

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

## Revision

Version 4  
7/29/22 3:58 PM

## Author

Charles Wilson

## Abstract

This document describes 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

This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC BY-SA-4.0)** License.

<https://creativecommons.org/licenses/by/4.0/legalcode>

# Application of Information

Within the context of **R155**, as presented in this document, the **AVCDL** can be used to support various activities identified within **R155** where cybersecurity interactions occur. It is expected that any organization seeking an **R155** CSMS approval will have the compliance group lead the interaction with the approval authority and coordinate with the cybersecurity group on the elements requiring that group's support.

Furthermore, given the scope of the full lifecycle supported by the **AVCDL**, it is expected that any implementer of the **AVCDL** or approval authority fully review the material in context. This is because there is an explicit traceability established by the **AVCDL** which removes the necessity to reiterate every precursor activity. This traceability is shown in the **AVCDL** primary document in section 18 **AVCDL Product Dependencies**.

It is assumed that since **R155** CSMS approval is achieved by the manufacturer, and that the application of the **AVCDL** may be in support of the overall activities of the manufacturer and/or any organization within the supply chain providing components for the vehicle under review.

Additionally, it is presumed that during organizational certification activities toward **R155** approval that individuals competent to explain and defend the processes expressed in and products generated by the application of the **AVCDL** will be available to the approval authority's examiners.

In addition to the **AVCDL** primary and secondary documents, the **AVCDL** elaboration documents provide contextual information which may be helpful to the approval authority.

## Interpretation Document Basis

This document uses the **R155** interpretation document **Proposals for Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system)** [ECE/TRANS/WP.29/2021/59], approved during the 183<sup>rd</sup> session (9-11 March 2021) as the basis for determining the **AVCDL** material relevant to each **R155** requirement.

A consolidated list of supporting material will be presented rather than an item-by-item breakdown. A more detailed breakdown has been presented in the **AVCDL Phase Requirement Product ISO 21434 Work Product Fulfillment** certification document.

**Note:** As the interpretation document was approved prior to the release of **ISO/SAE 21434**, its references to the that standard are based on the draft (DIS) and not the final (IS) version. Quotes from the interpretation document will be verbatim followed by notes when there is a deviation from the final version of the standard.

**Note:** A summary of the mapping from the DIS to IS versions of **ISO/SAE 21434** can be found in the **AVCDL mappings** spreadsheet, specifically in the **R155-AVCDL product (dual)** sheet.

# 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 the following requirement areas:

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

# AVCDL R155 Coverage

The items from **general** (7.1) are outside the scope of the AVCDL.

The following items from **cybersecurity management systems** (7.2) are outside the scope of the *AVCDL*:

- 7.2.1 compliance verification
- 7.2.2.3 timely risk mitigation
- 7.2.2.4(a) vehicle monitoring enrollment

The following items from **cybersecurity management systems** (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
- 7.2.2.4(b) threat extraction from vehicle logs
- 7.2.2.5 supplier deficiency management

The following items from **cybersecurity management systems** (7.2) are outside the scope of the *AVCDL*, but the *AVCDL* does provide supporting activities for them:

- 7.2.2.2(a) cybersecurity management

The items from **vehicle type** (7.3) and **reporting provisions** (7.4) are outside the scope of the *AVCDL*, but the *AVCDL* does provide supporting activities for them.

**Note:** A summary of the mapping from the **R155** requirements to the **AVCDL** phase requirements can be found in the **AVCDL mappings** spreadsheet, specifically in the **R155-AVCDL product (flat)** and **R155-AVCDL product (extra)** sheets.

## 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 not applicable in the context of the AVCDL supporting R155 as it is not intended to be evaluated.

#### Interpretation Document Basis

**Note:** There are no **ISO/SAE 21434** requirements which address this requirement.

#### Discussion

It is presumed that this requirement has no bearing on certification with respect to cybersecurity.

## 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 the manufacturer's organizational-level documentation.

#### Interpretation Document Basis

**Note:** There are no ISO/SAE 21434 requirements which address this requirement.

#### Discussion

The **AVCDL** forms the basis for a **cyber security management system** (CSMS) for the development, production, and post-production phases as defined in **R155**.

*2.3 "Cyber Security Management System (CSMS)" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks.*

The general structure of the **AVCDL** is laid out in its primary document and expanded upon in its secondary documents.

Since the **AVCDL** is not an implementation of these processes by an organization, but rather a coherent set of processes, the **AVCDL** supports, but does not fulfill this requirement.

