**Video Statement**
by the CEO of Allianz Deutschland AG
**Dr. Klaus-Peter Röhler**
for the **8th Allianz Autotag Digital**
**September 22, 2020**

Ladies and Gentlemen,

Allow me to extend a warm welcome to our eighth Allianz Autotag – which this year, for the first time, will be broadcasted **digitally** and **live all over Europe**. Our topic today is **IT Security in Connected Vehicles**:

Though bicycles may be gaining more and more appeal, **the car is and will remain Europe's most popular primary means of transportation**. The characteristics of today's vehicles have changed. They used to be isolated systems with an engine, but now they are **computer networks on wheels equipped with an Internet connection**. Millions of lines of software code along with control devices and sensors **are making new concepts** in mobility, comfort, and driving safety **possible**. These innovations are paving the way for highly automated driving. And just as "traditional" computer networks became a **target of cyber attacks**, vehicles are likewise increasingly exposed to cyber risks. Alongside the logistics and energy sectors, connected cars may become **one of the most important targets of IT crime**, because the number of connected vehicles will be increasing significantly in the next few years. In Europe alone, the IT service company Capgemini projects an **increase from 37 million connected cars in 2018 to 110 million by 2023**.

This means, that while IT security in connected cars is becoming even more significant, it is also presenting a challenge because **vehicles are goods with an extremely long useful life. From the viewpoint of IT security,** the **lifecycle** of a vehicle model – from development and production to use and recycling – is **20 to 30 years**. That stands in sharp contrast to two things:

- the enormous speed at which **computer performance is expanding**, and
- the concurrent **shrinking use cycles** of consumer electronics.

The particular challenge is **to keep the level of protection and security** of connected vehicles from **going down** throughout **the vehicle's lifecycle** to the

advantage of hackers, because their attacking methods continuously evolve. "Secure" means suitable protection from

- vehicle theft,
- vehicle damage, and
- unauthorized data access,
- but most of all, keeping the car's occupants and other road users safe.

I'd like to take a look here at six aspects of a car's lifecycle:

1. **The many people involved** in **development** and **production**
2. **Standards** and **requirements** for **type approval** of vehicles in Europe
3. **"Security by design"** in **development** and **after delivery**
4. **Secure access** to **vehicle data**
5. Hacking attacks and networking do not stop at **national borders**
6. **The future need for action**

Let's look **first of all at**:

1. The fact that the development and production of high-quality connected vehicles, and future highly automated models, **involve many people**...
   …and they're involved all along the value chain and throughout the vehicle's lifecycle. **This includes people involved in**
   - the departments at the vehicle manufacturers themselves, along with their suppliers at all levels,
   - the telecommunications industry, and
   - the software companies and developers, who are engaged not just in the product's creation but also in the services and products that only come into play once the vehicle is in operation.

Here manufacturers have to orchestrate countless digital interfaces that can otherwise open up **gateways for hacking attacks**.

2. **Standards** and **requirements** for **type approval** of vehicles in Europe

**Requirements** and **standards** are currently being defined, that will establish the **prerequisites** for **vehicles to be approved for road use** in the **European market**. In June, the UNECE World Forum for Harmonization of Vehicle Regulations drafted

**detailed requirements** for **managing cyber risks** and **over-the-air software updates.** These will be supplemented, probably in November 2020, by ISO Standard 21434, “Road vehicles – Cybersecurity engineering.” As a result, vehicle manufacturers will have to meet **detailed requirements** in many areas, including

- organizational requirements and certified processes and
- monitoring of and responsiveness for events **even after** the vehicle’s production period.

This will create a technical standard for automobile development, which makes it possible to **document compliance with the expected rules for vehicles’ type approval**. As we see it, these are important steps in the right direction. They can’t guarantee that vehicles won’t be hacked, but they make an important contribution to minimizing cyber risks.

3. “**Security by design**” in **development** and **after delivery**

Let’s have a look at the **technical security that plays a key role in development**, if only **because of the extensive networking of vehicle components**. Vehicles may incorporate 60 control devices or more, and each one of them needs to offer adequate security against manipulation in its specific application. For example, if the software on a device that controls the charging and power draw on an electric vehicle can be read out and the parameters can be changed, that offers a gateway for unauthorized tuning. This entails a substantial risk that the battery could overheat, and so it should absolutely be prevented.

But even **after a car is delivered and handed over,** the ability of its systems and electronics to work properly must still be guaranteed. **Over-the-air software updates** are already a reality today, and they allow software security to respond in a way that used to be possible only by taking the car in to the shop. **Product monitoring** and **early detection of attacks on a vehicle** by the vehicle manufacturers’ security operation centers will also have to contribute to the security of connected vehicles.

