AUTOMOTIVE CYBERSECURITY: CONNECTED CARS UNDER ATTACK

AUTHORS

ANTHONY DI PRIMA

Anthony DI PRIMA is a Senior Manager at Wavestone in charge of the Cybersecurity for Manufacturing & Industry 4.0 offer development, as well as the area of IoT and Smart Product cybersecurity, particularly in the automotive industry.

DR. THIEMO BRANDT

Dr. Thiemo BRANDT is a manager at Q_PERIOR responsible for the automotive team and the area of automotive cyber security.

This publication was written with the collaboration of Benoit Ladieu

At the beginning of 2019, Q_PERIOR and Wavestone established a partnership based on trust and transparency. We are very glad to see that the synergy between our two firms is being strengthened every day.

Throughout the years, our two companies have gained invaluable experience in the automotive industry, both in Germany and France, and we strongly believe that we can leverage this combined experience and create further value for our clients in Europe.

This joint paper illustrates our willingness to work together and share our beliefs. Cybersecurity is a competence area for us and is a focus of our partnership. In the automotive industry, new regulations will trigger a major transformation of car manufacturer's core activities, from car engineering to connected services, and cybersecurity will become a key requirement for future vehicle type approval.

INTRODUCTION

Future cars are on their (high)way to the digital world

Whether we want it or not, the automobile is getting connected, and we are not talking the occasional traffic information you already get from Google Maps on your smartphone, or even better, in your Apple CarPlay or Android Auto on your cars infotainment system. We are talking about a permanent connection of your car and its systems to the Internet. Car2X communication will include cars independently sending information to other cars, infrastructure and various backend systems.

Everyone owning a smartphone secretly knows that all his/her data is somehow shared with Apple, Google, Amazon and whatever fancy app you just downloaded to your homescreen. But what about the data of your car? Your personal movement profile, your home address, your work address, your favourite restaurant, your kid's school and everywhere you move (by car). Besides the question of who owns this data, the main question should be: who protects this data?

Compromising your data is bad and could be used against your will if not secured properly, and what's even worse is the potential risk of hacking your car. Let's say you are driving your connected car to work, like every other day. You are going 60mph on the highway and suddenly your steering wheel, which is no longer mechanically connected, rather controlled by 0 and 1, gets disconnected. Cybersecurity is not an issue that can be ignored by agreeing to the disclaimer; it's a threat to your own personal safety.

STATE OF THE ART

Where are we right now?

To understand where technology is going, we must investigate where technology is coming from. Manufacturing automobiles is not a new business model. In fact, there are several international OEMs which recently celebrated more than 100 years in the business. This creates a rich history of dealing with new and changing technologies over the last decades. So, what's the big deal about this new "connected car" technology? These past innovations mainly had one thing in common: they were all about the car and thus focusing on the hardware product. Therefore, while electric mobility is a major technology change in the automotive business, it is still a change in powertrain technology and, as a result, it is a hardware change which the OEM knows how to handle. Emerging technologies, like the Internet of Things (IoT) which includes the connected car, are no longer focusing on the hardware development of the products but rather on the software side of life. To state that software development is not the core competence of an automobile manufacturer would be a rather excessive understatement.

This change in technology is offering a range of opportunities, from new revenue potentials (e.g. on demand car functions) to new business models (e.g. shared mobility solutions). But what about the risks this new technology creates? Of course, there is the usual risks of failing to adapt this new technology into your product and thereby losing an advantage in relation to your competition. But that's not all. This new connected car technology comes with a risk of its own which software companies know all so well: the risks of cyber-attacks. The product in which you invested decades of know-how and billions in Research and Development for road and passenger safety is now getting connected to the Internet. This is opening the door for potential intrusions into your car's systems and is therefore creating the risk of compromising your well-developed product.

