Document Title	Safety Requirements for AUTOSAR Adaptive Platform and AUTOSAR Classic Platform
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	986

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R21-11

Document Change History

Date	Release	Changed by	Description
2021-11-25	R21-11	AUTOSAR Release Management	• add classic platform requirements chapter • add requirements for CP WDG, CP OS, CP E2E • rework top level safety requirements structure • add TLSR RS_SAF_00006 • update PHM, EM, SM requirements • update functional safety requirements to be AUTOSAR Platform and Foundation
2020-11-30	R20-11	AUTOSAR Release Management	• Initial release • Functional safety requirements for the AUTOSAR Adaptive Platform • Technical safety requirements for PHM, EM, SM, OS, PER, CM and UCM

Disclaimer

Table of Contents

1 Scope of Document

This document specifies safety requirements on the AUTOSAR Platform, the AUTOSAR Adaptive Platform in particular. This document elaborates the high level safety requirements written in RS_Main. It makes use of the intended functionality described in EXP_PlatformDesign document. The functional safety requirements are derived from the safety goals and hazards mentioned in EXP_SafetyOverview. Technical safety requirements towards the AUTOSAR functional cluster and safety relevant applications are derived from the functional safety requirements.

The AUTOSAR Classic Platform is not in scope.

No ASIL Ratings

The AUTOSAR consortium, especially the AUTOSAR Adaptive Platform Working Groups are only providing an architecture definition, descriptions of the functional blocks and a *proof of concept* implementation, it is not possible to add an ASIL rating to any requirement in this scope as described in ISO26262[1].

2 How to Read This Document

This document contains functional safety requirements which are generic and do not mention specific solutions/components of AUTOSAR. The technical safety requirements are then derived from functional safety requirements, which mention the specific responsibilities of AUTOSAR components. Each requirement has its unique identifier starting with the prefix "RS_SAF_" (for "Safety Requirement").

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 ([2]).

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 ([2]).

2.2 Conventions used

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as follows.

Note that the requirement level of the document in which they are used modifies the force of these words.

- MUST: This word, or the adjective "LEGALLY REQUIRED", means that the definition is an absolute requirement of the specification due to legal issues.
- MUST NOT: This phrase, or the phrase "MUST NOT", means that the definition is an absolute prohibition of the specification due to legal issues.
- SHALL: This phrase, or the adjective "REQUIRED", means that the definition is an absolute requirement of the specification.
- SHALL NOT: This phrase means that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED", means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

An implementation, which does not include a particular option, SHALL be prepared to interoperate with another implementation, which does include the option, though perhaps with reduced functionality. In the same vein an implementation, which does include a particular option, SHALL be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides.)

2.2.1 Requirement Identifier Coding

The unique identifier for safety requirements shall consist of

- a document identifier

- an identifier to distinguish functional safety requirements and technical safety requirements
- an identifier to identify a target component (either a Functional Cluster in the AUTOSAR Adaptive Platform or a Basic Software Component in the AUTOSAR Classic Platform)
- a requirement number

The coding pattern used in this requirements specification is `RS_SAF_<Z><YY><XX>`, where

Z is a single digit number, describing whether the requirement is a

0 safety goal or top level safety requirement functional safety requirement, where

YY *is reserved*

XX is a double digit number

1 functional safety requirement for the AUTOSAR Adaptive Platform, where

YY *is reserved*

XX is a double digit number

2 technical safety requirement for the AUTOSAR Adaptive Platform, where

YY is a double digit number, describing whether the requirement addresses

00 *reserved*

11 Platform Health Management (PHM)

12 Execution Management (EM)

13 State Management (SM)

14 Operating System (OS)

15 Persistency (PER)

16 Communication Management (CM)

17 Update and Configuration Management (UCM)

and

XX is a double digit number

3-9 reserved for future use, e.g. technical safety requirement for the AUTOSAR Classic Platform

3 Acronyms and abbreviations

The glossary below includes acronyms and abbreviations relevant to RS_Safety that are not included in the AUTOSAR Glossary [3].

Abbreviation / Acronym:	Description:
PHM	Platform Health Management
EM	Execution Management
SM	State Management
OS	Operating System
PER	Persistency
CM	Communication Management
UCM	Update and Configuration Management
S2S	Signal to Service
SG	Safety Goal

Table 3.1: Acronyms and Abbreviations

4 Requirements Specification

This chapter contains top level safety requirements (safety goals) for AUTOSAR in 4.1. Functional safety requirements in 4.2 are derived from these safety goals. The sub-chapter 4.3 contains technical safety requirements which are derived from the functional safety requirements.

