Document Title	Requirements on Update and Configuration Management
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	887

Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R20-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2020-11-30	R20-11	AUTOSAR Release Management	• Added traceability to RS SAFETY document
2019-11-28	R19-11	AUTOSAR Release Management	• Added UCM Master concept requirements • Changed Document Status from Final to published
2019-03-29	19-03	AUTOSAR Release Management	• Spelling fixes • Minor explanation improvements
2018-10-31	18-10	AUTOSAR Release Management	• Requirements on Operating System updates • Requirement on Security • Requirement on History
2017-03-29	18-03	AUTOSAR Release Management	• Requirements on Software Updates • Requirements on Data Transfer • Requirements on Version Reporting • Requirements on Validation
2017-10-27	17-10	AUTOSAR Release Management	• Initial release

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.

Table of Contents

1 Scope of Document

This document specifies requirements of the AUTOSAR Adaptive Platform on the Update and Configuration Management (UCM). The motivation of UCM is to provide a standardized way to install, update and uninstall software on the adaptive platform safely and securely.

2 Conventions to be used

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template TPS-StandardizationTemplate, chapter Support for Traceability.

The verbal forms for the expression of obligation specified in [TPS_STDT_-00053] shall be used to indicate requirements, see Standardization Template TPS-StandardizationTemplate, chapter Support for Traceability.

3 Acronyms and abbreviations

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

Abbreviation / Acronym:	Description:
UCM	Update and Configuration Management
UCM Master	UCM Master is distributing packages and coordinating an update campaign in a vehicle
Backend	Backend is a server hosting Software Packages
Platform Health Manager	The Platform Health Manager functional cluster performs health monitoring on the AUTOSAR Adaptive Platform

Table 3.1: Acronyms and Abbreviations

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

Table 3.2: Reference to Technical Terms

4 Constraints and assumptions

This chapter lists known limitations of UCM in terms of unimplemented requirements. The intent is to provide an indication how the AUTOSAR Adaptive Platform will evolve in future releases.

The functionality described above is subject to modification and will be considered for inclusion in a future release of this document.

5 Requirements Specification

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

5.1 Functional Overview

One of the declared goals of AUTOSAR Adaptive Platform is the ability to flexibly update the software and its configuration through local ("tester-based") or remote ("over-the-air") updates. UCM provides services for updating the software and its configuration running on AUTOSAR Adaptive Platform. UCM is responsible for updates of Adaptive Applications and changes to the AUTOSAR Adaptive Platform itself, including all functional clusters and the underlying OS. Therefore this document includes requirements on the following functionalities:

- Installation of new software:

    - Install software

    - Install persistent data for the software

- Update of already installed software:

    - Update software

    - Update persistent data for the software

- Uninstallation of installed software:

    - Remove software

    - Remove data created by the software

- Providing information of installed software:

    - Names of installed software

    - Versions of installed software

- Security and safety of the update process

    - Authenticity and integrity validation

    - Software dependency check

    - Recovery of software after failure during update process

5.2 Functional Requirements

5.2.1 Versions reporting

[RS_UCM_00002] UCM shall support reporting version information for an AUTOSAR Adaptive Platform ⌈

Type:	valid
Description:	The UCM shall provide functionality to retrieve version information describing the software installed on AUTOSAR Adaptive Platform.
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:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00010] UCM shall support reporting of Software Packages downloaded for AUTOSAR Adaptive Platform ⌈

Type:	valid
Description:	The UCM shall provide functionality to retrieve information describing the software downloaded, but not activated on AUTOSAR Adaptive Platform
Rationale:	AUTOSAR Adaptive Platform shall support downloading data and continuing it after re-establishing a lost connection.
Dependencies:	–
Use Case:	Retrieve list of downloaded packages to know which data still needs to be downloaded and which has been already downloaded and can now be installed.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00011] UCM shall support reporting software versions which have been installed and will be activated when new versions are activated ⌈

Type:	valid
Description:	After processing one or several Software Packages, UCM shall support reporting changes that are intended to be introduced to software configuration.

