REPLY
SPIKE

CYBERSECURITY MANAGEMENT SYSTEMS FOR THE AUTOMOTIVE MARKET

New vehicle technology brings with it rising security threats, which must be addressed by integrating cybersecurity best practices into the vehicle lifecycle. Reply's approach uses our extensive experience in the automotive cybersecurity sector to execute strategies custom-made.

SPIKE REPLY is the Reply cybersecurity company that specializes in security advisory, system integration, and operations, and provides consultancy services and integrated solutions.
We support our customers in applying pervasive security methodologies and tools at every stage of the digital transformation path, while also protecting the organizations from cyber-attacks by using advanced and innovative methods for identifying and analysing risks, vulnerabilities, and threats.
This approach allows enterprises to enhance their security posture while still continuing to operate in optimal conditions.

www.reply.com

EXECUTIVE SUMMARY

The ever-growing technology applied to vehicles has created, together with great, new possibilities of entertainment, interactivity, and safety, a new breed of information security threats and risk scenarios. Considering all the impacts such cyber-attacks can have on people, their data, and their safety, new technological and regulatory needs have arisen.

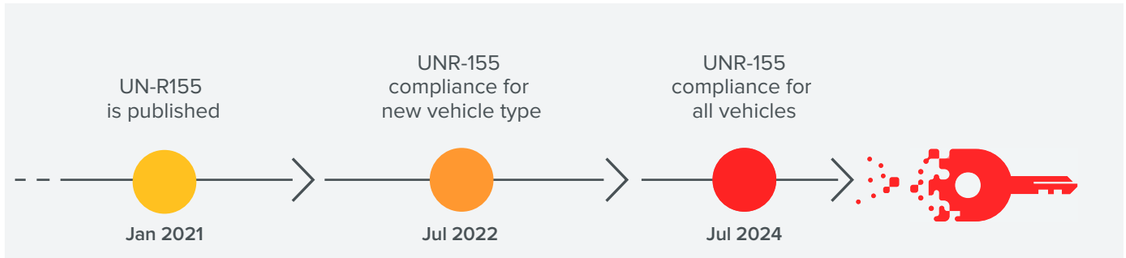
The United Nations Economic Commission for Europe (UNECE) has issued specific regulations to include cybersecurity requirements on vehicle electronics, the UN-R155 and UN-R156. Furthermore, in agreement with UNECE, the ISO council has issued the ISO/SAE 21434:2021 standard, entirely dedicated to vehicles' cybersecurity.

As required by UNECE, a key success factor for managing the new risks related to the vehicles and technological evolution is the integration of cybersecurity into vehicles' lifecycles, from their design and development, through production, maintenance, and update, to end-of-production and decommissioning. For this purpose, it is required to design, implement and maintain a Cybersecurity Management System (CSMS).

INDEX

THE REGULATORY CONTEXT ON VEHICLE CYBERSECURITY

Protecting road vehicles and their functions from cyber threats to electrical and electronic components is crucial for ensuring the safety of people.



For this purpose, and to define a baseline of common rules, the United Nations Economic Commission for Europe (UNECE) introduced the UN-R155 and the UN-R156, which respectively describe the minimum requirements for Cybersecurity Management System (CSMS) and Software Update Management System (SUMS).

The UN-R155 Regulation will become fully applicable in July 2024 requiring all carmakers to implement and apply a CSMS to their product lifecycle, including the components supplied by third parties, and to provide proof of such implementation during the homologation phase.

To access the homologation phase, an OEM (Original Equipment Manufacturer) must obtain in advance certification of its CSMS from the country's Type Approval Authority (i.e., the authority whose responsibility it is to approve homologation of vehicles), to demonstrate its complete coverage of UN-R155 requirements. In addition, while the UN-R155 introduces a grace period for the implementation of a CSMS, it already requires carmakers to provide evidence of having considered cybersecurity for new types of vehicles.

This regulation will significantly affect the entire automotive ecosystem and its stakeholders, involving the supply chain, since a failure of the OEM to meet the regulatory requirements or a failure of the supplier to provide enough pieces of evidence will affect the possibility to market the vehicles.

To support carmakers and suppliers alike, in 2021, ISO/SAE 21434 was released: being the standard explicitly referred to in UN-R155, it represents an approved "guideline" to ensure R155 compliance and thus to obtain approval for vehicle homologation. The standard deepens the concept of a Cybersecurity Management System.

Furthermore, in 2022 the ISO/PAS 5112 was published to provide specific criteria to audit ISO/IEC 21434-based CSMS, meaning it represents the guideline to manage an automotive cybersecurity audit program.