As recent cybersecurity incidents show, this is not an automotive specific problem, famous cyber-attacks pop up worldwide across all industries. From famous data breaches compromising 3 billion user accounts and their data at Yahoo (2014) to recent incidents at Toyota whereby the personal information of 3.1 million customers got hacked (April 2019), there isn't a day where you can't find a new cybersecurity incident being published. However, cyber-attacks do not stop at compromising data. In 2018, researchers at the Keen Security Lab (a Tencent company) managed to gain root access to the CAN-Bus of various new BMW models. This access allowed them to gain control of critical functions of the car, like engine control, steering and breaking. They managed to gain access locally by connecting a prepared USB-device and over the air by using the GSM network. This shows the potential of what is at risk. Your car can be secured to the highest standards in automotive development right now, with state-of-the-art assistant systems, passive safety & emergency assistants, and still, your car will not be safe.

So, what can we do and what needs to be done? Just like the fact that hackers rarely work alone, managing the risk of cyber-attacks will be a joint effort for the automotive industry. The lack of standards, rules and regulations for cybersecurity is a huge impediment right now. To answer our initial question, "Where are we right now?", we are in desperate need of a cybersecurity standard for connected cars, helping everyone involved in automotive development to reduce the risk of cyber-attacks.

STANDARD SETTING

In need of joint forces

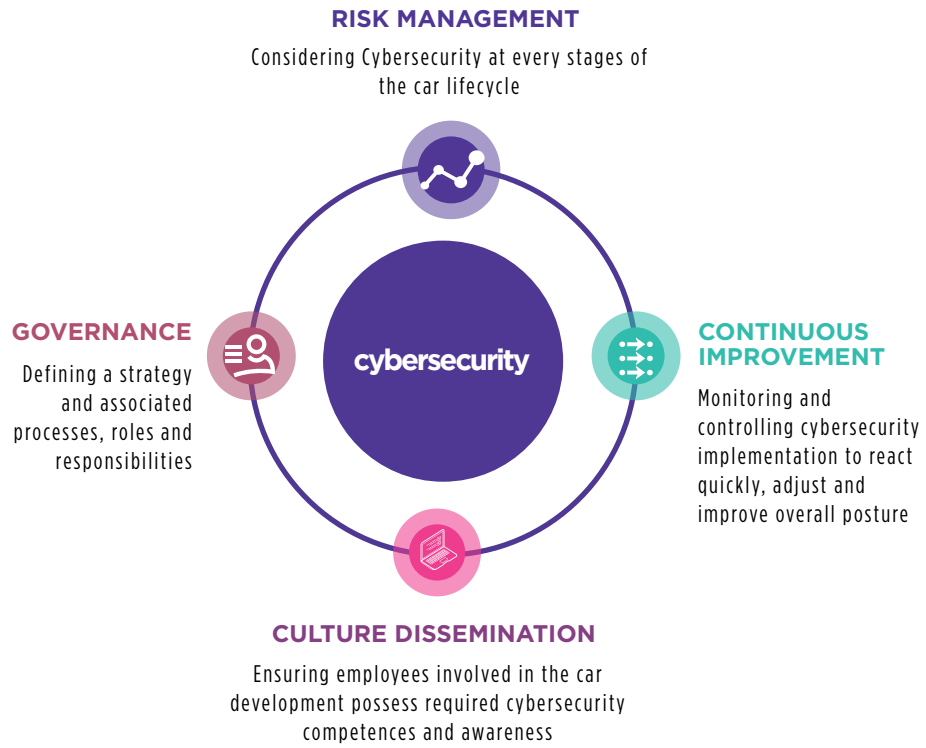
The specificities of managing cybersecurity for connected vehicles, which involve a complex engineering, sourcing and production environment, were not allowed to simply apply existing cybersecurity standards, such as ISO27k. A work group, headed by ISO and SAE, was created to define the ISO/SAE21434 – Cybersecurity for Road Vehicles Standard, superseding the SAE J3061 standard, in order to address the characteristics of the automotive industry. The ISO/SAE21434 standard is focused on proposing a framework to manage cybersecurity organization, processes, risks and so on, within the engineering of road vehicles onboard systems. The standard aims to clarify and align the cybersecurity activities and processes which shall be performed along the vehicle lifecycle within OEM and the whole supply chain. Providing common vocabulary, processes and requirements is a major challenge that is being tackled by the standard since the automotive industry relies on a wide ecosystem of suppliers and partners, involved in the design and production of vehicles. Also, managing cybersecurity over the road vehicles' lifecycle requires adapting the approach, moving from Information System Security to Product