▽

△

Rationale:	AUTOSAR Adaptive Platform shall support retrieving information which changes shall be activated when update sequence goes through activation phase.
Dependencies:	–
Use Case:	Retrieve list of installed software in order to check that all intended software have been installed and are ready for activation.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

[RS_UCM_00033]{DRAFT} UCM Master shall support reporting version information of a complete vehicle ⌈

Type:	draft
Description:	The UCM Master 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:	–

⌋(*RS_Main_00150*, *RS_Main_00491*, *RS_Main_00503*, *RS_Main_00650*)

5.2.2 Data management

[RS_UCM_00013] UCM shall check that it has enough resources to receive, process and store the Software Package and associated data ⌈

Type:	valid
Description:	UCM shall assure that it has enough resources to receive, process and store the Software Package and associated data. Resources may be for example memory, CPU time or network sockets. The resource check only covers the installation process. It is the responsibility of the integrator creating the Software Package to ensure enough resources for actual execution are available on the AUTOSAR Adaptive Platform (e.g. RAM, CPU time).
Rationale:	AUTOSAR Adaptive Platform shall protect itself from resource starvation.
Dependencies:	–

▽

△

Use Case:	Deny further transfers if no more resources for additional clients are available.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

[RS_UCM_00014]{DRAFT} **UCM shall check that correct amount of data has been transferred for the `Software Package`** ⌈

Type:	draft
Description:	UCM shall verify if the size of the received data is the same as the allocated amount stated in the download request in order to ensure the download was successful
Rationale:	UCM shall make sure complete `Software Package` was transferred.
Dependencies:	[RS_UCM_00013]
Use Case:	UCM shall assure that same amount of data has been transferred as was reserved in the downloaded request.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

[RS_UCM_00015]{DRAFT} **UCM shall remove all unneeded data after `Software Package` processing has finished** ⌈

Type:	draft
Description:	UCM shall remove all unneeded data such as logs, possible backups after `Software Package` processing has finished
Rationale:	UCM shall make sure all unneeded resources are freed after `Software Package` processing has finished.
Dependencies:	–
Use Case:	At the end of update process UCM shall remove log files, stored backups for `Software Package` and other temporary items created during update process.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

5.2.3 Data transfer

[RS_UCM_00025] UCM shall support receiving of `Software Package` data ⌈

Type:	valid
Description:	UCM shall receive the Software Package from a Client
Rationale:	AUTOSAR Adaptive Platform shall support receiving updates using the ara::com service interface only. Therefore no local, e.g. file-based transfer shall be used.
Dependencies:	–
Use Case:	Receive Software Package(s) from a DSA(Diagnostic Service Application).
Supporting Material:	–

⌋(*RS_Main_00503*)

[RS_UCM_00019] UCM shall support simultaneous transfers multiple Software Packages ⌈

Type:	valid
Description:	UCM shall support simultaneous transfers of multiple Software Packages
Rationale:	AUTOSAR Adaptive Platform shall support multiple update sources. Therefore several clients shall be able to transfer Software Packages to UCM simultaneously.
Dependencies:	[RS_UCM_00025]
Use Case:	Receive Software Package(s) from a DSA(Diagnostic Service Application).
Supporting Material:	–

⌋(*RS_Main_00503*)

5.2.4 Software updates

[RS_UCM_00001]{DRAFT} UCM shall support installing new software on AUTOSAR Adaptive Platform ⌈

Type:	draft
Description:	The UCM shall provide functionality to install new software on the AUTOSAR Adaptive Platform.
Rationale:	AUTOSAR Adaptive Platform shall support keeping software up-to-date and to introduce new features through out vehicles life cycle.
Dependencies:	–

▽

△

Use Case:	Introduce new functionality with new Adaptive Application or replace old functionality by replacing old Adaptive Application with new Adaptive Application.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00028]{DRAFT} UCM shall support updating Functional Clusters ⌈

