AVCDL Phase Requirement Product ISO 26262 Work Product Fulfillment Summary

Revision

Version 3
4/27/22 11:54 AM

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

ISO/SAE 26262 AVCDL Coverage

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

- 5.4.2.3 Safety culture – effective communication channels
- E.3.2 Concept phase
- E.3.3 Product development
- E3.4 Production and operation

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

- E.3.1 Functional safety management

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 section 3 **Philosophy**.

E.3 Potential interaction between functional safety and cybersecurity

Note: Annex E contains only informative (non-normative) material, and its implementation is not required for ISO 26262 certification.

E.3.1 Functional safety management

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

a. plans and milestones for cybersecurity activities
b. 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

a. cybersecurity threats analyzed as functional safety hazards

[Foundation-9] Threat Prioritization Plan (Foundation-9.1)
[Design-3] Attack Surface Analysis Report (Design-3.1)
[Design-4] Ranked / Risked Threat Report (Design-4.2)

b. hazards and associated risks to support the cybersecurity identification of threats

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

c. 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

a. 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)

b. 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)

c. functional safety design and implementation information

[Requirements-1]	Product-level Security Requirements (Requirements-1.2)
[Design-1]	Design Showing Security Considerations (Design-1.1)

d. 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)

e. 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

a. 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)