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

Revision

Version 9
2/13/23 12:07 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 and ITU X.1371 Text

The audience for this document is the certifying organization. As such it is necessary to provide excerpts from **UNECE WP.29 R155** and **ITU-T X.1371** in order to provide evidence of sufficiency. Excerpts from **Recommendation ITU-T X.1371 (2020),** ***Security threats to connected vehicles*** are used by permission from the International Telecommunications Union.

License

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 amendments to the Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system)** [**ECE/TRANS/WP.29/2022/61**], approved during the 187th session (21-24 June 2022) 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.

Construction of Argument

As noted in the previous section, this document uses the **R155** interpretation document **Proposals for amendments to the Interpretation Documents for UN Regulation No. 155 (Cyber security and cyber security management system)** [**ECE/TRANS/WP.29/2022/61**], approved during the 187th session (21-24 June 2022) as the basis for determining the **AVCDL** material relevant to each **R155** requirement.

Also referenced above are the **AVCDL mapping** spreadsheets. The purpose of these is purely reference (primarily for the creation of other materials).

Since the **R155** interpretation document has been revised to be based on references to the **ISO/SAE 21434** final (IS) version, the mapping spreadsheet used to show the **ISO/SAE 21434** requirements level information (ref: **R155-AVCDL product (revised)**). This sheet addresses each expected **ISO/SAE 21434** requirement for each **R155** requirement. In this sheet the color coding is clearly reflective of the fact that these sections were taken from the existing mapping sheets (ref: **434 req-AVCDL product**). This sheet was simplified rolling up any duplicate and/or eliminated information (ref: **R155-AVCD product (rollup)**). Further, since the inclusion of specific **ISO/SAE 21434** requirements are not the goal but rather the **AVCDL** products satisfying the **R155** requirements, the rollup sheet was flattened to show only the **R155** requirements (ref: **R155-AVCDL product (flat)**). This sheet shows only those elements of the **AVCDL** expressly called for by the **R155** requirements. Finally, material, which in my opinion support the **goals** of the **R155** requirements but is **not required** per **ISO/SAE 21434** is shown (in blue) in a consolidated sheet (ref: **R155-AVCDL product (extra)**). It is from this sheet that the **AVCDL Phase Requirement Product UNECE WP.29 R155 Work Product Fulfillment** document is now based.

The **AVCDL Phase Requirement Product UNECE WP.29 R155 Work Product Fulfillment** document is the focus for guiding the review, not the **AVCDL mapping** spreadsheet. The mapping spreadsheet is the mechanism for tracing the choices for item inclusion.

The supplemental material (highlighted in blue) from the mapping spreadsheet is available, it is included following the discussion section of the **R155** requirement being addressed.

The **AVCDL** primary document is expected to properly show the **R155** requirements for which there are explicit requirements within **ISO/SAE 21434** (not the supplemental material).

Note: The **AVCDL mapping** spreadsheets are only a tool used to enable the construction of the argument presented within this document. They are referenced only for the purpose of explanation and are not expected to be necessary to understanding how the **AVCDL** fulfills various **R155** requirements.

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
- 7.2.2.4(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
- 7.2.2.3 timely risk mitigation
- 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.

Supply Chain

It is understood that the cybersecurity of the vehicle extends beyond any single organization within the totality of the supply chain. The **AVCDL** specifically addresses the supply chain and how it is considered within the overall cybersecurity development lifecycle. The following AVCDL documents address the supply chain.

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

Note: **R155** has specific supply chain requirements which appear later in this document.

Supply-17.2.2.1(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 [7 "Distributed cybersecurity activities",] 9 "Concept ", 10 "Product development", and 11 "Cybersecurity validation" could be used to evaluate the Development phase of the CSMS.

Note: The above highlighted text is a proposed addition for revision 2 of the R155 interpretation document.

