Kaspersky ICS CERT

Cybersecurity in the automotive industry: Ensuring compliance with UNECE regulations

Anastasiya Oblogina
Sergey Melnikov

07.02.2024 Version 1.0

Introduction

Automotive cybersecurity has traditionally been a focus of public and regulatory attention. The "Uniform provisions concerning the approval of vehicles with regard to cyber security and cyber security management systems" (UN Regulation No. 155), which were adopted by the UNECE, are currently in the stage of being adapted at the national level. These provisions establish cybersecurity requirements that vehicle manufacturers must comply with in the production of all new types of vehicles, beginning July, 2022.

The UNECE also adopted "Uniform provisions concerning the approval of vehicles with regard to software updates and software update management systems" (UN Regulation No. 156), which stipulates security requirements for the process of updating firmware and applications installed in automotive systems.

The trigger for the adoption of Regulations 155 and 156 was likely the appearance of production vehicles with Level 3 automated driving functions on the consumer market (see Figure 1 for more information about automation levels).

From a technical point of view, the distinguishing feature of Level 3 is the autopilot's ability to take weighted decisions that account for surroundings, although in certain circumstances it is still necessary to switch to manual control of the vehicle.

In 2017, Audi came close to implementing Level 3 automated driving functions in the A8, but the company subsequently abandoned these plans due to legislative inconsistencies that existed at the time.

In 2021, the Honda Legend became the first vehicle with Level 3 automation approved for use on public roads, but this configuration of the car was available for lease only in Japan.

At the beginning of 2022, Mercedes-Benz launched production cars with Level 3 automation in the premium segment (S-Class and EQS), certified in accordance with the rules of UN Regulation No. 157 for lane keeping at speeds not exceeding 60 km/h. In 2022, Mercedes-Benz received a permit to use automated driving functions within Germany. It is slated to receive a permit in several US states in 2024.

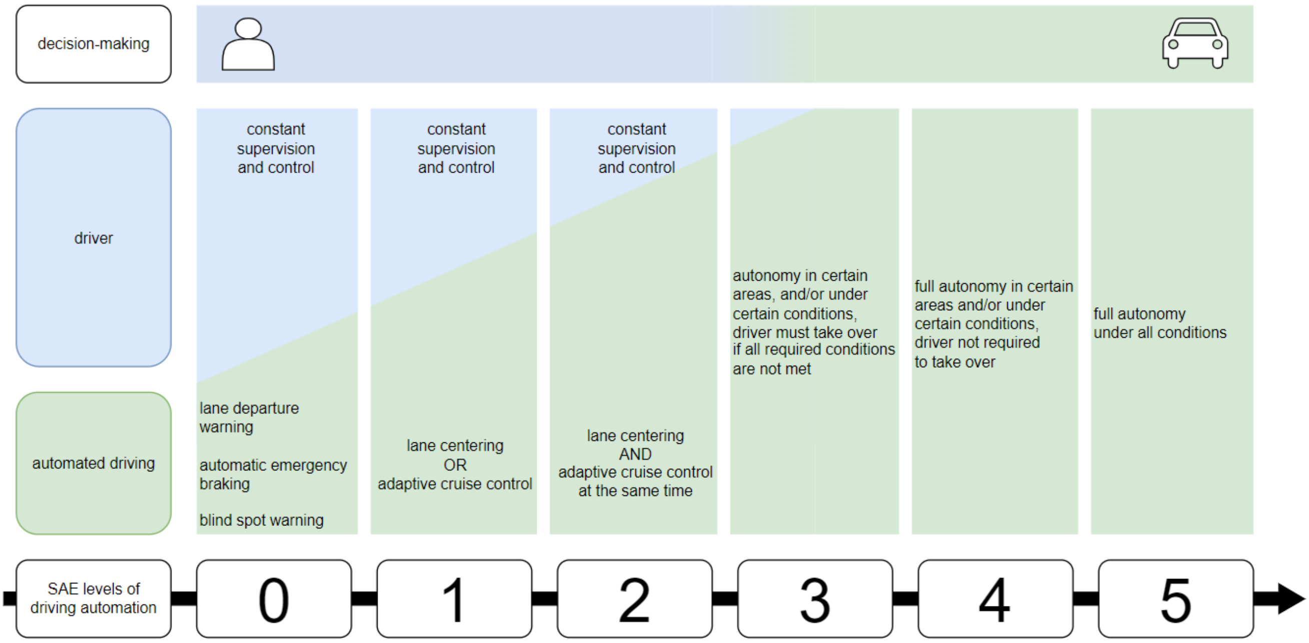

decision-making
driver
automated driving
SAE levels of driving automation
constant supervision and control
constant supervision and control
constant supervision and control
lane departure warning
automatic emergency braking
blind spot warning
lane centering OR adaptive cruise control
lane centering AND adaptive cruise control at the same time
autonomy in certain areas, and/or under certain conditions, driver must take over if all required conditions are not met
full autonomy in certain areas and/or under certain conditions, driver not required to take over
full autonomy under all conditions
0
1
2
3
4
5

Figure 1. SAE Levels of Driving Automation

Simultaneously with the appearance of production vehicles with Level 3 automation (Figure 1), national governments started to adapt legislation to allow these vehicles to use public roads. For example, in 2017 the Bundestag amended Germany's Road Traffic Act to allow the use of vehicles equipped with Level 3 driving automation systems on German roads. In July 2021, similar amendments for Level 4 automation entered into force.

According to this Act, a vehicle manufacturer must submit to authorized bodies (the Kraftfahrt-Bundesamt or an authorized technical service) the results of an analysis and assessment of cybersecurity risks and must demonstrate that the vehicle is properly protected from cyberattacks over its entire life cycle, from the development stage to end-of-life management.

However, national laws to establish vehicle manufacturers' responsibility for vehicle cybersecurity are not sufficient by themselves, since the vehicle market is global. This is why requirements must be unified at an international level.

The UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) works to harmonize vehicle standards on an international level. The regulatory requirements for vehicle manufacturers being developed by countries that belong to the forum invoke the principle of mutual recognition of certification results for vehicles and individual components. That is, the results of certification conducted in one UNECE member state are recognized in the rest of the member states.

