WHITE PAPER

AUTOMOTIVE CYBERSECURITY AND ITS IMPORTANCE FOR THE DEVELOPMENT OF FUTURE VEHICLES

THOMAS THURNER AND **GERHARD DI MATTIO**

DEKRA

Connectivity in current and future vehicles is becoming increasingly important, not only improving passenger comfort and safety, but also potentially posing threats. To ensure a high level of safety this paper presents the top issues as important levers for optimizing Cybersecurity for the automotive industry and their significance for the development of future vehicles. In addition, existing regulations and standards are highlighted and new approaches for the implementation of cybersecurity and the essential aspects of a V&V strategy are explained.

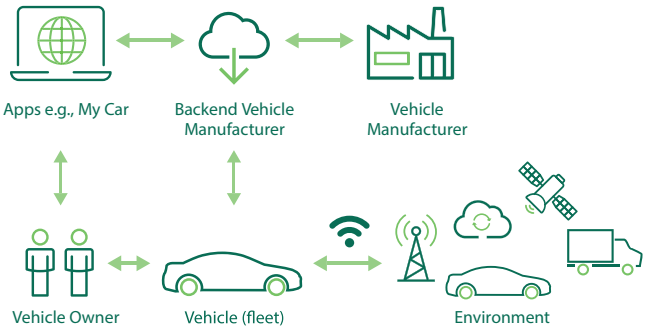
1 Introduction – threats

As connectivity becomes increasingly important to current and future vehicles, not only does it improve passenger comfort and safety, but it can also pose potential threats. Cyber hackers can exploit connectivity to penetrate vehicles and manipulate their systems. In the worst-case scenario, this can endanger the safety of passengers and other road users, resulting in accidents with fatal consequences.

Examples of vehicle communication interfaces (VCIs)

This creates the following attack surfaces:

- Direct access to vehicles, making it possible to infiltrate all kinds of USB components and exchange software and hardware components
- Close-range access to vehicles through keyless go and entry systems or Bluetooth/WiFi interfaces
- Cloud access to the backend systems of vehicle manufacturers via public networks:
  - Private apps used by vehicle owners (e.g. OEM apps that allow vehicles to be opened or locked, or sensor data to be accessed)
  - OEM remote diagnostic systems



Integration of vehicles into communication infrastructures

- Vehicle-to-infrastructure/vehicle-to-vehicle communication (V2I/V2V)

The issue of shielding vehicles from direct access – and the corresponding risk that systems may be manipulated – has close overlaps with the issue of key possession and the understanding vehicle owners and drivers have of legal or illegal tuning. Nonetheless, manufacturers are responsible for ensuring vehicles are safe from attacks through either near-range or remote systems.

Hacker attacks launched through public networks started to become a known problem through press reports in 2014/2015. By that time, if not earlier, it was evident that attacks launched remotely – from anywhere in the world – could expose connected vehicles to the risk of manipulation during use, and thus pose a potential danger to road users and the environment.

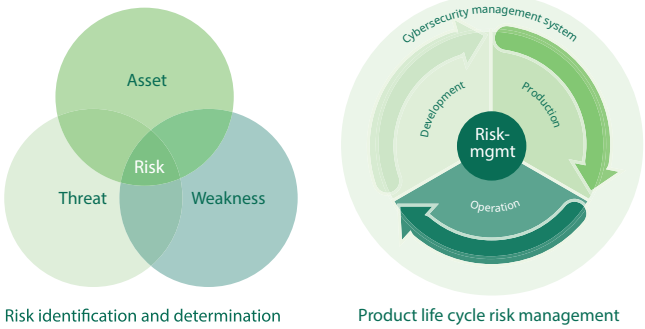
2 Regulations and standards

On the one hand, this threatening situation has been recognised by the UNECE World Harmonisation Forum for Vehicle Regulation in Geneva, which has now issued the new R155 cybersecurity regulation. In 2024, R155 will apply to vehicle registrations under national law in 56 countries (+ the EU as extra formal instance). This only affects vehicle manufacturers.

On the other hand, the International Organisation for Standardisation (ISO) joined forces with SAE International to release the new ISO/SAE 21434 standard (Road vehicles – Cybersecurity engineering). This establishes a technical and methodological basis for cybersecurity (CS) engineering and management. It affects both vehicle manufacturers and the supply industry.