[Supplier-1]	AVCMDS (Supplier-1.1)
[Supplier-2]	Supplier Self-reported Maturity (Supplier-2.1)
[Supplier-3]	Cybersecurity Interface Agreement (Supplier-3.1)
[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)
[Release-1]	Final Security Review Report (Release -1.1)
[Release -2]	Archive Manifest (Release -2.1)
[Release -3]	Release Phase Gate (Release -3.1)

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 8 "Continual cybersecurity activities", 13 "Operations and maintenance", and 14 "End of cybersecurity support and decommissioning" could be used to evaluate the Post-production phase of the CSMS;

[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)

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-05-06], [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-15-01], [RQ-15-02] , [RQ-15-03], [RQ-15-08].

[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)

Discussion

Risk identification as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. Specific R155 attacks (annex 5, part A) are discussed in section Notes Regarding R155 Annex 5 Part A. The following provide additional support for risk identification:

[Design-3] Attack Surface Analysis Report (Design-3.1)
[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.

Note: The **AVCDL** elaboration document **Understanding Cybersecurity Risk Freshness in an AVCDL Context** provides an extensive explanation of how the **AVCDL** is intended to be applied in order to ensure that changes in the product's cybersecurity posture are properly tracked.

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-15-15], [RQ-15-16], [RQ-15-04]. [RQ-15-05], [RQ-15-10], [RQ-15-17], [RQ-09-05], [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-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-09-07], [RQ-09-11], and [RQ-11-01];

Mitigations identified in Annex 5 of the Cyber Security Regulation shall be considered in the processes.

[Design-2]	Security Design Review Report (Design-2.1)
[Design-4]	Threat Report (Design-4.3)
[Verification-4]	Verification Phase Gate (Verification-4.1)

Discussion

Verification of risk management as supported by the **AVCDL** extends beyond the requirements of **ISO/SAE 21434**. Specific R155 mitigations (annex 5, parts B and C) are discussed in section Notes Regarding R155 Annex 5 Parts B and C.

The following provide additional support for verification of risk management:

[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

The aim of this requirement is to ensure the manufacturer has appropriate capabilities and processes for testing the vehicle type throughout its development and production phases.

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

[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

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)

The **AVCDL** provided for pre-manufacturing check to establish that all cybersecurity requirements, controls, and activities have been successfully implemented and completed:

[Release-1] Final Security Review Report (Release-1.1)
[Release-3] Release Phase Gate (Release-3.1)

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-08-07] [RQ-06-09]., [RQ-07-06].

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

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)

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-08-01], [RQ-08-02]. [RQ-08-03], [RQ-08-04], [RQ-08-05], [RQ-08-07], [RQ-08-08], [RQ-07-06], [RC-07-08], [RQ-13-01], and [RQ-13-02].

[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.

Note: The mechanism and timeliness aspects of this requirement is addressed in manufacturer's organizational-level documentation.

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-08-03], [RQ-08-04].

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]	Cybersecurity Incident Report (Operation-1.1)
[Operation-3]	Cybersecurity Incident Report (Operation-1.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

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

The intention of this requirement is to ensure that after the identified risks have been classified, a process has been established to determine the response time limit based on the classification results.

It is necessary to set the response deadline by processes such as triage and explain the monitoring process to see if it is executed within the deadline.

ISO/SAE 21434 can be used as the basis for evidencing the required processes, especially based on [RQ-08-07] and [RQ-08-08].

[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)

Note: The timeliness aspect of 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 8.3 "Cybersecurity Monitoring", 8.4 "Cybersecurity event evaluation", 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)

Discussion

It is important to recognize that privacy matters are outside the cybersecurity domain. These issues are the responsibility of the organization's privacy group. It is their responsibility to establish and enforce the activities and controls as required by various regulatory jurisdictions.

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-06-10], [RQ-07-04], [RC-07-05].

[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)

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).

