AVCDL Phase Requirement Product ISO/SAE 21434 Work Product Fulfillment

Summary

# Revision

Version 6

2/27/24 9:03 AM

# Author

Charles Wilson

# Abstract

This document summarizes how **AVCDL** phase requirement products fulfill **ISO/SAE 21434** work products.

# Motivation

This document is motivated by the need to justify the sufficiency of the **AVCDL** as a tailoring of **ISO/SAE 21434**.

# Audience / Use of ISO/SAE 21434 Text

The audience for this document is the certifying organization. As such it is necessary to provide excerpts from **ISO/SAE 21434** itself in order to provide evidence of sufficiency.

# License

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

[**https://creativecommons.org/licenses/by/4.0/legalcode**](https://creativecommons.org/licenses/by/4.0/legalcode)

**Note:** This material is extracted from the ISO/SAE 21434 specification. It is included here for reference only.

# ISO/SAE 21434 AVCDL Coverage

The following clauses are within the scope of the ***AVCDL***:

* [Distributed Cybersecurity Activities](#_15.11_Distributed_Cybersecurity) (7)
* [Continuous Cybersecurity Activities](#_15.3_Continuous_Activities) (8)
* [Concept](#_15.5_Concept_Phase) (9)
* [Product Development](#_15.6_Product_Development) (10)
* [Cybersecurity Validation](#_15.7_Validation_Phase) (11)
* [Production](#_15.8_Production_Phase) (12)
* [Operations and Maintenance](#_15.9_Operations_and) (13)
* [End of Cybersecurity Support and Decommissioning](#_15.10_Decommissioning_Phase) (14)
* [Threat Analysis and Risk Assessments Methods](#_15.4_21434_Risk) (15)

The following clauses are outside the scope of the ***AVCDL***:

* Cybersecurity Management
  + [Organizational Cybersecurity Management](#_15.1_Overall_Cybersecurity) (5)
  + [Project Dependent Cybersecurity Management](#_15.2_Project_Dependent) (6)

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

# Organizational Cybersecurity Management (5)

### WP-05-01: Cybersecurity policy, rules and processes

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-05-01] cybersecurity policy

[RQ-05-02] organization-specific rules and processes

[RQ-05-03] roles and responsibilities

[RQ-05-04] cybersecurity resources

[RQ-05-05] communication channels

[RQ-05-06] cybersecurity culture

[RQ-05-07] ensure competency

[RQ-05-08] continuous improvement process

[RQ-05-09] information sharing criteria

### Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, there is discussion in the **AVCDL** primary document and **AVCDL** phase requirements which support the organization in fulfilling this work product.

[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)

**Communication channels** are addressed in the **AVCDL** primary document section 3.3 – **Inter-group Communication**. **Continuous improvement** is addressed in the **AVCDL** primary document section 5 – **Continuous Improvement**. **Information sharing** is addressed in the **AVCDL** primary document section 3.2 – **Information Sharing**.

### WP-05-02: Evidence of competence management, awareness management and continuous improvement

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-05-07] ensure competency

[RQ-05-08] continuous improvement process

### Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, there is discussion in the **AVCDL** primary document and **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-1] Training Catalog (Foundation-1.1)

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

**Continuous improvement** is addressed in the **AVCDL** primary document section 5 – **Continuous Improvement**.

### WP-05-03: Evidence of the organization’s management systems

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-05-11] quality management system

[RQ-05-12] track product cybersecurity until end-of-life

### WP-05-04: Evidence of tool management

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-05-14] tool management

### Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-3] List of Approved Tools and Components (Foundation-3.1)

### WP-05-05: Organizational cybersecurity audit report

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-05-17] cybersecurity audit

# Project Dependent Cybersecurity Management (6)

### WP-06-01: Cybersecurity plan

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-06-01] assign project responsibilities

[RQ-06-02] identify cybersecurity-relevant components

[RQ-06-03] cybersecurity plan content

[RQ-06-04] assign project tracking responsibilities

[RQ-06-05] cybersecurity plan style

[RQ-06-06] include cybersecurity in project plan

[RQ-06-07] keep cybersecurity plan updated

[RQ-06-09] keep cybersecurity work products updated

[RQ-06-10] cybersecurity supplier interface definition

[RQ-06-11] cybersecurity plan in QMS

[RQ-06-12] work products in QMS

[RQ-06-14] tailored activity justification

[RQ-06-15] reuse analysis

[RQ-06-16] reuse analysis composition 1

[RQ-06-17] reuse analysis composition 2

[RQ-06-18] out-of-context tailored activities

[RQ-06-19] out-of-context development

[RQ-06-20] out-of-context integration

[RQ-06-21] off-the-shelf component use

[RQ-06-22] off-the-shelf component documentation deficiency

### Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, there is discussion in the **AVCDL** primary document and **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-2] Roles and Responsibilities Document (Foundation-2.1)

