| Document Title | Requirements on Vehicle Update and Configuration Management |
|---|---|
| **Document Owner** | AUTOSAR |
| **Document Responsibility** | AUTOSAR |
| **Document Identification No** | 1097 |

| | |
|---|---|
| **Document Status** | published |
| **Part of AUTOSAR Standard** | Adaptive Platform |
| **Part of Standard Release** | R24-11 |

| Document Change History | | | |
|---|---|---|---|
| **Date** | **Release** | **Changed by** | **Description** |
| 2024-11-27 | R24-11 | AUTOSAR Release Management | • Introduced standardized trace points requirements |
| 2023-11-23 | R23-11 | AUTOSAR Release Management | • Migration of document from standard RS Update And Configuration Management |

**Disclaimer**

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

# Contents

# 1    Scope of Document

This document specifies the requirements of the AUTOSAR Adaptive Platform on the Vehicle Update and Configuration Management (`V-UCM`). The motivation of `V-UCM` is to provide a standardized way to coordinate within a vehicle the installation, update and removal of software safely and securely.

# 2 Conventions to be used

## 2.1 Document Conventions

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([1]).

The verbal forms for the expression of obligation specified in [TPS_STDT_00053] shall be used to indicate requirements, see Standardization Template, chapter Support for Traceability ([1]).

## 2.2 Requirements Guidelines

No content, including subchapters.

### 2.2.1 Requirements quality

### 2.2.2 Requirements identification

### 2.2.3 Requirements status

# 3 Acronyms and abbreviations

The glossary below includes acronyms and abbreviations relevant to the `V-UCM` module that are not included in the AUTOSAR TR Glossary.

| Abbreviation / Acronym: | Description: |
|---|---|
| UCM | Update and Configuration Management |
| V-UCM | V-UCM is distributing packages and coordinating an update campaign in a vehicle |
| Backend | Backend is a server hosting Software Packages |

**Table 3.1: Acronyms and abbreviations used in the scope of this Document**

Below acronyms and abbreviations relevant for this document are included in the AUTOSAR TR Glossary. This is to avoid duplicate definition of the technical term. And to refer to the correct document.

| Term | Description: |
|---|---|
| Adaptive Application | see AUTOSAR TR Glossary |
| AUTOSAR Adaptive Platform | see AUTOSAR TR Glossary |
| Functional Cluster | see AUTOSAR TR Glossary |
| Service | see AUTOSAR TR Glossary |
| Electronic Control Unit | see AUTOSAR TR Glossary |
| Machine | see AUTOSAR TR Glossary |
| Manifest | see AUTOSAR TR Glossary |
| Software Package | see AUTOSAR TR Glossary |
| Software Cluster | see AUTOSAR TR Glossary |
| Vehicle Package | see AUTOSAR TR Glossary |
| Vehicle State Manager | see [2] AUTOSAR Glossary |

**Table 3.2: Reference to Technical Terms**

# 4 Requirements Specification

This chapter describes all requirements driving the work to define the AUTOSAR_AP_RS_VehicleUpdateAndConfigurationManagement.

## 4.1 Functional Overview

One of the declared goals of the `AUTOSAR Adaptive Platform` is the ability to flexibly update the software and its configuration through local ("tester-based") or remote ("over-the-air") updates. `V-UCM` provides services for updating the software and its configuration in a vehicle. `V-UCM` is coordinating an update campaign within the vehicle. Therefore this document includes requirements on the following functionalities:

- Interact with `Backend` to:
  - Identify `Software Clusters` that could be updated, installed or removed
  - Authenticate `Vehicle Package`
  - Confirm dependencies between `Software Clusters` within vehicle before starting campaign
  - Inform `Backend` of needed `Software Packages`, receives them and dispatch them to targeted `ECU`s

- Interact with `Vehicle State Manager`:
  - Inform which safety conditions that have to be applied according to `Vehicle Package`
  - Share the computed vehicle state to other Applications or `Functional Cluster`s involved in the update campaign

- Interact with Human Driver about update campaign:
  - Provides campaign state to trigger interaction with Human during update campaign
  - Get vehicle modification approval or consent from Human when configured in `Vehicle Package`

- Provide information of installed software in vehicle

- Provide information of update campaigns history

- Recovery in case of failure

## 4.2 Functional Requirements

### 4.2.1 Functional Cluster initialization

#### [RS_VUCM_00046] V-UCM initialization

*Upstream requirements:* RS_Main_00514

⌈

| Description: | V-UCM shall be initialized before starting to provide any services. |
|---|---|
| Rationale: | Calling APIs from uninitialized Functional Clusters that depend on prior initialization cannot be performed properly and may lead to undefined behavior. Therefore the API is only offered after internal initialization is completed. |
| Dependencies: | – |
| Use Case: | Startup of functional cluster |
| Supporting Material: | – |

⌋

### 4.2.2 V-UCM

#### [RS_VUCM_00038] V-UCM shall interact with driver
*Status:* DRAFT
*Upstream requirements:* RS_Main_00011

⌈

| Description: | V-UCM shall notify the driver intended actions of the campaign and act according to the driver's feedback |
|---|---|
| Rationale: | In order to make sure a vehicle update is performed in a state where the vehicle can safely perform the update if required, driver interaction, acknowledgment and action are needed. |
| Dependencies: | – |
| Use Case: | Update of safety critical application in a vehicle |
| Supporting Material: | – |