Finally, although the ISO/SAE 21434 focuses on cybersecurity, there are clear references to the impacts on the safety of people. ISO 26262 must be taken into account too, as it provides a framework for functional safety, to guide the development of safe vehicle components.

UN-R155 **COMPLIANCE REQUIREMENTS**	UN-R155 defines the **requirements** related to cyber security that all Car Makers and OEMs have to consider in the life cycle of a vehicle **(CSMS implementation).**
ISO/IEC 21434 **CSMS IMPLEMENTATION GUIDELINES**	150/IEC 21434 describe a **framework** to manage the cyber security in the whole manufacturing process, deepening the concept of **CSMS**.
ISO/PAS 5112 **ISO/IEC 21434 AUDIT CRITERIA**	The **ISO/PAS 5112** aims at providing guidelines to **audit a ISO/IEC 21434 based CSMS**.

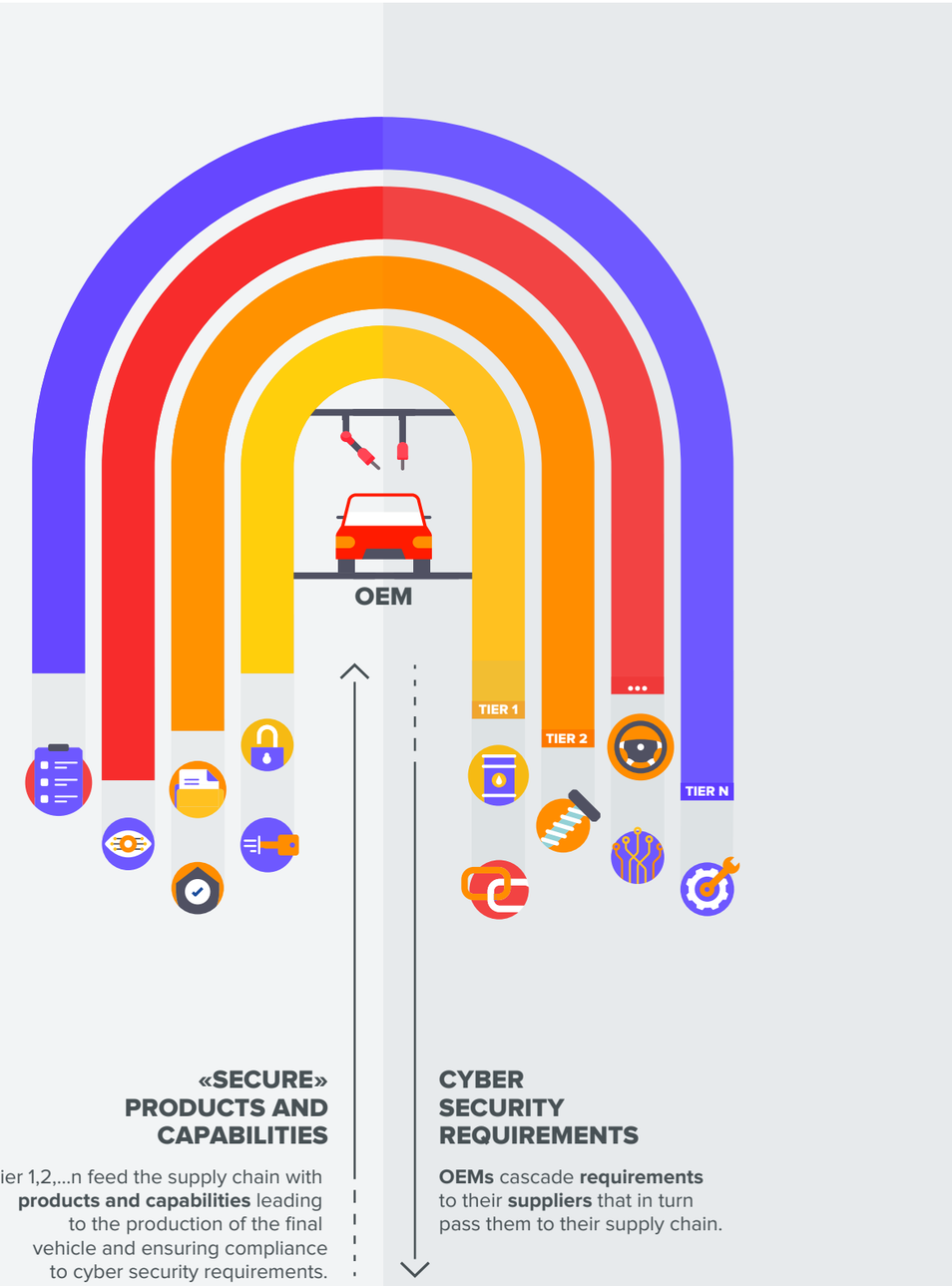
THE ROLE OF THE SUPPLY CHAIN

As carmakers rely on a broad range of suppliers, to reach an adequate security level of the CSMS, both UN-R155 and ISO/SAE 21434 are required to address the security of the supply chain. This activity is mandatory, for OEMs, to obtain the Certificate of Compliance needed for type approval, demonstrating that supplier-related risks are properly identified and managed.

