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

Document Status	Final
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	19-03

Document Change History

Date	Release	Changed by	Description
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

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 [1], 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 [1], 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 [2, AUTOSAR glossary].

Abbreviation / Acronym:	Description:
UCM	Update and Configuration Management
Platform Health Manager	The Platform Health Manager functional cluster performs health monitoring on the AUTOSAR Adaptive Platform

Below acronyms and abbreviations relevant for this document are included in the AUTOSAR Glossary [2]. This is to avoid duplicate definition of the technical term. And to refer to the correct document.

Term	Description
Adaptive Application	see [2] AUTOSAR Glossary
AUTOSAR Adaptive Platform	see [2] AUTOSAR Glossary
Functional Cluster	see [2] AUTOSAR Glossary
Service	see [2] AUTOSAR Glossary
Software Package	see [2] AUTOSAR Glossary

Table 3.1: 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 following requirements are described within this document but not otherwise considered in this release:

- [RS_UCM_00027]

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

5 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

6 Requirements Specification

6.1 Versions reporting

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

Type:	draft
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:	draft
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:	draft

▽

△

Description:	After processing one or several `Software Packages` `UCM` shall support reporting changes that are intended to be introduced to software configuration. Changes shall be identified with the software component name accompanied either with the updated version number or with information that software component has been removed.
Rationale:	`AUTOSAR Adaptive Platform` shall support retrieving information which software components will be updated 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 is ready for activation.
Supporting Material:	–

⌋(*RS_Main_00150*, *RS_Main_00503*)

6.2 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:	draft
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] `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] 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*)

6.2.1 Data transfer

[RS_UCM_00025] UCM shall support efficient streaming of Software Package data ⌈

Type:	draft
Description:	UCM shall support efficient streaming of Software Package data
Rationale:	AUTOSAR Adaptive Platform shall support updates originating from another AUTOSAR Adaptive Platform. 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:	draft
Description:	UCM shall support simultaneous transfers 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*)

6.3 Software updates

[RS_UCM_00001] 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] 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] 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] 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] 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:	draft
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] 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] 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] 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] UCM shall support atomic activation of installed or updated packages ⌈

Type:	draft
Description:	UCM shall support atomic activation of installed or updated packages
Rationale:	UCM shall apply the modifications to NVM in an inactive memory area and atomically switch when the modifications are finished.
Dependencies:	–
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_UCM_00008] 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_UCM_00018] UCM shall announce when an application has been installed, updated or uninstalled ⌈

Type:	draft
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] 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 safe state
Rationale:	UCM shall make sure that software should not be started up into inconsistent and unsafe 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_UCM_00031] 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*)

6.4 Logging, progress and status

[RS_UCM_00022] 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] 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] 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] 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*)

6.5 Validation

[RS_UCM_00006] 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] 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] 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] 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*)

7 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]	AUTOSAR shall support the development of reliable systems	[RS_UCM_00008]
[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_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]

8 References

[1] Standardization Template
AUTOSAR_TPS_StandardizationTemplate

[2] Glossary
AUTOSAR_TR_Glossary

[3] Main Requirements
AUTOSAR_RS_Main