Document Title	Requirements of State Management
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	909

Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R22-11

Document Change History

Date	Release	Changed by	Description
2022-11-24	R22-11	AUTOSAR Release Management	• Added requirements regarding functional safety
2021-11-25	R21-11	AUTOSAR Release Management	• Requirements from RS-Safety considered
2020-11-30	R20-11	AUTOSAR Release Management	• No content changes
2019-11-28	R19-11	AUTOSAR Release Management	• No content changes • Changed Document Status from Final to published
2019-03-29	19-03	AUTOSAR Release Management	• Updated requirements due to reworked intended design
2018-10-31	18-10	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.

Contents

1 Scope of Document

This document specifies requirements on State Management. State Management implements interfaces of State Manager on the AUTOSAR Adaptive Platform, because State Management is highly project specific and therefor to be implemented by the project itself.

1.1 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 Acronyms and Abbreviations

The glossary below includes acronyms and abbreviations relevant to the State Management module that are not included in the AUTOSAR glossary[2].

Terms:	Description:
Process	A process is a loaded instance of an Executable to be executed on a Machine.
Execution Management	The element of the AUTOSAR Adaptive Platform responsible for the ordered startup and shutdown of the AUTOSAR Adaptive Platform and Adaptive Applications.
State Management	The element defining modes of operation for AUTOSAR Adaptive Platform. It allows flexible definition of functions which are active on the platform at any given time.
Function Group	A Function Group is a set of coherent Modelled Processes which need to be controlled consistently. Depending on the state of the Function Group, processes (related to the Modelled Processes) are started or terminated. Modelled Processes can belong to more than one Function Group State (but at exactly one Function Group). "MachineState" is a Function Group with a predefined name, which is mainly used to control Machine lifecycle and processes of platform level Applications. Other Function Groups are sort of general purpose tools used (for example) to control processes of user level Applications.
Function Group State	The element of State Management that characterizes the current status of a set of (functionally coherent) user-level Applications. The set of Function Groups and their Function Group States is machine specific and are configured in the Machine Manifest [3].
Machine State	The state of Function Group "MachineState" with some predefined states (Startup/Shutdown/Restart).
Network Management	A Functional Cluster within the Adaptive Platform Services. Part of Communication Management.

Table 2.1: Technical Terms

The following technical terms used throughout this document are defined in the official [2] AUTOSAR Glossary or [3] TPS Manifest Specification – they are repeated here for tracing purposes.

Term	Description
Adaptive Application	see [2] AUTOSAR Glossary
Application	see [2] AUTOSAR Glossary
AUTOSAR Adaptive Platform	see [2] AUTOSAR Glossary
Executable	see [2] AUTOSAR Glossary
Functional Cluster	see [2] AUTOSAR Glossary
Machine	see [2] AUTOSAR Glossary
Manifest	see [2] AUTOSAR Glossary
Adaptive Platform Foundation	see [2] AUTOSAR Glossary
Adaptive Platform Services	see [2] AUTOSAR Glossary

Table 2.2: Glossary-defined Technical Terms

3 Requirements Specification

This chapter describes all requirements driving the work to define the State Management.

3.1 Functional Overview

This document specifies the requirements regarding the realization of the State Management on Adaptive Platform. Only the interfaces and abstract functionality will be defined, because State Management is highly project specific.

EM, PHM and SM are the main safety relevant functional clusters of the AUTOSAR Adaptive Platform. Consequently, their development may require certain processes to be followed - as recommended in ISO26262 and, for instance, RS_SAF_21301 [4]. A safety argumentation for the AUTOSAR Adaptive Platform, describing functional safety measures and use-cases is provided through Explanation of Safety Overview [5].