### 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:*

#### Discussion

The **AVCDL** itself forms the basis for a **cybersecurity management system** (CSMS) for the development, production, and post-production phases as defined in **R155**. The general structure of which is laid out in the **AVCDL** primary document. The below listed references are applicable to the phases in which they are referenced.

**Note:** **AVCDL** phase requirement products may provide support to multiple **R155** items.

## 7.2.2.1(a) development phase CSMS

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating the required phases of the CSMS. Clauses 9 "Concept Phase", 10 "Product Development", and 11 "Cybersecurity validation" could be used to evaluate the Development phase of the CSMS.*

[Foundation-3]	List of Approved Tools and Components (Foundation-3.1)
[Requirements-1]	Product-level Security Goals (Requirements-1.1)
[Requirements-1]	Product-level Security Requirements (Requirements-1.2)
[Design-1]	Design Showing Security Considerations (Design-1.1)
[Design-2]	Security Design Review Report (Design-2.1)
[Design-4]	Threat Modeling Report (Design-4.1)
[Design-4]	Ranked/Risked Threat Report (Design-4.2)
[Design-4]	Threat Report (Design-4.3)
[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)

### Discussion

The **development phase CSMS** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for the 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-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-2]	Requirements Phase Gate (Requirements-2.1)
[Design-3]	Attack Surface Analysis Report (Design-3.1)
[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)

## 7.2.2.1(b) production phase CSMS

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating the required phases of the CSMS. ... Clause 12 "Production" could be used to evaluate the Production phase of the CSMS.*

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

### Discussion

The **production phase CSMS** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for the 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)
[Implementation-4]	Component/Version – Product/Version Cross-reference Document (Implementation-4.1)

## 7.2.2.1(c) post-production CSMS

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating the required phases of the CSMS. ... Clauses 7 "Continuous cybersecurity activities", 13 "Operations and maintenance", and 14 "Decommissioning" could be used to evaluate the Post-production phase of the CSMS;*

**Note:** The final **ISO/SAE 21434** references are: clauses 8 “Continual cybersecurity activities”, 13 “Operations and maintenance”, and 14 “End of cybersecurity support and decommissioning”.

[Foundation-7]	Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Foundation-8]	Decommissioning Plan (Foundation-8.1)
[Foundation-9]	Threat Prioritization Plan (Foundation-9.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Design-4]	Ranked/Risked Threat Report (Design-4.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)
[Operation-2]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)
[Decommissioning-1]	Decommissioning Report (Decommissioning-1.1)

### Discussion

The **post-production phase CSMS** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for the post-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)
[Design-4]	Threat Report (Design-4.3)

## 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 manufacturer's organizational-level documentation.

#### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-05-01], [RQ-05-02], [RQ-05-07], [RQ-05-08];*

**Note:** The final **ISO/SAE 21434** references are: [RQ-05-01], [RQ-05-02], [RQ-05-06], and [RQ-05-07].

#### Discussion

Although the **risk management** interpretation document reference **ISO/SAE 21434** clause 5 “Organizational cybersecurity management” which is not supported by the **AVCDL**, as it is outside the scope of a development lifecycle, the AVCDL does provide supporting material as documented in the **AVCDL Phase Requirement Product ISO 21434 Work Product Fulfillment** certification document as listed below.

[Foundation-1]	Training Catalog (Foundation-1.1)
[Foundation-1]	System to Track Training Participation (Foundation-1.2)

### 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;*

#### Interpretation Document Basis

*ISO/SAE 21434, especially based on [RQ-08-01], [RQ-08-02], [RQ-08-08], [RQ-08-09].*

**Note:** The final **ISO/SAE 21434** references are: [RQ-15-01], [RQ-15-02], [RQ-15-08], and [RQ-15-09].

[Design-1]	Design Showing Security Considerations (Design-1.1)
[Design-4]	Ranked / Risked Threat Report (Design-4.2)

#### Discussion

**Risk identification** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for risk identification:

[Design-3]	Attack Surface Analysis Report (Design-3.1)
[Design-4]	Threat Modeling Report (Design-4.1)
[Design-4]	Threat Report (Design-4.3)

**Note:** The **AVCDL** elaboration document **Understanding TARA in an AVCDL Context** provides an extensive explanation of how the **AVCDL** mechanism for assessing and addressing threats maps into the nomenclature of the **ISO/SAE 21434** TARA.