4.1 Top Level Safety Requirements and Safety Goals

[RS_SAF_00001]{DRAFT} **Safe Execution** ⌈

Description:	AUTOSAR shall provide supporting mechanisms to monitor the control flow and manage the execution order of multiple applications with mixed safety criticality.
Rationale:	To ensure freedom from interference with respect to timing [1] and data processing.
AppliesTo:	FO
Supporting Material:	ISO26262 [1]

⌋(*RS_Main_00010*, *RS_Main_00011*, *RS_Main_00012*, *RS_Main_00030*)

[RS_SAF_00002]{DRAFT} **Safe Configuration** ⌈

Description:	AUTOSAR shall provide mechanisms to support correct configuration during the entire driving cycle of the vehicle.
Rationale:	AUTOSAR needs to provide measures and mechanisms to keep the configuration consistent through out the whole driving cycle of the vehicle.
AppliesTo:	FO
Supporting Material:	ISO 26262 [1]

⌋(*RS_Main_00010*, *RS_Main_00011*, *RS_Main_00012*, *RS_Main_00030*)

[RS_SAF_00003]{DRAFT} **Safe Update or Safe Upgrade** ⌈

Description:	AUTOSAR shall provide mechanisms to support correct update and upgrade of multiple platform and non-platform applications with mixed criticality.
Rationale:	AUTOSAR supports updatability during the life cycle of the machine and therefore the platform is responsible to ensure that these updates are performed correctly and safe.
AppliesTo:	FO
Supporting Material:	ISO 26262 [1]

⌋(*RS_Main_00010*, *RS_Main_00011*, *RS_Main_00012*, *RS_Main_00030*, *RS_Main_-00150*)

[RS_SAF_00004]{DRAFT} **Safe Exchange of Information** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe exchange (transmission and reception) of information between safety critical applications.
Rationale:	In a vehicle several ECUs with several software components are interrelating with each other to fulfill a goal or functionality. AUTOSAR provides standardized interfaces and mechanisms to achieve safe communication between these components. Safe communication with elements outside of the vehicle is also in scope.
AppliesTo:	FO
Supporting Material:	ISO 26262 [1]

⌋(*RS_Main_00010*, *RS_Main_00011*, *RS_Main_00012*, *RS_Main_00030*)

[RS_SAF_00005]{DRAFT} **Detection of Data Corruption** ⌈

Description:	AUTOSAR shall provide mechanisms to detect faults and failures while processing data, communicating with other systems or system elements.

▽

△

Rationale:	Mechanisms to detect faults and failures are required to achieve higher safety ratings and increase product quality. A list of potential failures is described in EXP_SafetyOverview [4] and ISO 26262 [1]. Incorrect specification or configuration is a potential source of failure.
AppliesTo:	FO
Supporting Material:	ISO 26262 [1]

⌋(*RS_Main_00010*)

[RS_SAF_00006]{DRAFT} **Safe Storage** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe storage for applications.
Rationale:	Many applications need to store and retrieve data from persistent or volatile memory. If the Application is safety critical, data elements need to be identified correctly and the data itself shall be checked to ensure that it has not been altered.
AppliesTo:	FO
Supporting Material:	ISO 26262 [1]

⌋(*RS_Main_00010*)

4.2 Functional Safety Requirements

[RS_SAF_10001]{DRAFT} **AUTOSAR shall provide mechanisms to support safe initialization of software components.** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe initialization of software components.
Rationale:	Safe initialization of the underlying hardware and the AUTOSAR Adaptive Platform functional cluster and services and the application software is required to ensure intended functionality.
Use Case:	SUC-02
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00001*, *RS_SAF_00002*)

[RS_SAF_10002]{DRAFT} **AUTOSAR shall provide mechanisms to support safe verification mechanisms of platform basic software modules, functional-clusters, software components, applications, services and their respective configuration data.** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe verification mechanisms of platform basic software modules, functional-clusters, software components, applications, services and their respective configuration data.
Rationale:	Due to the random hardware failures in the memory unit the data integrity is required to be verified to ensure no loss of data has occurred over time during operation, stand-by or powered off and has not been tampered with. Note: Not with respect to cybersecurity.
Use Case:	SUC-02, SUC-06
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00002, RS_SAF_00003*)