UNECE regulations regarding vehicle cybersecurity are in effect in 64 countries that have signed the 1958 Agreement[1]. On February 17, 1987, Russia (USSR) joined the 1958 Agreement, which regulates the activity of forum members states.

To sell their vehicles in the markets of member states, countries that do not belong to the ECE must ensure they comply with UNECE requirements.

The table below presents a list of vehicle categories covered by the requirements of UN Regulations 155 and 156:

Vehicle category	Category description	Applicable requirements
L6	Four-wheeled vehicles with a mass not exceeding 350 kg, engine displacement of 50 cc or less, and maximum design speed of 45 km/h	UN 155, if the vehicle complies with Level 3 automation or higher
L7	Four-wheeled vehicles with a mass not exceeding 400 kg and maximum continuous rated power of no more than 15 kW	UN 155, if the vehicle complies with Level 3 automation or higher
M	Vehicles with four or more wheels, designed to carry passengers	UN 155 and UN 156
N	Vehicles with four or more wheels, designed to carry cargo	UN 155 and UN 156
O	Trailers with at least one ECU	UN 155 and UN 156
R	Agricultural trailers	UN 156
S	Interchangeable towed agricultural and logging equipment	UN 156
T	Any motorized, wheeled, or tracked agricultural equipment with at least two wheeled axles, capable of moving faster than 6 km/h	UN 156

[1] An agreement on the acceptance of approved technical rules of the UN for wheeled vehicles and equipment and other parts that may be installed and/or used on wheeled vehicles, and on the conditions of mutual recognition of official certifications issued on the basis of these UN rules

Starting in July 2024, UN Regulations 155 and 156 will become mandatory not only for new types of vehicles, but also for all new vehicles produced. Some manufacturers have already begun to assess their own level of compliance and prepare for certification. However, this may be difficult in the absence of recommendations and technical regulations on ensuring compliance, which national regulators have not yet released.

We propose to investigate how to avoid turning certification preparation and the time and resources spent on it into purely "paper security", but instead to improve in practice the cybersecurity of vehicles and businesses in the automotive industry. To do this, we must first understand which objects are subject to these requirements and how we can systematize and minimize cybersecurity risks that are relevant for these objects.

We will explore these issues in this article. We will also consider what UN Regulations 155 and 156 require from vehicle manufacturers in reality, and show how to ensure compliance with requirements and prepare for certification if necessary.

Cybersecurity in the automotive industry

Cybersecurity is a very significant issue for every player in the automotive market – from major international professional associations to small suppliers of electronic components. Driving a car is associated with high risk for everybody on the road: drivers, passengers, and pedestrians. The need to ensure cybersecurity affects other stakeholders as well, such as vehicle fleet operator, carsharing and taxi service providers, and dealership networks.

The automotive industry has a geographically and hierarchically distributed and functionally complex supply chain that includes:

- *the vehicle manufacturer itself (OEM – Original Equipment Manufacturer);*
- *suppliers of individual vehicle systems and modules (Tier 1 suppliers), such as the gearbox, infotainment module, or engine control unit;*
- *their suppliers that make the individual components of the systems and modules, for example, microcircuits, sensors, controllers, operating systems, bearings, actuators, etc. (Tier 2 suppliers);*
- *as well as various service providers.*

For the supply chain participants mentioned above, the words "reliable and safe operation of cars" may imply differing goals, tasks, and usage scenarios. Still, all these participants are coming to a common understanding of the attributes of security that are associated with predictable vehicle behavior and that behavior's compliance with safety requirements. And they all have an interest in preserving these attributes.

What’s more, a vehicle manufacturer and its suppliers should have an interest in ensuring the security of not only their products (vehicles, components, software), but also their infrastructure. Security problems in vehicle manufacturing may lead to problems with vehicles, and that means they could potentially lead to injuries or the loss of life. This is precisely why external regulators impose so many mandatory requirements on the automotive industry.

Relevant cybersecurity risks

In the automotive industry, cybersecurity requirements apply at least to the following objects:

1. the product itself – that is, the vehicle and its components;
2. supporting infrastructure – for example, servers for updating the firmware of electronic control units (ECU);
3. the manufacturer’s ICT infrastructure, whose security is important for the development, manufacture, and subsequent support of products;
4. supply chain of a vehicle’s individual electronic components and systems.

Risks for the vehicle

Modern vehicles have a complex functionally-oriented architecture consisting of several hundreds of integrated electronic components. The broad range of functions (engine control, fuel system control, passenger safety, autopilot, infotainment system), architectures of communication interfaces used by individual components (CAN, LIN, Ethernet, Wi-Fi), communication links with external services and entities (Bluetooth, Wi-Fi, LTE) create a huge cyberattack surface in vehicles.

Successful attacks on vehicles demonstrate that adversaries can use a wide arsenal of tools to penetrate vehicle systems: from physical access to diagnostic ports or electric wiring of data buses, to remote exploitation of vulnerabilities in applications and data transfer protocols. However, in most instances an adversary does not go beyond hacking one or more connected ECUs in a single vehicle.

The consequences of a successful attack on a vehicle may include the theft or modification of data (personal data, payment information, and other user data), installation of malicious code/firmware, disruption or manipulation of individual vehicle functions, theft of the vehicle, physical damage to the vehicle, and injury or death of drivers, passengers, and pedestrians.

Note that such attack scenarios may be realized as a consequence of flaws in the architecture of vehicle systems and the technologies and software used, as well as a lack of crucial tests and checks in the early stages of vehicle development and production. Accordingly, a vehicle manufacturer must implement risk management not only for finished vehicles and their components, but also start doing so as early as possible – in the design stage, before development begins.

There are also indirect attacks on vehicles that exploit flaws in supporting infrastructure, or vulnerabilities in algorithms and protocols used for communications between the vehicle and external entities and services. Conversely, adversaries may use vulnerabilities in a vehicle's electronic systems (for example, vulnerabilities in protocols for authentication or data transfer in user applications) to penetrate the services of supporting infrastructure.

Supporting infrastructure risks

The supporting (backend) infrastructure of vehicle services is generally a cloud solution that includes application, data, and update servers. The services of supporting infrastructure can be deployed by the vehicle manufacturer as well as third-party platforms. Some services may be supported by taxi fleets (telemetry processing), auto repair shops (maintaining an electronic service log), charging station networks (supporting a loyalty program), etc.

