AVCDL Phase Requirement Product ISO 26262 Work Product Fulfillment Summary

Revision

Version 4
7/13/22 12:56 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

The audience for this document is the certifying organization.

License

Note: This document does not include ISO 26262 excerpts. Refer to the non-summary version of this document for inline excerpts.

Application of Information

The **AVCDL** is a cybersecurity-oriented work. It does not attempt to harmonize its nomenclature with those of other disciplines. Within the context of **ISO 26262**, as presented in this document, the **AVCDL** can be used to support various activities identified within **ISO 26262** where cybersecurity interactions occur. It is expected that any organization seeking an **ISO 26262** certification will have the safety group lead the interaction with the certification body 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 certification body 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**.

Additionally, it is presumed that during organizational certification activities toward **ISO 26262** certification 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 certification body's examiners.

Within the **AVCDL** there are a limited number of phase requirements which necessitate interaction with the safety group in their capacity of providing risk related support to the organization. These are summarized in the **AVCDL** primary document section 11 **Groups** which includes an abbreviated form of the **AVCDL roles and responsibilities** spreadsheet. It is worth noting that aside from the phase gates, there is active (responsible) interaction only in [Design-4] **Threat Modeling** and [Verification-2] **Threat Model Review**. This is because these represent design and not implementation defects. It is presumed that implementation defects require mitigation as non-functional requirements have not been properly implemented.

The primary interaction between safety and security is during execution of the [Foundation-9] **Threat Prioritization Plan**. The AVCDL secondary document by the same name describes this interaction in detail.

In addition to the **AVCDL** primary and secondary documents, the **AVCDL** elaboration document **Understanding TARA in an AVCDL Context** provides contextual information which may be more familiar to individuals within the safety group and certification body.

ISO 26262 Overview

Road Vehicles – Functional Safety is intended to address the functional safety aspects of electrical and electronic (E/E) systems within road vehicles.

Although cybersecurity is mentioned several times within the standard, it is only formally addressed in clause 5.4.2.3 (**Safety culture – effective communication channels**) and annex E (**Guidance on potential interaction of functional safety with cybersecurity**) of part 2 (**Management of functional safety**).

Note: Annex E is an informative (non-normative) section of **ISO 26262**. As such, there are no cybersecurity requirement or work products contained in the standard.

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.

Note: Bold blue text is used within discussion sub-sections to denote extracts from the ISO 26262 material under discussion in that section.

5.4.2 Safety culture

Note: This section is addressed by the **AVCDL** primary document section 3 - **Philosophy**.

5.4.2.3 effective communication channels

Note: It is presumed that the authority responsible for the effective communication between the safety and cybersecurity groups lies with the organization's overall project management.

Discussion

As indicated in **5.4.2.3**, the **organization** is responsible to **institute and maintain effective communication channels**. The cybersecurity group is a participant in this communication operating within the framework established by the organization.

In support of this communication, the **AVCDL** processes identify all involved groups and the specific actors from those groups necessary to undertake the activities within those processes. These groups are described in the **AVCDL** primary document section 3.4 – **Reference to Groups**. Additional information is provided both within each **AVCDL** phase requirements listed within the **AVCDL** primary document. Those phase requirements are summarized by responsible group in section 11 - **Groups** of the AVCDL primary document. For the purposes of this document the more relevant of these is section 11.4 **Risk**.

Note: There are no AVCDL phase requirements for which **risk** is responsible. An overview of the risk group participation can be seen in the **AVCDL** primary document table 3 – **AVCDL Phase Requirement – Group Mapping**.

Note: The **AVCDL** refers to risk generically as described in the **AVCDL** primary document section 3.4.5 **Risk**. Since safety is a specialization of the risk groups, when read by safety individuals, the expectation is that they will read **risk** as **safety**. This is mentioned in the same above referenced section.

Additionally, where information sharing takes place as part of the abovementioned communication, it will be managed on the organizational level as described in the **AVCDL** primary document section 3.2 **Information Sharing**.

A more extensive general discussion is provided in section 3 - **Philosophy** of the **AVCDL** primary document.

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.

This section of **ISO 26262** is only intended to provide guidance from the functional safety perspective. As such, the materials presented in this section are not intended to be evaluated with the same level of rigor as would those in normative sections. Materials are provided to support organizations as they establish interaction mechanisms appropriate to their overall organizational processes.

E.3.1 Functional safety management

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

a. plans and milestones for cybersecurity activities

Discussion

As **E.3.1** is addressing **safety management interaction with the management of cybersecurity**, this discussion is beyond the scope of the **AVCDL**. It is further presumed that the responsibility for the project **plans and milestones** (**E.3.1.a** above) of any group within the organization belong to an organizational level project / product management group.

As stated in the discussion of **4.5.3.2** above, all involved groups and the specific actors from those groups necessary to undertake the activities within the **AVCDL** are identified within each activity specified in each **AVCDL** phase requirement product workflow. It is presumed that this information will be used by the project / product management group in the planning and execution of product development, as well as coordination between all involved groups.