[RS_SAF_10005]{DRAFT} **AUTOSAR shall provide mechanisms to support safe shutdown and termination of applications, software components, basic software modules and services.** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe shutdown and termination of applications, software components, basic software modules and services.
Rationale:	Before termination of applications and services and/or shut-down of the AUTOSAR Adaptive Platform or the whole ECU, the dependent applications have to be terminated properly in the right order to prevent conflicts or failures or unexpected behavior. Ensure safe degradation, fault evacuation and fault containment.
Use Case:	[SUC-01], [SUC-06]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00001, RS_SAF_00003*)

[RS_SAF_10006]{DRAFT} **AUTOSAR shall provide mechanisms to support safe transition of states in a basic software module, software component, application or service life cycle.** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe transition of states in a basic software module, software component, application or service life cycle.
Rationale:	AUTOSAR Adaptive Platform is responsible for managing and monitoring the internal states of the application.
Use Case:	[SUC-01], [SUC-06]
AppliesTo:	FO
Dependencies:	–

▽

△

Supporting Material:	–

⌋()

[RS_SAF_10008]{DRAFT} **AUTOSAR shall provide mechanisms to support safe resource management for the AUTOSAR Adaptive Platform functional-clusters, applications and services and AUTOSAR Classic Platform basic software modules and software components.** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe resource management for the AUTOSAR Adaptive Platform functional-clusters, applications and services and AUTOSAR Classic Platform basic software modules and software components.
Rationale:	The functional clusters, applications and services of the AUTOSAR Adaptive Platform shall be ensured with adequate resources and availability to that resource in the expected time with sufficient freedom from interference. No unexpected or unhandled exception shall prevent access or delay access to a required and properly managed and authorized resource. Resources are - among other - CPU, runtime, memory consumption, net bandwidth, peripherals (like ADC, DAC, Timer) . . .
Use Case:	[SUC-01]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00001*, *RS_SAF_00002*, *RS_SAF_00004*)

[RS_SAF_10014]{DRAFT} **AUTOSAR shall provide an interface to support safe communication for basic software module, software component, application or services.** ⌈

Description:	AUTOSAR shall provide an interface to support safe communication for basic software module, software component, application or services.
Rationale:	In a vehicle several ECUs with several software components are interrelating with each other to fulfill a goal or functionality. AUTOSAR Adaptive Platform provides standardized interfaces and mechanisms to achieve safe communication between these components. Safe communication with elements outside of the vehicle is also in scope.
Use Case:	[SUC-03], [SUC-04], [SUC-05]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00004*)

[RS_SAF_10027]{DRAFT} **AUTOSAR shall provide mechanisms to prevent the loss of a valid configuration.** ⌈

Description:	AUTOSAR shall provide mechanisms to prevent the loss of a valid configuration.
Rationale:	AUTOSAR Adaptive Platform should provide mechanisms to switch back to the latest working configuration
Use Case:	[SUC-02], [SUC-06]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋*(RS_SAF_00002)*

[RS_SAF_10028]{DRAFT} **AUTOSAR shall provide mechanisms to support dependable scheduling of AUTOSAR Adaptive Platform functional-clusters, applications and services and AUTOSAR Classic Platform basic software modules and software components.** ⌈

Description:	AUTOSAR shall provide mechanisms to support dependable scheduling of AUTOSAR Adaptive Platform functional-clusters, applications and services and AUTOSAR Classic Platform basic software modules and software components.
Rationale:	Dependable scheduling is required to ensure the proper time-allocation for all the available functional-clusters, applications and services.
Use Case:	[SUC-01]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋*(RS_SAF_00001, RS_SAF_00002)*

[RS_SAF_10030]{DRAFT} **AUTOSAR shall provide mechanisms to support safe program execution.** ⌈

Description:	AUTOSAR shall provide mechanisms to support safe program execution.
Rationale:	The AUTOSAR Adaptive Platform shall offer flow monitoring mechanisms to detect and ensure that the intended program flow of functional-clusters and services as well as for user-applications and user-services is not violated.
Use Case:	[SUC-01]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00001*)

[RS_SAF_10031]{DRAFT} **AUTOSAR shall provide mechanisms to detect program execution time violation** ⌈

Description:	AUTOSAR shall provide mechanisms to detect program execution time violation
Rationale:	All the timing constraints of the functional-clusters, applications and services need to be supervised and monitored.
Use Case:	[SUC-01], [AP-UC-06]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00001*)

[RS_SAF_10037]{DRAFT} **AUTOSAR shall provide mechanisms to prevent unintended alteration of data.** ⌈

Description:	AUTOSAR shall provide mechanisms to prevent unintended alteration of data.
Rationale:	Due to the random hardware failures in the memory unit the data integrity is required to be verified to ensure no alteration to data has occurred over time during operation, stand-by or powered off and has not been tampered with. To achieve freedom from interference, the access to data needs to be managed and protected. Note: Not with respect to cybersecurity.
Use Case:	[SUC-06]
AppliesTo:	FO
Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00002*, *RS_SAF_00003*, *RS_SAF_00004*)