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

### WP-06-02: Cybersecurity case

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-06-23] cybersecurity case

### WP-06-03: Cybersecurity assessment report

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-06-24] per component assessment rationale

[RQ-06-25] component assessment rationale review

[RQ-06-26] component assessment sufficiency

[RQ-06-27] assessor independence

[RQ-06-28] assessment-necessary information access

[RQ-06-30] assessment scope

[RQ-06-31] assessment recommendations

[RQ-06-32] conditional acceptance

### Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Design-2] Security Design Review Report (Design-2.1)

### WP-06-04: Release for post-development report

**Note:** This work product is addressed in the organizational-level documentation.

[RQ-06-33] work products required before release

[RQ-06-34] evidence required before release

### Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Release-1] Final Security Review Report (Release-1.1)

# Distributed Cybersecurity Activities (7)

**Note:** The following two (2) requirements are not attached to any work products

### WP-07-X1: Supplier Capability

[RQ-07-01] evaluate supplier cybersecurity capability

[Supplier-1] AVCMDS (Supplier-1.1)

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

### WP-07-X2: Supplier Cybersecurity Quote

[RQ-07-03] supplier cybersecurity quote

**Note:** The work products related to this requirement are addressed by organization-level processes.

### WP-07-01: Cybersecurity Interface Agreement

[RQ-07-04] supplier cybersecurity interface agreement

[RQ-07-06] supplier vulnerability activities

[RQ-07-07] extra-cybersecurity CIA conflict

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

# Continual Cybersecurity Activities (8)

## Cybersecurity Monitoring (8.3)

### WP-08-01: Sources for cybersecurity monitoring

[RQ-08-01] cybersecurity monitoring sources

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

### WP-08-02: Triage triggers of cybersecurity information

[RQ-08-02] cybersecurity triage triggers

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

### WP-08-03: Cybersecurity event triage

[RQ-08-03] cybersecurity event triage

[Foundation-7] Incident Response Plan (Foundation-7.2)

[Operation-1] Cybersecurity Incident Report (Operation-1.1)

## Cybersecurity Event Evaluation (8.4)

### WP-08-04: Cybersecurity event assessment

[RQ-08-04] cybersecurity event assessment

[Foundation-7] Incident Response Plan (Foundation-7.2)

[Operation-2] Cybersecurity Incident Report (Operation-1.1)

## Vulnerability Analysis (8.5)

### WP-08-05: Vulnerability analysis

[RQ-08-05] identified weaknesses analysis

[RQ-08-06] weakness rejection rationale

[Foundation-7] Incident Response Plan (Foundation-7.2)

[Operation-2] Cybersecurity Incident Report (Operation-1.1)

## Vulnerability Management (8.6)

### WP-08-06: Evidence of managed vulnerabilities

[RQ-08-07] vulnerability 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)

[Operation-3] Cybersecurity Incident Report (Operation-1.1)

## Unanchored Work Product (8.6.2)

**Note:** The following requirement is not attached to any work products

### WP-08-X1: Apply incident response protocols

[RQ-08-08] apply incident response protocols

[Foundation-7] Incident Response Plan (Foundation-7.2)

[Operation-2] Cybersecurity Incident Report (Operation-1.1)

# Concept (9)

## Item Definition (9.3)

### WP-09-01: Item definition

[RQ-09-01] item definition

[RQ-09-02] item operational information

[Requirements-1] Product-level Security Goals (Requirements-1.1)

[Requirements-1] Product-level Security Requirements (Requirements-1.2)

## Cybersecurity Goals (9.4)

### WP-09-02: Threat analysis and risk assessment

[RQ-09-03] item analysis

[RQ-09-04] risk treatment

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

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

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

### WP-09-03: Cybersecurity goals

[RQ-09-05] risk treatment to cybersecurity goal mapping

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

### WP-09-04: Cybersecurity claims

[RQ-09-06] cybersecurity claims

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

### WP-09-05: Verification report

[RQ-09-07] goals / claims verification report

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

## Cybersecurity Concept (9.5)

### WP-09-06: Cybersecurity concept

[RQ-09-08] cybersecurity requirements to goals mapping

[RQ-09-09] requirements operational information

[RQ-09-10] attach requirements to components

[Design-1] Design Showing Security Considerations (Design-1.1)

### WP-09-07: Verification report of cybersecurity concept

[RQ-09-11] requirements allocation verification report

[Design-2] Security Design Review (Design-2.1)

# Product Development (10)

## Design (10.4.1)

### WP-10-01: Refined cybersecurity specification

[RQ-10-01] refined cybersecurity requirements

[RQ-10-02] requirement component allocation

[Design-1] Design Showing Security Considerations (Design-1.1)

