AVCDL Phase Requirement Product UNECE WP.29 R155 Work Product Fulfillment

Revision

Version 3
3/18/22 4:14 PM

Author

Charles Wilson

Abstract

This document summarizes how **AVCDL** phase requirement products fulfill **UNECE WP.29 R155** requirements.

Motivation

This document is motivated by the need to justify the sufficiency of the **AVCDL** for compliance with the cybersecurity elements of **UNECE WP.29 R155**.

Audience / Use of UNECE WP.29 R155 Text

The audience for this document is the certifying organization. As such it is necessary to provide excerpts from **UNECE WP.29 R155** itself in order to provide evidence of sufficiency.

License

UNECE WP.29 R155 Overview

Note: This material is extracted from the **UNECE WP.29 R155** specification. It is included here for reference only.

Addendum 154 – UN Regulation No. 155 is intended to address the cyber security and cyber security management system aspects of road vehicle approval.

Within this regulation, the specification contains two main requirement areas:

- 7.1 general
- 7.2 cybersecurity management systems (CSMS)
- 7.3 vehicle types
- 7.4 reporting provisions

The general (7.1), vehicle type requirements (7.3), and reporting provisions (7.4) are outside the scope of the AVCDL.

The following items from the CSMS requirements (7.2) are within the scope of the ***AVCDL***:

- 7.2.2.1(a) development phase CSMS
- 7.2.2.1(b) production phase CSMS
- 7.2.2.1(c) post-production CSMS
- 7.2.2.2(b) risk identification
- 7.2.2.2(c) risk assessment / treatment
- 7.2.2.2(d) verification of risk management
- 7.2.2.2(e) cybersecurity testing
- 7.2.2.2(f) risk assessment kept current
- 7.2.2.2(g) adaptable monitoring / response
- 7.2.2.2(h) cybersecurity controls tracking

The following items from the CSMS requirements (7.2) are outside the scope of the ***AVCDL***:

- 7.2.1 compliance verification
- 7.2.2.2(a) cybersecurity management
- 7.2.2.3 timely risk mitigation
- 7.2.2.4(a) vehicle monitoring enrollment
- 7.2.2.4(b) threat extraction from vehicle logs
- 7.2.2.5 supplier deficiency management

Note: Out-of-scope activities are addressed in organizational-level documentation.

7.1 General

7.1.1 UN regulation non-exclusion

The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.

Note: This requirement is addressed in organizational-level documentation.

7.2 Cyber Security Management Systems

7.2.1 vehicle certification

For the assessment the Approval Authority or its Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.

Note: This requirement is addressed in organizational-level documentation.

7.2.2.1 demonstration of scope

The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cyber Security Management System applies to the following phases:

7.2.2.1(a) development phase CSMS

[Foundation-1]	Training Catalog (Foundation-1.1)
[Foundation-1]	System to Track Training Participation (Foundation-1.2)
[Foundation-2]	Roles and Responsibilities Document (Foundation-2.1)
[Foundation-3]	List of Approved Tools and Components (Foundation-3.1)
[Foundation-4]	Global Security Goals (Foundation-4.1)
[Foundation-4]	Global Security Requirements (Foundation-4.2)
[Foundation-5]	Code Protection Plan (Foundation-5.1)
[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-9]	Threat Prioritization Plan (Foundation-9.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Requirements-1]	Product-level Security Goals (Requirements-1.1)
[Requirements-1]	Product-level Security Requirements (Requirements-1.2)
[Requirements-2]	Requirements Phase Gate (Requirements-2.1)
[Design-1]	Design Showing Security Considerations (Design-1.1)
[Design-2]	Security Design Review Report (Design-2.1)
[Design-3]	Attack Surface Analysis Report (Design-3.1)
[Design-4]	Threat Modeling Report (Design-4.1)
[Design-4]	Ranked/Risked Threat Report (Design-4.2)
[Design-4]	Threat Report (Design-4.3)
[Design-5]	Design Phase Gate (Design-5.1)
[Implementation-1]	List of Tools and Components Used (Implementation-1.1)
[Implementation-2]	Build Process Documentation (Implementation-2.1)
[Implementation-3]	Secure Settings Document (Implementation-3.1)
[Implementation-4]	Component/Version – Product/Version Cross-reference Document (Implementation-4.1)
[Implementation-5]	Secure Development (Implementation-5.1)
[Implementation-6]	Currently Used Deprecated Functions Document (Implementation-6.1)