[RS_SAF_10038]{DRAFT} **AUTOSAR shall provide mechanisms to support that the safety relevant software is only updated/upgraded in a state that cannot cause a hazardous situation.** ⌈

Description:	AUTOSAR shall provide mechanisms to support that the safety relevant software is only updated/upgraded in a state that cannot cause a hazardous situation.
Rationale:	The update of safety critical application should be done when the car is stationary and at a safe location e.g. a parking garage.
Use Case:	[SUC-02]
AppliesTo:	FO

▽

△

Dependencies:	–
Supporting Material:	–

⌋(*RS_SAF_00003*)

4.3 Technical Safety Requirements

4.3.1 AUTOSAR AdaptivePlatform

4.3.1.1 Functional Cluster: Platform Health Management (PHM)

[RS_SAF_21101]{DRAFT} **Platform Health Management shall be implemented at least according the highest safety integrity level from any process that is supported on the platform.** ⌈

Description:	Platform Health Management shall be implemented at least according the highest safety integrity level from any process that is supported on the platform.
Rationale:	Platform Health Management is responsible for ensuring part of the safe execution of safety relevant processes/applications, it should at least be developed with the highest ASIL as the process/application that is being executed.
Use Case:	An ASIL C, B and QM Application is running on the adaptive Platform. PHM shall supervise the ASIL C and B application, therefore PHM shall be implemented with an ASIL C
AppliesTo:	AP
Dependencies:	PHM
Supporting Material:	–

⌋(*RS_SAF_10002*, *RS_SAF_10030*, *RS_SAF_10031*)

[RS_SAF_21102]{DRAFT} **If supervision of State Management fails then Platform Health Management shall trigger a watchdog reset.** ⌈

Description:	If supervision of State Management fails then Platform Health Management shall trigger a watchdog reset.
Rationale:	Since State Management is a fundamental functional cluster of the Adaptive AUTOSAR, if it fails then Platform Health Management (which controls the watchdog) shall trigger a reset which is the only reasonable option
Use Case:	SM is managing a safety critical application. Supervision of SM fails and is detected by PHM. PHM shall trigger a watchdog reset.

▽

△

AppliesTo:	AP
Dependencies:	PHM, SM
Supporting Material:	–

⌋(*RS_SAF_10006*, *RS_SAF_10030*, *RS_SAF_10005*)

[RS_SAF_21103]{DRAFT} **If supervision of Execution Management fails then Platform Health Management shall trigger a watchdog reset.** ⌈

Description:	If supervision of Execution Management fails then Platform Health Management shall trigger a watchdog reset.
Rationale:	Since Execution Management is a fundamental functional cluster of the Adaptive AUTOSAR, if it fails then Platform Health Management (which controls the watchdog) shall trigger a reset which is the only reasonable option
Use Case:	EM is managing safety critical applications and supervision of EM fails and is detected by PHM. PHM shall trigger a watchdog reset.
AppliesTo:	AP
Dependencies:	PHM, EM
Supporting Material:	–

⌋(*RS_SAF_10006*, *RS_SAF_10030*, *RS_SAF_10005*)

[RS_SAF_21104]{DRAFT} **Platform Health Management shall monitor the aliveness of safety relevant applications and services.** ⌈

Description:	Platform Health Management shall monitor the execution frequency of safety relevant applications and services.
Rationale:	Alive Supervision is one of the mechanisms of Platform Health Management by which it monitors safety relevant processes/applications.
Use Case:	A safety critical application with alive supervision get stuck at some point in time during execution. PHM detects that the supervised application is not alive.
AppliesTo:	AP
Dependencies:	PHM
Supporting Material:	–

⌋(*RS_SAF_10031*)

[RS_SAF_21105]{DRAFT} **Platform Health Management shall monitor the control flow of safety relevant applications and services.** ⌈

Description:	Platform Health Management shall monitor the control flow of safety relevant applications and services.
Rationale:	Logical Supervision is one of the mechanisms of Platform Health Management by which it monitors safety relevant processes/applications.
Use Case:	A safety critical application is developed to follow a specific control flow and is suddenly not behaving as intended. PHM detects the control flow violation.
AppliesTo:	AP
Dependencies:	PHM
Supporting Material:	–

⌋(*RS_SAF_10005*, *RS_SAF_10006*, *RS_SAF_10030*)