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 "[WP-09-03] Cybersecurity goals" and "[WP-09-06] Cybersecurity concept". It further describes exhaustive risk assessment in clause 15 "Threat analysis and risk assessment methods". This is documented in "[WP-09-02] TARA";

[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 determination of risk and the deduced Cybersecurity goals and concept based on the identified risks. The results are documented in "[WP- 09-03] Cybersecurity goals" and "[WP-09-06] Cybersecurity concept";

[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 the ensure that specific cybersecurity properties holds 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. Specific R155 mitigations (annex 5, parts B and C) are discussed in section Notes Regarding R155 Annex 5 Parts B and C.

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)

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 steps to make conclusions for the architecture. "[WP-15- 03] Threat scenarios" documents the potential threats to the storage and execution of aftermarket software, services, application or data. In "[WP-09-06] Cybersecurity concept" the appropriate and proportionate measures are being described.

[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-10-07] Integration and verification report", "[WP-11-01] Validation report".

[Implementation-11] Implementation Phase Gate (Implementation-11.1)
[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)
[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. Identifying sources for cybersecurity monitoring is provided in [RQ- 08-01] and documented in "[WP-08-01] Sources for cybersecurity information".

[Foundation-7] Cybersecurity Monitoring Plan (Foundation-7.1)

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-08-05] 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-08-04] Weaknesses from cybersecurity events" and "[WP-08-06] Evidence of managed vulnerabilities". Both can be used as the basis for the required reporting.

[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

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.

Notes Regarding R155 Annex 5

This section provides discussion as to how R155 Annex 5 is addressed in the context of the AVCDL. As various requirements expressly calls out items enumerated in R155 Annex 5; it is appropriate to address the general relationship of those items within the context of the **AVCDL**.

It is useful to call out two things when considering Annex 5. First, parts A, B, and C have elements missing. This is because the material in this annex is sourced from the recommendations of the UNECE WP.29 task force on cybersecurity and over-the-air issues [ref. UNECE WP.29 GRVA-01-17 **Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA**]. This document contains the full list and additional references. Second, the ITU created a document [ref. ITU-T X.1371 **Security threats to connected vehicles**] which provides elaboration on the attacks enumerated in GRVA-01-07.

Part A

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

Attacks 1, 2, 3, and 13 are either IT or OT in nature and therefore not within the scope of the **AVCDL**. Attacks 4 through 12, 15 through 29, and 31, 32 can be addressed within the scope of the **AVCDL** in that those attacks can be applied against the product itself.

Note: Attacks 14 and 30 are not included in R155 Annex 5, Part A.

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

The attacks within the scope of the AVCDL are either generalities or process in nature and not security controls which can be attached to elements' functional requirement as non-function cybersecurity requirements. Each of these attacks will be addressed individually.

Attack 4

Spoofing of messages or data received by the vehicle

X.1371 Elaboration

Spoofing messages by impersonation can occur. In the case of messages used in a V2X communications and global navigation satellite system (GNSS), invalid messages can be received by a vehicle due to an impersonation attack. In addition, if there are many vehicles on a specific road, a Sybil attack can be carried out in order to spoof other vehicles.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authenticity

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Packets

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Network
- Protocol

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Communication crossing trust boundaries shall ensure data integrity.
- Communication crossing trust boundaries shall be authenticated.

Discussion

Rather than looking at the vague "spoofing" (used in two different senses in this attack) and only considering it for incoming data, the AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the integrity and authenticity of in motion data (packets) within the context of the vehicle. Further, these considerations are applied to both the network (standard) and protocol (custom) communication layers.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 5

Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data

X.1371 Elaboration

If there is a vulnerability or weakness in the vehicle, illegal remote access or malware intrusion attack can be made through the vehicle's communication channels. As a result, the communication channel may enable many security threats as follows:

- *code injection, e.g., software binary code that has been tampered with might be injected into the communication stream;*
- *manipulation of vehicle-held data or code;*
- *overwriting of vehicle-held data or code;*
- *erasure or deletion of vehicle-held data or code;*

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Configuration Data
- Databases
- Unstructured Data
- Credentials

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Network
- Protocol
- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.
- Configuration data modification shall only be made by authorized entities.
- Databases shall be segregated to achieve the principle of least access.
- Unstructured data access shall be granted based on the principle of least privilege.
- Credentials shall be modified only by authorized entities.