[Implementation-7] Static Analysis Report (Implementation-7.1)
[Implementation-8] Dynamic Analysis Report (Implementation-8.1)
[Implementation-9] Secure Code Review Summary (Implementation-9.1)
[Implementation-10] Fuzz Testing Report (Implementation-10.1)
[Implementation-11] Implementation Phase Gate (Implementation-11.1)
[Verification-1] Penetration Testing Report (Verification-1.1)
[Verification-2] Updated Threat Model (Verification-2.1)
[Verification-3] Updated Attack Surface Analysis (Verification-3.1)
[Verification-4] Verification Phase Gate (Verification-4.1)

7.2.2.1(b) production phase CSMS

[Foundation-1] Training Catalog (Foundation-1.1)
[Foundation-1] System to Track Training Participation (Foundation-1.2)
[Foundation-2] Roles and Responsibilities Document (Foundation-2.1)
[Foundation-7] Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7] Incident Response Plan (Foundation-7.2)
[Design-4] Ranked/Risked Threat Report (Design-4.2)
[Design-4] Threat Report (Design-4.3)
[Implementation-4] Component/Version – Product/Version Cross-reference Document (Implementation-4.1)
[Operation-1] Cybersecurity Incident Report (Operation-1.1)
[Operation-2] Software Deployment Report (Operation-2.1)

7.2.2.1(c) post-production CSMS

[Foundation-1] Training Catalog (Foundation-1.1)
[Foundation-1] System to Track Training Participation (Foundation-1.2)
[Foundation-2] Roles and Responsibilities Document (Foundation-2.1)
[Foundation-8] Decommissioning Plan (Foundation-8.1)

7.2.2.2 Risk Management

The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered, including risks and mitigations listed in Annex 5. This shall include:

7.2.2.2(a) cybersecurity management

The processes used within the manufacturer’s organization to manage cyber security;

Note: This requirement is addressed in organizational-level documentation.

7.2.2.2(b) risk identification

The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered;

[Design-1]	Design Showing Security Considerations (Design-1.1)
[Design-3]	Attack Surface Analysis Report (Design-3.1)
[Design-4]	Threat Modeling Report (Design-4.1)
[Design-4]	Ranked/Risked Threat Report (Design-4.2)
[Design-4]	Threat Report (Design-4.3)

7.2.2.2(c) risk assessment / treatment

The processes used for the assessment, categorization and treatment of the risks identified;

[Foundation-9]	Threat Prioritization Plan (Foundation-9.1)
[Design-2]	Security Design Review Report (Design-2.1)
[Design-3]	Attack Surface Analysis Report (Design-3.1)
[Design-4]	Threat Modeling Report (Design-4.1)
[Design-4]	Ranked/Risked Threat Report (Design-4.2)
[Design-4]	Threat Report (Design-4.3)

7.2.2.2(d) verification of risk management

The processes in place to verify that the risks identified are appropriately managed;

[Design-2]	Security Design Review Report (Design-2.1)
[Verification-2]	Updated Threat Model (Verification-2.1)
[Verification-3]	Updated Attack Surface Analysis (Verification-3.1)

7.2.2.2(e) cybersecurity testing

The processes used for testing the cyber security of a vehicle type;

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Design-1]	Design Showing Security Considerations (Design-1.1)
[Design-2]	Security Design Review Report (Design-2.1)
[Implementation-7]	Static Analysis Report (Implementation-7.1)
[Implementation-8]	Dynamic Analysis Report (Implementation-8.1)
[Implementation-9]	Secure Code Review Summary (Implementation-9.1)
[Implementation-10]	Fuzz Testing Report (Implementation-10.1)
[Verification-1]	Penetration Testing Report (Verification-1.1)

7.2.2.2(f) risk assessment kept current

The processes used for ensuring that the risk assessment is kept current;

[Verification-2]	Updated Threat Model (Verification-2.1)
[Verification-3]	Updated Attack Surface Analysis (Verification-3.1)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)

7.2.2.2(g) adaptable monitoring / response

The processes used to monitor for, detect and respond to cyber-attacks, cyber threats and vulnerabilities on vehicle types and the processes used to assess whether the cyber security measures implemented are still effective in the light of new cyber threats and vulnerabilities that have been identified.

[Foundation-4]	Global Security Goals (Foundation-4.1)
[Foundation-4]	Global Security Requirements (Foundation-4.2)
[Foundation-7]	Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)

7.2.2.2(h) cybersecurity controls tracking

The processes used to provide relevant data to support analysis of attempted or successful cyber-attacks.

