thalesgroup.com

THALES

THALES AUTOMOTIVE

Securing Connected Cars for your Safety

THALES

The challenge of a vehicle that combines **reliable connectivity & robust cybersecurity**

The connected vehicle is at the crossroads of multiple stakes. Among those stakes, two 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 embed reliable connectivity capable of withstanding the rigours of urban environments while supporting both critical systems and infotainment applications. 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 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 (WP29).

Already adopted on June 2020, the cybersecurity aspect of the UNECE WP29 regulation dedicated to Cybersecurity Management System (CSMS) and Software Update Management System (SUMS) will come into force as early as January 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 Cyber Security Management System (CSMS). The challenge for the automotive industry is therefore to provide optimal security for the connected vehicle while complying with future regulations and standards.

To achieve the goal of an autonomous connected vehicle that is as efficient as it is safe, Thales is committed to offering its expertise and solutions to automotive manufacturers and equipment suppliers so that they can meet these ultimate challenges.

THALES

Thales's end-to-end comprehensive offer for **connected & autonomous vehicles**

Thales's dedicated automotive connectivity solutions, advanced security expertise and device lifecycle management platform allow automotive manufacturers to meet the security and connectivity requirements of the future's connected car. Because achieving the connected and autonomous car is also a race for competitive positioning and brand image, OEMs and Tier one suppliers need to inspire confidence and trust in their connected car offerings if they are to penetrate this promising and growing market.

At Thales, we deeply believe that our expertise and solutions can help fulfill that purpose. Our value proposition for OEMs and Tier one suppliers revolves around four key features we believe every connected car must deliver:

→ **Robust and trusted security**
→ **Always-on, reliable connectivity**
→ **Device lifecycle management**
→ **Worldwide and seamless operation**

We have developed a range of solutions that incorporate these four principles and combine high-end connectivity with robust cybersecurity to meet the requirements of automotive manufacturers and suppliers.

As our cybersecurity and connectivity solutions are two sides of the same coin, they ultimately contribute to an improved user experience and better vehicle customization.

The Connected Car

How connectivity is revolutionizing the way we travel from A to B

Voice assistants
are built into dashboards to keep you connected to your home and digital workspace

Payment
for parking, battery charging and shopping using integrated near-field communication and mobile wallet apps

Real-time information
on traffic and parking spaces, received by an in-car eSIM or WiFi hotspot, improves journey planning

Smartphone integration
brings Apple™ and Android™ operating systems, and their entertainment functions onto your dashboard over the internet

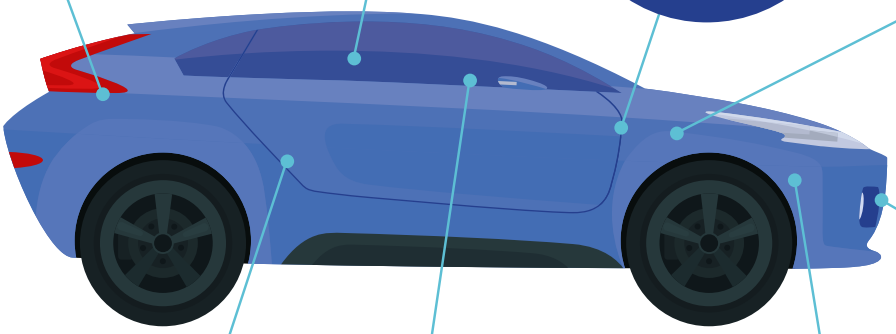
Location-triggered
marketing alerts you to local businesses of interest when you're nearby

In-car eSIMs and WiFi hotspots
keep cars connected to 5G networks and the wider IoT ecosystem

Streaming and gaming
services transform the car into an immersive entertainment space

Public Key Infrastructure (PKI)
uses encryption, authentication and identity checks to keep the data moving to and from your car secure

Personal data is protected
with security by design, over-the-air software updates and privacy regulations



Lasers and sensors
detect obstacles humans might not see – the car analyzes this data and takes action to avoid a collision

Communication
improves navigation systems and broadcasts position and speed to other connected cars to avoid accidents

Detection systems
alter lighting and temperature to improve driver alertness when sensors pick up signs of driver fatigue

Battery life is optimized
by smart sensors that detect when charge is low and alerts the driver when service is needed

1. Reliable & permanent connectivity to enable the connected vehicle full potential

As more and more Electronic Control Units (ECUs) and new functionalities are embedded in vehicles, connectivity is becoming a key concern for manufacturers and OEMs 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 but even more importantly, safety related services like mandatory eCall.

At Thales, we know connectivity delivers performance. Reliable connectivity for connected cars can provide everything from telematics to preventive maintenance to accident prevention and enhanced entertainment systems. Any connected automobile must be able to transmit data rapidly and reliably. A delay of any kind could confuse the driver and even cause accidents. Guaranteeing high-quality connectivity, the interoperability of integrated solutions and the security of systems against intrusions is our top priority.

Thales's dedicated automotive connectivity solutions, advanced security expertise and device lifecycle management platform allow you to meet the requirements of the connected car of today and tomorrow. OEMs and Tier one suppliers use our dedicated eSIMs, and cellular modules, which are used for a wide range of applications.

➔ Car manufacturers and automotive suppliers trust Thales to manage worldwide cellular connectivity.
As the automotive world becomes increasingly connected, Thales makes it secure and easy to navigate.
Customers rely on Thales to master connectivity throughout a vehicle's lifetime.
Our connectivity solutions and remote management expertise simplify the end-user experience and help car manufacturers to facilitate their supply chain.
As an integral actor in mobile standardization, Thales brings a unique experience in cellular connectivity.
We currently serve more than 450 mobile operators worldwide.