Type:	draft
Description:	The UCM shall provide functionality to update the AUTOSAR Adaptive Platform.
Rationale:	AUTOSAR Adaptive Platform shall support keeping the AUTOSAR Adaptive Platform up-to-date and to introduce fixes to the AUTOSAR Adaptive Platform software.
Dependencies:	–
Use Case:	Updating the AUTOSAR Adaptive Platform with latest features and fixes.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00029]{DRAFT} UCM shall support updating the underlying Operating System ⌈

Type:	draft
Description:	The UCM shall provide functionality to update the Operating System hosting the AUTOSAR Adaptive Platform.
Rationale:	AUTOSAR Adaptive Platform shall provide support for updating the entire vehicle software, including the Operating System under hosting the AUTOSAR Adaptive Platform, in order to enable updating Operating System with fixes and new features through out the life-cycle of the vehicle
Dependencies:	–
Use Case:	Over-the-air updates including Operating System updates.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00003]{DRAFT} UCM shall support updating installed software on Adaptive Platform ⌈

Type:	draft
Description:	UCM shall provide functionality to update already installed software.
Rationale:	AUTOSAR Adaptive Platform shall support keeping software up-to-date through vehicle's life cycle.
Dependencies:	–
Use Case:	Update an application to achieve updated or fixed functionality.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00020]{DRAFT} **UCM shall support cancellation of an update or install operation** ⌈

Type:	draft
Description:	UCM shall support cancellation of an update or install operation
Rationale:	AUTOSAR Adaptive Platform shall support cancel of an update on user request.
Dependencies:	–
Use Case:	User can request cancellation of an operation if the installation or update is unwanted.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00026] UCM shall process installation of new Software Packages, updates and removal of existing Software Packages sequentially ⌈

Type:	valid
Description:	UCM shall process installation of new software, updates and removal of Software Packages sequentially, only one Software Package can be processed in time.
Rationale:	AUTOSAR Adaptive Platform shall support safe installation of Software Packages, therefore it shall not be possible to apply several modifications to installed software simultaneously.
Dependencies:	–
Use Case:	Software Packages are transferred by multiple clients. One client starts installing, the other has to wait until installation is finished to install packages transferred by it.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00017]{DRAFT} **UCM shall support installing and updating the persistent data storage for an Adaptive Application** ⌈

Type:	draft
Description:	The UCM shall process the persistent data in the Software Package so that it is available through Persistency
Rationale:	To support changing the Adaptive Application configurations.
Dependencies:	–
Use Case:	Install a Software Package to change the configuration for an Adaptive Application
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00004]{DRAFT} **UCM shall support uninstalling software on AUTOSAR Adaptive Platform** ⌈

Type:	draft
Description:	The UCM shall provide functionality to uninstall already installed software.
Rationale:	AUTOSAR Adaptive Platform shall support removing unwanted, outdated or malfunctioning software.
Dependencies:	–
Use Case:	Uninstall an application which will be replaced with other installed application or which is not needed anymore.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00005]{DRAFT} **UCM shall make sure that persistent data owned by uninstalled software is deleted** ⌈

Type:	draft
Description:	The UCM shall make sure that also persistent data is deleted with uninstalled software.
Rationale:	Make sure the uninstall process does not leave unused data.
Dependencies:	–
Use Case:	Make sure install and uninstall cycle do not leave unused data and does not cause memory issues.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00021]{DRAFT} **UCM shall support atomic activation of installed or updated Software Clusters** ⌈

Type:	draft
Description:	`UCM` shall support atomic activation of installed or updated `Software Clusters`
Rationale:	`UCM` shall apply the modifications to NVM in an inactive memory area and atomically switch when the modifications are finished.
Dependencies:	–
Use Case:	Install or update `Software Clusters`
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

[RS_UCM_00008]{DRAFT} **`UCM` shall support a recovery mechanism in case of failed update process** ⌈

Type:	draft
Description:	`UCM` shall assure that, in case of failed update process, the system will recover to the state it was before the update process started.
Rationale:	A failed update shall not result in a loss of desired functionality of the `AUTOSAR Adaptive Platform`.
Dependencies:	[RS_UCM_00021]
Use Case:	After a failed remote update the `AUTOSAR Adaptive Platform` recovers to the previous system state.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*, *RS_Main_00011*, *RS_SAF_21701*, *RS_SAF_-21704*)