⌋

**[RS_VUCM_00036] `V-UCM` shall use platform communication services for interacting with `UCM`s**

Status: DRAFT

Upstream requirements: RS_Main_00011, RS_Main_00501, RS_Main_00503

⌈

| Description: | `V-UCM` shall know all `UCM`s reachable in Vehicle. |
|---|---|
| Rationale: | In order for `V-UCM` to distribute received `Software Packages`, it needs to discover the other `UCM`s that could perform any modifications within the vehicle. |
| Dependencies: | – |
| Use Case: | Complete vehicle `Electronic Control Unit`s update |
| Supporting Material: | – |

⌋

### 4.2.3 Update coordination and safety

**[RS_VUCM_00043] `V-UCM` shall orchestrate a software update campaign according to the `Vehicle Package`'s `Manifest`**

Status: DRAFT

Upstream requirements: RS_Main_00011, RS_Main_00150, RS_Main_00650

⌈

| Description: | To control an update campaign, the `V-UCM` will get from the `Backend` the `Vehicle Package` as unique input. Thus, `V-UCM` shall be able to parse them and understand how it shall conduct the related update campaign operations. |
|---|---|
| Rationale: | `V-UCM` shall be instructed in which sequence and with what conditions an update shall be performed |
| Dependencies: | – |
| Use Case: | Vehicle update |
| Supporting Material: | – |

⌋

### [RS_VUCM_00035] V-UCM shall coordinate software update in a vehicle across multiple Electronic Control Units

Status: DRAFT

Upstream requirements: RS_Main_00011, RS_Main_00503, RS_SAF_10027

⌈

| Description: | V-UCM is responsible of coordinating the distribution and processing of Software Packages in several ECUs |
|---|---|
| Rationale: | There could be dependencies between Machines or ECUs that shall be resolved by a central entity in the vehicle and that require specific processing or activation ordering |
| Dependencies: | – |
| Use Case: | Complete vehicle Electronic Control Units update |
| Supporting Material: | – |

⌋

### [RS_VUCM_00037] V-UCM shall ensure it is safe to perform any modification to the vehicle

Status: DRAFT

Upstream requirements: RS_Main_00011, RS_SAF_10038

⌈

| Description: | V-UCM shall start any update, removal or install of Software Packages depending of safety requirements and kind of Software Package |
|---|---|
| Rationale: | Software Package can have big or no impact on vehicle safety |
| Dependencies: | – |
| Use Case: | Performing an update of autonomous driving features will require for instance to have vehicle standing still, closed doors, etc. but a simple service might not have to consider vehicle safety. |
| Supporting Material: | – |

⌋

### 4.2.4 Versions reporting

### [RS_VUCM_00033] V-UCM shall support reporting version information of a complete vehicle

Status: DRAFT

Upstream requirements: RS_Main_00150, RS_Main_00491, RS_Main_00503, RS_Main_00650

⌈

| Description: | The V-UCM shall provide functionality to retrieve version information describing the software installed in a complete vehicle. |
|---|---|
| Rationale: | AUTOSAR Adaptive Platform shall support keeping software up-to-date through vehicle's lifecycle. |
| Dependencies: | – |
| Use Case: | Retrieve version information of the installed software to determine which software needs to be installed, updated or removed. |
| Supporting Material: | – |

⌋

### 4.2.5 History, progress and status

### [RS_VUCM_00034] V-UCM shall record all V-UCM's action history

Status: DRAFT

Upstream requirements: RS_Main_00491, RS_Main_00650

⌈

| Description: | V-UCM shall keep history of campaign and aggregate all UCMs history. |
|---|---|
| Rationale: | Keeping history can be needed for Legal reasons or to help troubleshoot failing updates. |
| Dependencies: | – |
| Use Case: | Support could be proposed to vehicle driver if an update is failing. Also, failing updates can be critical information for an OEM willing to monitor release of an update. |
| Supporting Material: | – |

⌋

**[RS_VUCM_00042]** `V-UCM` **shall provide an interface to read the state of an update campaign**

   *Status:*                     DRAFT

   *Upstream requirements:*   RS_Main_00491, RS_Main_01008

⌈

| Description: | `V-UCM` shall inform `Backend` at what stage is the update campaign for instance during and OTA update. |
|---|---|
| Rationale: | If a vehicle update is failing, it is important to know which `UCM` and at what state any failure occurred. |
| Dependencies: | – |
| Use Case: | Vehicle update |
| Supporting Material: | – |

⌋

## 4.2.6   Validation

**[RS_VUCM_00039]** `V-UCM` **shall prevent processing of compromised** `Vehicle Packages`

   *Status:*                     DRAFT

   *Upstream requirements:*   RS_Main_00514, RS_Main_01008

⌈

| Description: | `V-UCM` shall verify `Vehicle Packages` integrity and authenticity using strong and state of the art cryptographic techniques |
|---|---|
| Rationale: | A `Vehicle Package` may be subject to attacks during an OTA transmission |
| Dependencies: | – |
| Use Case: | Authentication and consistency check of `Vehicle Package` prevents any changes to the Adaptive Platform from a malicious package. |
| Supporting Material: | – |