[RS_SAF_21106]{DRAFT} **Platform Health Management shall monitor that the duration between the checkpoints of safety relevant applications and services are within the configured time limits.** ⌈

Description:	Platform Health Management shall monitor that the duration between the checkpoints of safety relevant applications and services are within the configured time limits.
Rationale:	Deadline Supervision is one of the mechanisms of Platform Health Management by which it monitors safety relevant processes/applications.
Use Case:	A safety critical application is developed to reach specific checkpoints in a defined time window and is suddenly not behaving as intended. PHM detects the violation.
AppliesTo:	AP
Dependencies:	PHM
Supporting Material:	–

⌋(*RS_SAF_10031*)

[RS_SAF_21107]{DRAFT} **Platform Health Management shall notify State Management in case an AUTOSAR Adaptive Platform functional cluster, application or service other than Execution Management and State Management fails.** ⌈

Description:	Platform Health Management shall notify State Management in case an AUTOSAR Adaptive Platform functional cluster, application or service other than Execution Management and State Management fails.
Rationale:	Since the recovery actions are coordinated in SM, the failures shall be reported to SM except if SM or EM themselves fail.
Use Case:	PHM supervises a safety critical application. This application fails. PHM detects the issue and reports to SM.
AppliesTo:	AP

▽

△

Dependencies:	PHM, SM
Supporting Material:	–

⌋(*RS_SAF_10005*, *RS_SAF_10006*)

4.3.1.2 Functional Cluster: Execution Management (EM)

[RS_SAF_21201]{DRAFT} **Execution Management shall be implemented at least according the highest safety integrity level from any process that is supported on the platform.** ⌈

Description:	Execution Management shall be implemented at least according the highest safety integrity level from any process that is supported on the platform.
Rationale:	EM manages process instantiation and termination 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 EM in the system
Use Case:	An ASIL C, B and QM Application is running on the adaptive Platform. EM shall execute the ASIL C, B and the QM application, therefore EM shall be implemented with an ASIL C.
AppliesTo:	AP
Dependencies:	EM
Supporting Material:	–

⌋(*RS_SAF_10001*)

[RS_SAF_21202]{DRAFT} **Execution Management shall support fully deterministic execution (time determinism and data determinism) so that higher ASIL levels can be achieved even when using parallel processing.** ⌈

Description:	Execution Management shall support fully deterministic execution (time determinism and data determinism) so that higher ASIL levels can be achieved even when using parallel processing.
Rationale:	According to ISO 26262-6 Table 3 one principle of software architectural design is restricted use of interrupts to achieve determinism, which is highly recommended to achieve ASIL D.
Use Case:	Two instances of the same application of the same ASIL can be executed for decomposition to reach the higher ASIL level (with some additional measure)
AppliesTo:	AP
Dependencies:	EM
Supporting Material:	–

⌋(*RS_SAF_10028*, *RS_SAF_10030*, *RS_SAF_10031*, *RS_SAF_10005*)

4.3.1.3 Functional Cluster: State Management (SM)

[RS_SAF_21301]{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*)

[RS_SAF_21302]{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*)

4.3.1.4 Operating System (OS)

[RS_SAF_21401]{DRAFT} **The OS shall support a mechanism that prevents starvation of applications or processes on the basis of CPU usage (under the respect of available resources).** ⌈

Description:	The OS shall support a mechanism that prevents starvation of applications or processes on the basis of CPU usage (under the respect of available resources).
Rationale:	To achieve freedom from interference it is necessary to prevent processes from being adversely affected by other processes that are consuming of excessive resources.
Use Case:	A QM application and a ASIL B application are executed on the same core. OS ensures the defined amount of execution time for safety relevant application.
AppliesTo:	AP
Dependencies:	OS
Supporting Material:	–

⌋(*RS_SAF_10008*, *RS_SAF_10028*, *RS_SAF_10031*)

[RS_SAF_21402]{DRAFT} **The OS shall support resource reservation for memory in the interval [min,max]. If max is not specified it shall be considered as unlimited.** ⌈

Description:	The OS shall support resource reservation for memory in the interval [min,max]. If max is not specified it shall be considered as unlimited.
Rationale:	To achieve freedom from interference it is necessary to prevent processes from adversely affecting other processes, through consumption of excessive resources. To this end the OS mechanisms to configure minimum guarantees on available memory are necessary. Optionally a maximum can be configured - if not specified the process can consume all memory that is not otherwise reserved.
Use Case:	A QM application and a ASIL application are executed on the same machine. OS is ensuring all applications are only getting the defined amount of memory allocated.
AppliesTo:	AP
Dependencies:	OS
Supporting Material:	–

⌋(*RS_SAF_10008*)

[RS_SAF_21403]{DRAFT} **Operating System shall ensure that only allowed memory accesses are made.** ⌈

Description:	Operating System shall ensure that only allowed memory accesses are made.
Rationale:	To achieve freedom from interference it is necessary to prevent processes from adversely affected other processes. Access to private memory which is reserved for a process shall be protected against un-allowed accesses from other processes.

