AVCDL Phase Requirement Product ISO 24089 Work Product Fulfillment Summary

Revision

Version 1
2/28/24 5:10 PM

Author

Charles Wilson

Abstract

This document describes how **AVCDL** phase requirement products fulfill **ISO 24089** work products.

Motivation

This document is motivated by the need to justify the sufficiency of the **AVCDL** for compliance with **ISO 24089**.

Audience / Use of ISO 24089 Text

The audience for this document is the certifying organization. As such it is necessary to provide numerous excerpts from **ISO 24089** itself to provide evidence of sufficiency.

License

Note: This material is extracted from the ISO 24089 specification. It is included here for reference only.

Application of Information

Within the context of **ISO 24089**, as presented in this document, the **AVCDL** can be used to support various activities identified within **ISO 24089** where cybersecurity interactions occur. It is expected that any organization seeking **ISO 24089** certification 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 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**.

It is assumed that since **ISO 24089** certification is achieved by each supplier in addition to 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 **ISO 24089** 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.

In addition to the **AVCDL** primary and secondary documents, the **AVCDL** elaboration documents provide contextual information which may be helpful to the certification body.

Construction of Argument

As noted in the previous section, this document uses the **ISO 24089:2023 *Road vehicles — Software update engineering*** as the basis for determining the **AVCDL** material relevant to each **ISO 24089** requirement.

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

The **AVCDL mapping** spreadsheet used to show the **ISO 24089** requirements level information maps **ISO 24089** requirements to **AVCDL** phase requirement products (ref: **089 req-AVCDL product)**. This sheet addresses each expected **ISO 24089** requirement and shows those **AVCDL** phase requirements products which fulfill or support them. 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**). It is from this sheet that the **AVCDL Phase Requirement Product ISO 24089 Work Product Fulfillment** document is based.

The **AVCDL Phase Requirement Product ISO 24089 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 **AVCDL** primary document is expected to properly show the **ISO 24089** 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 **ISO 24089** requirements.

ISO 24089 Overview

Note: This material is extracted from the ISO 24089 specification. It is included here for reference only.

Road Vehicles – Software Update Engineering is intended to address the requirements for software update in road vehicles.

The focus of the specification is generally outside the scope of the ***AVCDL***. There are, however, supporting activities provided by the AVCDL. These will be noted.

The clauses of **ISO 24089** with work products are:

- Organization level software update requirements (4)
- Project level software update requirements (5)
- Infrastructure for software update engineering design and development (6)
- Software update-capable vehicles and components development (7)
- Software update package development (8)
- Software update campaign operations (9)

Note: Out-of-scope activities are addressed by the noted non-cybersecurity group.

Note: As the specification uses only a dot notation, work products will be prefixed by **WP-** and requirements by **RQ-** to distinguish them more readily.

Organizational Level Software Update Requirements (4)

WP-4.4.1: Organizational rules and processes

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

[RQ-4.3.1.1] software changes done per ISO 24089

[RQ-4.3.1.2] establish, document and maintain software update rules and processes

[RQ-4.3.4.1] establish, implement and maintain a document management system

[RQ-4.3.4.3] consider the privacy implications of software update

[RQ-4.3.4.4] establish, implement and maintain a configuration management system

[RQ-4.3.4.5] establish, implement and maintain a quality management system

[RQ-4.3.4.6] establish, implement and maintain a change management system

Discussion

Although the **AVCDL** does not address this work product, many of the above listed requirements are presumed to be in place in order for the **AVCDL** to be implement.

WP-4.4.2: Records of organizational management

[RQ-4.3.1.3] comply with ISO/SAE 21434, ISO 26262-6 and ISO 26262-8

Note: This requirement is partially supported.

Discussion

Although the **AVCDL** does not completely address this requirement, it is explicitly compliant with **ISO/SAE 21434**. **ISO 26262** compliance is the responsibility of safety.

[RQ-4.3.4.2] establish, implement and maintain a requirements management system

[RQ-4.3.4.5] establish, implement and maintain a quality management system

Note: These requirements are addressed in the organizational-level documentation.

Discussion

Although the **AVCDL** does not address this work product, many of the above listed requirements are presumed to be in place in order for the **AVCDL** to be implement.