Security. While there are some similarities in terms of Cybersecurity Management Systems (CSMS), the cybersecurity framework to be set is specific and aims to integrate cybersecurity in processes owned by Engineering, Procurement, Quality, Manufacturing, IT, etc.

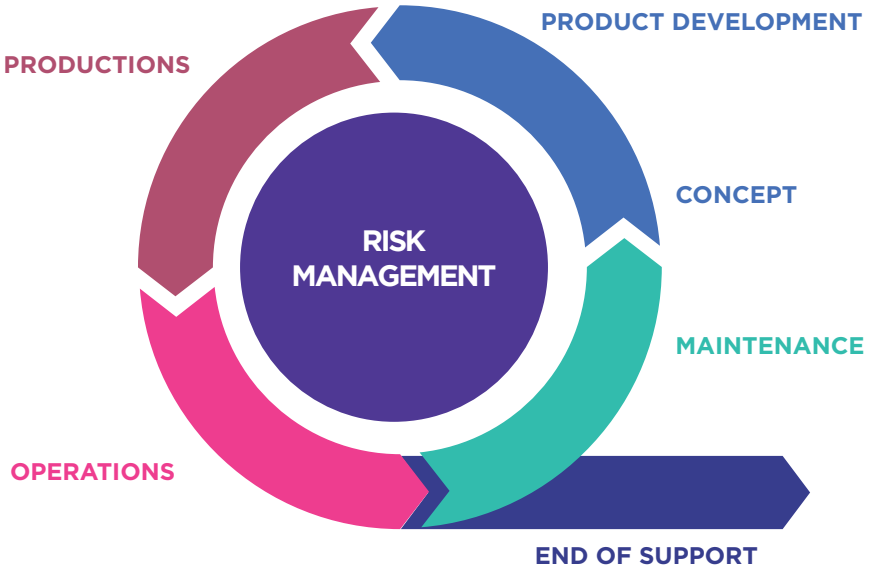
Cybersecurity Management System

The ISO/SAE21434 standard sets up the connected vehicle Cybersecurity Management System (CSMS) by defining requirements for the overall cybersecurity management. This standard also allow OEMs to refer to ISO31000 recommendations on this topic. The CSMS shall include, at the minimum, cybersecurity policy, strategy and rules, global roles and responsibilities, awareness, competences management and continuous improvement. By leveraging on this Management System, OEMs shall implement a risk-based approach at every stage of the connected vehicles' lifecycle, from conception to their decommissioning.

CYBERSECURITY FUNDAMENTAL REQUIREMENTS



RISK MANAGEMENT THROUGHOUT A VEHICLE'S LIFECYCLE



This approach must be relevant with the potential safety, financial, operational and privacy impacts defined by the standard. Risk management and reporting to the appropriate management must be set up in order to limit impacts, such as passenger safety due to cybersecurity risks, while keeping conception and operations costs under control.

Cybersecurity framework for road vehicle lifecycle

The standard then defines the cybersecurity activities to be performed throughout the vehicle lifecycle. During the Concept and Product Development phase, cybersecurity activities are required in order to enable security by design. During **the Concept phase**, onboard systems, for which the cybersecurity assessment is relevant, must be must be designed and thoroughly documented in order to identify risks and associated treatment decisions based on acknowledged cybersecurity objectives and adversary model.