Note: There is no material within the AVCDL specifically addressing project management as it is outside the scope of a lifecycle document. As noted in **AVCDL** primary document **Table 1 – Relationship Among Standards** (note), the AVCDL does not address either **ISO 21434** clause 5 - **overall cybersecurity management** or **ISO 21434** clause 6 - **project dependent cybersecurity management**.

Note: Project management is governed by **ISO 21500** - **Guidance on Project Management**.

---

b. coordination of the management of field monitoring activities

Discussion

The **coordination of the management of field monitoring activities** (**E.3.1.b** above) is outside the of scope of the **AVCDL** as it is the responsibility of the operational technology (**OT**) group. Support of the OT group is provided for within the **AVCDL** in the areas of cybersecurity-specific **field monitoring** as discussed in the **AVCDL** secondary document **Cybersecurity Monitoring Plan**, cybersecurity-specific **incident reporting** as discussed in the **AVCDL** secondary document **Incident Response Plan**, and cybersecurity-specific **tracking and resolution** as discussed in the **AVCDL** secondary document **Cybersecurity Incident Report**.

Additional background information is laid out in the **AVCDL** primary document in the following phase requirements:

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

E.3.2 Concept phase

a. cybersecurity threats analyzed as functional safety hazards

Discussion

As stated in **E.3.2.a** above, there is a need to consider **cybersecurity threats to be analysed as a hazard from a functional safety perspective**. Within the **AVCDL** this analysis is conducted as part of the implementation of the threat prioritization process. This process is applied uniformly to all identified potential cybersecurity threats, regardless of their source. This uniform application ensures that the safety aspect is always considered. The general discussion of the threat prioritization process is laid out in the **Threat Prioritization Plan AVCDL** secondary document. The specific application of the threat prioritization process which engages a risk analysis is contained in **Ranked / Risked Threat Report AVCDL** secondary document.

Note: **ISO 21434** specifies that not only safety be considered, but also several other risk dimensions. This is discussed in the **AVCDL** primary document section 3.4.5 **Risk**.

Within the context of this item (**E.3.2.a**), the two processes where a safety risk analysis would be applied with respect to the **ISO 26262** concept phase are threat modeling and attack surface analysis as discussed in the **AVCDL** secondary document **Attack Surface Analysis Report** and threat modeling as discussed in the **AVCDL** secondary document **Threat Modeling Report**. Both generate threat candidates which are fed into the ranking / risking process as discussed in the **AVCDL** secondary document **Ranked / Risked Threat Report** and finally the threat report process as discussed in the **AVCDL** secondary document **Threat Report**.

Additional background information is laid out in the **AVCDL** primary document in the following phase requirements:

[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

Discussion

As stated in **E.3.2.b** above, **functional safety can provide information such as hazards and associated risks to support the cybersecurity identification of threats**. It is presumed that this information would be documented at non-functional safety requirements attached to their corresponding functional requirements or as safety notes attached to the functional design documentation. This information is presumed to be available to cybersecurity per **ISO 26262 5.4.2.3** (**Safety culture**).

Note: Any such information would be considered as a normal input to the **AVCDL** design phase activities such as design review as discussed in the **AVCDL** secondary document **Security Design Review**, threat modeling as discussed in the **AVCDL** secondary document **Threat Modeling Report**, and attack surface analysis as discussed in the **AVCDL** secondary document **Attack Surface Analysis Report**.

Additional background information on processes where safety input would be applied is laid out in the **AVCDL** primary document in the following phase requirements:

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

c. cybersecurity strategies or countermeasures

Discussion

E.3.2.c above is addressing sharing of information from cybersecurity to safety on the topic of **cybersecurity strategies or countermeasures** so that safety may **determine potential impacts on safety goals or safety concepts**. This is backward looking information as indicated by the contextualization to **a detected attack**. This is further emphasized by the fact that **E.3.2** covers the concept phase of **ISO 26262**. The implication being that safety will have access to information regarding the mitigation **strategies** (**countermeasures**) either used or recommended by cybersecurity when dealing with **detected** (past) **attack**s.

As noted in **4.5.3.2** above, information sharing is discussed in the **AVCDL** primary document section 3.2 **Information Sharing**.

It is presumed that any sufficiently mature organization will take into consideration past learnings when establishing **goals** and **concepts**, as one does in the concept phase of **ISO 26262**.

Additional background information on the type of information available from **detected attack**s is laid out in the **AVCDL** primary document in the following phase requirements:

[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

Discussion

E.3.3.a above is addressing sharing of information from cybersecurity to safety on the topic of **cybersecurity strategies or countermeasures** relating to **design and implementation** so that safety may **determine potential impacts on safety concept and the system design**.