⌋

### 4.2.7 Standardization of Log and Trace Messages

### [RS_VUCM_00047] `UCM` shall support standardized trace points

*Status:* DRAFT

*Upstream requirements:* RS_Main_01026

⌈

| Description: | `V-UCM` shall support standardized trace points during the update campaign process. |
|---|---|
| Rationale: | Providing standardized trace points during update campaign provides information of the ongoing events during different phases of campaign like vehicle package transfer, software package transfer, package processing and campaign result. |
| Dependencies: | ara::log |
| Use Case: | Tracing of different phases of update campaign. |
| Supporting Material: | – |

⌋

## 4.3   Non-Functional Requirements

No content.

# 5 Requirements Tracing

The following table references the features specified in  [3] and links to the fulfillments of these.

| Requirement | Description | Satisfied by |
|---|---|---|
| **[RS_Main_00011]** | Mechanisms for Reliable Systems | [RS_VUCM_00035] [RS_VUCM_00036] [RS_VUCM_00037] [RS_VUCM_00038] [RS_VUCM_00043] |
| **[RS_Main_00150]** | AUTOSAR shall support the deployment and reallocation of AUTOSAR Application Software | [RS_VUCM_00033] [RS_VUCM_00043] |
| **[RS_Main_00491]** | Function Monitoring | [RS_VUCM_00033] [RS_VUCM_00034] [RS_VUCM_00042] |
| **[RS_Main_00501]** | AUTOSAR shall support redundancy concepts | [RS_VUCM_00036] |
| **[RS_Main_00503]** | AUTOSAR shall support change of communication and application software at runtime. | [RS_VUCM_00033] [RS_VUCM_00035] [RS_VUCM_00036] |
| **[RS_Main_00514]** | System Security Support | [RS_VUCM_00039] [RS_VUCM_00046] |
| **[RS_Main_00650]** | AUTOSAR shall support up - and download of data and software | [RS_VUCM_00033] [RS_VUCM_00034] [RS_VUCM_00043] |
| **[RS_Main_01008]** | AUTOSAR shall provide secure communication with off-board entities | [RS_VUCM_00039] [RS_VUCM_00042] |
| **[RS_Main_01026]** | AUTOSAR shall support tracing and profiling on the target and onboard | [RS_VUCM_00047] |
| **[RS_SAF_10027]** | AUTOSAR shall provide mechanisms to prevent the loss of a valid configuration. | [RS_VUCM_00035] |
| **[RS_SAF_10038]** | AUTOSAR shall provide mechanisms to support that the safety relevant software is only updated/upgraded in a state that cannot cause a hazardous situation. | [RS_VUCM_00037] |

**Table 5.1: Requirements Tracing**

# 6 References

[1] Standardization Template
AUTOSAR_FO_TPS_StandardizationTemplate

[2] Glossary
AUTOSAR_FO_TR_Glossary

[3] Main Requirements
AUTOSAR_FO_RS_Main

# A Appendix

No content.

# B  Change history of AUTOSAR traceable items

Please note that the lists in this chapter also include traceable items that have been removed from the specification in a later version. These items do not appear as hyperlinks in the document.

## B.1  Traceable item history of this document according to AUTOSAR Release R23-11

### B.1.1  Added Requirements in R23-11

| Number | Heading |
|---|---|
| [RS_VUCM_00033] | `V-UCM` shall support reporting version information of a complete vehicle |
| [RS_VUCM_00034] | `V-UCM` shall record all `V-UCM`'s action history |
| [RS_VUCM_00035] | `V-UCM` shall coordinate software update in a vehicle across multiple `Electronic Control Unit`s |
| [RS_VUCM_00036] | `V-UCM` shall use platform communication services for interacting with `UCM`s |
| [RS_VUCM_00037] | `V-UCM` shall ensure it is safe to perform any modification to the vehicle |
| [RS_VUCM_00038] | `V-UCM` shall interact with driver |
| [RS_VUCM_00039] | `V-UCM` shall prevent processing of compromised `Vehicle Packages` |
| [RS_VUCM_00042] | `V-UCM` shall provide an interface to read the state of an update campaign |
| [RS_VUCM_00043] | `V-UCM` shall orchestrate a software update campaign according to the `Vehicle Package`'s `Manifest` |
| [RS_VUCM_00046] | `V-UCM` initialization |

**Table B.1: Added Requirements in R23-11**

### B.1.2  Changed Requirements in R23-11

### B.1.3  Deleted Requirements in R23-11

## B.2 Traceable item history of this document according to AUTOSAR Release R24-11

### B.2.1 Added Requirements in R24-11

| Number | Heading |
|---|---|
| [RS_VUCM_00047] | UCM shall support standardized trace points |

**Table B.2: Added Requirements in R24-11**

### B.2.2 Changed Requirements in R24-11

### B.2.3 Deleted Requirements in R24-11