Fundamental principles that affect both regulatory frameworks:

- All manufacturers should consider the organisation and methodology of systematic CS activities. This entails the existence and operation of a cybersecurity management system (CSMS) covering the entire product life cycle with respect to CS activities.
- Evidence must be provided of comprehensive product protection mechanisms aimed at minimising risk.



Risk assessment and management

2.1 Software updates

Software updates have strong overlaps with CS. Unknown vulnerabilities in introduced software are usually discovered by hackers when something special happens and this is then exploited as a route to launch an attack. Since almost all vehicle electronic control units (ECUs) allow software to be reloaded, updates are a good way to fix software vulnerabilities. This includes over-the-air (OTA) updates sent to vehicles via public networks.

Accordingly, corresponding requirements have been established on both the standardisation and regulatory levels:

- UNECE R156: Uniform provisions concerning the approval of vehicles with regard to software updates and software update management systems
- ISO 24089: Road vehicles – Software update engineering

In the following, it is assumed that software updates are a given and it is therefore not discussed in detail how they are implemented.

2.2 UNECE R155

This regulation translates into domestic laws governing vehicle registration in all countries party to the UNECE 1958 Agreement.

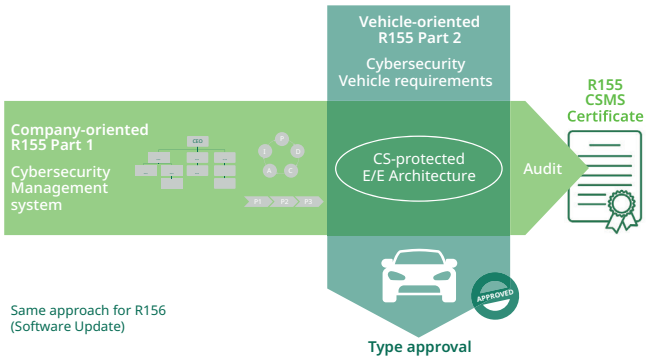
Contracting parties to the UNECE 1958 Agreement [1]

[1] Source: wikimedia.org

This is why the requirements placed on OEMs are formulated on a higher abstraction level than they would be in a standard. Because there is a relatively high degree of discretion regarding how regulations are interpreted, the UNECE also provides further documentation to support interpretation.

OEMs must prove that they have a CSMS in place, they must demonstrate its effectiveness in use, and they must continuously review and maintain their CSMS as a management system. This must be verified by a technical service (TS) and certified by an authority (in Germany: the Kraftfahrt-Bundesamt, or KBA). In UNECE countries (1958 Agreement), an electrical/electronic (E/E) architecture with the specified CS properties cannot be approved according to homologation requirements until it has gained valid CSMS certification.

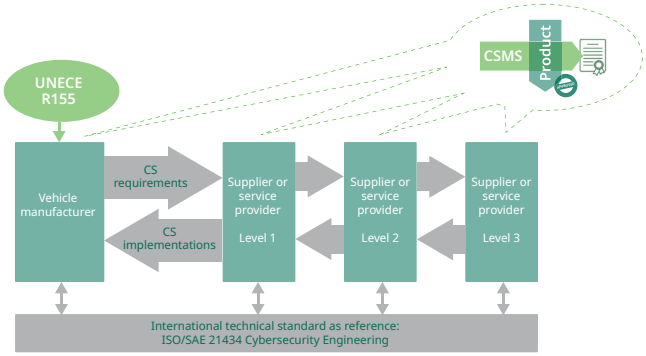
This is a completely new situation for vehicle manufacturers, entailing successful auditing of the organisation – in a highly complex area – as a prerequisite for homologation. CSMS certificates must be reviewed annually and renewed every three years.



The UNECE R155 and R156

- Prerequisites and rules for internal CS activities on an organisational and project level
- CS threat analysis, risk identification and risk management, both for the product itself and for its development and use (TARA: threat analysis and risk assessment)
- Defined CS processes and methods for development, production and aftersales (operation of the product, maintenance, decommissioning)
- Clear rules for CS activities for partners and suppliers, including respective responsibilities
- CS monitoring: continuous monitoring of internationally accessible information on known and new vulnerabilities in product components, infrastructures and tools, as well as threats, attack paths and successful attacks

The connection between regulation R155 and ISO standards ISO/SAE 21434 is shown in the figure below.