When the concept enters **the Product Development phase**, previously identified cybersecurity requirements must be refined to formalize security specifications which are integrated into hardware and software components design. In this phase, OEMs must ensure specifications are well integrated into the designs by suppliers. Before entering **the Post-Development phase**, a validation at the component, system and vehicle level must be performed to confirm the correct application of cybersecurity requirements and specifications, allowing to validate and further follow the residual risks through the achievement of cybersecurity objectives. The validation includes functional testing of cybersecurity features, vulnerability and penetration testing on hardware and software, but also an end-to-end approach. These activities require specific skills and expertise, as well as an external point of view. The OEM can rely on independent laboratories to evaluate their products. At the completion of **the Product Development phase**, all proof of compliance shall be available for the prior cybersecurity activities.

The production plan and logistic processes shall ensure that cybersecurity requirements from the Concept and Product Development phase are implemented for the product and prevent the integration of cybersecurity vulnerabilities during the Production phase and shipping of vehicles. It means that the OEM shall onboard their manufacturing and suppliers in the construction of their compliance program.

Two main cybersecurity activities shall be set-up during **the vehicle's operational life** by the OEM in order to manage vehicles' residual risks and to take into account emerging vulnerabilities and threats:

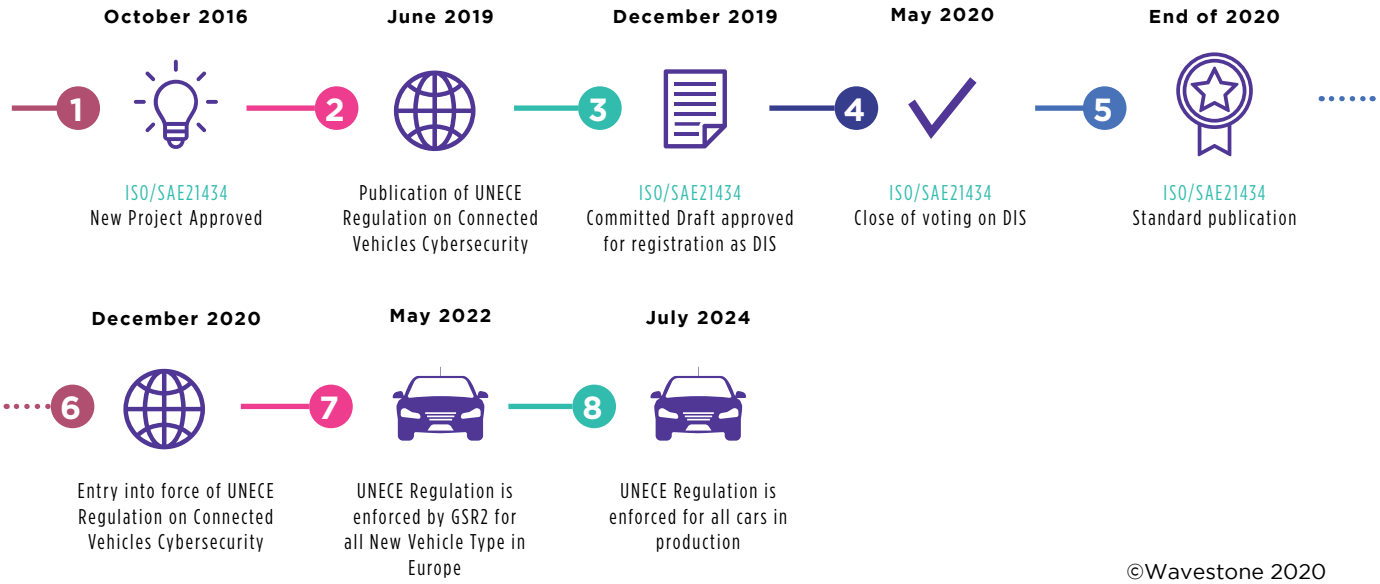
- **Operations to monitor vulnerabilities**, threats evolutions and possible mitigations, assess the cybersecurity events, and defines **processes for incident response** in order to manage events outside the normal course of operations.
- **Maintenance and updates to provide requirements and responsibilities** regarding vehicle maintenance and ensure cybersecurity during and after updates of hardware and software.