It is worth highlighting the vehicle telematics service, which not only collects and analyzes information about the operation of vehicle systems, but may also include C&C servers that under certain circumstances are capable of sending control signals to vehicle systems (for example, commands to remotely start the engine or lock or unlock doors).

The following are examples of attacks on supporting infrastructure:

- uploading and installing a fake update;
- uploading fake backup copies of data or configurations;
- sending illegitimate commands from an adversary's C&C server to a vehicle;
- attack on the servers of supporting infrastructure (for example, network management servers for charging stations) and the subsequent leaking of personal data and payment information;
- changes made while servicing a vehicle at an auto repair shop that result in a breach of security (configuration changes, deployment of a rootkit, etc.).

Attacks on the servers and network of supporting infrastructure may disrupt their operation and result in the theft, manipulation, loss, or spoofing of the data being processed. Examples of attacks on supporting infrastructure include infecting backend servers with malware (for example, ransomware) or stealing data after exploiting vulnerabilities in authentication or session management algorithms.

If the services or data of supporting infrastructure become unavailable, certain infotainment system functions may become unavailable too, and more serious consequences may follow: failure of the driver assist system during driving, or the inability to unlock the vehicle or start the engine.

For vehicle manufacturers and other stakeholders, any weakness in a component of a future vehicle or supporting infrastructure is fraught with long-term risks. Poorly written component code and unsecure architecture in the over-the-air update infrastructure do not immediately affect the security and continuity of processes. However, in the long term, the vehicle may not be able to withstand cyberattacks, potentially impacting security and functionality. As a result, the manufacturer might be forced to recall some products or invest in expensive activities to offset risks.

Risks for the manufacturer’s ICT infrastructure

A vehicle manufacturer is an industrial organization whose structure combines the ordinary ICT infrastructure of a back office, i.e., auxiliary and supporting business units (accounting department, legal department, logistical support for the office, etc.), with the infrastructure of the development unit, the production segment, and the servers of the supporting infrastructure.

Threats associated with ICT infrastructure are characterized by high operational risks. An intrusion into the information systems of the back office, the R&D department or the production infrastructure through the ICT infrastructure could disrupt production schedules, delay or halt production, cause malware infections of firmware or updates, and lead to leaks of design information, including leaks of intellectual property and know-how.

For example, on August 29, 2023, Kendrion, a Dutch manufacturer of electromagnetic car parts and control units, reported that its ICT infrastructure had been hacked and that unknown attackers had gained access to the company’s business systems. Kendrion disabled the attacked systems and launched an investigation into the incident, bringing in external experts to assist. The company did not deny the possibility of a data leak, but did not provide details about the type of information the attackers may have accessed. LockBit, a ransomware group, claimed responsibility for the attack and threatened to publish the leaked data on September 2. On September 5, Kendrion announced that key business systems had been restored.

And on March 27, 2023, SAF-HOLLAND SE, a German manufacturer of chassis components for trucks and cargo trailers, disclosed a cyberattack on its ICT systems. While responding to the incident, the targeted systems were disabled, halting production at several of the company's sites. Company officials estimated that the downtime would range from seven to 14 days. In May, it was announced that the cyberattack resulted in a temporary loss of revenue of approximately 40 million euros.

Car manufacturing and development typically involve strict deadlines for the release of specific models. Accordingly, when processes that support core activities (production and development) are disrupted as a result of a successful attack, serious risks of missed deadlines and financial losses arise.

A disruption of the work of supporting business units negatively affects the development schedule, causing deadlines to slip and incurring additional costs to restore the normal operation of the back office as well as the main with development and production processes. With fixed release dates for new models, less time and resources remain for product development and launch activities. Accordingly, slipping deadlines may negatively affect code quality (resulting in so-called technical debt) or lead to the selection of non-optimal or inadequate vehicle security measures and tools.

Most risks related to the ICT infrastructure are short term. An exception is threats to vehicles and their components that are planted through hacked infrastructure and backdoors left in code. However, the operational risks associated with cyberattacks, for example, ransomware and data stealers, are more likely and relevant at present.

Cybersecurity risks associated with supply chains

Vehicle manufacturers may not be able to come up with an objective assessment of the maturity of security practices in a supply chain. This can lead to disruptions of supply processes and the compromise of supplied components and services.

Suppliers may not provide information about components they use that are developed by third parties. A vehicle manufacturer may also lack information about whether a supplier uses secure software development practices, what checks they have in place, and at what stages these checks are performed. Notices about discovered vulnerabilities may be missing or may not be published promptly. Critical security updates may not be released for vehicle components. Vulnerabilities in a vehicle's supporting infrastructure may not be fixed.

When a supplier is attacked and its operations are disrupted, supply obligations may not be fulfilled, the production schedule for the final product may be missed, and production may have to be put on hold. The goal of complex attacks on suppliers may be to introduce backdoors into device firmware.

The lack of confidence in the security of purchased components and services forces vehicle manufacturers to devote additional resources to testing their safety and implementing measures to mitigate identified risks.

It is worth noting that the commentary on UN Regulation 155 recommends that vehicle manufacturers at least identify and consider the risks not only of their own direct suppliers of individual vehicle systems and modules, but also of second-tier suppliers who produce components for these vehicle systems and modules.

Considering the current cybersecurity threats identified above, we propose to examine the regulator's requirements and understand how vehicle manufacturers can not only ensure formal compliance, but also develop an optimal approach that can help them to minimize both the short-term and long-term risks.

Requirements of UNECE and international standards

UN Regulations 155 and 156 contain top-level requirements that can be divided into two categories: process-oriented requirements, which have to do with security management at the level of the organization, and project-oriented requirements, which have to do with ensuring the security of everything being produced – whether the vehicles themselves or individual systems and components.

According to these regulations, compliance with the requirements is certified by audits conducted by authorized supervisory bodies or technical services and organizations. As a result of these audits, a Vehicle Type Approval (VTA) is issued.