[RS_UCM_00018] `UCM` shall announce when an application has been installed, updated or uninstalled ⌈

Type:	valid
Description:	`UCM` shall make information available for other Functional Clusters that software configuration has changed
Rationale:	Several Functional Clusters need to be constantly aware of current software features or configurations have been changed
Use Case:	`UCM` shall provide information of installed or updated application for Functional Clusters which subscribed to this information. E.g. Execution Manager to manage start of the application or for Health Manager to monitor the functionality of the application.
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

[RS_UCM_00027]{DRAFT} **UCM shall be able to safely recover from unexpected interruption.** ⌈

Type:	draft
Description:	At startup, UCM shall be able to identify if some action was interrupted and exited in an uncontrolled way and needs to be reverted or finished to return the software into the previous state
Rationale:	UCM shall make sure that software should not be started up into inconsistent and not updatable state
Use Case:	After unexpected reset or crash UCM shall identify that there was an interruption while an action was on going and UCM shall handle this by reverting or by finishing the unfinished action.
Dependencies:	–
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503, RS_SAF_21701, RS_SAF_21703)*

[RS_UCM_00031]{DRAFT} **UCM shall prevent installation of arbitrary previous version of an Adaptive Application or the Adaptive Platform** ⌈

Type:	draft
Description:	UCM shall check that the version of the provided Software Package is not older, than the one that has been installed previously and prevent any attempt to install it.
Rationale:	UCM shall prevent installation of a version containing vulnerabilities which would allow security exploitation.
Use Case:	An attacker could explore security vulnerabilities in the older version to hack the AUTOSAR Adaptive Platform.
Dependencies:	–
Supporting Material:	–

⌋*(RS_Main_00150)*

5.2.5 Logging, progress and status

[RS_UCM_00022]{DRAFT} **UCM shall support logging of the update or installation process** ⌈

Type:	draft
Description:	UCM shall support logging of the update or installation process
Rationale:	UCM shall support the logging of update or installation process to enable debugging of a failed update or installation
Dependencies:	–
Use Case:	After a failed remote or local update the user accesses log information.
Supporting Material:	–

⌋*(RS_Main_00150)*

[RS_UCM_00023]{DRAFT} **UCM shall provide an interface to read progress of the update** ⌈

Type:	draft
Description:	UCM shall provide an interface to read progress of the update
Rationale:	Make the information available to user
Dependencies:	–
Use Case:	Provide progress information in order to indicate to the user of the off-board tester that ongoing update is alive and progressing.
Supporting Material:	During a UCM operation the user would like to have an idea of how long will it take to complete the operation and if an error occurs.

⌋*(RS_Main_00150)*

[RS_UCM_00024]{DRAFT} **UCM shall provide an interface to read the state of UCM** ⌈

Type:	draft
Description:	UCM shall provide an interface to read the status of UCM
Rationale:	UCM shall provide its state to clients which can then react on changing states.
Dependencies:	–
Use Case:	One client is installing packages, another client has to wait until the state allows the next operation.
Supporting Material:	–

⌋*(RS_Main_00503)*

[RS_UCM_00032]{DRAFT} **UCM shall provide an interface to return UCM's action history** ⌈

Type:	draft
Description:	UCM shall provide an interface to return UCM's action history.
Rationale:	UCM shall provide its action history to help AUTOSAR Adaptive Platform troubleshooting.
Dependencies:	–
Use Case:	In order to investigate the lifecycle of the Adaptive Platform an interface for extracting UCM's action history has to be provided.
Supporting Material:	–

⌋(*RS_Main_00150*)

[RS_UCM_00034]{DRAFT} **UCM Master shall record all UCM Master's action history** ⌈

Type:	draft
Description:	UCM Master shall keep history of campaign and aggregate all UCM subordinates 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_Main_00491, RS_Main_00650*)