▽

△

Use Case:	A QM application and a ASIL application are executed on the same machine. OS prevents the QM application from changing the memory assigned to the safety critical application.
AppliesTo:	AP
Dependencies:	OS
Supporting Material:	–

⌋(*RS_SAF_10008*)

4.3.1.5 Functional Cluster: Persistency (PER)

[RS_SAF_21501]{DRAFT} **Persistency shall add integrity information to the persistent data if such a mechanism does not already exist in the operating system.** ⌈

Description:	Persistency shall add integrity information to the persistent data if such a mechanism does not already exist in the operating system
Rationale:	To be able to detect data corruption (violating data integrity), integrity information such as CRC is needed to be added when storing data. If there exists an existing underlying mechanism which provides such a functionality with the required integrity, e.g. within the OS, then this takes away AUTOSARs responsibility.
Use Case:	A safety critical application requests to store data to a persistent storage. Persistency adds data integrity information and stores the data.
AppliesTo:	AP
Dependencies:	PER
Supporting Material:	–

⌋(*RS_SAF_10037*)

[RS_SAF_21502]{DRAFT} **Persistency shall check the integrity of persistent data when reading it if this is not already done by the operating system.** ⌈

Description:	Persistency shall check the integrity of persistent data when reading it if this is not already done by the operating system.
Rationale:	Without an integrity check during read, a corrupted piece of data being read can be wrongly treated as correct. If there exists an existing underlying mechanism which provides such a functionality with the required integrity, e.g. within the OS, then this takes away AUTOSARs responsibility.
Use Case:	A safety critical application requests data from a persistent storage. Persistency reads requested data and checks the integrity information.

▽

△

AppliesTo:	AP
Dependencies:	PER
Supporting Material:	–

⌋(*RS_SAF_10037*)

4.3.1.6 Functional Cluster: Communication Management (CM)

[RS_SAF_21601]{DRAFT} **Communication Management shall provide mechanisms for detection of errors during the exchange of information among software components, by considering all faults listed in the ISO standard (ISO 26262:6-2018 D.2.4).** ⌈

Description:	Communication Management shall provide mechanisms for detection of errors during the exchange of information among software components, by considering all faults listed in the ISO standard (ISO 26262:6-2018 D.2.4).
Rationale:	This requirement is created initially to fulfill the goal of AUTOSAR in supporting the development of safety-related systems by offering safety measures and mechanisms. As users may build project-specific applications, it is only possible for AUTOSAR to provide the safe exchange of information. ISO 26262 is mentioned and to be followed, as it is the international standard for functional safety of E/E systems for automotive.
Use Case:	Two ASIL rated applications on different control devices shall exchange information through a component (HW or SW) with a lower rated ASIL. Communication Management shall support safety mechanisms like a counter, a checksum and a timestamp to allow the ASIL applications or the CM implementations to detect and ensure that the information has been transmitted correctly, in time and in-order.
AppliesTo:	AP
Dependencies:	CM[E2E]
Supporting Material:	–

⌋(*RS_SAF_10014*, *RS_SAF_10037*)

[RS_SAF_21602]{DRAFT} **Communication Management shall, based on individual safety concepts, allow integrators to select and configure the set of safety mechanisms to detect communication faults.** ⌈

Description:	Communication Management shall, based on individual safety concepts, allow integrators to select and configure the set of safety mechanisms to detect communication faults.

▽

△

Rationale:	The AUTOSAR Platform is designed to be used in various applications. It is possible that for specific applications, a particular type of fault will not occur. Therefore, it is reasonable to have the configurability such that integrators may freely select the set of mechanisms to be deployed.
Use Case:	A hi-level design change or new information requires a different communication protection mechanism. An integrator can select the proper protection by changing the Manifest. Communication Management uses the changed descriptor after a system update.
AppliesTo:	AP
Dependencies:	CM[E2E]
Supporting Material:	–

⌋(*RS_SAF_10014*, *RS_SAF_10037*)

4.3.1.7 Functional Cluster: Update and Configuration Management (UCM)

[RS_SAF_21701]{DRAFT} **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.** ⌈