[Foundation-3]	List of Approved Tools and Components (Foundation-3.1)
[Implementation-1]	List of Tools and Components Used (Implementation-1.1)
[Implementation-2]	Build Process Documentation (Implementation-2.1)
[Implementation-4]	Component/Version – Product/Version Cross-reference Document (Implementation-4.1)
[Implementation-6]	Currently Used Deprecated Functions Document (Implementation-6.1)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)
[Operation-2]	Software Deployment Report (Operation-2.1)

7.2.2.3 timely risk mitigation

The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that, based on categorization referred to in paragraph 7.2.2.2 (c) and 7.2.2.2 (g), cyber threats and vulnerabilities which require a response from the vehicle manufacturer shall be mitigated within a reasonable timeframe.

Note: This requirement is addressed in organizational-level documentation.

7.2.2.4 Vehicle Monitoring

The vehicle manufacturer shall demonstrate that the processes used within their Cyber Security Management System will ensure that the monitoring referred to in paragraph 7.2.2.2 (g) shall be continual. This shall:

7.2.2.4(a) vehicle monitoring enrollment

Include vehicles after first registration in the monitoring;

Note: This requirement is addressed in organizational-level documentation.

7.2.2.4(b) threat extraction from vehicle logs

Include the capability to analyse and detect cyber threats, vulnerabilities and cyber-attacks from vehicle data and vehicle logs. This capability shall respect paragraph 1.3. and the privacy rights of car owners or drivers, particularly with respect to consent.

Note: This requirement is addressed in organizational-level documentation.

7.2.2.5 supplier deficiency management

The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers, service providers or manufacturer's sub-organizations in regards of the requirements of paragraph 7.2.2.2.

[Supplier-1] AVCMDS (Supplier-1.1)
[Supplier-2] Supplier Self-reported Maturity (Supplier-2.1)
[Supplier-3] Cybersecurity Interface Agreement (Supplier-3.1)

7.3 Vehicle Types

Note: Requirements in this section are addressed in organizational-level documentation.

Note: Although activities within the **AVCDL** may be used to support these requirements, they are the responsibility of the manufacturer and not the supplier.

7.3.1 certificate of compliance

The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.

7.3.2 management of type

The vehicle manufacturer shall identify and manage, for the vehicle type being approved, supplier-related risks.

7.3.3 critical element identification

The vehicle manufacturer shall identify the critical elements of the vehicle type and perform an exhaustive risk assessment for the vehicle type and shall treat/manage the identified risks appropriately. The risk assessment shall consider the individual elements of the vehicle type and their interactions. The risk assessment shall further consider interactions with any external systems. While assessing the risks, the vehicle manufacturer shall consider the risks related to all the threats referred to in Annex 5, Part A, as well as any other relevant risk.

7.3.4 type risk protection

The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented.

In particular, for type approvals prior to 1 July 2024, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority.

7.3.5 type risk countermeasures

The vehicle manufacturer shall put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.

7.3.6 sufficient testing

The vehicle manufacturer shall perform, prior to type approval, appropriate and sufficient testing to verify the effectiveness of the security measures implemented.

7.3.7(a) detect / prevent cyberattacks

Detect and prevent cyber-attacks against vehicles of the vehicle type.

7.3.7(b) vehicle cybersecurity monitoring

Support the monitoring capability of the vehicle manufacturer with regards to detecting threats, vulnerabilities and cyber-attacks relevant to the vehicle type.

7.3.7(c) provide forensic capability

Provide data forensic capability to enable analysis of attempted or successful cyber-attacks.

7.3.8 use standard crypto modules

Cryptographic modules used for the purpose of this Regulation shall be in line with consensus standards. If the cryptographic modules used are not in line with consensus standards, then the vehicle manufacturer shall justify their use.

7.4 Reporting

Note: Requirements in this section are addressed in organizational-level documentation.

7.4.1 periodic monitoring report

The vehicle manufacturer shall report at least once a year, or more frequently if relevant, to the Approval Authority or the Technical Service the outcome of their monitoring activities, as defined in paragraph 7.2.2.2.(g)), this shall include relevant information on new cyber-attacks. The vehicle manufacturer shall also report and confirm to the Approval Authority or the Technical Service that the cyber security mitigations implemented for their vehicle types are still effective and any additional actions taken.

7.4.2 defect report

The Approval Authority or the Technical Service shall verify the provided information and, if necessary, require the vehicle manufacturer to remedy any detected ineffectiveness.

If the reporting or response is not sufficient the Approval Authority may decide to withdraw the CSMS in compliance with paragraph 6.8.