Discussion

Considering attacks via communication channels is ineffective at creating actual testable controls. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the authorization to manipulation at rest data (executables, configuration data, databases, unstructured data, credentials) within the context of the vehicle. Further, these considerations are applied to both the network (standard), protocol (custom) communication, and application layers.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 6

Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks

X.1371 Elaboration

Messages from an unreliable or untrusted source can be received through communication channels. Man-in-the-middle attacks and session hijacking are possible through communication channels. For example, an attack against a communication gateway in the vehicle allows an attacker to downgrade the software of an ECU or firmware of the gateway using known vulnerabilities of the software by a replay attack where repeatedly valid data transfers are made by malicious intent.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authenticity

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Packets

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Network
- Protocol
- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Communication crossing trust boundaries shall ensure data integrity.
- Communication crossing trust boundaries shall be authenticated.
- Custom protocols shall use current best practices for authentication and key exchange (NIST SP 800-57, 63B, 131 and 133).

Discussion

Rather than looking at the channel, the AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the integrity and authenticity of in motion data (packets) within the context of the vehicle. Further, these considerations are applied to both the network (standard) and protocol (custom) communication layers.

Note: These requirements are applied independently and depend upon the context of the communication.

Note: Well-formed packets should be using sequence numbers per best practices.

Attack 7

Information can be readily disclosed

X.1371 Elaboration

Information can be readily disclosed through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders. That is, information exchanged over the communication channel can be eavesdropped by malicious interception, interfering radiation and monitoring communications. To this end, the attacker can gain unauthorized access rights to files.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Confidentiality

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Logs
- PII
- Packets

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Network
- Protocol
- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Logs shall be stored in encrypted volumes.
- Logs shall avoid storing PII data and other regulated or sensitive data.
- Logs shall be stored in a manner that protects the data's confidentiality.
- PII shall be stored in a way that maintains confidentiality.
- PII shall be encrypted when transmitted across trust boundaries.
- Communication crossing trust boundaries that cannot be secured shall be isolated.
- Communication crossing trust boundaries shall ensure data confidentiality.
- Standard network protocols shall be secured using cybersecurity best practices.

Discussion

Although it may be true that information disclosure attacks exist, this information is ineffective at creating actual testable controls. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the confidentiality of in motion and at rest data (logs, PII, packets) within the context of the vehicle. Further, these considerations are applied to both the network (standard), protocol (custom) communication, and application layers.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 8

Denial of service attacks via communication channels to disrupt vehicle functions

X.1371 Elaboration

An attacker can conduct a denial-of-service attack via a communication channel by sending a large volume of garbage data to the vehicle information system so that vehicle functions are mostly disrupted. On the other hand, in the cases of platooning or vehicle-to-vehicle communication, the attacker could prevent necessary data from being sent to the other vehicles in the group so that other vehicles lose control because of lack of data from the other vehicles. This is called a "black hole attack".

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Availability

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Configuration Data
- Databases
- Unstructured Data
- Logs
- Packets

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Network
- Protocol
- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- The system shall enter a safe state when a safety-critical data store is not available.
- Logs shall be stored in a location that will persist in a crash.
- Logs shall fully pre-allocate their storage to ensure catastrophic events are recorded.
- Communication crossing trust boundaries shall ensure data availability.

Discussion

Although it may be true that denial of service attacks may disrupt vehicle operations, this information is ineffective at creating actual testable controls. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the availability of in motion and at rest data (configuration data, databases, unstructured data, logs, packets) within the context of the vehicle. Further, these considerations are applied to both the network (standard), protocol (custom) communication, and application layers.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 9

An unprivileged user is able to gain privileged access to vehicle systems

X.1371 Elaboration

By means of illegal accesses through communication channels, an unprivileged user can gain privileged access, such as root access, to the system. This is called "unauthorized privilege escalation" and once this escalation is successful, an attacker can do things that normal users cannot.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Configuration Data
- Databases
- Unstructured Data
- Credentials

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.
- Configuration data modification shall only be made by authorized entities.
- Databases shall be segregated to achieve the principle of least access.
- Unstructured data access shall be granted based on the principle of least privilege.
- Credentials shall be modified only by authorized entities.