The OEM shall also anticipate processes and features to enable **secure decommissioning** of vehicle products that may impact the cybersecurity state when necessary and communicate accordingly about end of cybersecurity support for products.

Outlook

A first draft of the standard was released by the work group at the end of 2019 and the final draft is forecasted for mid-2020. The first regulatory body to frame a regulation based on the ISO/SAE21434 standard is the United Nations through the World Forum for Harmonization of Vehicle Regulations (UNECE WP.29). Indeed, this regulation will impose on the signatory countries a way to manage connected vehicles' cybersecurity, conforming to ISO/SAE21434 specifications.

ISO/SAE 21434 AND UNECE PUBLICATION SCHEDULE

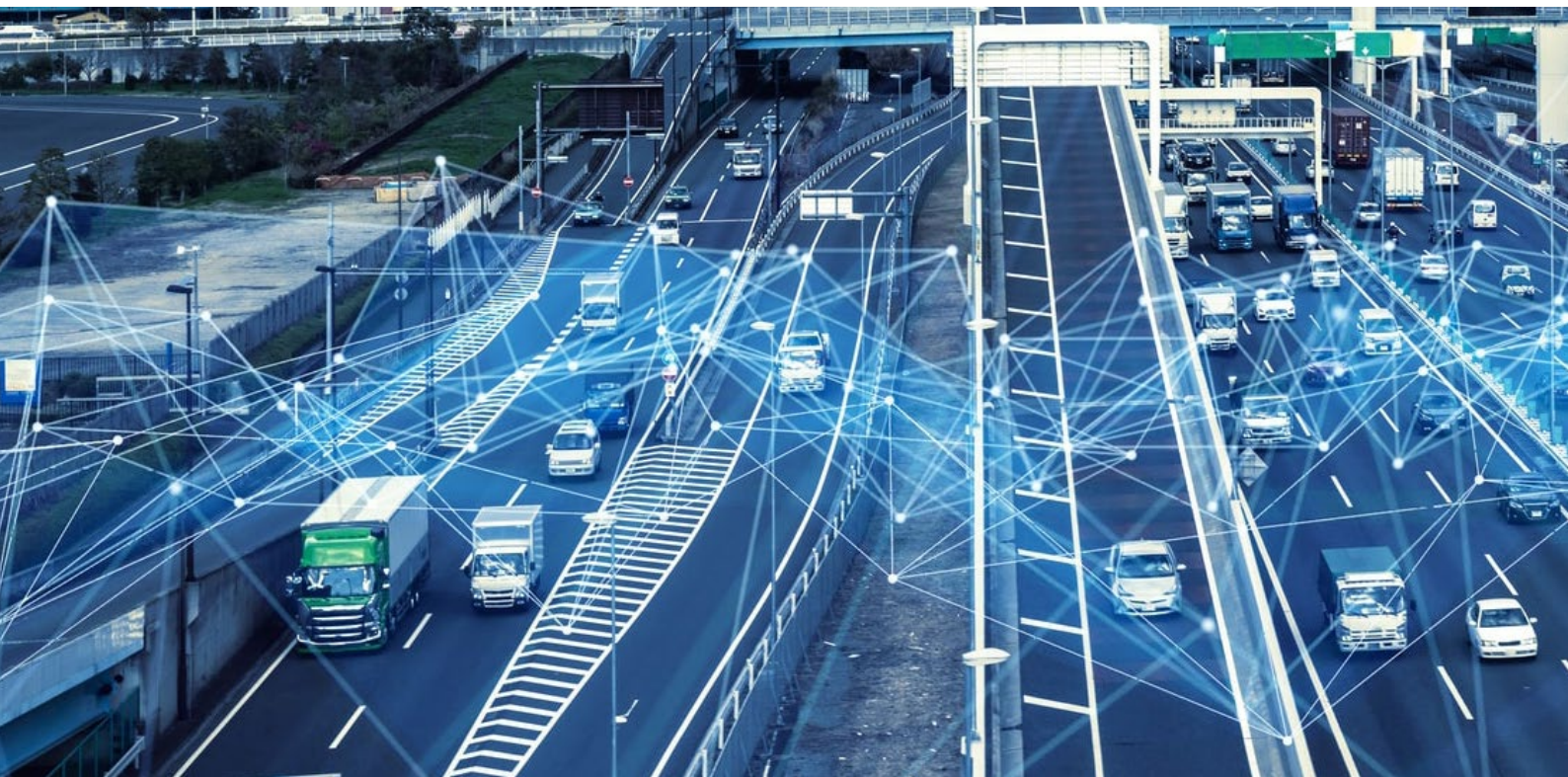


In order to approve any new type of vehicle, two requirements will be enforced by the UNECE regulation, which are:

- an **audit approval** of the organization's cybersecurity management system, which is valid for 3 years
- an assessment of **implemented cybersecurity measures** for the new type of vehicle

These two requirements must be approved by the National Technical Services to validate compliance so that the vehicle can obtain a type approval certificate. For European countries, the European Commission will enforce these requirements for all new vehicle types to be approved as of May 2022.

In the automotive industry, conception and development cycles generally last 3 years or more, this means that OEMs must already consider these requirements in their current programs. However, considering the complexity of the OEM internal ecosystem and its interfaces, compliance programs, including strategy framing and change management, are mandatory to fully set-up cybersecurity integration in all required processes.



SUMMARY

Why cybersecurity should be the focus of every car manufacturer?

So which problems are solved by adapting these new standards to your product development? First, the standard can help the individual OEM to implement the relevant cybersecurity activities in their development process and thereby ensure that everyone is applying the same rules and regulations. These standardized cybersecurity activities will reduce the level of exposure of the car against cyber-attacks and, by extension, will reduce the risk of compromising your car's and your customer's safety. Second, the standard will regulate the level of cybersecurity for the entire lifecycle of the car. This will help to maintain the appropriate level of cybersecurity, not only for the release of the car, but for the whole lifecycle of the car. This will require the OEM to release continuous updates to their connected car while it's already out on the market and on the streets.