Therefore, automotive suppliers should expect to be required to:

- Meet compliance requirements and enforce cybersecurity of their products/capabilities, as defined by UN-R155
- Collaborate in defining the cybersecurity plan for the carmakers and in remediating vulnerabilities, if any
- Be ready to support carmakers in their audit programs.

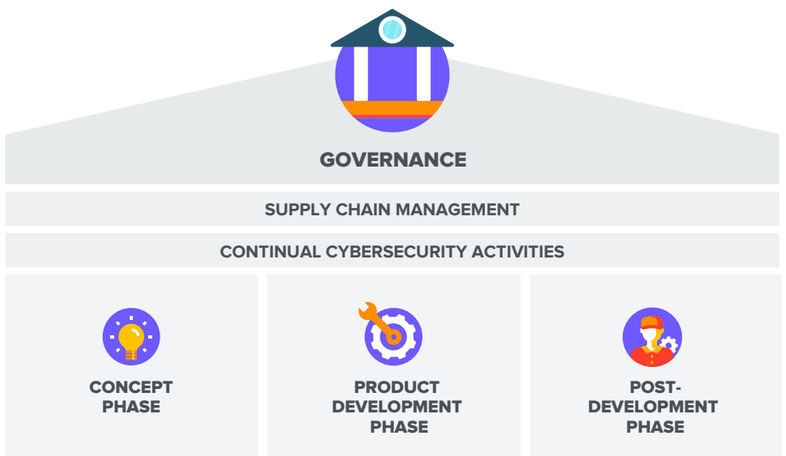
In this context, automotive suppliers can also leverage ISO/SAE 21434 to demonstrate an adequate level of cybersecurity. ISO/SAE 21434 compliance is not mandatory but it represents an opportunity to meet carmakers' expectations; with the implementation of an applicable and auditable CSMS, organizations can benefit from a competitive advantage in the automotive market.

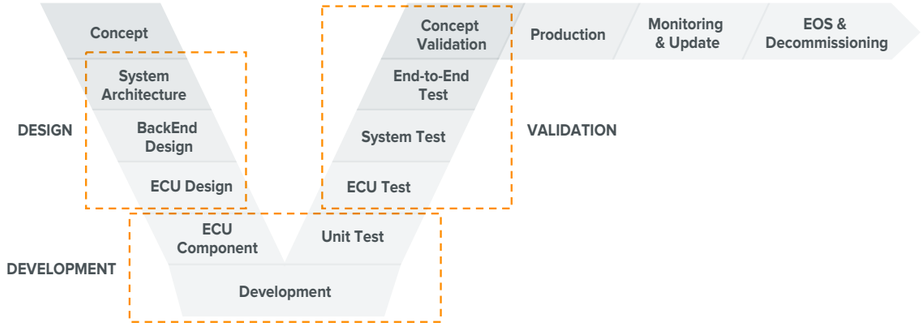


CSMS KEY ELEMENTS

According to UN-R155, the Cybersecurity Management System (CSMS) is “a systematic risk-based approach defining organizational processes, responsibilities, and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks”.

The CSMS, as defined in ISO/SAE 21434, provides a common framework as well as security requirements for cybersecurity processes. To ensure proper cybersecurity risk management through the entire product lifecycle, the CSMS follows the Automotive V-Model, ensuring appropriate consideration of cybersecurity from the concept phase all the way through to the decommissioning phase of electrical and electronic systems in road vehicles, including their components and interfaces.





GOVERNANCE

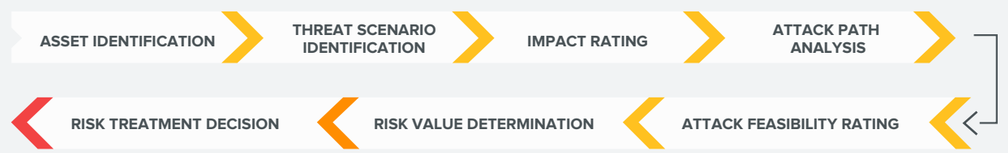
Before the beginning of the concept and design of an electronic control unit (ECU), the company (being a carmaker or a supplier) should define and implement processes and procedures to be applied in the different phases of the vehicle lifecycle, identifying the related roles and responsibilities and with a specific focus on the organization’s cybersecurity culture.