3.2 Functional Requirements

3.2.1 State Management

[RS_SM_00001]{DRAFT} **State Management shall coordinate and control multiple sets of Applications.** ⌈

Description:	State Management shall allow to change the availability of Applications based on internal decision and/or external requests.
Rationale:	State Management shall coordinate and control one or multiple sets of Applications (Function Group State) and the platform (Machine State) itself so that the machine behaves as to fulfill the intended system design of a particular project.
Dependencies:	–
Use Case:	Provide interface to influence State Managements internal states.
Supporting Material:	–

⌋*(RS_Main_00050, RS_Main_00460)*

[RS_SM_00004]{DRAFT} **State Management shall provide standardized interfaces.** ⌈

Description:	State Management implementation shall be portable between different AUTOSAR Adaptive Platform compliant stacks. State Management shall only depend on the standardized interfaces when it interacts with other Functional Cluster. Therefor State Management shall provide interfaces over at least ara::com.
Rationale:	
Dependencies:	
Use Case:	Support error reaction of "Platform Health Management", configure Application availability based on "Diagnostic" and "Update and Configuration Management"
Supporting Material:	

⌋*(RS_Main_00060, RS_Main_01002, RS_Main_01005)*

[RS_SM_00005]{DRAFT} **State Management internal states.** ⌈

Description:	State Management shall support to change State Managements its internal states based on external inputs
Rationale:	State Management shall support to implement one or more state machines. State Management shall change its internal states in a project-specific manner based on requests from external inputs via its provided interfaces. State Management may reflect the changes of its internal states based on project-specific requirements via its provided interfaces.
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋*(RS_Main_00460)*

3.2.2 Support for Diagnostics

[RS_SM_00100]{DRAFT} **State Management shall support ECU reset** ⌈

Description:	State Management shall support to reset the ECU.
Rationale:	Diagnostic Application [6] shall support ECUReset according to ISO 14229-1 [7]. State Management shall handle and coordinate the requests from Diagnostic Application.
Dependencies:	–
Use Case:	–
Supporting Material:	–

⌋*(RS_Main_00260)*

3.2.3 Virtualization support / Hierarchical State Management

[RS_SM_00200]{DRAFT} **State Management shall provide an interface between State Management instances.** ⌈

Description:	State Management shall provide an interface between State Management instances used in a hierarchically manner.
Rationale:	In a virtualized/hierarchical environment several instances of State Management will be active. Instances with lower priority have to be controlled by instances with a higher priority
Dependencies:	
Use Case:	The components are possibly provided by different vendors, working on different microcontrollers or virtual machines. On each controller or (virtual) machine a separate instance of State Management might be used and it should be possible to operate these instances in a hierarchically manner.
Supporting Material:	

⌋*(RS_Main_00511)*

3.2.4 Calibration and variant support

[RS_SM_00300]{DRAFT} **State Management shall support variant handling based on calibration data.** ⌈

Description:	State Management shall evaluate calibration data. State Management should (or not) set Function Groups to specified Function Group State depending on read configuration data.
Rationale:	
Dependencies:	
Use Case:	For different car lines, countries or regions different Function Groups will be allowed to be started. State Management evaluates this information from calibration data to enable only the wanted Function Groups.
Supporting Material:	

⌋*(RS_Main_00261, RS_Main_00360)*

3.2.5 Dynamic communication paths

[RS_SM_00400]{DRAFT} **State Management shall establish communication paths dynamically.** ⌈

Description:	State Management shall be able to evaluate which communication channels are needed by Applications and therefor by their corresponding Function Group. Opening and closing of these channels shall be done by requesting them from Network Management.
Rationale:	
Dependencies:	
Use Case:	Applications as part of aFunction Group will have a need to use communication with other ones. Therefore State Management evaluates this information from configuration and requests Network Management to establish or shutdown the corresponding communication channel.
Supporting Material:	

⌋*(RS_Main_01002, RS_Main_01005)*

[RS_SM_00401]{DRAFT} **State Management shall control Applications depending on dynamic communication paths .** ⌈

Description:	State Management shall be able to evaluate which Applications and therefor their corresponding Function Group are needed by establishing communication channels. starting and stopping of Applications shall be done on request from Network Management.
Rationale:	
Dependencies:	
Use Case:	Applications as part of a Function Group will have a need to use communication with other ones. Therefore State Management evaluates this information from configuration and requests Execution Management to set a Function Group (and therefor the related Applications) to a dedicated state.
Supporting Material:	

⌋*(RS_Main_01002, RS_Main_01005)*

3.2.6 Recovery actions

[RS_SM_00601]{DRAFT} **State Management shall coordinate recovery actions.** ⌈

Description:	State Management shall coordinate recovery actions.
Rationale:	State Management is a central functional cluster to which Platform Health Management reports supervision failures and State Management decides which recovery action (e.g. functional group state change, notification to a safe application or even ECU reset) should be triggered.
Use Case:	PHM supervises a safety critical application. This application fails. PHM detects the issue and reports to SM. SM coordinates the error recovery actions.
AppliesTo:	AP
Dependencies:	SM, PHM
Supporting Material:	–