4. **Secure access** to **vehicle data**

**Secure access to vehicle data** is **crucial** for a **working mobility ecosystem** – and by that I mean in “both directions”:

- a connected car must be **adequately protected** from **cyberattacks**

- but at the same time, it has to permit **discrimination-free access** to the vehicle data easily and secure so that third parties can perform servicing.

Ultimately, that would be very similar to a smartphone: The **operating system** is the **foundation**, but it's the many apps and uses that really make a smartphone what it is for the user.

As insurer, we too consider ourselves an **integral part of this ecosystem**. We have a fundamental interest in **adequately securing data access** and **developing practical solutions with the industry**. Based on a well-informed risk calculation, we offer services and products for our customers like telematic rate plans, for instance. That includes digital processes that assist in the event of a claim, from acknowledgement and analysis and appraisal to processing vehicle claims using a smartphone.

Here Allianz is relying heavily on **prevention** and on **early recognition of loss scenarios**. Using the extensive data about specific claims that we've collected at the Allianz Center for Technology, we remain in close communication with manufacturers and **can help recognize developments early on** and **exert a positive influence on them.** A good illustration of that is **vehicle theft**. For more than two years now, it has been possible to order cars that have a **"virtual key."** That key opens, locks, and starts the car by using a smartphone, which replaces a conventional car key. After a car is stolen, the vehicle's operator has to provide us with the full set of keys when claiming the loss. But how can they turn in a virtual key to the insurer? How can they prove that the vehicle was really stolen, and not just being used by an authorized driver who somehow "acquired" a virtual key at some point? And the insurer has to answer the questions: What do we need to investigate, and how? So in a joint leadership collaboration with RCAR – an association of automobile research centers from Europe, Asia, North America, South America, and Australia – we helped define an international **standard for virtual vehicle keys** so that we can compensate our clients quickly and without complications after a total theft, even when a virtual key was used. On top of that, to protect our clients the **standard also defines yardsticks for the IT security of the entire system**, including the vehicle, the smartphone, the back end, the communications, and user interactions.

5. **Hacking attacks and networking don't stop at national borders**

We're certain that the growing IT risks for connected vehicles can be countered only by a **sensible cooperation among everyone involved** – and **at the European level**. As was shown by Fiat Chrysler's recall of 1.4 million vehicles after a 2015 hacker attack in the U.S., thousands of vehicles could also be affected across borders by a single attack in Europe as well. The financial loss from these attacks is great. Recalling all the affected vehicles had cost the vehicle manufacturer $600 million.

## 6. The future need for action

Given the **challenges** that **hacking attacks** and **potential pan-European cumulative risks** present to the **industry**, and to us as **insurer,** there's a need for action in **two areas in particular**:

1. It must become possible to **detect hacker attacks** on individual vehicles and fleets **quickly and early on.** First of all, that involves fending off the attacks, but it also entails determining possible damage. **In line with** what we discussed at the **seventh Allianz Autotag** – about the use of vehicle data to investigate accidents in automated driving – we also believe that it's necessary **to recognize and record cyber attacks.** Storing them with an **independent data trustee** – where **only technical data** and **no personal data** is transmitted – could comply with data protection laws and both cover the involved parties' **needs for information** and enable the **development of appropriate loss statistics**. This would make the **risks to society assessable** and **calculable.**

2. **Fast detection** and **response** to cyberattacks requires **not only company-specific solutions** but also **a multi-industry, pan-European platform** for the companies involved in the mobility ecosystem. To effectively address the challenges I've outlined, **we're calling for a European solution at the eighth Allianz Autotag: a multi-industry Automotive Security Information Center.**

   We're dealing with a potential threat that doesn't stop at company walls or national borders, and we believe that such a **center needs to combine the competencies of multiple institutions**, including government agencies, vehicle manufacturers, automotive suppliers, telecommunications operators,

research institutions, the repair industry, and the insurance industry. The primary purpose of an Automotive Security Information Center would be to ensure that the mobility ecosystem can prepare for and respond to security threats, vulnerabilities, and incidents so that everyone involved can optimally manage their own business risks and the customer's risks as third parties. Everyone involved can exchange their information, deduce threats from documented attacks, and then develop **steps for individual** and **joint IT risk management**. As an **operator**, in addition to a public organization, private companies or associations can also come under consideration for this purpose. The collected information about detected and actual events will accumulate in a **knowledge database**. Having access to this information will be important for the automotive industry and for scientists, researchers, trainers, and policymakers. This kind of interdisciplinary exchange of information will **encourage transparency** and **thus security as well**. In addition, ethical computer hackers known as **white hat hackers** could make a further constructive contribution toward IT security, even outside traditional professional conferences. This group can be expanded with the addition of institutionalized forensics and insurance companies.

**Europe is one of today's leaders** in **vehicle development** and **construction**. But we'll only be able to maintain that leadership if we're **also leaders** in **IT security for vehicles** and the **entire mobile ecosystem**.