### 7.2.2.2(c) risk assessment / treatment

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

#### Interpretation Document Basis

*ISO/SAE 21434, especially based on [RQ-08-11], [RQ-08-04], [RQ-08-06], [RQ-08-10], [RQ-08-12], [RQ-09-07], [RQ-05-06], [RQ-09-08];*

**Note:** The final **ISO/SAE 21434** references are: [RQ-15-15], [RQ-15-04], [RQ-15-05], [RQ-15-10], [RQ-15-17], [RQ-09-05], [RQ-15-16], and [RQ-09-06].

[Design-4]	Ranked / Risked Threat Report (Design-4.2)
[Design-4]	Threat Report (Design-4.3)

#### Discussion

**Risk assessment and treatment** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for risk assessment and treatment:

[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)

**Note:** The **AVCDL** elaboration document **Understanding TARA in an AVCDL Context** provides an extensive explanation of how the **AVCDL** mechanism for assessing and addressing threats maps into the nomenclature of the **ISO/SAE 21434** TARA.

#### 7.2.2.2(d) verification of risk management

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

##### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-09];*

**Note:** The final **ISO/SAE 21434** references are: [RQ-09-07].

[Design-4]                      Threat Report (Design-4.3)

##### Discussion

**Verification of risk management** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for verification of risk management:

[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)

**Note:** The **AVCDL** elaboration document **Understanding TARA in an AVCDL Context** provides an extensive explanation of how the **AVCDL** mechanism for assessing and addressing threats maps into the nomenclature of the **ISO/SAE 21434** TARA.

## 7.2.2.2(e) cybersecurity testing

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

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-09-10], [RQ-10-01], [RQ-11-01], [RQ-11-02], [RQ-12-01];*

**Note:** The final **ISO/SAE 21434** references are: [RQ-09-08], [RQ-10-01], [RQ-11-01], N/A (folded into [RQ-11-01]), and [RQ-12-01].

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Design-1]	Design Showing Security Considerations (Design-1.1)
[Verification-4]	Verification Phase Gate (Verification-4.1)

### Discussion

Cybersecurity testing as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for cybersecurity testing:

[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;*

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-11-03], [RQ-06-08], [RQ-07-05], [RQ-07-06].*

**Note:** The final **ISO/SAE 21434** references are: N/A (folded into [RQ-08-07], [RQ-06-09], [RQ-08-07], and N/A (folded into [RQ-08-07].

[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Foundation-9]	Threat Prioritization Plan (Foundation-9.1)
[Design-4]	Ranked / Risked Threat Report (Design-4.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)
[Operation-2]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)

### Discussion

By design the **AVCDL** encourages the automation of nearly all activities within the lifecycle. It is the responsibility of those applying the **AVCDL** within their organizations to ensure that the information generated by the various requirements, design, analysis, and verification processes is leveraged to create a feedback loop ensuring the freshness of risk assessments.

Risk assessment freshness as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for risk assessment freshness:

[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)

Additional material is covered in the **Understanding Cybersecurity Risk Freshness in an AVCDL Context** elaboration document.

## 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.*

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-01], [RQ-07-02], [RQ-07-03], [RQ-07-04], [RQ-07-05], [RQ-15-04], [RQ-15-05], [RC-15-03], [RQ-13-01], [RQ-13-02], [RQ-13-03].*

**Note:** It is presumed that the inclusion of [RC-15-03] (responsibility matrix) is in error, and that it should have been [RQ-15-03] (cybersecurity interface agreement).

**Note:** The final **ISO/SAE 21434** references are: [RQ-08-01], [RQ-08-02], [RQ-08-03], [RQ-08-04], [RQ-08-07], [RQ-07-06], [RQ-07-07], [RQ-07-04], [RQ-13-01], N/A (folded into [RQ-13-01], and N/A (folded into [RQ-13-01]).

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-7]	Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Foundation-9]	Threat Prioritization Plan (Foundation-9.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Design-4]	Ranked / Risked Threat Report (Design-4.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)
[Operation-2]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)
[Supplier-3]	Cybersecurity Interface Agreement (Supplier-3.1)

### Discussion

It is important to consider that large portions of the **monitoring** and **response** processes are in the operational technology (**OT**) domain and not the product domain. The abovementioned **AVCDL** phase requirement products cover only those aspects which relate to the product itself and not peripheral systems (deployment ecosystem, cloud infrastructure, ...).