First, vehicle manufacturers must ensure cybersecurity management at the level of the organization and obtain certificates for their cybersecurity management system (CSMS) and software update management system (SUMS).
The certificates are valid for a maximum of three years. To obtain them, a vehicle

manufacturer must demonstrate that the organizational processes listed above comply with the following requirements as part of cybersecurity management and update management:

- threat assessment and risk analysis (TARA);
- continuous monitoring, incident detection and response;
- vulnerability management;
- component supply chain management and service management;
- security update management;
- notification of supervisory bodies regarding the results of cybersecurity monitoring, including any cyberattacks.

Next, vehicle manufacturers must obtain a VTA for the production of each individual vehicle type. Valid CSMS and SUMS certificates are mandatory to obtain a VTA, so vehicle manufacturers must regularly renew these certificates.

In addition to presenting valid CSMS and SUMS certificates for each project (a project is understood to include development, production, and maintenance of a particular vehicle type), a vehicle manufacturer must implement cybersecurity practices for the vehicle.

Unfortunately, UN Regulations 155 and 156 establish only high-level requirements and do not answer the question of which actions vehicle manufacturers must take and in which sequence in order to be certified and obtain approval to make their products in the markets of UNECE member states.

ISO/SAE 21434, which was approved in August 2021, may help. Figure 2 shows the structure of the standard.

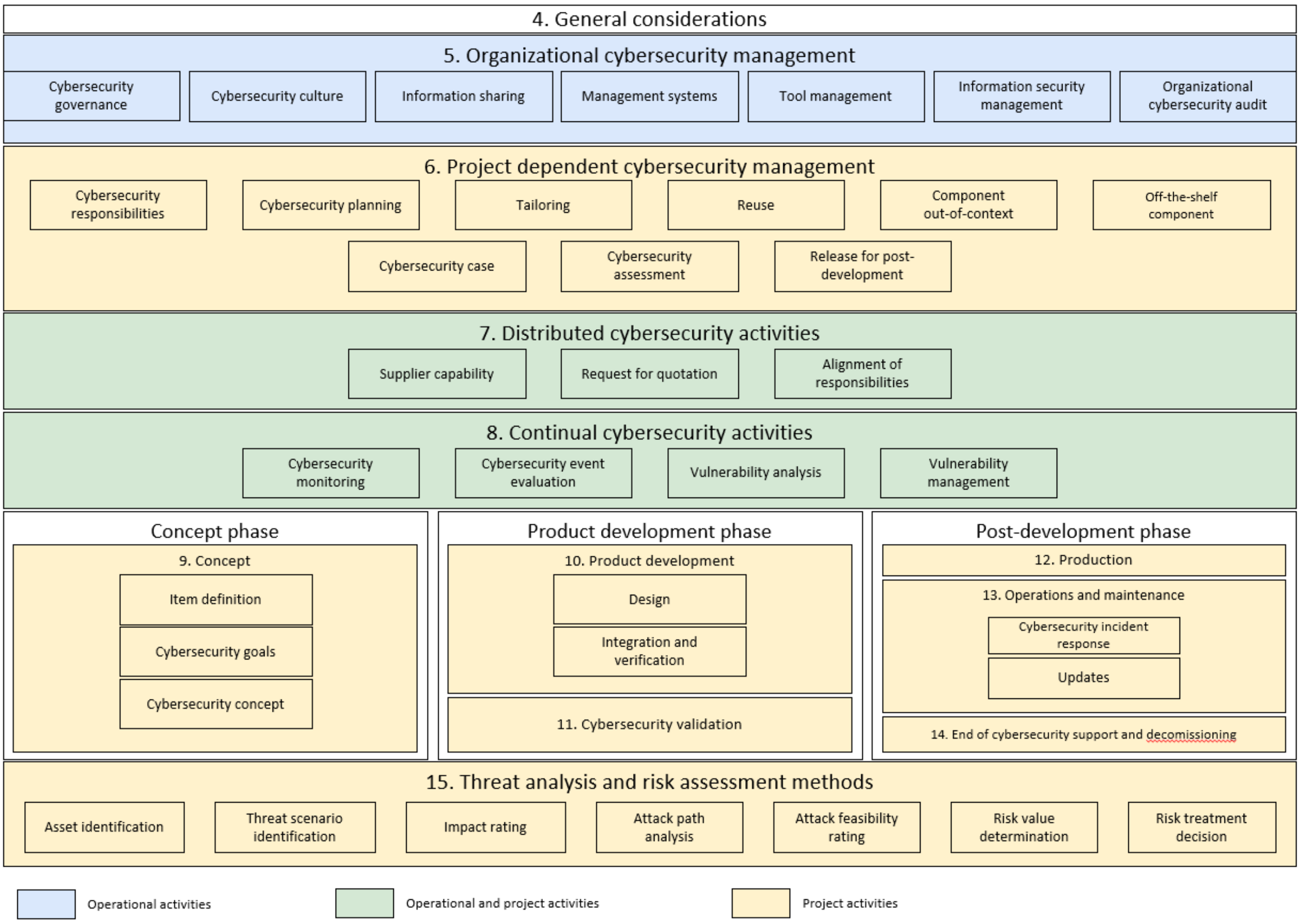

4. General considerations
5. Organizational cybersecurity management
Cybersecurity governance
Cybersecurity culture
Information sharing
Management systems
Tool management
Information security management
Organizational cybersecurity audit
6. Project dependent cybersecurity management
Cybersecurity responsibilities
Cybersecurity planning
Tailoring
Reuse
Component out-of-context
Off-the-shelf component
Cybersecurity case
Cybersecurity assessment
Release for post-development
7. Distributed cybersecurity activities
Supplier capability
Request for quotation
Alignment of responsibilities
8. Continual cybersecurity activities
Cybersecurity monitoring
Cybersecurity event evaluation
Vulnerability analysis
Vulnerability management
Concept phase
9. Concept
Item definition
Cybersecurity goals
Cybersecurity concept
Product development phase
10. Product development
Design
Integration and verification
11. Cybersecurity validation
Post-development phase
12. Production
13. Operations and maintenance
Cybersecurity incident response
Updates
14. End of cybersecurity support and decomissioning
15. Threat analysis and risk assessment methods
Asset identification
Threat scenario identification
Impact rating
Attack path analysis
Attack feasibility rating
Risk value determination
Risk treatment decision
Operational activities
Operational and project activities
Project activities

Figure 2. Structure of ISO/SAE 21434

Like UN Regulations 155 and 156, ISO/SAE 21434 deals with cybersecurity management at the level of the organization and the implementation of security practices as part of a project. Three phases are identified in the project lifecycle: the concept phase, the development phase (which includes cybersecurity development and validation) and the post-development phase (which includes production, operation, and maintenance, as well as the end of cybersecurity support and decommissioning). Individual sections of ISO/SAE 21434 are devoted to relationships with suppliers, ensuring cybersecurity continuity, and methods for threat analysis and risk assessment.