Cybersecurity strategies or countermeasures are embodied within the cybersecurity requirements for the product as discussed in the **AVCDL** secondary document **Product-level Security Requirements**. It is presumed that these requirements constrain functional requirements. This information is presumed to be available to safety. Additional considerations are fed back into these requirements upon review of the functional design with respect to cybersecurity as discussed in the **AVCDL** secondary document **Design Showing Security Considerations**.

As noted in **4.5.3.2** above, information sharing is discussed in the **AVCDL** primary document section 3.2 **Information Sharing**.

Additional background information on the type of information available from **design and implementation** is laid out in the **AVCDL** primary document in the following phase requirements:

[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

Discussion

E.3.3.b above is addressing sharing of information from cybersecurity to safety on the topic of **cybersecurity software and hardware design considerations** so that safety may **determine potential impacts on software and hardware safety requirements and design constraints**.

Cybersecurity software and hardware design considerations are embodied within the cybersecurity requirements for the product as discussed in the **AVCDL** secondary document **Product-level Security Requirements**. It is presumed that these requirements constrain functional requirements. This information is presumed to be available to safety. Additional considerations are fed back into these requirements upon review of the functional design with respect to cybersecurity as discussed in the **AVCDL** secondary document **Design Showing Security Considerations**.

As noted in **4.5.3.2** above, information sharing is discussed in the **AVCDL** primary document section 3.2 **Information Sharing**.

Additional background information on the type of information available from **software and hardware design considerations** is laid out in the **AVCDL** primary document in the following phase requirements:

[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)

c. functional safety design and implementation information

Discussion

E.3.3.c above is addressing sharing of information from safety to cybersecurity on the topic of **design and implementation of safety measures** so that safety may **communicate functional safety constraints that can be relevant to cybersecurity**.

Functional safety constraints are presumed to be embodied within the safety requirements for the product. It is presumed that these requirements constrain functional requirements. This information is presumed to be available to cybersecurity. This information will be considered as part of body of product requirements during the application of cybersecurity requirements to the functional requirements as discussed in the **AVCDL** secondary document **Product-level Security Requirements**.

As noted in **4.5.3.2** above, information sharing is discussed in the **AVCDL** primary document section 3.2 **Information Sharing**.

Additional background information on the type of information available expected in the cybersecurity requirements process is laid out in the **AVCDL** primary document in the following phase requirements:

[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

Discussion

E.3.3.d above is addressing joint participation in **analysis activities** by **safety and cybersecurity** to **uncover potential cybersecurity impacts on functional safety**.

In **E.3.2.a** above it has already been stated that within the **AVCDL** this [safety] risk analysis is conducted as part of the implementation of the threat prioritization process. Since every cybersecurity threat is subjected to review by safety for assessment of **impact on functional safety**, it can be asserted that the AVCDL prescribes joint **safety and cybersecurity** participation in **analysis activities**. It is further presumed that in the process of assessing [safety] risk that safety will use the information gleaned from such analysis to **uncover potential cybersecurity impacts on functional safety**.

Note: The aside in **E.3.3.d** above, **safety analyses can also consider the impact of cybersecurity strategies and countermeasures**, has already been addressed separately in **E.3.2.c** above.

---

e. cybersecurity countermeasures to address systematic failures

Discussion

E.3.3.e above is addressing sharing of information from cybersecurity to safety regarding **cybersecurity countermeasures** addressing **systematic failures**. The intent is that safety be able to **determine the potential impacts on functional safety**.

Note: The example provided in **E.3.3.e** above is an irrelevant elaboration within the context of the recommendation.

In **E.3.2.a** above it has already been stated that within the **AVCDL** this [safety] risk analysis is conducted as part of the implementation of the threat prioritization process. Since every cybersecurity threat is subjected to review by safety for assessment of **impact on functional safety**, it is presumed that safety will be noting classes of failure modes, including ones which would lead to **systemic failures**. Safety could establish mechanisms to track the cybersecurity mitigations related to these threats and establish additional safety requirements to address them as a class.

Note: It is outside the scope of the AVCDL or this document to opine on what methodologies or mechanisms safety might use to accomplish the identification of failure mode classes or mechanisms for tracking them.

E.3.4 Production and operation

a. cybersecurity incident resolution strategies

Discussion

E.3.3.e above is addressing sharing of information from cybersecurity to safety regarding **cybersecurity incident resolution strategies resulting from cybersecurity incident response** to **consider potential impacts on functional safety**.

Note: The constraint in **E.3.3.e** above limiting consideration to those **due to design changes resulting** is unnecessary within the context of the interaction between cybersecurity and safety afforded by the **AVCDL**.

In **E.3.2.a** above it has already been stated that within the **AVCDL** this [safety] risk analysis is conducted as part of the implementation of the threat prioritization process. Since every cybersecurity threat is subjected to review by safety for assessment of **impact on functional safety**, it is presumed that safety will be involved in the review of every **cybersecurity incident response**.

Additional background regarding **cybersecurity incident response** is laid out in the **AVCDL** primary document in the following phase requirements:

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