Discussion

Although it may be true that there may exist attacks allowing escalation of privilege, this information is ineffective at creating actual testable controls. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the control of access to authorized entities regarding at rest data (executables, configuration data, databases, unstructured data, credentials) within the context of the vehicle. Further, these considerations are applied to application layer.

Note: These requirements are applied independently and depend upon the context of the asset in question.

Attack 10

Viruses embedded in communication media are able to infect vehicle systems

X.1371 Elaboration

After finding vulnerabilities in the vehicle system, viruses or malware can be injected into the vehicle system through communication channels. The viruses can become an administrator with privileged access and can conduct any intended attacks in the vehicle. For example, if the virus encrypts any files and information without authorization in the targeted vehicle system, which is called "ransomware", then the vehicle system will lose its function.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.

Discussion

Rather than focusing on a specific vector for the introduction of viruses, the AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the integrity of executables. These considerations are applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 11

Messages received by the vehicle, or transmitted within it, contain malicious content

X.1371 Elaboration

Messages received by the vehicle (e.g., diagnostic messages or messages from other vehicles) or transmitted within it, may contain malicious content. In the case of IVNs, an attacker can modify the software of ECUs by means of virus injection … and join the vehicle network as a member by using impersonation.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Packets

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Communication crossing trust boundaries shall ensure data integrity.

Discussion

Rather than focusing on a specific vector for the introduction of viruses (malicious content), the AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the integrity of packets. These considerations are applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the communication.

Note: It is important to note that neither standard (network) or custom (protocol) layers are designed to deal with detection or elimination of malicious content. It is the task of the application layer software to appropriate condition the communication channel to ensure data integrity.

Attack 12

Misuse or compromise of update procedures

X.1371 Elaboration

Regardless of whether the update used is conducted in a local or physical manner or through OTA, the update procedure can include threats using fabricating system update programs or compromised firmware.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.

Discussion

Rather than focusing on the update procedures as a special case, the AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the integrity of executables generally. These considerations are applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 15

Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack

X.1371 Elaboration

A legitimate user (e.g., owner, operator or maintenance engineer) can be an innocent victim and be tricked into taking an action to unintentionally load malicious code (malware) or enable an attack. Furthermore, the legitimate user often does not follow defined security procedures.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- N/A

Cybersecurity Layers

The following cybersecurity layers may be involved:

- N/A

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is not an attack against the vehicle systems, but a behavioral issue. Within the context of the AVCDL, product development has multiple overlapping sets of checks to instruct, encourage, enforce, and verify the application of cybersecurity best practices.

Attack 16

Manipulation of the connectivity of vehicle functions enables a cyber-attack

X.1371 Elaboration

Manipulation of the connectivity of vehicle functions enables a cyberattack. This threat can be considered in the following vehicle elements:

- *manipulation of functions designed to remotely operate systems: remote key, immobilizer, and charging pile;*
- *manipulation of vehicle telematics: e.g., remotely unlock cargo;*
- *manipulation through an interface with a short-range wireless system or sensors.*

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- N/A

Cybersecurity Layers

The following cybersecurity layers may be involved:

- N/A

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is about leveraging a connected system in order to gain a foothold for further attacks. This is addressed by attack surface analysis and threat modeling processes. These establish the points of contact and interplay between the various systems comprising the vehicle.

Note: There also exists IT and OT aspects which need to be addressed, but these are outside the scope of the AVCDL.