Description:	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.
Rationale:	A failed update of a safety relevant software can cause a hazardous situation and to avoid such a situation, Update and Configuration Management shall ensure that it stays in a safe operating mode.
Use Case:	A system update has been performed and the new configuration is not stable and crashes. The system shall transition to a safe operating mode because the safety integrity is not ensured any more.
AppliesTo:	AP
Dependencies:	UCM
Supporting Material:	–

⌋(*RS_SAF_10038*)

[RS_SAF_21702]{DRAFT} **If a safety relevant software is updated/installed Update and Configuration Management shall verify the integrity of the updated or newly installed software.** ⌈

Description:	If a safety relevant software is updated/installed Update and Configuration Management shall verify the integrity of the updated or newly installed software.

▽

△

Rationale:	Update and Configuration Management shall ensure that the updated safety relevant software is installed correctly.
Use Case:	A system update is going to be performed. The update package contains several modules. Update and Configuration Management shall check that the information within the update package is extracted and stored properly.
AppliesTo:	AP
Dependencies:	UCM
Supporting Material:	–

⌋(*RS_SAF_10001*, *RS_SAF_10002*, *RS_SAF_10005*, *RS_SAF_10006*, *RS_SAF_-10008*, *RS_SAF_10028*)

[RS_SAF_21703]{DRAFT} **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.** ⌈

Description:	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
Rationale:	The safety feature whose update failed shall be either available as it was or a retry should be made which eventually results in the updated safety feature. Unless this happens, the function group state which ensures that a hazardous situation cannot occur, shall not be changed.
Use Case:	–
AppliesTo:	AP
Dependencies:	UCM
Supporting Material:	–

⌋(*RS_SAF_10038*)

[RS_SAF_21704]{DRAFT} **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.** ⌈

Description:	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.
Rationale:	During transmission of a new configuration errors may occur and the integrity check may fail. To allow to continue operation Update and Configuration Management shall provide a mechanism to roll back or load another known and consistent configuration which is considered safe.

▽

△

Use Case:	–
AppliesTo:	AP
Dependencies:	UCM
Supporting Material:	–

⌋(*RS_SAF_10027*)

4.3.2 AUTOSAR ClassicPlatform

4.3.2.1 Basic Software: Watchdog Manager (WDGM)

[RS_SAF_31101]{DRAFT} **Watchdog Manager inherits highest safety integrity level from Software Component.** ⌈

Description:	Watchdog Manager shall inherit at least the highest safety integrity level from any Software Component that is running on the platform.
Rationale:	Watchdog Manager is responsible for ensuring part of the safe execution of safety relevant software components/applications, it should at least be developed with the highest ASIL as the software component/application that is being supervised.
Use Case:	An ASIL C, B and QM Application is running on the Classic Platform. WdgM shall supervise the ASIL C and B application, therefore WdgM shall be implemented with an ASIL C.
AppliesTo:	CP
Dependencies:	WdgIf, Wdg Drv
Supporting Material:	–

⌋(*RS_SAF_10001*)

[RS_SAF_31102]{DRAFT} **Watchdog Manager monitors aliveness.** ⌈

Description:	Watchdog Manager shall monitor the aliveness of safety relevant software components/applications and modules.
Rationale:	Alive Supervision is one of the mechanisms of Watchdog Manager by which it monitors safety relevant software components/applications and modules.
Use Case:	A safety critical functionality with alive supervision gets stuck at some point in time during execution. WdgM detects that the supervised application is not alive.
AppliesTo:	CP
Dependencies:	WdgIf, Wdg Drv

▽

△

Supporting Material:	–

⌋(*RS_SAF_10031*)

[RS_SAF_31103]{DRAFT} **Watchdog Manager monitors control flow.** ⌈

Description:	Watchdog Manager shall monitor the control flow of safety relevant software components/applications and modules.
Rationale:	Logical Supervision is one of the mechanisms of Watchdog Manager by which it monitors safety relevant software components/applications and modules.
Use Case:	A safety relevant functionality is developed to follow a specific control flow and is suddenly not following the intended sequence. Watchdog Manager detects the control flow violation.
AppliesTo:	CP
Dependencies:	WdgIf, Wdg Drv
Supporting Material:	–

⌋(*RS_SAF_10005*, *RS_SAF_10006*, *RS_SAF_10030*)