WP-4.4.3: Documentation of continuous improvement

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

[RQ-4.3.2.1] establish, perform and maintain a continuous improvement process
[RQ-4.3.2.2] establish, perform and maintain a process to verify changes remain compliant

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. **Continuous improvement** is addressed in the **AVCDL** primary document section 5 – **Continuous Improvement**. **Keeping work products updated** is addressed in the **AVCDL** primary document section 8.7 – **Freshness of Products and Materials.**

WP-4.4.4: Information sharing policy

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

[RQ-4.3.3.1] define an information sharing policy (internal / external)

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-7] Incident Response Plan (Foundation-7.2)

Information sharing is addressed in the **AVCDL** primary document section 3.2 – **Information Sharing**.

WP-4.4.5: Audit report

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

[RQ-4.3.5.1] an independent audit shall be performed (compliance with ISO 24089)

Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, the **AVCDL** is capable of supporting audit efforts as part of its **ISO/SAE 21434** compliance.

Project Level Software Update Requirements (5)

WP-5.4.1: Software update project plan

[RQ-5.3.1.1] develop a project plan

Note: This requirement is addressed in the organizational-level documentation.

[RQ-5.3.1.3] assign roles and responsibilities

Discussion

Although the **AVCDL** does not completely address this work product, as it applies to multiple groups across the organization, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

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

WP-5.4.2: Documentation of software update project

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

[RQ-5.3.1.2] manage and store documentation for each software update project

Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, the **AVCDL** is capable of supporting documentation management and storage efforts as part of its **ISO/SAE 21434** compliance.

WP-5.4.3: Requirement tailoring rationale

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

[RQ-5.3.2.2] rationale provided for tailoring

Discussion

Although the **AVCDL** does not directly address this work product, as it is an organization-level responsibility, it should be noted that the **AVCDL** can be considered as a tailoring of **ISO/SAE 21434**.

WP-5.4.4: Interoperability confirmation documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-5.3.3.1] ensure interoperability between development and deployment processes

Discussion

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

[Foundation-10]	Deployment Plan (Foundation-10.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

WP-5.4.5: Documentation of integrity preservation process

Note: This work product is addressed in the development group’s documentation.

[RQ-5.3.4.1] establish, implement and maintain a process to preserve the integrity of update materials during distribution (all possible forms)

Discussion

Although the **AVCDL** does not completely address this work product, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Release-2]	Archive Manifest (Release-2.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

Infrastructure for Software Update Engineering Design and Development (6)

WP-6.4.1: Cybersecurity risk management documentation

[RQ-6.3.1.1]	cybersecurity risk management of software update infrastructure

[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)

WP-6.4.2: Vehicle configuration information documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-6.3.2.1]	vehicle configuration information management infrastructure
[RQ-6.3.2.2]	vehicle configuration information integrity infrastructure
[RQ-6.3.2.3]	vehicle configuration information distribution infrastructure
[RQ-6.3.2.4]	software systems / components dependency identification infrastructure
[RQ-6.3.2.5]	software update package compatibility verification infrastructure

Discussion

Although the **AVCDL** does not completely address this work product, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-10]	Deployment Plan (Foundation-10.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

Additionally, the **AVCDL** provides elaboration documents which support this effort. **Manifest Generation** covers the provisioning / update package manifest creation.

WP-6.4.3: Software update campaign documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-6.3.3.1]	notification infrastructure
[RQ-6.3.3.2]	software update campaign results management infrastructure

WP-6.4.4: Software update package documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-6.3.4.1]	software update package creation / storage infrastructure
[RQ-6.3.4.2]	software update package target association infrastructure
[RQ-6.3.4.3]	software update campaign recipient identification infrastructure
[RQ-6.3.4.4]	software update package distribution infrastructure
[RQ-6.3.4.5]	vehicle resource capacity to ingest software update package determination infrastructure
[RQ-6.3.4.6]	software update package integrity infrastructure

Discussion

Although the **AVCDL** does not completely address this work product, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Release-2]	Archive Manifest (Release-2.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

Additionally, the **AVCDL** provides elaboration documents which support this effort. **Manifest Generation** covers the provisioning / update package manifest creation.

WP-6.4.5: Failure recovery documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-6.3.4.7]	software update failure recovery infrastructure

Software Update-capable Vehicles and Components Development (7)

WP-7.4.1: Risk management documentation

[RQ-7.3.1.1] management of software update process functional safety risk
[RQ-7.3.1.2] management of software update process safety risk due to misuse of software

Note: These requirements are addressed in the safety group's documentation.

