AVCDL Phase Requirement Product ISO 26262 Work Product Fulfillment Summary

# Revision

Version 2

2/7/22 1:06 PM

# Author

Charles Wilson

# Abstract

This document summarizes how **AVCDL** phase requirement products fulfill **ISO 26262** work products.

# Motivation

This document is motivated by the need to justify the sufficiency of the **AVCDL** for compliance with the cybersecurity elements of **ISO 26262**.

# Audience / Use of ISO 26262 Text

The audience for this document is the certifying organization. As such it is necessary to provide excerpts from **ISO 26262** 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 26262** specification. It is included here for reference only.

# ISO/SAE 26262 AVCDL Coverage

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

* [5.4.2.3](#_5.4.2.3_effective_communication) Safety culture – effective communication channels
* [E.3.2 Concept phase](#_E.3.2_Concept_phase)
* [E.3.3 Product development](#_E.3.3_Product_development)
* [E3.4 Production and operation](#_E.3.4_Production_and)

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

* [E.3.1 Functional safety management](#_E.3.1_Functional_safety)

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

Note: Bullet lists from **ISO 26262** have been converted to a numbered format for ease of reference.

# 5.4.2 Safety culture

## 5.4.2.3 effective communication channels

Note: This section is addressed by the **AVCDL** primary document.

# E.3 Potential interaction between functional safety and cybersecurity

## E.3.1 Functional safety management

Note: Items in this section are addressed by organization-level processes.

1. plans and milestones for cybersecurity activities
2. coordination of the management of field monitoring activities  
     
   [Foundation-7] Cybersecurity Monitoring Plan (Foundation-7.1)  
   [Foundation-7] Incident Response Plan (Foundation-7.2)  
   [Operation-1] Cybersecurity Incident Report (Operation-1.1)

Note: Although out of scope, the above listed activities should be considered.

## E.3.2 Concept phase

1. cybersecurity threats analyzed as functional safety hazards  
     
   [Foundation-11] Threat Prioritization Plan (Foundation-9.1)  
   [Design-3] Attack Surface Analysis Report (Design-3.1)  
   [Design-4] Ranked / Risked Threat Report (Design-4.2)
2. hazards and associated risks to support the cybersecurity identification of threats  
     
   [Design-4] Threat Modeling Report (Design-4.1)
3. cybersecurity strategies or countermeasures  
     
   [Design-4] Ranked / Risked Threat Report (Design-4.2)  
   [Design-4] Threat Report (Design-4.3)

## E.3.3 Product development

1. cybersecurity design and implementation technical information  
     
   [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)
2. cybersecurity software and hardware design considerations  
     
   [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)  
   [Implementaiton-4] Component/Version – Product/Version Cross-reference Document  
    (Implementation-4.1)  
   [Implementaiton-5] Secure Development (Implementation-5.1)
3. functional safety design and implementation information  
     
   [Requirements-1] Product-level Security Requirements (Requirements-1.2)  
   [Design-1] Design Showing Security Considerations (Design-1.1)
4. harmonized safety and cybersecurity analysis activities  
     
   [Design-1] Design Showing Security Considerations (Design-1.1)  
   [Design-3] Attack Surface Analysis Report (Design-3.1)  
   [Design-4] Threat Modeling Report (Design-4.1)
5. cybersecurity countermeasures to address systematic failures  
     
   [Implementaiton-1] List of Tools and Components Used (Implementation-1.1)  
   [Implementaiton-4] Component/Version – Product/Version Cross-reference Document  
    (Implementation-4.1)

## E.3.4 Production and operation

1. cybersecurity incident resolution strategies  
     
   [Foundation-7] Cybersecurity Monitoring Plan (Foundation-7.1)  
   [Foundation-7] Incident Response Plan (Foundation-7.2)  
   [Operation-1] Cybersecurity Incident Report (Operation-1.1)