CONCEPT PHASE

The concept phase addresses the evaluation of vehicle functionalities and the definition of cybersecurity risks, goals, and requirements. Considering that the CSMS strengthens the “Security by Design” approach, from the beginning of any project, it is fundamental to adopt specific methodologies to perform threat analysis and risk assessment activities to identify proper mitigation measures before the development phase.

Threat analysis and risk assessment (TARA) is the method to determine the extent to which a road user (e.g., Driver, Vehicle Owner, Passenger or Pedestrian) can be impacted by a threat scenario.

A TARA methodology should be defined as a standalone process, which can be invoked from any point in the lifecycle of a product (e.g., during the product development phase, to verify the implementations and to address the new evolutions of technologies and threats which may have arisen). While there can be several TARA methodologies, they must all follow a common structure to ensure coverage and alignment with ISO/SAE 21434 clauses, as defined below.



PRODUCT DEVELOPMENT PHASE

The product development phase addresses the definition of cybersecurity detailed requirements, their implementation, and verification on both hardware and software components of ECUs and vehicles alike. The product development phase ends with a validation step, where the cybersecurity goals are verified before the start of production, and any weakness identified is addressed following the vulnerability management process

POST-DEVELOPMENT PHASE

This phase addresses cybersecurity during the post-development phase, specifically focusing on three sub-phases.

- **Production**: the focus is to ensure that the cybersecurity requirements for the production lines are identified and implemented by avoiding new vulnerabilities introduced during the manufacturing/assembly process
- **Cybersecurity incident response and update** includes monitoring of security events and incident management, together with the update processes. The monitoring and incident response activities can be performed through the implementation of a Vehicle-SOC (or VSOC).

  The management of the update process is both considered within the ISO/SAE 21434 and in UN-R156. Such activity requires managing the update chain (from development to validation, distribution, and installation of the update) to foresee and apply specific cybersecurity controls and secure software and hardware on the vehicles and ECUs.

  In the Automotive sector, **Vehicle Security Operations Centers (VSOCs)** address the complexity of cyber-attacks targeting networks such as connected vehicles and their components or services. An effective VSOC allows stakeholders to monitor vehicles, fleets, and the entire connected vehicle infrastructure in near real-time, ensuring cyber threat detection throughout the lifecycle of a vehicle and the safety and security of vehicles, services, fleets, and road users.

  A VSOC can be implemented by adopting different approaches.

  Improve the existing SOC: organizations with an existing SOC can expand it to encompass Vehicle Security.
  Create a new one: organizations can implement and manage a platform that follows the end to end process, from the discovery of vulnerabilities to the management of the incident detected.
  Outsourcing: organizations can outsource the VSOC to a security service provider with specific automotive-related security capabilities.

- **End of cybersecurity support and decommissioning**. When a carmaker or a supplier stops providing cybersecurity support to vehicles and ECUs, it is important to plan the activity involving all the stakeholders, to avoid knowingly leaving vulnerable devices or causing incidents, which may damage a brand's reputation or even endanger people.

HOW TO IMPLEMENT A CSMS

Reply's approach to addressing regulatory compliance and implementing a CSMS is tailor-made, designed according to the specific features of any given context, and based on our deep experience in the automotive cybersecurity sector.

ASSESSMENT & GAP ANALYSIS.

This is the first step, necessary to start the path toward UN-R155, UN-R156, and ISO/SAE 21434 compliance. Evaluation of the current cybersecurity posture and the gap analysis activities aim at defining the strategies to be adopted and at prioritizing the actions to be undertaken.

CSMS DESIGN.

The Design phase objective is to draft all CSMS components (e.g., TARA methodology and supporting tools, Incident Management processes, etc.).

CSMS IMPLEMENTATION.

This phase involves the rollout of the defined CSMS, and the implementation of the designed policies, processes, controls, and technologies affecting the product lifecycle.

CSMS MAINTENANCE.

The objective of this phase is to maintain the CSMS valid and effective, operating the system according to processes and controls implemented with a continuous improvement approach (e.g., TARA execution, VSOC running activities).

SPIKE REPLY'S AUTOMOTIVE SECURITY CAPABILITIES

Leveraging the skills described above and the deep knowledge of automotive security issues, Reply can support customers in achieving UN-R155 and UN-R156 compliance, defining their compliance program as well as executing it or addressing specific project streams, by offering a wide portfolio that includes various activities and consulting strategies.

