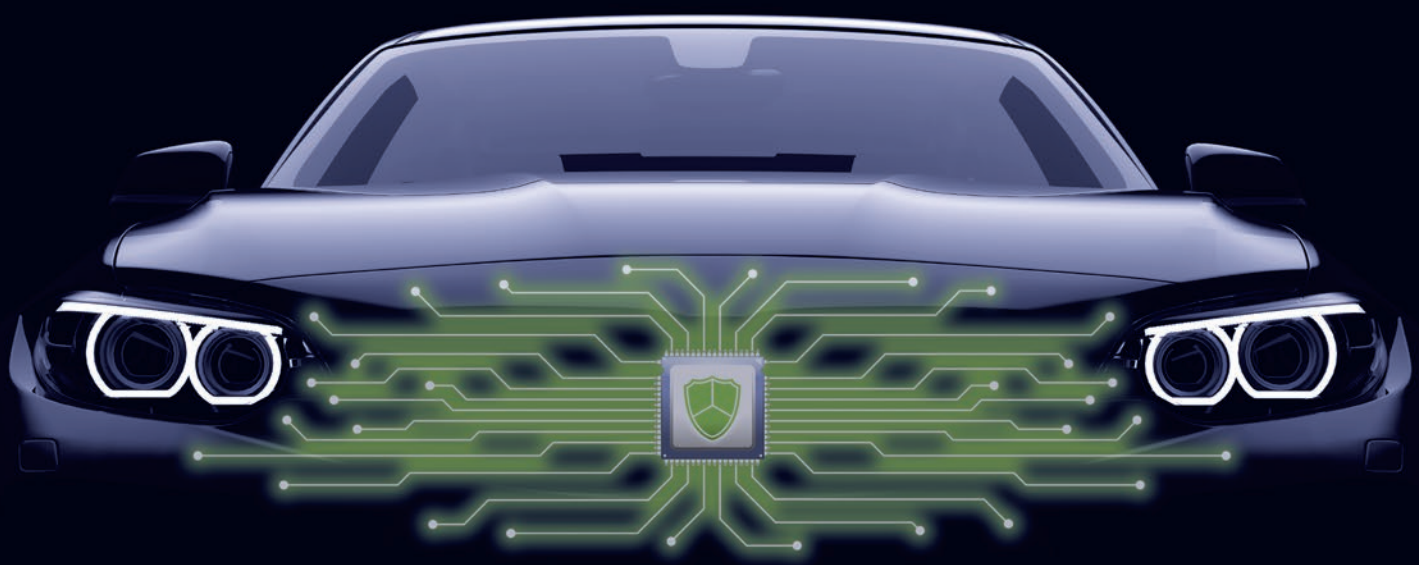
escrypt
SECURITY. TRUST. SUCCESS.

in co-operation with
KPMG

Whitepaper

How digitalization and automation present automotive manufacturers and suppliers with new security challenges.

Cybersecurity full speed ahead



When Carl Benz unveiled the automobile in 1886, he had rather different safety/security concerns than today's automakers. From mechanical safety to the invention of the seatbelt, a century of automotive development would play out before cybersecurity became relevant. Since then, various cyber attacks on cars have brought the topic to the attention of the general public and of lawmakers. A working group at the United Nations is now developing a regulation that represents a paradigm shift for the entire sector: in the future, the type approval of vehicles will be possible only when a certified cybersecurity management system (CSMS) is in place. This means cybersecurity needs to be on the agenda of every automotive CEO.

Contents

Evolution of automotive cybersecurity

One of the first published hacks of an automobile was carried out by a group of scientists led by Stephen Checkoway in 2009. They describe how they connected a laptop to the car's onboard diagnostics port in order to gain access to the vehicle's internal network. This allowed them to manipulate critical systems in the car. For example, they were able to switch off the engine and block the brakes. In such attacks, scientists use various weak points in the vehicle network and ECUs to send manipulated data records to the car's embedded systems and tamper with their functions. Although hackers would be hard pushed to connect a laptop to the vehicles of their victims, they could nonetheless use smaller, remote-controlled devices to wreak their mischief and jeopardize the safety of road users.