Adaptable monitoring and response as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for adaptable monitoring and response freshness:

[Foundation-4]	Global Security Goals (Foundation-4.1)
[Foundation-4]	Global Security Requirements (Foundation-4.2)

## 7.2.2.2(h) cybersecurity controls tracking

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

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-07-03].*

**Note:** The final **ISO/SAE 21434** references are: [RQ-08-03].

[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)

### Discussion

The **AVCDL** provides comprehensive and detailed processes to manage all cybersecurity relevant issues. Issues which result from **successful cybersecurity attacks** are treated in the same manner as those stemming from other sources. This ensure that no cybersecurity relevant issue is given a lesser treatment.

Cybersecurity controls tracking as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for cybersecurity controls tracking:

[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-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.*

#### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing the required processes, especially based on [RQ-05-02].*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

#### Discussion

The **AVCDL** processes are by design organization independent. The choice of an organization to impose time boxes on various activities is handled at the organizational level within policies governing various workflows. Additional imposed response time boxes may exist within the context of supplier service level agreements (SLAs).

## 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 manufacturer’s organizational-level documentation.

#### Interpretation Document Basis

**Note:** There are no **ISO/SAE 21434** requirements which address this requirement.

#### Discussion

It is important to consider that large portions of the **monitoring** and **response** processes are in the operational technology (OT) domain and not the product domain. The enrollment and monitoring of vehicles falls wholly in the OT domain.

### 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.*

#### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on 7.3 "Cybersecurity Monitoring", 7.4 "Cybersecurity event assessment", 7.5 "Vulnerability analysis".*

**Note:** The final **ISO/SAE 21434** references are: 8.3 “Cybersecurity monitoring”, 8.4 “Cybersecurity event evaluation”, and 8.5 “Vulnerability analysis”.

[Foundation-7]	Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)

## 7.2.2.5 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.*

### Interpretation Document Basis

*ISO/SAE 21434 can be used as the basis for evidencing and evaluating as required, especially based on [RQ-06-09], [RQ-15-03], [RC-15-02].*

**Note:** The final **ISO/SAE 21434** references are: [RQ-06-10], [RQ-07-04], and N/A.

[Supplier-3]                      Cybersecurity Interface Agreement (Supplier-3.1)

### Discussion

Supplier deficiency management as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for supplier deficiency management:

[Supplier-1]                      AVCMDS (Supplier-1.1)

[Supplier-2]                      Supplier Self-reported Maturity (Supplier-2.1)

## 7.3 Vehicle Types

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

### Discussion

The **AVCDL** is intended to address cybersecurity at the product level. It may be applied in part, or in whole, anywhere in the supply chain. It is not designed to address the unique issues surrounding vehicle type. This area requires systems to provide a coherent view of all aspects of the supply chain as well as the coordination with regulatory bodies. As such, the **AVCDL** can only provide partial material support.

### 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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

**Note:** There are no **ISO/SAE 21434** requirements which address this requirement.

#### Discussion

Within the context of a vehicle or component thereof which applies the **AVCDL**, adequate cybersecurity consideration would minimally be the implementation of those aspects which fulfill the requirements of **ISO/SAE 21434**.



## 7.3.2 management of type

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

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

### Interpretation Document Basis

*This requirement specifically references gaining sufficient information from the supply chain and is linked to 7.2.2.5.*

*ISO/SAE 21434.*

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

### Discussion

Supplier deficiency management as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for supplier deficiency management:

[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Foundation-9]	Threat Prioritization Plan (Foundation-9.1)
[Design-4]	Ranked / Risked Threat Report (Design-4.2)
[Design-4]	Threat Report (Design-4.3)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)
[Operation-2]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)

### 7.3.3 critical element risk assessment

*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.*

**Note:** This requirement is addressed in manufacturer’s organizational-level documentation.

#### Interpretation Document Basis

*ISO/SAE 21434 describes the way to define the concept. This also includes the consideration of critical elements based on risk treatment decisions. The results are documented in "Cybersecurity goals" and "Cybersecurity concept". [It] further describes exhaustive risk assessment in clause 8 "Risk assessment methods". This is documented in Threat analysis and risk assessment;*

**Note:** The final **ISO/SAE 21434** references are: clause 15 “Threat analysis and risk assessment methods”.

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

#### Discussion

**Critical element risk assessment** as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. The following provide additional support for critical element risk assessment.

**Note:** The **AVCDL** elaboration document **Understanding TARA in an AVCDL Context** provides an extensive explanation of how the **AVCDL** mechanism for assessing and addressing threats maps into the nomenclature of the **ISO/SAE 21434** TARA.

**Note:** The **AVCDL** secondary document **Element Cybersecurity Relevancy** provides a process for establishing cybersecurity relevant elements. The criticality of an element is determined during threat modeling.