More generally, thanks to the competence brought by a highly skilled team of experts focused on automotive security, which spans all cybersecurity-related matters, we ensure an end-to-end approach to vehicular and vehicle component cybersecurity.

Due to our skills related to security advisory topics, system integration, and security operations, our automotive security offering provides both consultancy services and integrated solutions implementation.

ASSESSMENT & STRATEGY DEFINITION

- Assess and evaluate the current cybersecurity posture to meet UN-R155 and UN-R156 compliance
- Evaluate the compliance against other applicable regulations (e.g. IATF, TISAX)
- Provide a detailed Gap Analysis
- Define the strategies and remediation activities to meet regulatory requirements

Reply's offering in this context combines our advisory and technical capabilities, ensuring that the analysis performed and the strategies are defined considering the peculiarities of the automotive sector and the related technical characteristics.

In this context, we can leverage our knowledge of regulations, standards, and frameworks in scope.

SUPPORT ACTIVITIES

CYBERSECURITY ENGINEERING & SECURITY BY DESIGN

Vehicle cybersecurity engineering according to ISO/SAE 21434 and Regulation UNECE/WP R155.

Thanks to deep-rooted security skills, Reply assists organizations in identifying, evaluating, and vetting the most appropriate measures according to cybersecurity best practices, standards, and principles. Our extensive expertise in both the cybersecurity and automotive fields, allows us to provide customized and valuable solutions to organizations to achieve regulatory compliance and attain increased cybersecurity maturity.

Reply supports clients in assessing and implementing state-of-the-art cybersecurity engineering processes for automotive technologies. Our activities address several areas: from the design of cybersecurity requirements to the performance of threat analysis and risk assessments.

THIRD PARTY RISK MANAGEMENT

Management of the suppliers related risks through the contract lifecycle (suppliers evaluation, monitoring,..)

Reply's offering also encompasses third-party risk management to ensure that potential threats and vulnerabilities coming from external organizations are promptly recognized and handled to avoid weakening the cybersecurity posture of the vehicle.

CONNECTED VEHICLE ICT SECURITY

Security services related to backend application used by Connected Vehicles (e.g. Service Delivery Platform, Authenticated Diagnostic, ...)

Reply supports Automotive Customers by providing capabilities to protect the vehicle against cyber-attacks that take advantage of the major vehicle connectivity and its exposed communication channels.
The main Business Services offered by Reply in this context include:

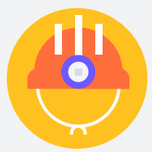
- Custom Analysis, Design, and Development of ECU's identity provisioning during manufacturing compatible with regulation, including Trusted Information Security Assessment eXchange (TISAX) standard, and business production requirements
- Support in Secure key provisioning within high-performance systems for manufacturing
- Custom integration with Customer Identity Systems
- V2X Integration Services (V2I, Vehicle to Infrastructure; V2V, Vehicle to Vehicle; V2G, Vehicle to Grid; V2N, Vehicle to Network; V2P, Vehicle to Pedestrian; V2D, Vehicle to Device).

SECURE DEVELOPMENT & TESTS

Secure development and execution of penetration testing for vehicle components or networks

Reply can support organizations to support secure development processes and identify and select the most appropriate cybersecurity use cases to be tested.

Once the appropriate use cases are chosen, Reply can perform penetration tests by adopting cutting-edge technologies, providing meaningful reports, and advising on the appropriate remediation actions to implement to increase the security posture of the components and, consequently, of the vehicle.



MANUFACTURING SECURITY

Implementation, integration and management of V-PKI (SW Sign, ECU Identity, ADA)

In this context, Reply's offering aims at:

- protecting production lines from intruders, eavesdropping, and viruses
- creating products with a strong and unique Digital Identity
- verifying and enforcing third parties' security.

To reach these objectives, Reply has the proper skills to support the implementation, integration, and management of V-PKI (SW Sign, ECU Identity, ADA) and in the definition of the proper data protection strategies (e.g., through the implementation of HSM).

CSMS OPERATION & THREAT INTELLIGENCE

- **V-SOC and PSIRT implementation and management**
- **Vulnerabilities management**

Reply support aims at enhancing cybersecurity operation capabilities by providing expertise in several fields.

- Development of a VSOC: to support the identification and management of events that may be identified by clients, carmakers, or suppliers, and to guide the implementation of platforms to manage the incidents detected.
- Vulnerability and incident management: support to identify the vulnerabilities by examining various sources, either publicly available or from sources such as threat intelligence and VSOC. Reply can also support the implementation of a correlation engine between the vulnerabilities found and the company's products, to make the results of the previous step profitable and expendable.