### WP-10-02: Cybersecurity requirements for post-development

[RQ-10-03] post-development cybersecurity consideration

[Requirements-2] Product-level Security Requirements (Requirements-2.1)

### WP-10-03: Documentation of the modeling, design, or programming languages and coding guidelines

[RQ-10-04] tool selection criteria

[RQ-10-05] tool insufficiency mitigation

[Foundation-3] List of Approved Tools (Foundation-3.1)

### WP-10-04: Verification report for the cybersecurity specifications

[RQ-10-08] cybersecurity specifications verification

[Verification-2] Updated Threat Model (Verification-2.1)

[Verification-3] Updated Attack Surface Model (Verification-3.1)

## Integration and Verification (10.4.2)

### WP-10-05: Vulnerability analysis report

[RQ-10-07] cybersecurity requirement verification

[RC-10-12] verification of weaknesses minimization

[RQ-10-13] documented rationale for not testing

[Verification-2] Updated Threat Model (Verification-2.1)

[Verification-3] Updated Attack Surface Model (Verification-3.1)

### WP-10-06: Integration and verification specification

[RQ-10-10] integration and verification specification

[Verification-1] Penetration Testing Report (Verification-1.1)

[Verification-2] Threat Model Review (Verification-2.1)

[Verification-3] Attack Surface Analysis Review (Verification-3.1)

### WP-10-07: Integration and verification reports

[RQ-10-09] verification of requirements fulfillment

[RQ-10-11] test coverage metrics

[RC-10-12] verification of weaknesses minimization

[RQ-10-13] documented rationale for not testing

[Implementaiton-11] Implementation Phase Gate (Implementation-11.1)

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

# Cybersecurity Validation (11)

## Cybersecurity Validation of the Item at Vehicle Level (11.0)

### WP-11-01: Validation report

[RQ-11-01] validation activities

[RQ-11-02] validation activities rationale

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

# Production (12)

## Production (12.0)

### WP-12-01: Production control plan

[RQ-12-01] production control plan

[RQ-12-02] production control plan specification

[Foundation-6] Release Integrity Plan (Foundation-6.1)

[Foundation-10] Deployment Plan (Foundation-10.1)

**Note:** The following requirement is not attached to any work products

### WP-12-X1: Production control plan implementation

[RQ-12-03] production control plan implementation

[Operation-4] Software Deployment Report (Operation-4.1)

# Operations and Maintenance (13)

## Cybersecurity Incident Response (13.3)

### WP-13-01: Cybersecurity incident response plan

[RQ-13-01] incident response plan

[Foundation-7] Incident Response Plan (Foundation-7.2)

### WP-13-X1: Cybersecurity incident response plan implementation

[RQ-13-02] incident response plan implementation

[Operation-1] Cybersecurity Incident Report (Operation-1.1)

## Updates (13.4)

**Note:** The following requirement is not attached to any work products

### WP-13-X2: Update implementation

[RQ-13-03] update plan

[Foundation-10] Deployment Plan (Foundation-10.1)

# End of Cybersecurity Support/Decommissioning (14)

## WP-14-01 Procedures to communicate end of cybersecurity support

[RQ-14-01] procedures to communicate cybersecurity end-of-support

[Foundation-8] Decommissioning Plan (Foundation-8.1)

**Note:** The following requirement is not attached to any work products

## WP-14-X1 Decommissioning requirements

[RQ-14-02] decommissioning cybersecurity requirements

[Foundation-8] Decommissioning Plan (Foundation-8.1)

# Threat Analysis and Risk Assessment Methods (15)

**Note:** Further elaboration on this topic is provided in **Understanding TARA in an AVCDL Context** AVCDL elaboration document.

## WP-15-01: Damage scenarios

[RQ-15-01] damage scenarios

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

## WP-15-02: Identified assets and cybersecurity properties

[RQ-15-02] asset identification

[Design-1] Design Showing Security Considerations (Design-1.1)

## WP-15-03: Threat scenarios

[RQ-15-03] threat scenarios identification

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

## WP-15-04: Impact rating

[RQ-15-04] damage scenarios impact analysis

[RQ-15-05] damage scenario impact severity

[RQ-15-06] safety impact ratings

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

## WP-15-05: Attack paths

[RQ-15-08] attack paths identification

[RQ-15-09] attack path mapped to threat scenario

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

## WP-15-06: Attack feasibility rating

[RQ-15-10] attack feasibility rating

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

## WP-15-07: Risk values

[RQ-15-15] risk value determination

[RQ-15-16] risk value scale

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

## WP-15-08: Risk treatment decision per threat scenario

[RQ-15-17] risk treatment considerations

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