⌋*(RS_SAF_10005, RS_SAF_10006)*

3.3 Non-Functional Requirements

[RS_SM_00600]{DRAFT} **State Management shall be implemented at least according to the highest safety integrity level from any process that is managed by State Management.** ⌈

Description:	State Management shall be implemented at least according to the highest safety integrity level from any process that is managed by State Management.
Rationale:	SM manages state changes and recovery actions of all the processes and therefore needs to be developed and executed according to the same safety standards as the highest rated safety application managed by SM in the system
Use Case:	An ASIL C, B and QM Application is running on the adaptive Platform. SM shall manage the ASIL C, B and the QM application, therefore SM shall be implemented with an ASIL C.
AppliesTo:	AP
Dependencies:	SM
Supporting Material:	–

⌋*(RS_SAF_10001)*

4 Requirements Tracing

The following table references the features specified in [8] and links to the fulfillments of these.

Feature	Description	Satisfied by
[RS_Main_00050]	AUTOSAR shall provide an Execution Framework towards applications to implement concurrent application internal control flows	[RS_SM_00001]
[RS_Main_00060]	Standardized Application Communication Interface	[RS_SM_00004]
[RS_Main_00260]	Runtime Diagnostics Means	[RS_SM_00100]
[RS_Main_00261]	AUTOSAR shall provide means for calibration	[RS_SM_00300]
[RS_Main_00360]	Variant Management Support	[RS_SM_00300]
[RS_Main_00460]	AUTOSAR shall standardize methods to organize mode management on Application, ECU and System level	[RS_SM_00001] [RS_SM_00005]
[RS_Main_00511]	AUTOSAR shall support virtualization	[RS_SM_00200]
[RS_Main_01002]	AUTOSAR shall support service-oriented communication	[RS_SM_00004] [RS_SM_00400] [RS_SM_00401]
[RS_Main_01005]	AUTOSAR shall establish communication paths dynamically	[RS_SM_00004] [RS_SM_00400] [RS_SM_00401]
[RS_SAF_10001]	AUTOSAR shall provide mechanisms to support safe initialization of software components.	[RS_SM_00600]
[RS_SAF_10005]	AUTOSAR shall provide mechanisms to support safe shutdown and termination of applications, software components, basic software modules and services.	[RS_SM_00601]
[RS_SAF_10006]	AUTOSAR shall provide mechanisms to support safe transition of states in a basic software module, software component, application or service life cycle.	[RS_SM_00601]

5 References

[1] Standardization Template
AUTOSAR_TPS_StandardizationTemplate

[2] Glossary
AUTOSAR_TR_Glossary

[3] Specification of Manifest
AUTOSAR_TPS_ManifestSpecification

[4] Safety Requirements for AUTOSAR Adaptive Platform and AUTOSAR Classic Platform
AUTOSAR_RS_Safety

[5] Explanation of Safety Overview
AUTOSAR_EXP_SafetyOverview

[6] Specification of Diagnostics
AUTOSAR_SWS_Diagnostics

[7] Unified diagnostic services (UDS) – Part 1: Application layer (Release 2013-03)
http://www.iso.org

[8] Main Requirements
AUTOSAR_RS_Main

A History of Constraints and Specification Items

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

A.1 Constraint and Specification Item History of this document according to AUTOSAR Release R22-11

A.1.1 Added Traceables in R22-11

Number	Heading
[RS_SM_00600]	State Management shall be implemented at least according to the highest safety integrity level from any process that is managed by State Management.
[RS_SM_00601]	State Management shall coordinate recovery actions.

Table A.1: Added Traceables in R22-11

A.1.2 Changed Traceables in R22-11

Number	Heading
[RS_SM_00400]	State Management shall establish communication paths dynamically.
[RS_SM_00401]	State Management shall control Applications depending on dynamic communication paths .