Attack 17

Hosted third-party software

X.1371 Elaboration

An infotainment system in modern vehicles connected to the IVN may allow installation of third-party applications. The third-party applications can be corrupted or have poor software security and be used as methods to attack vehicle systems.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is a supply chain attack. As such, it is not directly addressed in the AVCDL. There are multiple cybersecurity processes which should be applied to all binaries (including third-party ones) prior to allowing them to be integrated into the vehicle. These include (but are not limited to):

- Application of the full AVCDL process set
- AV scans (2)
- code signing
- chain of custody
- SBOM
- Sandbox analysis

Note: The ITU example provided is for an infotainment system.

Attack 18

Devices connected to external interfaces

X.1371 Elaboration

The functions of connectivity bring external interfaces and the devices connected to them can be used as a means to attack vehicle systems with the following vulnerable interfaces:

- *external interfaces such as USB port: to attack through code injection;*
- *infected media with the virus: the virus can attack the in-vehicle system via the infected media;*
- *diagnostic access: diagnostic functions accessed by Bluetooth dongles in OBD ports are used to view the status of vehicles and manipulate vehicle parameters that are included in the vehicle software.*

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Availability

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Hardware

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Physical

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Hardware components shall enable only the utilized connective features.
- Non-essential physical communication ports shall be disabled.

Discussion

This is not an attack, but a general observation that any non-isolated system must protect against malicious inputs. There is an obvious (stated) consideration that the AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the availability of hardware. These considerations are applied at the physical layer.

This is addressed by attack surface analysis process. There is also an implicit (unstated) consideration that the AVCDL considers as global requirements governing appropriate handling of data integrity and resource authorization. These have been referenced is several of the preceding attacks and so will not be reiterated here.

Note: These requirements are applied independently and depend upon the context of the communication.

Attack 19

Extraction of vehicle data/code

X.1371 Elaboration

Sensitive or credential data are targets for extraction because they may contain the following useful information for financial gain:

- *copyright or proprietary software of the vehicle;*
- *the owner's private information, such as personal identity, payment account information, address book information, location information and vehicle electronic ID;*
- *cryptographic keys, etc.*

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Configuration Data
- Databases
- Unstructured Data
- Credentials

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.
- Configuration data modification shall only be made by authorized entities.
- Databases shall be segregated to achieve the principle of least access.
- Unstructured data access shall be granted based on the principle of least privilege.
- Credentials shall be modified only by authorized entities.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that access to resources (executables, configuration data, databases, unstructured data, and credentials) is allowed only after proper authorization. These considerations are generally applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Attack 20

Manipulation of vehicle data/code

X.1371 Elaboration

By manipulating the vehicle data or code, attackers could impersonate or repudiate the rightful owner's behaviour. The following manipulation methods can be identified:

- *illegal/unauthorized changes to a vehicle's electronic ID;*
- *identity fraud: if a user wants to display another identity when communicating with toll systems and manufacturer backend systems;*
- *action to circumvent monitoring systems: hacking, tampering with or blocking messages, such as operating data recorder (ODR) tracker data or number of runs;*
- *data manipulation to falsify vehicle driving data, e.g., mileage, driving speed, driving directions and vehicle's reference time;*
- *unauthorized changes to system diagnostic data;*
- *firmware version fraud: the latest firmware having a patch to counter some vulnerability can be replaced by the old version without the patched.*

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Configuration Data
- Databases
- Unstructured Data
- Credentials
- Logs

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.
- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.
- Configuration data integrity shall be validated prior to use.
- Configuration data modification shall only be made by authorized entities.
- Databases shall be segregated to achieve the principle of least access.
- Unstructured data access shall be granted based on the principle of least privilege.
- Credentials shall be modified only by authorized entities.
- Logs shall be stored in a manner that protects the data's integrity.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that access (authorization) to and integrity of resources (executables, configuration data, databases, unstructured data, credentials, and logs) is handled appropriately. These considerations are generally applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Attack 21