This brings us to the question: what isn't solved by the new upcoming standards and what is still to be done? The new standard ISO21434, as explained above, is focusing on the car and the car only. There are no rules and regulations regarding backend, third party or any connected systems. This lack of regulation increases the danger of cyber-attacks to systems outside of the car, and thereby increases the risk of compromising your car through the connection to these systems. In simple words, there is still a lack of a standard for the whole connected car environment. In the future, we need a clear end-to-end approach for the whole connected mobility eco system.

At Wavestone and Q_PERIOR, we believe that, in the future, a standard in cybersecurity will become as important as the NCAP crash test standard is today. This standard has saved lives since 1996 and led to further improvements in passive and active safety systems. In the future, the risk of cyber-attacks will become the main threat for the whole automotive industry. For this reason, a standard for cybersecurity is necessary, not only for the car, but for the whole connected mobility ecosystem.

Q_PERIOR

www.q-perior.com

We at Q_PERIOR are committed to doing everything we can to deliver first-class results for our customers.

Q_PERIOR is an internationally active and independent management consultancy. The company advises customers in a service- and solution-oriented manner with cross-sectoral subject competence as well as a profound understanding of business and IT requirements. As one of the leading German management consultancies, Q_PERIOR sees itself as a partner in digital transformation.

With more than 1,200 consultants at 15 locations worldwide, Q_PERIOR is listed in fifth place among German management consultancies (Lünendonk®).

WAVESTONE

www.wavestone.com

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to inform and guide large companies and organizations in their most critical transformations, with the ambition of a positive outcome for all stakeholders. That's what we call «The Positive Way." Wavestone draws on over 3,000 employees across 8 countries. It is a leading independent player in European consulting. Wavestone is listed on Euronext Paris and recognized as a Great Place to Work®.