In 2010, a 20-year-old managed to manipulate over 100 cars via remote control, such that they would no longer start. The "Texas Auto Center" rental company had fitted hardware in its hire cars that could be controlled via an online system. This system allowed the rental firm to deactivate the ignition if the customer did not pay. The hacker had been made redundant a short time previously and now gained access to the system via an employee account. Subsequently, he got control of the corresponding hardware components of the rental car fleet.

An even more critical situation arose in 2015, when Charlie Miller and Chris Valasek managed to take remote control of a Jeep. Via the SUV's entertainment system, they gained access to its multimedia systems, windshield wipers, and air-conditioning system and controlled the brakes and the speed of the vehicle. They stopped the car, whose driver had been hired as a tester, in the middle of the highway. To do this, they did not need a cable to connect up with the car as in the paper from 2009, but used the vehicle's internet connection. As a result, Chrysler had to recall and patch around 1.4 million vehicles.

These days, there are regular reports of new attacks, most of which exploit the increasing digitalization and connectivity of vehicles. This development highlights the risk that insufficiently protected vehicles pose for manufacturers, owners, and road users. With the increasing number and complexity of the IT systems fitted in cars, the demands placed on cybersecurity are growing rapdily. Viewing a vehicle as a closed-off system is the opposite of a adequate, risk-based security approach. New digital (online) services being offered in cars, communication between vehicles and manufacturers (over-the-air updates), vehicle-to-vehicle communication (car-2-car), communication between cars and infrastructure (car-2-infrastructure), and communication with smartphones and devices from third-party providers – all these developments present huge attack surfaces that need to be systematically analyzed and controlled. ■

New requirements for cybersecurity in vehicles

Activities are underway worldwide to further regulate and standardize automotive cybersecurity. There are legislative proposals in the US Congress, the Cybersecurity Act in the EU, the Chinese ICV program, and new guidelines from JASPAR in Japan. They all share three main trends: a stronger focus on the specifics of the automotive industry when addressing cybersecurity; the challenge and requirement to uphold security in the field; and the increasingly compulsory nature of regulations and the inclusion of cybersecurity at type approval. These trends are particularly visible in the UNECE WP.29 TF-CS/OTA and in the ISO/SAE 21434, which define explicit management systems for the protection of vehicles.

UNECE WP.29 TF-CS/OTA

The United Nations World Forum for Harmonization of Vehicle Regulations (WP.29) is currently drafting a regulation that makes cybersecurity relevant for the approval of new vehicle types. The TF-CS/OTA task force's proposal consists of two core requirements: the operation of a certified cybersecurity management system (CSMS); and the application of the CSMS to the specific vehicle type at the time of type approval. The EU is planning to make these requirements mandatory from 2022.

Considering typical development times in the automotive sector, manufacturers and suppliers need to start implementing these cybersecurity requirements today to ensure their next products receive type approvals. To do this, they must follow a risk-based approach that can continuously determine, achieve, and maintain a suitable risk level for the vehicle type, its external interfaces, and its subsystems. This includes managing dependencies and information from suppliers, service providers, and other third parties from a cybersecurity perspective.

In view of the constantly changing threat environment and the length of vehicle type lifetimes, a primary focus of a compliant CSMS is on the phase after the start of production and on continuous risk management during vehicle operation. As a result, automotive security must be tackled on the technical and the organizational level. While manufacturerer and suppliers can draw on experience with information security standards such as the ISO 27000 series, the principal challenge in the design of a CSMS consists in taking the specifics of the automobile into account. In addition to the high complexity both of the product and of the supply chain, other critical aspects are the interactions with functional safety, the observance of environmental regulations, and theft protection.