Erasure of data/code

X.1371 Elaboration

Unauthorized deletion or manipulation of the system event logs may occur. This falsification often makes it impossible to analyse data or makes it difficult to search for the cause of the attack.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Configuration Data
- Databases
- Unstructured Data
- Credentials
- Logs

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.
- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.
- Configuration data integrity shall be validated prior to use.
- Configuration data modification shall only be made by authorized entities.
- Databases shall be segregated to achieve the principle of least access.
- Unstructured data access shall be granted based on the principle of least privilege.
- Credentials shall be modified only by authorized entities.
- Logs shall be stored in a manner that protects the data's integrity.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that access (authorization) to and integrity of resources (executables, configuration data, databases, unstructured data, credentials, and logs) is handled appropriately. These considerations are generally applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Attack 22

Introduction of malware

X.1371 Elaboration

By using many attack methods, introducing malware into a vehicle system is the first step in an attacker's activity. There are various attack interfaces for introducing malware, such as using external interfaces and infected physical modules.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.
- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that access (authorization) to and integrity of executables is handled appropriately. These considerations are generally applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Attack 23

Introduction of new software or overwrite existing software

X.1371 Elaboration

The introduction of new software or the overwriting of existing software with that which is malicious, may have a serious cybersecurity impact on the vehicle control system or information system.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.
- Processes receiving data crossing a trust boundary shall be sandboxed.
- Processes shall be granted the smallest set of privileges.
- Only authorized entities shall perform control operations on executables.
- Privileged access shall be permitted only for singular, specific, time-limited operations.
- The system shall contain only secure default privileged accounts if a privileged account is necessary.
- Processes shall have unique owners.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that access (authorization) to and integrity of executables is handled appropriately. These considerations are generally applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Attack 24

Disruption of systems or operations

X.1371 Elaboration

A denial-of-service attack against the vehicle system may be triggered on the internal network by flooding messages in a CAN bus or by provoking faults on an ECU via a high rate of messages.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Availability

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Packets

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Network
- Protocol

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Communication crossing trust boundaries shall ensure data availability.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that availability of communications channel (the packets therein) is maintained. These considerations are generally applied at the network and protocol layers.

Note: The application of this requirement presumes use of well-documented best practices and depends upon the context of the communication.

Attack 25

Manipulation of vehicle parameters

X.1371 Elaboration

Manipulation of vehicle parameters may have a strong influence on the vehicle system, e.g., unauthorized access to falsify:

- *the configuration parameters of a vehicle's key functions, such as brake data or airbag deployment threshold;*
- *the charging parameters, such as charging voltage, charging power, battery temperature, etc.*

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Integrity
- Authorization

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Configuration Data

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Configuration data integrity shall be validated prior to use.
- Configuration data modification shall only be made by authorized entities.

Discussion

This is not an attack, but rather a possible outcome of an attack. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure that access (authorization) to and integrity of configuration data is handled appropriately. These considerations are generally applied at the application layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Attack 26

Cryptographic technologies can be compromised or are insufficiently applied

X.1371 Elaboration

Cryptographic technologies can be compromised or are insufficiently applied. Cryptographic keys or certificates including credentials, such as password, can be exploited. For example, if weak cryptographic keys are used or the cryptographic keys are not updated for a long time, the cryptographic system may be broken by brute force attacks. Insufficient use of cryptographic technologies can also lead to leakage of cryptographic keys or credentials. Furthermore, the risk of information leakage can be increased by the use of already broken and obsolete cryptographic technologies.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Confidentiality
- Integrity
- Authenticity

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Packets
- Memory
- Hardware

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Physical
- Network
- Protocol
- Application

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- Persistent storage shall be encrypted.
- Update payloads shall be decrypted at time of use.
- Update payloads shall be encrypted at build time.
- Update payloads shall be stored encrypted.
- Executable integrity shall be cryptographically verified.
- Standard network protocols shall be secured using cybersecurity best practices.
- Communication crossing trust boundaries shall ensure data integrity.
- Communication crossing trust boundaries shall be authenticated.
- Custom protocols shall use current best practices for authentication and key exchange (NIST SP 800-57, 63B, 131 and 133).
- Cryptographic material stored in memory shall be handled appropriately.
- Cryptographic material stored in memory shall be validated prior to use.
- Cryptographic operations shall use a mechanism that is backed by a hardware root of trust.