[RS_UCM_00042]{DRAFT} **UCM Master shall provide an interface to read the state of an update campaign** ⌈

Type:	draft
Description:	UCM Master 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 subordinate and at what state any failure occurred.
Dependencies:	–
Use Case:	Vehicle update
Supporting Material:	–

⌋(*RS_Main_00491, RS_Main_01008*)

5.2.6 Validation

[RS_UCM_00006]{DRAFT} **UCM shall verify `Software Package` authenticity and integrity using strong cryptographic techniques** ⌈

Type:	draft
Description:	UCM shall only allow installation of authenticated Software Packages on the Adaptive Platform
Rationale:	AUTOSAR Adaptive Platform shall ensure that Software Packages are unmodified and come from trusted origins
Dependencies:	–
Use Case:	Protection of AUTOSAR Adaptive Platform from hacking attempts from untrusted origin.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00012]{DRAFT} **UCM shall check the consistency of transferred `Software Package`** ⌈

Type:	draft
Description:	UCM shall check the consistency of the received Software Package.
Rationale:	AUTOSAR Adaptive Platform shall make sure that the Software Package can be installed safely.
Dependencies:	–
Use Case:	To detect possible errors which might have occurred during creation of the Software Package, UCM shall check that provided Software Package meta-data and content match.
Supporting Material:	–

⌋*(RS_Main_00150, RS_Main_00503)*

[RS_UCM_00007]{DRAFT} **UCM shall check that software dependencies are fulfilled** ⌈

Type:	draft
Description:	UCM shall check dependencies configured for a Software Package.
Rationale:	AUTOSAR Adaptive Platform shall make sure that the dependencies of the considered package are fulfilled.
Dependencies:	–
Use Case:	Check that installed software is able to run with all needed dependencies available on AUTOSAR Adaptive Platform.

▽

△

Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

[RS_UCM_00030]{DRAFT} **UCM shall be able to verify the updated software during activation** ⌈

Type:	draft
Description:	UCM shall require the updated software to be executed and verified before declaring that SW was successfully activated.
Rationale:	UCM shall declare activation to be successful only after it detects that Execution Manager can execute the software successfully.
Dependencies:	–
Use Case:	Ensuring that safety-critical application can be executed and thus monitored by the Platform Health Manager.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*, *RS_SAF_21702*)

[RS_UCM_00039]{DRAFT} **UCM Master shall prevent processing of compromised Vehicle Packages** ⌈

Type:	draft
Description:	UCM Master 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:	–

⌋(*RS_Main_00514*, *RS_Main_01008*)

5.2.7 UCM Master

[RS_UCM_00035]{DRAFT} **UCM Master shall coordinate software update in a vehicle across multiple Electronic Control Units** ⌈

Type:	draft
Description:	UCM Master 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_Main_00011, RS_Main_00503, RS_SAF_21703)

[RS_UCM_00036]{DRAFT} **UCM Master shall use platform communication services for interacting with UCM subordinates** ⌈

Type:	draft
Description:	UCM Master shall know all UCMs reachable in Vehicle.
Rationale:	In order for UCM Master to distribute received Software Packages, it needs to discover the other UCMs that could perform any modifications within the vehicle.
Dependencies:	–
Use Case:	Complete vehicle Electronic Control Units update
Supporting Material:	–

⌋(RS_Main_00011, RS_Main_00501, RS_Main_00503)

[RS_UCM_00037]{DRAFT} **UCM Master shall ensure it is safe to perform any modification to the vehicle** ⌈

Type:	draft
Description:	UCM Master 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:	–

⌋(RS_Main_00011, RS_SAF_21701, RS_SAF_21703)

[RS_UCM_00038]{DRAFT} **UCM Master shall interact with driver** ⌈

Type:	draft
Description:	UCM Master 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, acknowledgement and action are needed.
Dependencies:	–
Use Case:	Update of safety critical application in a vehicle
Supporting Material:	–

⌋*(RS_Main_00011)*

[RS_UCM_00043]{DRAFT} **UCM Master shall orchestrate a software update campaign according to the Vehicle Package's Manifest** ⌈

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

⌋*(RS_Main_00011, RS_Main_00150, RS_Main_00650)*

6 Requirements Tracing

The following table references the features specified in [1] and links to the fulfillments of these.

