five Security Operation Centres (SOC) around the world made up of cybersecurity experts to assist connected vehicles on the road in detecting and responding in real time to potential cyber attacks.

Thales designs, builds and operates cybersecurity solutions and services to protect all critical assets of the automotive industry players. We draw on decades of security experience across highly demanding markets. Our solutions allow the deployment of secure connected services by bringing trust between mobility stakeholders, minimizing risks and protecting end-users´ privacy.

As the dream of connected and autonomous cars become a reality, cybersecurity experts like Thales will be the drivers of trust for this burgeoning technology ecosystem. Thales' security-by-design approach with cybersecurity built-in from car conception and throughout the lifecycle will add trust, help prevent cyber attacks and respond quickly to any intrusions. Since 2013, Thales has been supporting car manufacturers and equipment suppliers with its vision, technologies and cybersecurity expertise and will continue to lead the automotive industry into the autonomous future.



About Thales

Thales serves customers in very diverse environments, from the bottom of the oceans to the edge of space and cyberspace. They – and we – are active in five areas that are essential for our society to make the world go round: Digital Identity and Security, Ground Transportation, Defence and Security, Aerospace and Space.

With over 83,000 employees in 68 countries, including more than 25,000 engineers and researchers, Thales offers a unique capability to create and deploy equipment, systems and services that meet the most complex security needs. Its exceptional international presence enables it to work as closely as possible with its customers around the world.

At Thales, we have a DNA of innovation and make heavy investments in the four key digital technologies of Connectivity, Big Data, Artificial Intelligence and Cybersecurity. Leveraging our solid technological foundations, we support vehicle and system manufacturers in all aspects of cybersecurity, both onboard the vehicle and in its environment: from assessing the risks associated with new functions to testing the security level of installed equipment or the entire vehicle. From defining the security policy to guarantee end-to-end vehicle security to the components that secure communications and software execution. From creating a digital infrastructure to supporting the implementation of digital functionalities.

Contact us:
Website: Thales Automotive Cybersecurity

> Thalesgroup.com <

© Thales 2021. All rights reserved. Thales, the Thales logo, are trademarks and service marks of Thales and are registered in certain countries, 22 June 2021.