Table A.2: Changed Traceables in R22-11

A.1.3 Deleted Traceables in R22-11

Number	Heading
[RS_SM_00101]	State Management shall support diagnostic reset cause

Table A.3: Deleted Traceables in R22-11

A.1.4 Added Constraints in R22-11

none

A.1.5 Changed Constraints in R22-11

none

A.1.6 Deleted Constraints in R22-11

none

A.2 Constraint and Specification Item History of this document according to AUTOSAR Release R21-11

A.2.1 Added Traceables "in R21-11"

Number	Heading
[RS_SM_00001]	State Management shall coordinate and control multiple sets of Applications.
[RS_SM_00004]	State Management shall provide standardized interfaces.
[RS_SM_00005]	State Management internal states.
[RS_SM_00100]	State Management shall support ECU reset
[RS_SM_00101]	State Management shall support diagnostic reset cause
[RS_SM_00200]	State Management shall provide an interface between State Management instances.
[RS_SM_00300]	State Management shall support variant handling based on calibration data.
[RS_SM_00400]	State Management shall establish communication paths dynamically.
[RS_SM_00401]	State Management shall control Applications depending on dynamic communication paths .

Table A.4: Added Traceables "in R21-11"

A.2.2 Changed Traceables "in R21-11"

none

A.2.3 Deleted Traceables "in R21-11"

none

A.2.4 Added Constraints "in R21-11"

none

A.2.5 Changed Constraints "in R21-11"

none

A.2.6 Deleted Constraints "in R21-11"

none

A.3 Constraint and Specification Item History of this document according to AUTOSAR Release R20-11

A.3.1 Added Traceables in R20-11

Number	Heading
[RS_SM_00001]	State Management shall coordinate and control multiple sets of Applications.
[RS_SM_00004]	State Management shall provide standardized interfaces.
[RS_SM_00005]	State Management internal states.
[RS_SM_00100]	State Management shall support ECU reset
[RS_SM_00101]	State Management shall support diagnostic reset cause
[RS_SM_00200]	State Management shall provide an interface between State Management instances.
[RS_SM_00300]	State Management shall support variant handling based on calibration data.
[RS_SM_00400]	State Management shall establish communication paths dynamically.
[RS_SM_00401]	State Management shall control Applications depending on dynamic communication paths .

Table A.5: Added Traceables in R20-11

A.3.2 Changed Traceables in R20-11

none

A.3.3 Deleted Traceables in R20-11

none

A.3.4 Added Constraints in R20-11

none

A.3.5 Changed Constraints in R20-11

none

A.3.6 Deleted Constraints in R20-11

none

A.4 Constraint and Specification Item History of this document according to AUTOSAR Release R19-11

A.4.1 Added Traceables in 19-11

none

A.4.2 Changed Traceables in 19-11

Number	Heading
[RS_SM_00004]	State Management shall provide standardized interfaces.
[RS_SM_00300]	State Management shall support variant handling based on calibration data.
[RS_SM_00400]	State Management shall establish communication paths dynamically.

Table A.6: Changed Traceables in 19-11

A.4.3 Deleted Traceables in 19-11

Number	Heading
[RS_SM_00500]	State Management shall support efficient resource usage.

Table A.7: Deleted Traceables in 19-11

A.4.4 Added Constraints in 19-11

none

A.4.5 Changed Constraints in 19-11

none

A.4.6 Deleted Constraints in 19-11

none

A.5 Constraint and Specification Item History of this document according to AUTOSAR Release R19-03

A.5.1 Added Traceables in 19-03

Number	Heading
[RS_SM_00004]	State Management shall provide standardized interfaces.
[RS_SM_00005]	State Management internal states.
[RS_SM_00401]	State Management shall control Applications depending on dynamic communication paths .

Table A.8: Added Traceables in 19-03

A.5.2 Changed Traceables in 19-03

Number	Heading
[RS_SM_00001]	State Management shall coordinate and control multiple sets of Applications.
[RS_SM_00200]	State Management shall provide an interface between State Management instances.
[RS_SM_00400]	State Management shall establish communication paths dynamically.

Table A.9: Changed Traceables in 19-03

A.5.3 Deleted Traceables in 19-03

Number	Heading
[RS_SM_00002]	State Management shall support Component State change requests.
[RS_SM_00201]	State Management shall provide the interface over ara::com.

Table A.10: Deleted Traceables in 19-03

A.5.4 Added Constraints in 19-03

none

A.5.5 Changed Constraints in 19-03

none

A.5.6 Deleted Constraints in 19-03

none