Connections between the UNECE regulation and the ISO standard

2.3 ISO/SAE 21434

This standard covers CS risk management throughout the product life cycle, affecting almost all areas of a typical company (R&D, procurement, production, aftersales, HR, IT, QM, marketing, risk and auditing, ...):

So, over and above organisational requirements, how do these regulations and standards affect vehicle development, especially the entire E/E architectures of vehicles, or individual E/E components and systems?

3 New approaches to implementing cybersecurity

A CSMS contains all processes, corresponding process artifacts, descriptions, guidelines and procedural models in order to protect a product effectively from cyber attacks and keep this protection in place for as long as possible during the lifetime of the product. Processes must be defined, implemented, applied in a controlled manner and subjected to continuous monitoring and improvement processes.

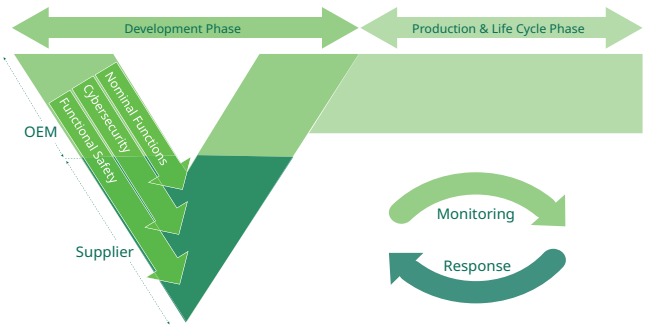
Within the specific conceptual and development context, this entails:

1) CS risk assessment based on TARA methods (according to ISO/SAE 21434) looking at functions on a vehicle level based on a first rough design of an E/E architecture
2) The management of identified CS risks (avoid, reduce, transfer, accept) and if necessary the introduction of iterative changes to initial E/E designs
3) Definition of CS goals, with associated CS requirements, each broken down, in addition to usual specifications affecting functions and functional safety (FuSa). This requires close coordination with stakeholders responsible for functional development, FuSa and CS.
4) Continuous reviewing and adaptation of TARA during development (iterative process)
5) Determination of the nature, scope and duration of the CS support required for products, including rules for termination of support and end of product life
6) Signing of a cybersecurity interface agreement (CIA) with suppliers and service providers, with clear designation and assignment of responsibilities based on the RASIC project management tool
7) Monitoring of CS-relevant information before and during development in order to incorporate new findings via change management procedures
8) Implementation of a verification and validation (V&V) strategy including CS safeguards (vulnerability scanning, fuzz and penetration testing)
9) Final checks on all CS activities looking at the effectiveness, completeness, correctness and consistency of CS assessment, before release for production can take place. This includes the formulation and approval of CS specifications for production and maintenance by means of a post-development report.

Integrating the CS activities outlined above into existing development processes entails:

- Consideration of cybersecurity in parallel to functional development and FuSa
- Extension of the previous V-model (used for the systems development life cycle) to include incident management during the post-development phase. This involves monitoring, including the identification of (new) threats and attacks on a company's products already with customers.

Both of these aspects are shown in the figure below. If this affects products that are already with customers, making it necessary to switch to an incident response level, remedial measures must be introduced with a suitable 'reverse loop' to the normal process of serial development, including analogous V&V activities for corresponding CS 'remedies'.



The extended V-model

4 CS verification and validation (V&V)

A CS V&V strategy basically encompasses four aspects.

4.1 Vulnerability checks

An overview of the known weaknesses and vulnerabilities of components used in hardware and software (libraries, hardware-related firmware, RTOS, ...). Vulnerability checks are performed through continuous CS monitoring, offering insights into the past in order to learn from known errors. The aim is to implement new solutions without known weaknesses.

4.2 Functional testing

The implementation of CS requirements can be checked by using requirement-based assessment methods on a component, system, domain and vehicle level. This must, however, consider whether it is actually possible to assess objects under CS conditions in a real environment, because all testing would be seen by a component as an attack. As a result, objects being subjected to testing need special modes of operation (similar to debug environments) that allow for CS function testing. These operating modes must be extremely tightly protected and monitored, however, so that they cannot be exploited by potential attackers. At the same time, it is important to ensure test objects are continuously monitored during operation by the OEM backend. Test rigs and testing systems must therefore be included in this monitoring as a matter of principle.