## 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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

### Interpretation Document Basis

*ISO/SAE 21434 describes the identification of risk and the deduced Cybersecurity goals and concept based on the identified risks. The results are documented in [WP-09-04] Cybersecurity goals and [WP-09-07] Cybersecurity concept;*

**Note:** The final **ISO/SAE 21434** references are: [WP-09-03] and [WP-09-06].

[Design-1]	Design Showing Security Considerations (Design-1.1)
[Design-4]	Threat Report (Design-4.3)

### Discussion

The **AVCDL** ensures systematic coverage of cybersecurity risk by the application of cybersecurity requirements from the global security requirements catalog tailored to the elements under consideration. The requirements in the catalog are derived through application of the security requirements taxonomy (**Security Requirements Taxonomy**) to ensure that appropriate cybersecurity properties are considered for all identified asset types within the scope of the layer they present themselves. These requirements represent **mitigations** as they are controls applied to ensure that specific cybersecurity properties hold true. Since these requirements are also the basis for threat modeling, they provide a consistent application of controls since violation of modeling rules directly points to a corresponding cybersecurity requirement.

The following provide additional support for **risk protection**:

[Foundation-4]	Global Security Requirements (Foundation-4.2)
[Requirements-1]	Product-level Security Requirements (Requirements-1.2)
[Design-4]	Threat Modeling Report (Design-4.1)
[Design-4]	Ranked/Risked Threat Report (Design-4.2)

## Specific R155 Mitigations

As this requirement expressly calls out **mitigations** enumerated in R155 Annex 5, Part B and C; it is appropriate to address the general relationship of those mitigation with the **AVCDL**. Mitigations M1 through M7 are either IT or OT in nature and therefore not within the scope of the **AVCDL**. Mitigations M8 through M24 can be addressed within the scope of the **AVCDL** in that those mitigation can be applied to product cybersecurity in additional to either IT or OT cybersecurity.

**Note:** A summary of R155 mitigations is provided in the **UNECE WP.29 R155** spreadsheet.

**Note:** Mitigation M17 is not included in R155 Annex 5, Part B or C.

The following mitigations are either generalities or process in nature and not security controls which can be attached to elements' functional requirement as non-function cybersecurity requirements:

M6	Systems shall implement security by design to minimize risks
M7	Access control techniques and designs shall be applied to protect system data/code
M8	Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data
M9	Measures to prevent and detect unauthorized access shall be employed
M13	Measures to detect and recover from a denial of service attack shall be employed
M14	Measures to protect systems against embedded viruses/malware should be considered
M15	Measures to detect malicious internal messages or activity should be considered
M16	Secure software update procedures shall be employed
M18	Measures shall be implemented for defining and controlling user roles and access privileges, based on the principle of least access privilege
M19	Organizations shall ensure security procedures are defined and followed including logging of actions and access related to the management of the security functions
M22	Security controls shall be applied to external interfaces
M23	Cybersecurity best practices for software and hardware development shall be followed
M24	Best practices for the protection of data integrity and confidentiality shall be followed for storing personal data

These are addressed either as best practices recommendations throughout the **AVCDL** corpus, general documents such as **Secure Design Principles**, or in **AVCDL** phase requirements including:

### [\[Implementation-5\] Secure Development \(Implementation-5.1\)](#)

The remainder of the mitigations are addressed either directly or through a combination of requirements from the global security requirements catalog. The **cybersecurity requirements per taxonomy** spreadsheet shows the relationship between the global requirements and the security requirements taxonomy.

### 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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

#### Interpretation Document Basis

*ISO/SAE 21434 describes on a process base steps to make conclusion for the architecture. This aspect is to be considered in [WP-08-03] Threat scenarios.*

**Note:** The final **ISO/SAE 21434** references are: [WP-15-03].

[Design-4]                      Threat Modeling Report (Design-4.1)

#### Discussion

Given that the **AVCDL** is focused on vehicle's cybersecurity development lifecycle, it only speaks to the **dedicated environment** comprised of the vehicle. Supporting infrastructure such as the cloud-based services or operation centers are not addressed by the **AVCDL**.

Any **aftermarket** (post-production) changes would be subject to the same processes as the originally certified vehicle type. Additional material is covered in the **Understanding Cybersecurity Risk Freshness in an AVCDL Context** elaboration document.