ISO/SAE 21434

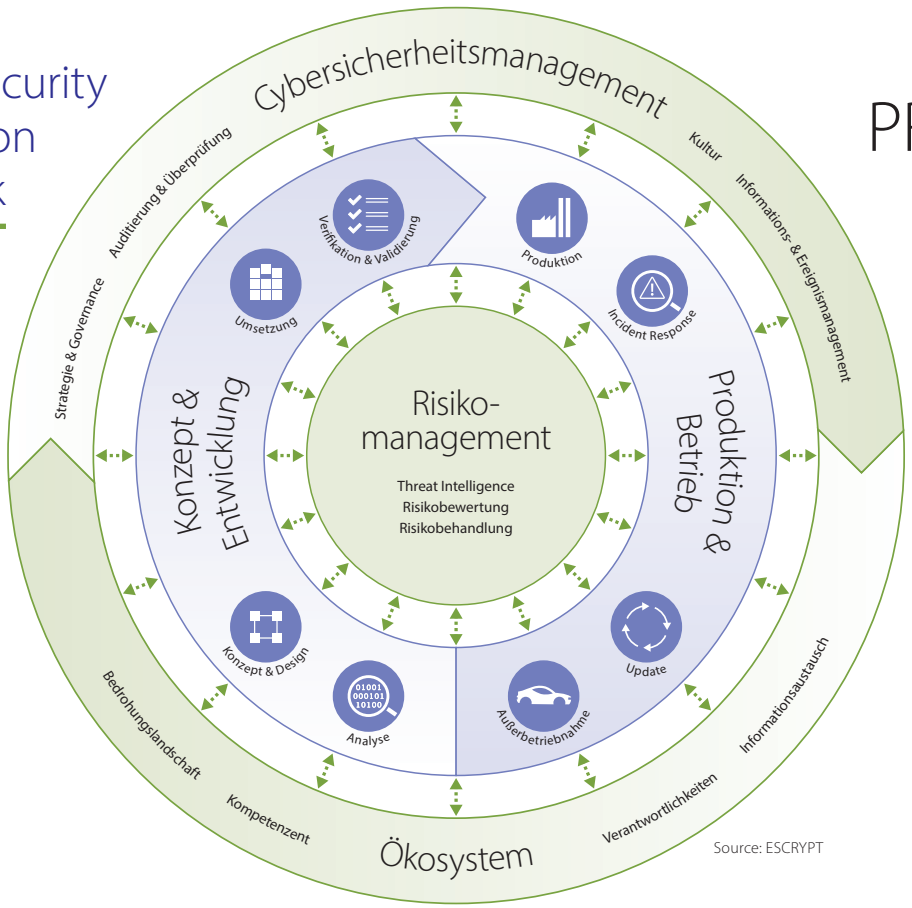
Alongside the TF-CS/OTA, the automotive industry is also developing the ISO/SAE 21434 standard for the cybersecurity of vehicles within the framework of the International Organization for Standardization (ISO) and SAE International. Similar to the CSMS defined by WP.29, this standard puts the focus on appropriate security organization and having adequate processes throughout the life cycle of vehicles in order to protect them from cyber attacks. Given that an accompanying document to the UN draft regulation refers consistently to this standard for the implementation of CSMS requirements, the ISO/SAE 21434 warrants particular attention. It will create a industry-wide common terminology and joint understanding of key activities upon which manufacturers and suppliers can build their interfaces, shared responsibilities, and processes. The final version is expected at the end of 2020. ■

Impact on the automotive industry

The automotive industry is no stranger to government regulation. However, there have been only a few examples of statutory regulations relating to automotive product security. On account of OEMs' growing demand for transparency about their suppliers' maturity of information security, the German Association of the Automotive Industry (VDA) has drawn up a catalog for information security assessments (ISAs). With the Trusted Information Security Assessment Exchange (TISAX) model, OEMs have a mechanism at their disposal for checking how suppliers handle sensitive data, based on the catalog – for example, in the context of prototypes.

In addition to TISAX, ISO/SAE 21434 now also sets requirements for cybersecurity and product security. In recent years, the automotive industry has strengthened vehicle protection. With the advent of the UN regulation, however, cybersecurity will be binding; rather, it will become a prerequisite for business success and competitiveness for both manufacturers and suppliers. In the context of the digital transformation, it is a question not just of fulfilling the regulation, but of finding the best possible approach with the maximum effectiveness for the corporate strategy and product roadmap. Companies must implement comprehensive organizational and technical measures that will enable them to define, control, manage, and improve cybersecurity on an ongoing basis along the entire value chain. Consequently, demand is already growing today for what are known as gap analyses, which measure a CSMS's implementation status and derive targeted improvement roadmaps based on the results. ■

Product Security Organization Framework



Source: ESCRYPT

Expert support

Like many other industries, the automotive industry will face a shortage of skilled personnel in this field. Experts who understand both cybersecurity and the special requirements of the automotive industry are rare. At the same time, digitalization is raising cyber risk levels so fast that in-house knowledge for automotive product security typically does not keep pace. Companies will find it difficult to solve all security challenges with their own resources in time. The inclusion of cybersecurity in type approval means it is critical to reliably implement all requirements as efficiently as possible at the first attempt.