4.3 Penetration testing

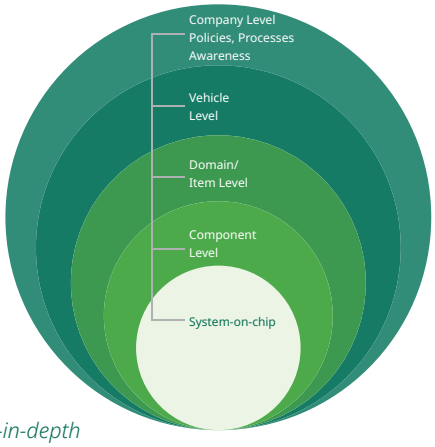
Even after checking for vulnerabilities, after ensuring compliance with design, programming and coding rules, and after conducting comprehensive functional testing, it is still possible for vulnerabilities to remain undetected and these may be identified and exploited by attackers at a later date. This is why high-risk components are subjected to additional checks, or so-called penetration testing. This is a validation method used by experienced specialists (posing as hackers) in an attempt to compromise an object of interest (e.g. an ECU) over a certain period of time. If they are unsuccessful, this is tantamount to confirmation that CS targets have been successfully achieved, although there is always a residual risk that certain vulnerabilities went undetected.

4.4 Fuzz testing/fuzzing

Fuzz testing is used to round off CS validation. Test objects are subjected to a variety of random inputs, or a critical combination of inputs, with the aim of putting systems under stress and, if possible, rendering them uncontrollable and vulnerable such that they can be exploited by attackers.

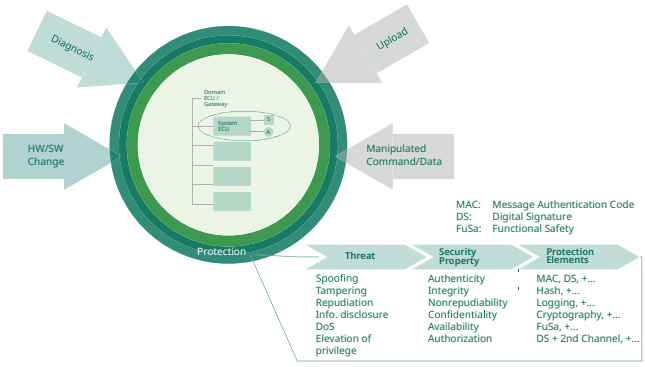
5 Security by design – potential solutions

The cybersecurity of a product can only be assessed from a holistic standpoint. Assessing all TARA factors for functions on a vehicle level shows which assets require protection, points to any potential threats functions may be exposed to and provides scores for the level of CS risk. To reduce risk levels, CS targets are defined, typically based on threat types (e.g. STRIDE categories). Meeting these CS targets results in general protection mechanisms (by threat or protection elements), as described in the CS requirements. The protection mechanisms can then be introduced according to defence-in-depth principles and thus used on multiple occasions.



Defence-in-depth

To do this, several protection or isolation levels are defined that attackers would have to break through in order to compromise the overall system. On the highest level comes the vehicle itself, under which there are domains, systems or components representing further levels that can be separated and isolated via bus systems, firewalls and segmented buses. Each of these levels is equipped with the same protection mechanisms, although the method of implementation is adapted to the respective level.



Possible protection mechanisms on the system or ECU level

5.1 Examples of protection mechanisms

An overview of the known weaknesses and vulnerabilities of components used in hardware and software (libraries, hardware-related firmware, RTOS, ...). Vulnerability checks are performed through continuous CS monitoring, offering insights into the past in order to learn from known errors. The aim is to implement new solutions without known weaknesses.