## 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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

### Interpretation Document Basis

*Manufacturers may describe the verification and validation measure implemented in accordance with ISO/SAE 21434 in form of [WP-09-08] Verification report of cybersecurity concept, [WP-10-03] Verification report for the refined cybersecurity specification, [WP-11-02] Validation report.*

**Note:** The final **ISO/SAE 21434** references are: [WP-09-07], [WP-10-05] and [WP-09-05].

[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)
[Verification-4]	Verification Phase Gate (Verification-4.1)

### Discussion

The **AVCDL** uses a combination of controls (requirements) and phase gates to ensure that **sufficient testing** takes place. Additional material is covered in the **Understanding Verification and Validation in an AVCDL Context** elaboration document.

The following provide additional support toward **sufficient testing**:

[Requirements-2]	Requirements Phase Gate (Requirements-2.1)
[Design-5]	Design Phase Gate (Design-5.1)
[Implementation-11]	Implementation Phase Gate (Implementation-11.1)
[Release-3]	Release Phase Gate (Release-3.1)

## 7.3.7 Cyberattacks

*The vehicle manufacturer shall implement measures for the vehicle type to:*

### 7.3.7(a) detect / prevent cyberattacks

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

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

#### Interpretation Document Basis

**Note:** There are no ISO/SAE 21434 requirements which address this requirement.

#### Discussion

This requirement combines two distinct modalities which should have been addressed separately. The first (**detect cyberattacks**) is actually the focus of the requirement **7.3.7(b) vehicle cybersecurity monitoring** [below] and will be addressed there. As to the second (**prevent cyberattacks**), the **AVCDL** supports this requirement generally in that the **AVCDL** provides a methodology for minimizing cybersecurity risk.

### 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.*

**Note:** This requirement is addressed in manufacturer’s organizational-level documentation.

#### Interpretation Document Basis

*ISO/SAE 21434. A list of sources for cybersecurity monitoring is provided in clause 7.3.*

**Note:** The final **ISO/SAE 21434** references are: clause 8.3 “Cybersecurity Monitoring”.

[Foundation-7]	Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Operation-1]	Cybersecurity Incident Report (Operation-1.1)

#### Discussion

The processes detailed within the **AVCDL** in the areas of **monitoring** and **incident response** are designed to mesh with those undertaken by **OT**. Additional material is covered in the **Software Bill of Materials Lifecycle** elaboration document. This elaboration document provides insight into the interactions between the various processes involved in **monitoring** and **incident response**.

Additional support for **vehicle cybersecurity monitoring** is covered in the above section addressing **7.2.2.2 (g) adaptable monitoring / response**.



### 7.3.7(c) provide forensic capability

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

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

#### Interpretation Document Basis

*ISO/SAE 21434. ... The results of analysis and how to document it is described in [WP-07-04] Vulnerability analysis.*

**Note:** The final **ISO/SAE 21434** references are: [WP-08-04].

[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Operation-2]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)

#### Discussion

The primary methodology behind **forensic analysis** within **AVCDL** is detailed in the **Incident Response Plan** secondary document. As with the previous requirement, additional contextualization is covered in the **Software Bill of Materials Lifecycle** elaboration document.

### 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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

#### Interpretation Document Basis

**Note:** There are no **ISO/SAE 21434** requirements which address this requirement.

#### Discussion

The use of standard cryptographic modules is discussed in the **Secure Design Principles** AVCDL secondary document. The following provide additional support for the use of standard cryptographic modules:

[Design-1]                      Design Showing Security Considerations (Design-1.1)  
[Implementation-5]        Secure Development (Implementation-5.1)

## 7.4 Reporting

**Note:** Requirements in this section are addressed in manufacturer's 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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

#### Interpretation Document Basis

*ISO/SAE 21434 defines [WP-07-02] Results from the triage of cybersecurity information and [WP-07-04] Vulnerability Analysis. Both can be used as the baseline for the required reporting.*

[Foundation-7]	Cybersecurity Monitoring Plan (Foundation-7.1)
[Foundation-7]	Incident Response Plan (Foundation-7.2)
[Operation-2]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)

#### Discussion

Additional support for reporting is covered in the above section addressing **7.2.2.2 (g) adaptable monitoring / response**.

## 7.4.2 approval defect reporting

*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.*

**Note:** This requirement is addressed in manufacturer's organizational-level documentation.

### Interpretation Document Basis

**Note:** There are no **ISO/SAE 21434** requirements which address this requirement.

### Discussion

It is presumed that this requirement has no bearing on certification with respect to cybersecurity as it speaks to the interaction between the approval authority and the manufacturer.