[RQ-7.3.1.3] management of software update process cybersecurity risk

[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)

Discussion

Although cybersecurity is a source of risk, it is not itself a risk domain. A discussion of this is provided in the **AVCDL** primary document section 3.4.4 – **Risk**. Additional supporting material is provided in the **AVCDL** elaboration document, **Understanding Cybersecurity Risk Freshness in an AVCDL Context**. Finally, material in the **AVCDL** certification document, **AVCDL Phase Requirement Product UNECE WP.29 R155 Work Product Fulfillment**, section 7.2.2.2 **Risk Management**, supports this argument.

WP-7.4.2: Vehicle configuration information documentation

Note: This work product is addressed in the development group's documentation.

[RQ-7.3.2.1] process to extract a vehicle's configuration information
[RQ-7.3.2.2] process to maintain the integrity of a vehicle's configuration information
[RQ-7.3.2.3] process to identify components targeted by software update package

WP-7.4.3: Software update campaign documentation

Note: This work product is addressed in the development group's documentation.

[RQ-7.3.3.1] process to inform related parties
[RQ-7.3.3.2] process to obtain software update process go-ahead

WP-7.4.4: Software update package documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-7.3.4.1] process to distribute software update package
[RQ-7.3.4.2] process to perform software update
[RQ-7.3.4.3] process to determine if update conditions are met
[RQ-7.3.4.4] process to arbitrate simultaneous access requests to ensure safe vehicle state
[RQ-7.3.4.5] process to manage software update package download interruption
[RQ-7.3.4.6] process to verify integrity and authenticity of software update package
[RQ-7.3.4.7] process to maintain integrity of software update packages and their contents
[RQ-7.3.4.8] process to perform a compatibility check prior to activation
[RQ-7.3.4.9] process to ensure safe vehicle state throughout software update process
[RQ-7.3.4.10] process to ensure safe vehicle state if update fails

Discussion

Although the **AVCDL** does not completely address this work product, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-6] Release Integrity Plan (Foundation-6.1)
[Foundation-10] Deployment Plan (Foundation-10.1)
[Release-2] Archive Manifest (Release-2.1)
[Operation-4] Software Deployment Report (Operation-4.1)

Software Update Package Development (8)

WP-8.4.1: Documentation of update package contents and targets

[RQ-8.3.1.1] list of software update's targeted components
[RQ-8.3.1.2] SBOM

Note: These requirements are addressed in the development group's documentation.

Discussion

Although the **AVCDL** does not completely address these requirements, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Release-2] Archive Manifest (Release-2.1)

Additionally, the **AVCDL** provides elaboration documents which support this effort. **Software Bill of Materials Lifecycle**, covers the SBOM. **Manifest Generation** covers the provisioning / update package manifest creation.

[RQ-8.3.1.3] identification of compatibility with existing software and hardware
[RQ-8.3.1.4] identification of dependencies with existing software and hardware
[RQ-8.3.1.5] identification of necessary in-vehicle resources and conditions for software update
[RQ-8.3.1.6] identification of software update distribution methods

Note: These requirements are addressed in the development group's documentation.

[RQ-8.3.1.7] identification of necessary cybersecurity actions

[Foundation-6] Release Integrity Plan (Foundation-6.1)
[Foundation-10] Deployment Plan (Foundation-10.1)
[Operation-4] Software Deployment Report (Operation-4.1)

[RQ-8.3.1.8] identification of necessary user / technician actions

Note: This requirement is addressed in the development group's documentation.

WP-8.4.2: Assembly of software update package

[RQ-8.3.2.1] process to create software update package

Note: This requirement is addressed in the development group's documentation.

Although the **AVCDL** does not completely address this requirement, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Release-2]	Archive Manifest (Release-2.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

[RQ-8.3.2.2] process to ensure only specified software is included in update package
[RQ-8.3.2.3] update package shall have a unique identifier

Note: These requirements are addressed in the development group's documentation.

WP-8.4.3: Verification and validation documentation

[RQ-8.3.3.1] verification and validation shall be performed before release

Note: This requirement is addressed in the development group’s documentation.

Discussion

Although the **AVCDL** does not completely address this requirement, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[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)
[Verification-4]	Verification Phase Gate (Verification-4.1)
[Release-1]	Final Security Review Report (Release-1.1)
[Release-3]	Final Phase Gate (Release-3.1)

[RQ-8.3.3.2] evaluation of software update’s compatibility with existing hardware / software
[RQ-8.3.3.3] validation of software update’s dependencies shall be performed
[RQ-8.3.3.4] consideration of software update deployment resource requirements
[RQ-8.3.3.5] implications of software update deployment failure
[RQ-8.3.3.6] verification and validation of software update’s exact scope

Note: These requirements are addressed in the development group’s documentation.

