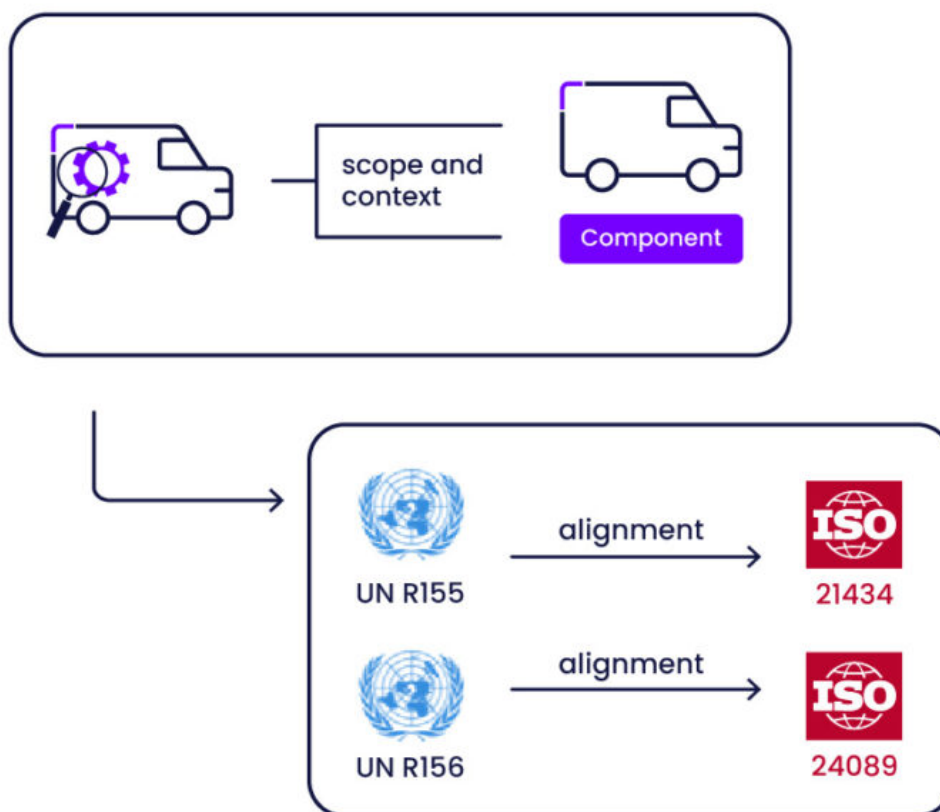


Automotive Cybersecurity – Gap Analysis

Author: Dr. Yuri Gil Dantas

Published: 6 October 2025

Reading time: 3 mins



Why Performing a Gap Analysis?

Cybersecurity has become a crucial discipline for the automotive domain. This is due to the introduction of advanced technologies such as connected systems, automated driving systems, and over-the-air updates. Additionally, with the introduction of cybersecurity regulations, particularly regulation UN R155 [1] and regulation UN R156 [2], cybersecurity has become mandatory for Original Equipment Manufacturers (OEMs). Suppliers are also affected by those regulations because OEMs often request their suppliers to follow the regulation's requirements. Prior to market introduction, the OEM is required to successfully complete the homologation process, a stringent evaluation ensuring conformity with automotive standards and regulatory frameworks, such as those governing cybersecurity.

Conducting a cybersecurity gap analysis is crucial for identifying weaknesses before they escalate into critical issues – such as failing the homologation process. FEV provides comprehensive cybersecurity gap analysis services tailored to both OEMs and suppliers. By leveraging the insights from FEV's analysis and implementing the recommended measures, customers can ensure their vehicles or components meet compliance standards, are fully prepared for homologation, and benefit from enhanced overall security, while avoiding costly delays.

A Systematic Approach

The core of the cybersecurity gap analysis service is a systematic and comprehensive approach designed to provide clear insights into the current state of the automotive vehicle or components. Figure 1 illustrates the gap analysis

approach, while its description is provided below:

1. **Scope Definition:** The system of interest is defined, i.e., whether the developed product is the entire vehicle or a specific component.
2. **Regulatory Analysis:** Regulation requirements are identified, and their applicability is checked, i.e., which regulation requirements are applicable to the system of interest.
3. **Standard Alignment:** Alignment of regulation requirements with their corresponding standards, i.e., an alignment between regulation requirements from UN R155 to ISO/SAE 21434 and regulation requirements from UN R156 with ISO 24089. This alignment ensures that regulation requirements are directly tied to the corresponding work products from those standards (i.e., ISO/SAE 21434 or ISO 24089).
4. **Work Product Evaluation:** -Evaluation of the work products in terms of availability and completeness. If a work product is available, an in-depth evaluation is performed to check whether the work product meets its corresponding requirements.
5. **Recommendations:** Detailed recommendations are provided for any incomplete or missing work products. The goal is to provide clear guidance on how to meet the open requirements, and effectively deliver the corresponding work products, ensuring compliance with regulation requirements.