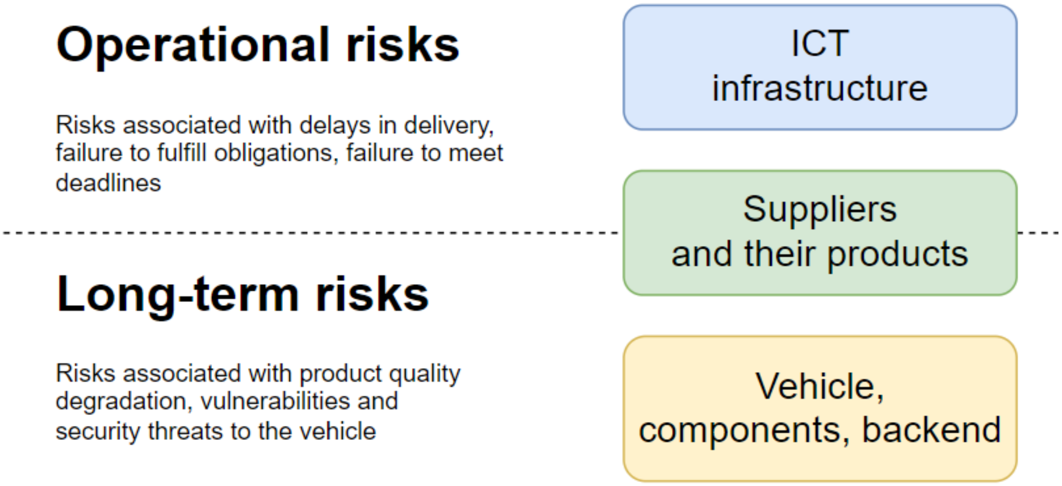
ISO/SAE 21434 elaborates on the top-level requirements found in UN Regulations 155 and 156 regarding ensuring cybersecurity.

ISO/SAE 21434 is a reference point not only for external auditors and representatives of authorized certification bodies, but also for vehicle manufacturers with respect to the definition of the audit scope and the completeness and consistency of audit criteria and evidence.

A vehicle manufacturer can use the list of documents and artifacts provided by the standard to prepare for the certification.

In the previous section, “Relevant cybersecurity risks”, we identified the objects to which cybersecurity requirements apply, and divided their inherent risks into short-term (operational) and long-term (see Figure 3). Below we consider approaches to managing short-term and long-term risks to ensure compliance with the requirements of UN Regulations 155 and156 and ISO 21434.

Figure 3. Short-term (operational) and long-term risks


Operational risks
Risks associated with delays in delivery, failure to fulfill obligations, failure to meet deadlines
Long-term risks
Risks associated with product quality degradation, vulnerabilities and security threats to the vehicle
ICT infrastructure
Suppliers and their products
Vehicle, components, backend

Managing risks for compliance with UNECE requirements

The processes that ensure the cybersecurity of the vehicle, supply chain, and supporting and ICT infrastructure must be built organically into the vehicle manufacturer’s existing management system. Roles and responsibilities for ensuring cybersecurity must be assigned according to the zones of responsibility of individual business units.

Risk management for a vehicle and supporting infrastructure

The vehicle manufacturer’s main goal is to produce a safe product. Risks and threats for the vehicle must be considered at all stages of the product lifecycle. According to ISO 26262, the lifecycle of a vehicle project is divided into 5 phases (we will use this division, because the phases defined in ISO 26262 are more detailed than those in ISO 21434):

- concept phase;
- product development phase;
- production phase;
- operation and maintenance phase;
- end of cybersecurity support and decommissioning phase.

First of all, it is necessary to develop cybersecurity requirements for the product and make them part of its architecture. The main difficulty is that the requirements may represent different levels of technical detail. They may vary from "the vehicle must be unlocked only by a signal from an electronic fob" to "the user certificate verification algorithm embedded in the electronic fob should use RSA with a key that is at least 2048 bits in length".

The requirements undergo a series of transformations at various levels. Based on the requirements of ISO 21434, we can create a diagram that clarifies how this should take place:

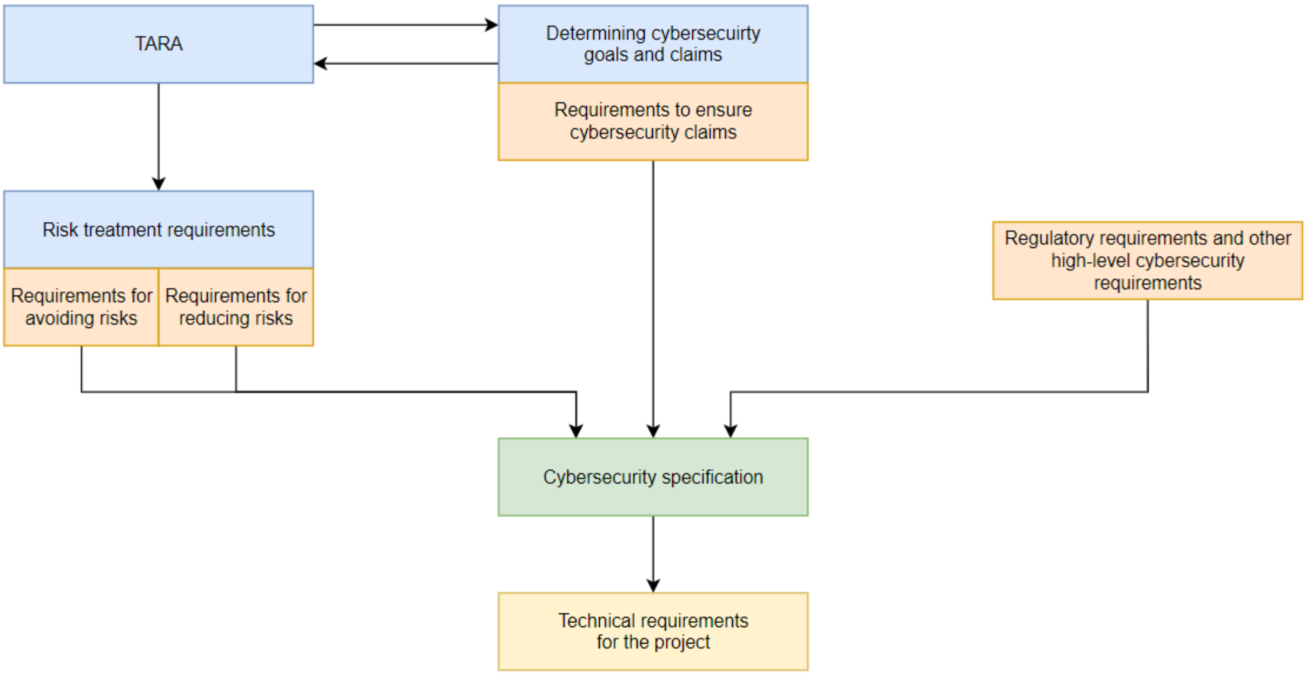

TARA
Determining cybersecuirty goals and claims
Requirements to ensure cybersecurity claims
Risk treatment requirements
Requirements for avoiding risks
Requirements for reducing risks
Regulatory requirements and other high-level cybersecurity requirements
Cybersecurity specification
Technical requirements for the project

Figure 4. Creation of technical requirements based on TARA and cybersecurity goals

Concept phase

In the concept phase, the first step is to perform threat analysis and risk assessment (TARA). TARA is performed both for individual components and for the vehicle as a whole. TARA outcomes include not only security risk values for the product, but also the development of measures required to minimize these risks.

According to the standard, cybersecurity goals and claims are determined based on the TARA outcome. Cybersecurity goals describe the desired state in terms of “What are we protecting and from what?” They are supplemented by cybersecurity claims that specify the context that facilitates or complicates the achievement of cybersecurity goals.

For each threat scenario, a decision is made on what risk treatment options should be for the associated risks. If the decision involves risk reduction, at least one cybersecurity goal is formulated to protect against the threat realized in that scenario. If the risk associated with a threat is retained, then a cybersecurity claim is created that explains this decision.

As an example, let us consider the hacking of critical systems, such as advanced driver assistance system (ADAS), by means of a remote attack and penetration into the vehicle’s infotainment system. The cybersecurity goal in this threat scenario is to protect the ADAS from penetration via the vehicle’s other systems. To implement this protection, the vehicle manufacturer develops a domain architecture for the vehicle network, where all communication between individual security domains is controlled by a central gateway with a hardware root of trust. In this instance, we use a cybersecurity claim that the communication of individual vehicle systems through the central gateway is secure. This cybersecurity claim flows from the cybersecurity goal of another component – the gateway itself – which ensures secure communication of other systems.

In practice, TARA and defining cybersecurity goals and claims are performed at the same time: in part, the goals and claims are obvious even before assessing the anticipated attack scenarios; threat analysis is performed based on a general understanding of the tasks of protecting processes and assets, and then goals and claims are refined.

These cybersecurity goals and claims are augmented with the regulator’s requirements that were not accounted for during the procedures listed above, as well as other high-level business requirements.

Product development phase

At the beginning of the development phase, the security champion consolidates all the high-level cybersecurity requirements into a cybersecurity specification for an individual component (or the entire vehicle). This documented specification to define the architecture, select technologies, and refine technical characteristics.

Next, based on the high-level requirements from the entire component (or vehicle) specification, the cybersecurity champion works with specialists responsible for ensuring the security and reliability of the code to create a list of security requirements for the technical design and operation of the component (or vehicle). These specialists can be product architects or lead developers. The technical requirements must be coordinated with them to eliminate as many errors as possible in the formulation and implementation of requirements in the early stages of development. If identified problems cannot be solved, it is necessary to return to the previous steps: revise the specification, adjust the security objectives, or perform TARA again. These activities will require far fewer resources than making fundamental changes to a nearly finished component or vehicle in the later stages of development.

The agreed list of technical requirements is passed to the development teams. Developers must implement all technical requirements defined by the security champion so that the product satisfies the requirements of the cybersecurity specification.

Code quality must be tracked, applying procedures and tools for static analysis and code reviews, module testing, security checks of third-party code, and functional security testing. A security awareness program should be set up for developers to promote the principles of secure coding that will help minimize the number of code vulnerabilities introduced during the product development.

To verify that cybersecurity goals have been achieved in accordance with the V-model (this is a model for organizing development processes, which requires verification of the results at various stages of development; for more details, see ISO 26262), and for future audits, requirements must be traced at all levels.

The development phase is completed with validation testing. Compliance with the established requirements is verified for all usage scenarios, among other things in order to guarantee functional safety.

Functional safety is about the hazards and consequences of unintentional mistakes made during development, as well as unintentional malfunctions that are not detected on time at the production facility. However, it would be impossible to verify cybersecurity using the same methods that are used to verify functional safety. This is because cyberattacks are the result of adversaries' deliberate actions, and many claims that apply to functional safety do not apply to those attacks.

Moreover, without additional investigation, it is usually not known in advance which claims will not work. Consequently, it is impossible to create an exhaustive set of test scenarios based on the specification, and testing every possible scenario (all possible input data combined with all acceptable operating conditions) is an absolutely unattainable goal.

Therefore, testing security properties is less of a craft and more an art, and automakers should create separate teams of people with specific skills and expertise in practical cybersecurity who work closely with the development and functional safety departments.

The lack of such people in the labor market is a systemic problem. The only solution is to bring in external organizations to verify code quality, search for vulnerabilities in developed products, and conduct penetration testing.