Requirement	Description	Satisfied by
[RS_Main_00011]	AUTOSAR shall support the development of reliable systems	[RS_UCM_00008] [RS_UCM_00035] [RS_UCM_00036] [RS_UCM_00037] [RS_UCM_00038] [RS_UCM_00043]
[RS_Main_00150]	AUTOSAR shall support the deployment and reallocation of AUTOSAR Application Software	[RS_UCM_00001] [RS_UCM_00002] [RS_UCM_00003] [RS_UCM_00004] [RS_UCM_00005] [RS_UCM_00006] [RS_UCM_00007] [RS_UCM_00008] [RS_UCM_00010] [RS_UCM_00011] [RS_UCM_00012] [RS_UCM_00013] [RS_UCM_00014] [RS_UCM_00015] [RS_UCM_00017] [RS_UCM_00018] [RS_UCM_00020] [RS_UCM_00021] [RS_UCM_00022] [RS_UCM_00023] [RS_UCM_00026] [RS_UCM_00027] [RS_UCM_00028] [RS_UCM_00029] [RS_UCM_00030] [RS_UCM_00031] [RS_UCM_00032] [RS_UCM_00033] [RS_UCM_00043]
[RS_Main_00491]	AUTOSAR shall provide means for logging	[RS_UCM_00033] [RS_UCM_00034] [RS_UCM_00042]
[RS_Main_00501]	AUTOSAR shall support redundancy concepts	[RS_UCM_00036]

[RS_Main_00503]	AUTOSAR shall support change of communication and application software at runtime.	[RS_UCM_00001] [RS_UCM_00002] [RS_UCM_00003] [RS_UCM_00004] [RS_UCM_00005] [RS_UCM_00006] [RS_UCM_00007] [RS_UCM_00008] [RS_UCM_00010] [RS_UCM_00011] [RS_UCM_00012] [RS_UCM_00013] [RS_UCM_00014] [RS_UCM_00015] [RS_UCM_00017] [RS_UCM_00018] [RS_UCM_00019] [RS_UCM_00020] [RS_UCM_00021] [RS_UCM_00024] [RS_UCM_00025] [RS_UCM_00026] [RS_UCM_00027] [RS_UCM_00028] [RS_UCM_00029] [RS_UCM_00030] [RS_UCM_00033] [RS_UCM_00035] [RS_UCM_00036]
[RS_Main_00514]	AUTOSAR shall support the development of secure systems	[RS_UCM_00039]
[RS_Main_00650]	AUTOSAR shall support up - and download of data and software	[RS_UCM_00033] [RS_UCM_00034] [RS_UCM_00043]
[RS_Main_01008]	AUTOSAR shall provide secure communication with off-board entities	[RS_UCM_00039] [RS_UCM_00042]
[RS_SAF_21701]	Update and Configuration Management (UCM) shall orchestrate the recovery to a safe operating mode in case of failed update process of a safety relevant software.	[RS_UCM_00008] [RS_UCM_00027] [RS_UCM_00037]
[RS_SAF_21702]	In case of software update/install of a safety relevant software, Update and Configuration Management shall verify the update/installation by checking the integrity of the updated or newly installed software.	[RS_UCM_00030]
[RS_SAF_21703]	If the verification of the update/installation of a safety relevant software fails, Update and Configuration Management shall ensure that a transition from non-hazardous state to a potentially hazardous state is not made unless the safety feature is available.	[RS_UCM_00027] [RS_UCM_00035] [RS_UCM_00037]

[RS_SAF_21704]	Update and Configuration Management shall verify the integrity of the new configuration and ensure that a well known configuration can be used in case the verification fails.	[RS_UCM_00008]

Document ID 887: AUTOSAR_RS_UpdateAndConfigManagement

7 References

[1] Main Requirements
AUTOSAR_RS_Main