Our dedicated automotive connectivity solutions offer:

M2M Robust cellular modules

M2M technology for the automotive industry offers cellular connectivity and services that enrich the "mobile" lifestyle of drivers and their passengers by providing high-speed, low-latency connectivity and a range of advanced features including mobile Wi-Fi hotspots, Internet radio, web services and an enhanced navigation system. However, by its very nature, the automotive environment is demanding as opposed to other more stable environments; as a result, wireless technology must withstand extreme temperatures, vibration and humidity on the road. In addition, automotive manufacturers are subject to strict regulation that equally applies to the connected car.

Embedded LTE solutions

With embedded LTE solutions, car manufacturers can offer low-latency broadband connectivity and a set of advanced features and services that improve the "on-the-road experience" for drivers and their passengers. Users can simultaneously enjoy in-vehicle voice and data services with, for example, one passenger searching the Internet for the best restaurant nearby while another calls to make a reservation.

Automotive dedicated eSIMs

Embedded M2M SIM cards identify vehicles, encrypt communications and provide global connectivity for intelligent vehicle systems, including eCall emergency call solutions, vehicle telematics and navigation. Automotive eSIMs are designed to endure extreme conditions. Secure remote connection services simplify the manufacturing process and improve safety as MFF2 SIM cards are integrated and installed during the manufacturing process. As a result, wireless service providers can be selected or switched without increasing exposure to tampering and damage. In the future, the activation of a secure service in the cloud and next-generation features such as vehicle ignition with a secure ID, integrated NFC and mobile wallet applications will further improve driver and passenger comfort.

eSIMs management through "On-Demand Connectivity (ODC)" platform

"On-Demand Connectivity" is Thales's eSIM management platform designed to securely and remotely manage the lifecycle of cellular subscriptions. To bring the best out of our eSIMs and connectivity modules, the ODC platform remotely manage:

- **The versatile deployment of "build once - deploy anywhere":** cars are able to instantly connect with cellular networks anywhere on the globe and transmit data over a range of networks. This means that they can be sold in different regions and still operate in tunnels, underground, or in remote locations without new factory settings ;
- **eSIMs subscription:** switching from one Mobile Network Operator (MNO) to another with activated, personalized and interoperable services becomes a lot easier and doesn't require new factory run for vehicles ;
- **A secure environment that only authorizes encryption-based digitally signed updates to be downloaded on-board.**

With 200 deployments worldwide and counting, Thales's eSIM management platform is a worldwide reference across mobile operators, operator alliances, car manufacturers.

2. A new kind of threat for a new kind of vehicle: the challenge of cybersecurity

The advancement of electrical and electronic architecture along with the digitalization of the car ecosystem leads to an abundance of software code and connectivity.

This increasing connectivity is causing widespread disruption across the automotive industry as it generates many vulnerable threat points and ample opportunities for cyber-attacks; not only in the car but also along the entire value chain. Cyber attacks and data breach incidents pose severe risks to the automotive industry as they directly impact driver safety, data privacy, and service continuity.

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

A new wave of proper guidelines, regulations and standards are manifesting themselves 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 UNECE WP29 regulation (CSMS and SUMS) adopted on June 2020, require automotive OEMs to integrate cybersecurity activities along the entire value chain; in other words, to adopt a « security by design » approach.

Cybersecurity is thus within the connected vehicle indissociable from the safety of the vehicle, the protection of the users and ultimately the trust people have in connected cars.

Thales has been following the development of the UN regulations and other automotive security standards for a long time. That is why we are 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.

➔ **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 from aerospace to banking where we developed expertise on embedded systems, industrial networks and cloud computing. Our solutions allow the deployment of secure connected services by bringing trust between mobility stakeholders, minimizing risk and protecting end-users' privacy.**

Our cyber consulting expertise promote a "security by design" approach as required by the new UNECE WP29 regulation with an end-to-end vision. We are able to provide an advanced cybersecurity expertise, from factory to road by deploying:

1 REGULATION COMPLIANCY

Providing consulting and support to build cyber regulations compliant policies

- Elaboration of a specific cybersecurity policy for connected vehicles and embedded architectures within the IT/IS perimeter
- Implementation of a cyber policy that will facilitate the alignment of the cyber strategy among the different stakeholders 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 vehicle 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

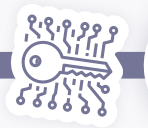
Based on the conclusions of the risk analysis and in accordance with the threat model, we define an architecture and specify technical security measures to be implemented in the global architecture.

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

3. Leveraging Thales key **technologies & expertise in security**

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 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 cyber security, 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.

Thales's automotive solutions cover all cybersecurity and connectivity needs of the connected car

Thales Automotive Technologies →	M2M Cellular module	LTE Solutions	Automotive E-Sim	Trusted Key Management solution	On-Demand Connectivity platform	Cyber consulting expertise	Cyber attack detection (SOC)
Key features every connected car must have ↓							
Robust cybersecurity	✓	✓	✓	✓	✓	✓	✓
Reliable connectivity	✓	✓	✓	✓	✓		
Device life cycle management	✓	✓	✓	✓			✓
Worlwide & seamless operation	✓	✓	✓	✓	✓		✓

Our active involvement with major industrial associations and regulations of the automotive sector

CARCONNECTIVITY consortium®

European Commission C-ITS

5GAA Automotive Association

3GPP A GLOBAL INITIATIVE

AUTOSAR™ Enabling continuous innovations

ETSI

AUTOMOTIVE GRADE LINUX

GENIVI®

CAR 2 CAR COMMUNICATION CONSORTIUM

UNECE

AUTO-ISAC Automotive Information Sharing and Analysis Center

Thales: Together, building a future we can all trust

THALES

Contact:
automotivesolutions@thalesgroup.com