Cooperation of ESCRYPT and KPMG

The consultancies ESCRYPT and KPMG offer expert services to guide manufacturers and suppliers successfully through the process of developing compliant security solutions. ESCRYPT has a wealth of experience in taking automotive cybersecurity from concept to series production and subsequently maintaining the targeted security level during operation. KPMG is an expert in information security and in the assessment and rollout of security management systems. Their cooperation takes these strengths and combines them to holistic approach that increases the utility for customers. For example, any changes that are required at the organizational and process levels can be designed in such a way that the effects on the development and the operation of the security solutions are taken into account and optimized.

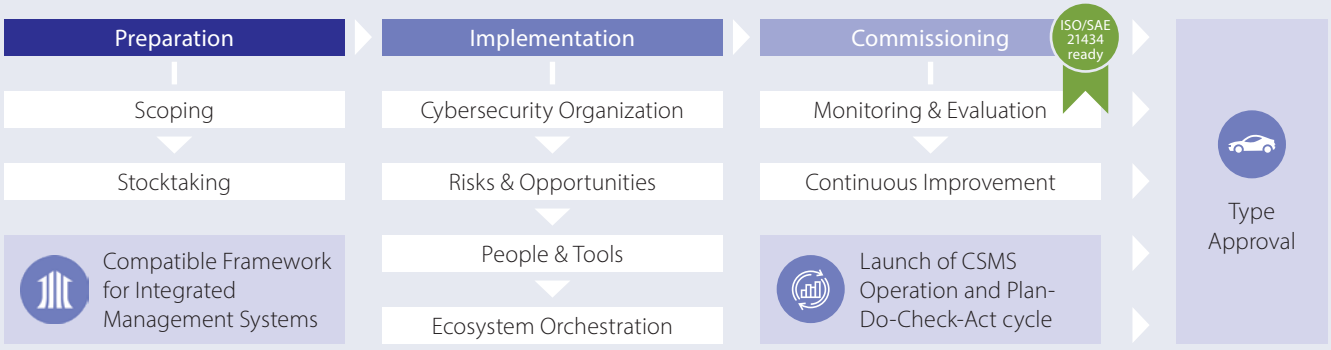
Proven approach

ESCRYPT and KPMG support the automotive industry in all relevant markets and niches, from manufacturers of luxury sports cars to the global top 5 OEMs and leading suppliers for highly automated driving. The services follow a proven methodology based on decades of experience that the cooperation partners have built up. The framework for rolling out a CSMS consists of three main steps: a) preparation, b) implementation, and c) commissioning and continuous improvement.

Building on existing strengths

In light of the complexity of the overall challenge posed by digitalization and the onus of proving cybersecurity that will soon be compulsory for type approval, it is vital to avoid reinventing the wheel. Instead, existing strengths must be leveraged and build upon and partial solution must be integrated into a full compliant cybersecurity management system. Existing strenghts may include information security management systems (ISMSs), quality management systems, and established practices for achieving functional safety. To help with this process, ESCRYPT and KPMG offer specialized audits and fit/gap analyses that identify potential gaps to the relevant standards and uncover existing strengths, enabling companies to establish benchmarks and prioritize measures that will maximize return on investment and lead companies to their goal by the quickest and best possible route. ■

Proven and structured methodology for rollout of a CSMS



Source: ESCRYPT

Contact

Dr. Moritz Minzlaff
Senior Manager
moritz.minzlaff@escrypt.com
Telephone +49 30 40369-1901

Holger Breuing
Director Strategy and Portfolio Management
holger.breuing@escrypt.com
Telephone +49 711 3423-3116

ESCRYPT GmbH
Wittener Straße 45
44789 Bochum, Germany
Telephone +49 234 43870-200
info@escrypt.com

www.escrypt.com

Hans-Peter Fischer
Partner, Cyber Security
hpfischer@kpmg.com
Telephone +49 69 9587-2404

Jan Stölting
Senior Manager, Cyber Security
jstoelting@kpmg.com
Telephone +49 69 9587-6273

KPMG AG Wirtschaftsprüfungsgesellschaft
THE SQUAIRE
60549 Frankfurt, Germany
Telephone: +49 69 9587-0

www.kpmg.com
www.kpmg.com/socialmedia

Status: 02/2020