[RQ-8.3.3.7] verification and validation of software update’s cybersecurity actions

[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)
[Verification-4]	Verification Phase Gate (Verification-4.1)
[Release-1]	Final Security Review Report (Release-1.1)
[Release-3]	Final Phase Gate (Release-3.1)

[RQ-8.3.3.8] verification and validation of software update’s user / technician actions

Note: This requirement is addressed in the development group’s documentation.

WP-8.4.4: Release approval documentation

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

[RQ-8.3.4.1]	software update package release approval contingent upon successful verification and validation

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.

[Verification-4]	Verification Phase Gate (Verification-4.1)
[Release-3]	Release Phase Gate (Release-3.1)

Software Update Campaign Operations (9)

WP-9.4.1: Software update campaign plan documentation

Note: This requirement is addressed in the development group’s documentation.

[RQ-9.3.1.1] determine software update purpose

Note: This requirement is addressed in the development group’s documentation.

[RQ-9.3.1.2] assign roles and responsibilities

Note: This requirement is addressed in the development group’s documentation.

Discussion

Although the **AVCDL** does not completely address this requirement, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

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

[RQ-9.3.1.3] specify components for software update package

Note: This requirement is addressed in the development group’s documentation.

Discussion

Although the **AVCDL** does not completely address this requirement, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Release-2] Archive Manifest (Release-2.1)

[RQ-9.3.1.4] confirm specified package components have been approved for release

Note: This requirement is addressed in the development group’s documentation.

Discussion

Although the **AVCDL** does not completely address this requirement, as it is the responsibility of the development group, there are **AVCDL** phase requirements which support the organization in fulfilling this work product.

[Release-3] Release Phase Gate (Release-3.1)

[RQ-9.3.1.5] determine hardware and software versions in target to be replaced
[RQ-9.3.1.6] determine software update methods to be used
[RQ-9.3.1.7] create a process to identify update targets
[RQ-9.3.1.8] determined conditions and resources needed to perform software update
[RQ-9.3.1.9] system and software dependencies shall be determined
[RQ-9.3.1.10] specify software update failure corrective action

Note: These requirements are addressed in the development group’s documentation.

[RQ-9.3.1.11] cybersecurity measures for the software update campaign shall be determined

[Foundation-6]	Release Integrity Plan (Foundation-6.1)
[Foundation-10]	Deployment Plan (Foundation-10.1)
[Release-2]	Archive Manifest (Release-2.1)
[Operation-4]	Software Deployment Report (Operation-4.1)

[RQ-9.3.1.12] determined special equipment and training needed to perform software update
[RQ-9.3.1.13] the need for user confirmation of the software update shall be determined
[RQ-9.3.1.14] a process to determine related parties, appropriate information, and method of communication shall be created
[RQ-9.3.1.15] create software update plan

Note: These requirements are addressed in the development group’s documentation.

WP-9.4.2: Software update campaign execution documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-9.3.2.1] vehicle’s current configuration shall be obtained
[RQ-9.3.2.2] identification of specific vehicles matching target configuration
[RQ-9.3.2.3] completion of clause 8 requirements
[RQ-9.3.2.4] software update package shall be distributed
[RQ-9.3.2.5] ensure conditions for update are met
[RQ-9.3.2.6] software update process shall arbitrate simultaneous multiple access requests to prevent entry into an unsafe vehicle state
[RQ-9.3.2.7] software update package integrity and authenticity shall be verified before installation
[RQ-9.3.2.8] software update compatibility satisfaction shall be verified before installation
[RQ-9.3.2.9] communicate update availability to vehicle users
[RQ-9.3.2.10] vehicle user should be informed of the update’s availability before attempting an update
[RQ-9.3.2.11] user confirmation of update commencement should be obtained
[RQ-9.3.2.12] software updates requiring user actions shall be communicated to the user
[RQ-9.3.2.13] qualified personnel perform the update using appropriate equipment
[RQ-9.3.2.14] in the case of update failure, corrective action will be taken
[RQ-9.3.2.15] software update progress status should be obtained
[RQ-9.3.2.16] results of software update shall be appropriately reported in a timely manner
[RQ-9.3.2.17] communicate software update information and changes to related parties

WP-9.4.3: Software update campaign completion documentation

Note: This work product is addressed in the development group’s documentation.

[RQ-9.3.3.1] manage and store records of software update campaign
[RQ-9.3.3.2] communicate end of update campaign to vehicle user and related parties