Discussion

This is not an attack, but rather an observation. The AVCDL global security requirements catalog specifies exact, constrained, and testable requirements based on the desire to ensure the confidentiality, integrity, and authenticity of assets (executables, packets, memory, hardware). These considerations may be applied at every layer.

Note: These requirements are applied independently and depend upon the context of the asset under consideration.

Note: Many requirements presume implementation through the application of well-known best practices.

Attack 27

Parts or supplies could be compromised to permit vehicles to be attacked

X.1371 Elaboration

Hardware or software used in a vehicle ecosystem can be engineered so that it fails to meet design criteria to defend against an attack. Parts or supplies in a vehicle can be compromised to permit vehicles to be attacked.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- N/A

Cybersecurity Layers

The following cybersecurity layers may be involved:

- N/A

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is not an attack, but rather a scenario. The AVCDL specifies mechanisms for the assessment of supplier capabilities, establishment of cybersecurity activities, and assignment of responsibilities. It is presumed that cybersecurity must be established and maintained throughout the supply chain.

Attack 28

Software or hardware development permits vulnerabilities

X.1371 Elaboration

The presence of software bugs can be a basis for potentially exploitable vulnerabilities. This is particularly true if the software has not been tested to verify whether known bad code or bugs are present and to reduce the risk of unknown bad code or bugs being present.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- N/A

Cybersecurity Layers

The following cybersecurity layers may be involved:

- N/A

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is not an attack, but rather a hypothetical generalization. The AVCDL specifies processes which support a standard ISO 15288 / ISO 12207 development process. These processes far exceed the expectations established in ISO 21434.

Attack 29

Network design introduces vulnerabilities

X.1371 Elaboration

If network access is allowed while unnecessary communication ports are left open, attacks such as unauthorized access are likely to increase.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- N/A

Cybersecurity Layers

The following cybersecurity layers may be involved:

- N/A

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is not an attack, but rather a hypothetical generalization. The AVCDL attack surface analysis and threat modeling processes address this concern.

Attack 31

Unintended transfer of data can occur

X.1371 Elaboration

Private or sensitive data can be leaked when the users of a vehicle change (e.g., when the vehicle is sold or used for hire with a different person).

Cybersecurity Properties

The following cybersecurity properties are challenged:

- Confidentiality

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- Executables
- Configuration Data
- Databases
- Unstructured Data
- Credentials
- Logs
- PII

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Physical

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is not an attack, but rather a result of improper controls on data within the vehicle. The AVCDL addresses this in the decommissioning process documents.

Attack 32

Physical manipulation of systems can enable an attack

X.1371 Elaboration

Physical manipulation of systems such as OEM hardware is likely to lead to attacks. For example, a man-in-the-middle attack is possible if unauthorized hardware is added to the vehicle.

Cybersecurity Properties

The following cybersecurity properties are challenged:

- N/A

Cybersecurity Assets

The following cybersecurity assets may be impacted:

- N/A

Cybersecurity Layers

The following cybersecurity layers may be involved:

- Physical

Cybersecurity Requirements

The following global cybersecurity requirements address this attack vector:

- N/A

Discussion

This is not an attack, but rather a scenario. The AVCDL addresses this via the attack surface analysis process.

Note: Any actual attack enabled by the introduction into or modification of system elements would be covered by mechanism addressing these attacks presented earlier in this section.

Parts B and C

Note: Because parts B and C reference the same set of mitigations they are considered together.

Mitigations M1 through M5 are either IT or OT in nature and therefore not within the scope of the **AVCDL**. Mitigations M6 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)

Mitigations M10, M11, M12, M20, and M21 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.