Even before the production phase begins, at the contract phase, it is necessary to determine the security requirements for third-party components and the maturity of the security practices of third-party developers and suppliers. A contract should stipulate that the supplier must ensure the product's compliance with these requirements and present cybersecurity testing results and other confirming evidence to the vehicle manufacturer. During mass production, a vehicle manufacturer performs random checks of each batch of components in order to monitor their compliance with cybersecurity requirements.

For each type of product supplied, a test plan can be created based on the requirements for supplied components from the cybersecurity specification.

Production phase

According to ISO 21434, when the production phase begins, it is necessary to analyze all production operations and develop a production control plan that includes:

- a description of the steps to implement the cybersecurity requirements for the production, operation and maintenance and decommissioning phases (the standard combines these phases into a single post-development phase);
- a list of equipment and tools for the production phase;
- security controls to prevent unauthorized changes in production;
- procedures for evaluating the completeness of implementation and validating the security requirements for the production, operation and maintenance and decommissioning phases.

Note that in the production stages it is necessary to pay attention not only to the production process itself, but also to ensure the security of:

- logistics and storage of components and finished products;
- procedures for flashing firmware and downloading software;
- ICT infrastructure of assembly lines.

If the range of supplied components changes or a supplier changes, checks must be put in place to confirm that the new components comply with cybersecurity requirements. Such checks may include, for example, integration testing.

Intermediate quality checks, known as quality gates, must be planned for each production stage to confirm not only the required quality and functional security, but also the proper implementation of cybersecurity requirements. The process can only proceed to the next stage of production after passing the corresponding check. An example of such a check is monitoring the authenticity and integrity of the control unit software after its firmware has been updated.

Operation and maintenance phase

For the operations and maintenance phase, special attention should be paid to maintaining the cybersecurity status of the vehicle and the supporting infrastructure. (For information on the cybersecurity of supporting infrastructure, see the “Risk management for supporting infrastructure” section below.)

To maintain the cybersecurity of the vehicle, it is necessary to:

- monitor information about discovered vulnerabilities and changes in the threat landscape;
- establish security monitoring of the supporting infrastructure and incident response processes;
- establish monitoring of information about compromised suppliers and processes for responding to incidents involving supply chains and trusted (authorized) partners;
- rapidly respond to vulnerabilities, threats and incidents, including developing and installing patches, notifying users, and reassessing risks.

Some functionality (monitoring, secure downloading and installation of updates, user/owner change scenarios, etc.) is implemented in the vehicle, and some is implemented in supporting infrastructure.

End of cybersecurity support and decommissioning phase

In the end of cybersecurity support and decommissioning phase, both the user and the user's data must remain protected even after individual components have been disposed of or reused. Procedures for warning and notifying users, permanently deleting user data, fulfilling obligations with respect to data storage, and revoking all residual access rights are determined in advance.

Risk management for supporting infrastructure

Just as with risks for the vehicle itself, implementation of cybersecurity requirements must begin in the early stages of the development and implementation of supporting infrastructure.

Risks of attacks on supporting infrastructure can be minimized by implementing a proper network topology and segmentation, secure protocols for authentication, authorization, and data encryption, antivirus protection, procedures for controlling access to the system, vulnerability management, and incident monitoring and response.

The negative effects of a denial-of-service attack can be dealt with using a redundant service architecture, load balancing between individual clusters, and processes for creating backup copies and recovery that are sufficiently mature from a cybersecurity perspective.

In the stage of maintaining supporting infrastructure, it is necessary to make provision for maintenance windows for installation of security updates and deployment of new security systems. Incident response drills must be conducted on a regular basis.

If part of the supporting infrastructure is administered by external organizations, for example, by authorized service centers, or if external organizations have access to individual segments of the supporting infrastructure, then the vehicle manufacturer should use a comprehensive approach to reduce risks of the supporting infrastructure being compromised. The manufacturer should formulate cybersecurity requirements that oblige the external organizations to implement required measures independently. If the external organization lacks the necessary resources and competencies or only has user access to the supporting infrastructure, the vehicle manufacturer must itself come up with a solution that will protect the supporting infrastructure.

To be confident that supporting infrastructure complies with cybersecurity requirements, the vehicle manufacturer must regularly conduct cybersecurity audits and penetration testing, taking into consideration all potential scenarios in which external organizations use the supporting infrastructure.

Risk management for the manufacturer’s ICT infrastructure

When it comes to risk management for the ICT infrastructure, it should be kept in mind that the vehicle manufacturer needs to view the ICT infrastructure as the starting point of complex attacks whose ultimate target is the vehicle, supporting infrastructure, and the data of passengers and vehicle owners (individuals as well as legal entities).

The vehicle manufacturer’s staff must include, at a minimum, a cybersecurity administrator and a cybersecurity department head who are responsible for ensuring cybersecurity. Corporate practices and technical security solutions are used to protect the office network and endpoints. Inside the organization’s perimeter, cybersecurity events should be monitored and incident response procedures should be defined. All of the organization’s employees should be trained and instructed as part of a cybersecurity culture and awareness program.

Threat analysis must also consider the fact that adversaries may potentially target development and manufacturing processes, such as the management of development tools or production documentation, that are specific to manufacturing companies.

As for regulatory requirements in this regard, we can note that UN Regulation 155 emphasizes the need to ensure the cybersecurity of the manufacturer’s infrastructure, but the relevant requirements are quite abstract. At the same time, ISO 21434 includes an entire chapter dedicated to organizational cybersecurity management.

By all appearances, the regulations’ authors assume that organizations have a sufficiently high cybersecurity maturity level, and may even assume implementation of the ISO 27000 series of standards, which is augmented by a range of requirements specific to vehicle manufacturing.

Supply chain risk management

Agreements are typically concluded with suppliers to reduce supply-related risks. Some cybersecurity requirements in these agreements may pertain to preventing threats, and some may be about remediating the effects of threats. For example, a supplier could be required to provide evidence that personnel have completed a cyberthreat awareness course in a timely manner, and that the enterprise has implemented organizational and technical measures to prevent attacks.

In this case, the residual risks can be reduced with additional levers, such as forcing the supplier to provide protection against attacks or to quickly deal with the consequences of attacks by imposing penalties for unresolved critical vulnerabilities and by imposing cybersecurity requirements on supplied components. These measures are a good way to reduce short-term risks.