Secure diagnostics

- Authentication of the on-board diagnostics (OBD) access device via the OEM backend
- Diagnostic firewall: execution of diagnostic tasks only in dedicated vehicle states
- Authorisation approvals through OEM backend
- Public key infrastructure

ECU security

- Authenticated access
- External devices used for diagnostics or programming require access authorisation, which is granted via the OEM backend. The integrity of transmitted data must also be ensured.
- Secure booting
- It must be ensured that systems can only be booted using the correct software released by the OEM.
- ECU operating modes
- An ECU must have different operating modes during its life cycle, and it must be possible to switch securely between modes (with authentication).
  - Development, V&V
  - Production
  - Operation/use
  - Diagnostics and software uploads
- Key and certificate management
- Keys and certificates establish an important basis for authentication and encryption in order to secure confidentiality.
- Software integrity checks
- Checks on the authenticity of software/configurations.
- Hardening of CS operating systems and crypto/high-security modules (HSMs)
- HSM modules for storing keys securely and the support/implementation of crypto algorithms and 'hardened' operating systems.
- Hypervisor protection
- Protected and fully isolated sandboxes for unknown apps from the internet, such as telematic/entertainment control units.

General vehicle security

- Secure release of functions
  Activation of purchasable vehicle functions or the release of functions that depend on driving situations.
- Secure recording of data (secure logging)
  Accurately timed, tamperproof logging of internal processes for forensic data analysis in case of error, but also for general documentation purposes.
- Intrusion detection
  Detection of process anomalies caused by attacks/manipulation.
- Encryption
  Safeguarding of confidentiality.
- General protection against the installation of compromised or outdated software and the unwanted modification of authorisations.

Network security, on- and off-board

- Authentication, integrity checks and, if necessary, the encryption of messages on CAN, FlexRay and automotive Ethernet in real time (SecOC or IPse)
- End-to-end security
  Critical functions adhere to the principle of end-to-end confirmation. Reciprocal checks are made at both the immediate point of transmission and the actual point of reception in order to confirm integrity and authenticity. This includes on-board as well as off-board communication between the vehicle and the OEM backend (TLS, VLAN).

6 Conclusion

The automotive industry is currently undergoing a period of rapid change as modernday vehicles become increasingly digital. Assistance systems, self-driving vehicles, smartphone integration and wireless communication between vehicles and their surroundings (V2X) and other vehicles (V2V) have now become key customer expectations, and carmakers are responding to this demand in an effort to maintain or grow market share.

To customers, such functions offer added convenience and security, but the more extensive and thus also more complex they become, the more time and effort industry needs to invest to protect those systems.

Accordingly, the measures required to create connected cars must be based on clearly formulated and universally binding guidelines.

UN Regulations 155 and 156, as well as the ISO/SAE 21434 and ISO 24089 standards, have created a framework for this. To implement them, it is not necessary to reinvent the wheel, however.

Cybersecurity is a new and challenging field for the automotive industry, and fortunately other industries already offer a number of sophisticated processes and tools that can be adapted and reused as required, even if product life cycles in the automotive sector are significantly longer than those of other electronic products.

The cybersecurity of a vehicle thus begins with the concept phase, and given the specific nature of automotive technology, such as the need for suitable encryption and authentication mechanisms, or the need for secure operating systems and communication buses, suitable approaches that can be adopted in this area are ‘secure by design’ and ‘defence-in-depth’.

Combined with the introduction of suitable secure development methods, such as repeated risk assessments (TARA) and special V&V methods, this can minimise the risk of vulnerabilities arising along the entire supply chain – vulnerabilities that may otherwise go undiscovered during product development.

Want to know more? Visit our website or get in touch with our experts!

Thomas Thurner
Head of Automotive Cyber Security Services
of the Digital & Product Solutions division at DEKRA

thomas.thurner@dekra.com

Gerhard di Mattio
Delivery Manager Cybersecurity
of the Digital & Product Solutions division at DEKRA

gerhard.dimattio@dekra.com

About Digital & Product Solutions

Innovating safety and security by creating the intelligent testing solutions that contribute to making the digitalized and connected world a safer place. We are the experts in testing and certifying products and new digital technologies.
We deliver solutions from Cybersecurity, Artificial Intelligence, Big Data, to Connectivity, Product Safety, Electromagnetic Compatibility & Radiofrequency, Product Certification, Medical Devices and Automotive Testing.
Through a global network of 48 state-of-the-art test laboratories and facilities, we offer a broad portfolio of product testing services based on national and international standards as well as industry and customer requirements.

www.dekra-dps.com