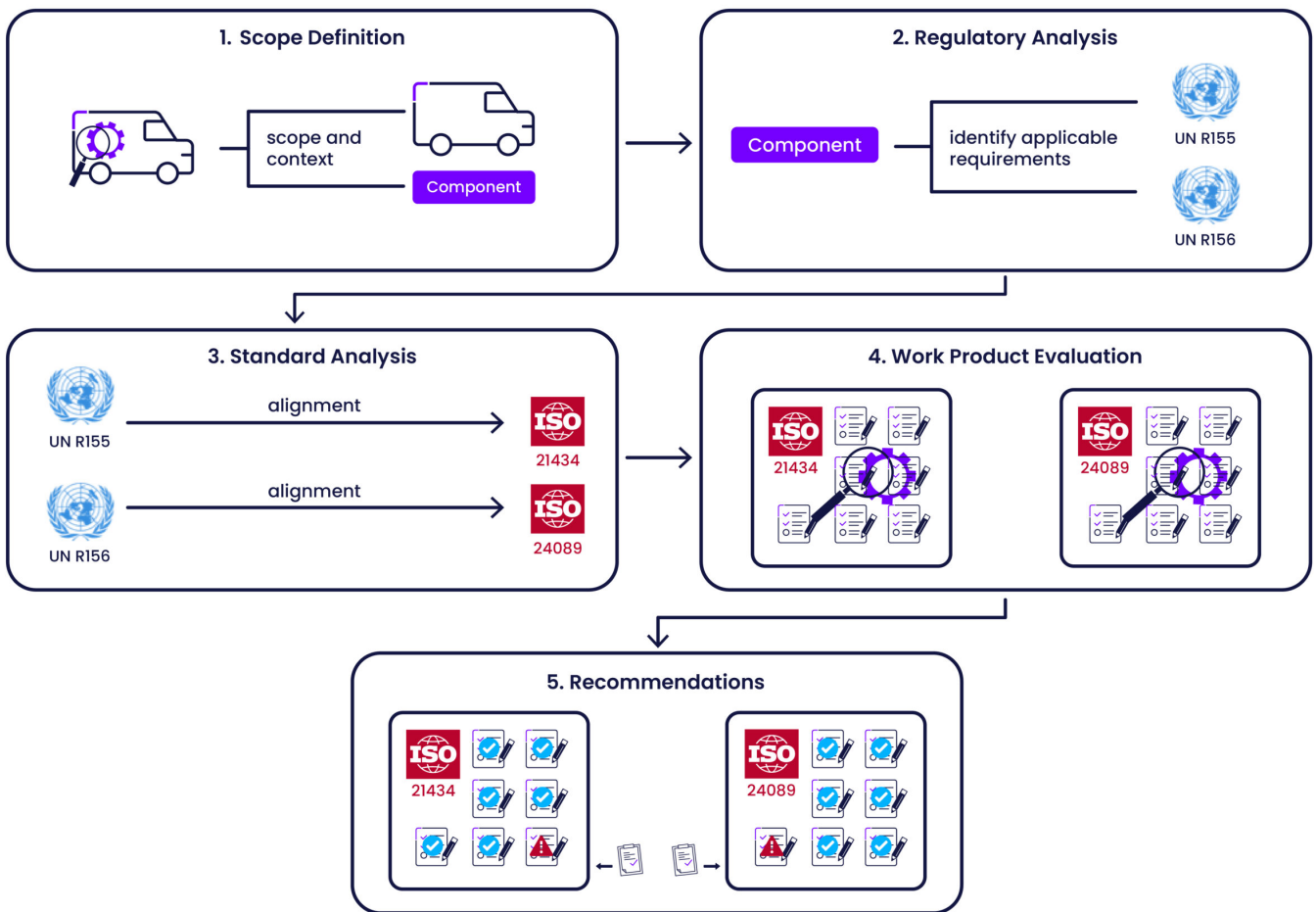


Figure 1: Illustration of our gap analysis approach

The benefits of the approach are clear: By systematically identifying and addressing cybersecurity gaps, OEMs and suppliers are assisted in reducing the risk of cybersecurity attacks and ensuring regulatory compliance. This not only protects the end-users of the vehicle or component but also helps OEMs and suppliers in achieving full compliance and protecting their own reputation.

Contact

If you are an OEM or a supplier seeking to ensure your vehicles or components meet the cybersecurity regulation requirements, our expert team is here to assist you. Contact us today for more details on how our systematic and comprehensive cybersecurity gap analysis can help you achieve full compliance.

References

[1] United Nations Economic Commission for Europe, “UN Regulation No. 155 – Cyber security and cyber security management”, <https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf>, 4 March 2021.

[2] United Nations Economic Commission for Europe, “UN Regulation No. 156 – Software update and software update management system”, <https://unece.org/sites/default/files/2024-03/R156e%20%282%29.pdf>, 4 March 2021.