A more comprehensive approach should be applied to long-term risks associated with flaws and vulnerabilities in supplied components' code, which are not obvious at first glance. These flaws may manifest themselves later, possibly in the finished vehicle. All possible measures must be employed to prevent flaws in the development stage and to discover potential vulnerabilities as soon as possible.

The responsibility for these measures is shared by the manufacturer and the supplier in accordance with a Cybersecurity Interface Agreement. For example, the manufacturer can define cybersecurity goals and claims for a component, and put forward high-level requirements for the component, which should be included in the specification. The supplier, in turn, implements these requirements, and ensures the security of the development process (all these points must be covered by the contract). Under the contract, the supplier may assess the risks of its component, with the manufacturer accepting those results as part of a complete, broader assessment. The manufacturer tests received components for compliance with the cybersecurity requirements, goals, and claims.

The testing of supplied components should not be finished together with the development phase. At a certain frequency, the manufacturer should check the supplied components even after the development phase has ended. This can help to detect vulnerabilities and to guarantee that cybersecurity has not been compromised, for example, by cyberattacks on the supplier.

In the contract, it is important to place special emphasis on sharing the responsibility and the action plan in the event that supplied components are found not to comply with the specification, or vulnerabilities are discovered in supplied components during testing or operation. It is important to explicitly define the timeframe and manner in which the supplier is obliged to respond to information about vulnerabilities with different severity scores. The established timeframes allow the supplier to allocate resources and set a budget for fulfilling its obligations in accordance with the roadmap.

In the context of eliminating vulnerabilities, the problem of supervising suppliers at various levels must be kept in mind. In the automotive industry, the structure of the interactions between various organizations forms a complex branched network: each supplier of vehicle components may have several sub-suppliers of component parts, software, microcircuits, and materials.

State regulators should help solve the problem by harmonizing their cybersecurity laws with international regulations and standards, such as UN 155/156, and by entering into partnership agreements with other states to mutually recognize the certification of vehicles and vehicle components.

In this case, vehicle manufacturers can simply cite international regulations in the contract, and it will be easier for suppliers to ensure that their components comply with uniform cybersecurity requirements without having to worry about running afoul of idiosyncrasy of regional and local legislation.

Strategy for implementing cybersecurity requirements

UN Regulations 155 and 156 and the ISO/SAE 21434 standard discussed in this article are quite broad in scope. They govern cybersecurity not only for the vehicles being developed and operated, but also for many of the processes and ICT infrastructure of the vehicle manufacturer itself. By defining the necessary components to ensure cybersecurity, the regulations and standard leave the vehicle manufacturer free to choose the means and methods to achieve the required level of cybersecurity (the appendices to ISO/SAE 21434 are advisory in nature and illustrate an approach to identifying and assessing cybersecurity risks).

In practice, vehicle manufacturers can use UN 155 and 156 and ISO/SAE 21434 as guidelines to help them properly manage vehicle cybersecurity, even if they are not seeking a UNECE Certificate of Compliance for CSMS.

To minimize the cost of ensuring cybersecurity, it should be “built in” at the design stage. However, the stakeholders of a company implementing cybersecurity practices typically prefer an ad hoc approach. In addition, companies focus on secure development and the security of the code and components of the vehicle itself. In doing so, they may neglect some long-term risks.

These risks can stem from a flawed vehicle architecture, vulnerabilities, or compromised third-party services and components that attackers can later use in attacks on the vehicle.

If an incident occurs, the damage and remediation may be more expensive than doing what is necessary to develop a secure architecture and implement the necessary security practices in the initial design phase. When considering short-term cybersecurity risks, failing to assess the impact of a compromised ICT infrastructure can have similar consequences for a vehicle manufacturer.

First, it is necessary to define the cybersecurity requirements for the product and address them in its architecture. This is done using the functional safety approach familiar to automobile manufacturers, namely by defining security goals and requirements (see the "Concept Phase" section).

Security objectives should support business, quality, and functional safety goals, be agreed upon by all stakeholders, and be documented for a specific project. Clearly articulating and adopting cybersecurity objectives in the concept phase will help eliminate many of the contradictions and inconsistencies between vehicle concept and implementation.

A second important step in the early stages is to build your team with the necessary competencies to implement and maintain cybersecurity practices. Some of these tasks may be outsourced to third parties, for example, if strict deadlines have been set for the development and launch of products in the automotive market and it is not possible to develop the necessary competencies in your team within these deadlines.

Third, a comprehensive and systematic approach must be taken to implementing the required cybersecurity practices. The same level of maturity in security practices could be sufficient, insufficient, or excessive, depending on the vehicle manufacturer's goals and priorities.

An acceptable option for implementing cybersecurity practices could be the following sequence of steps:

1. establish a cybersecurity management system, i.e., develop and implement basic cybersecurity procedures and policies within the organization;
2. develop a cybersecurity plan that defines the list of protective measures and stages for their implementation;
3. secure the company's ICT infrastructure by minimizing the risk of attacks on development departments and production sites;
4. secure supporting infrastructure and external services by minimizing the risk of an attack on a vehicle under development or in use;
5. ensure that the project lifecycle meets relevant cybersecurity requirements, from design and secure development to vehicle decommissioning and the recycling of individual components.

The proposed path is resource-intensive, complex, involves all stages of the vehicle life cycle, and takes a long time. It is very likely that vehicle manufacturers will be tempted to cut corners, limit themselves to analyzing the vehicle itself, and essentially discard all steps except the cybersecurity and vehicle security plan during the development phase. Unfortunately, given the pressure of cybercrime and in an era of connected and software-defined vehicles, such a decision could have disastrous consequences for both the manufacturer as well as the owners and passengers of modern cars.

What should vehicle manufacturers do when faced with the need to implement cybersecurity practices based on UNECE regulations and ISO/SAE 21434?

We recommend starting with the understanding that implementing cybersecurity practices is not a sprint somewhere in the middle of the development phase, but rather a marathon that lasts the life cycle of the vehicle (or even longer) and requires a sensible strategy. Before the marathon begins, a road map (or plan) of the course is drawn up and divided into small sections to be covered with the minimum resources required, taking into account the competencies of the vehicle manufacturer. In this case, the winning strategy is a balanced approach to planning and systematic progress from the simple to the complex.

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com