[RS_SAF_31104]{DRAFT} **Watchdog Manager monitors deadline.** ⌈

Description:	Watchdog Manager shall monitor that the duration between the checkpoints of safety relevant software components/applications and modules are within the minimum and maximum configured time limits.
Rationale:	Deadline Supervision is one of the mechanisms of Watchdog Manager by which it monitors safety relevant functionalities.
Use Case:	A safety critical application is developed to reach specific checkpoints in a defined time window and is suddenly not behaving as intended. WdgM detects the violation.
AppliesTo:	CP
Dependencies:	WdgIf, Wdg Drv
Supporting Material:	–

⌋(*RS_SAF_10031*)

4.3.2.2 Basic Software: Operating System (OS)

[RS_SAF_31201]{DRAFT} **Memory Protection of Applications** ⌈

Description:	The Operating System shall prevent applications from performing write accesses outside their assigned memory regions
Rationale:	To achieve freedom from interference it is necessary to prevent applications from adversely affecting other applications. Access to private memory which is reserved for applications shall be protected against un-allowed write accesses from other applications.
Use Case:	A QM application and a ASIL application are executed on the same machine. OS prevents the QM application from changing the memory assigned to the safety critical application.
AppliesTo:	CP
Dependencies:	OSEK OS
Supporting Material:	–

⌋(*RS_SAF_10037*)

[RS_SAF_31202]{DRAFT} **Timing Protection of Applications** ⌈

Description:	The Operating System shall prevent applications from exceeding their assigned execution time budgets
Rationale:	A timing fault in one application might trigger a chain of timing faults and this shall be prevented.
Use Case:	A QM application and a ASIL application are executed on the same machine. OS prevents the QM application from propagating its delay to the safety critical application.
AppliesTo:	CP
Dependencies:	OSEK OS
Supporting Material:	–

⌋(*RS_SAF_10031*)

4.3.2.3 E2E Protection

[RS_SAF_31301]{DRAFT} **E2E Protection with E2E Transformer and E2E Library** ⌈

Description:	Communication Service, E2E Transformer and E2E Library shall provide mechanisms for detection of errors during the exchange of information among software components, by considering all faults listed in the ISO standard (ISO 26262:6-2018 D.2.4). **The Result of the E2E check needs to be published to the application.** If E2E Transformer is used RTE Interfaces need to be developed according to the same ASIL Level as the Application and data being transformed.
Rationale:	This requirement is created initially to fulfill the goal of AUTOSAR in supporting the development of safety-related systems by offering safety measures and mechanisms. As users may build project-specific applications, it is only possible for AUTOSAR to provide the safe exchange of information. ISO 26262 is mentioned and to be followed, as it is the international standard for functional safety of E/E systems for automotive.
Use Case:	Two ASIL rated applications on different control devices shall exchange information through a component (HW or SW) with a lower rated ASIL. E2E Transformer and E2E Library shall support safety mechanisms like a counter, a checksum and a timestamp to allow the ASIL applications or the E2E Transformer and E2E Library implementations to detect and ensure that the information has been transmitted correctly, in time and in-order.
AppliesTo:	CP
Dependencies:	E2E Library, E2E Transformer, RTE, SWC
Supporting Material:	–

⌋(*RS_SAF_10014*, *RS_SAF_10037*)

[RS_SAF_31302]{DRAFT} **Allow integrators to configure safety mechanisms to detect communication faults** ⌈

Description:	Communication Service, E2E Transformer and E2E Library shall, based on individual safety concepts, allow integrators to select and configure the set of safety mechanisms to detect communication faults.
Rationale:	Different communication buses and data information may have different needs to be protected by the E2E. Therefore, it is reasonable to have the configurability (pre-deployment) such that integrators may freely select the set of mechanisms to be deployed.
Use Case:	A hi-level design change or new information requires a different communication protection mechanism. An integrator can select the proper protection by changing the Manifest.
AppliesTo:	CP
Dependencies:	E2E Library, E2E Transformer, RTE, SWC
Supporting Material:	–

⌋(*RS_SAF_10001*)

5 Requirements Tracing

The following table references the requirements specified in [5] and links to the fulfillment of these.

Feature	Description	Satisfied by
[RS_Main_00010]	Safety Mechanisms	[RS_SAF_00001] [RS_SAF_00002] [RS_SAF_00003] [RS_SAF_00004] [RS_SAF_00005] [RS_SAF_00006]
[RS_Main_00011]	Mechanisms for Reliable Systems	[RS_SAF_00001] [RS_SAF_00002] [RS_SAF_00003] [RS_SAF_00004]
[RS_Main_00012]	Highly Available Systems Support	[RS_SAF_00001] [RS_SAF_00002] [RS_SAF_00003] [RS_SAF_00004]
[RS_Main_00030]	Safety Related Process Support	[RS_SAF_00001] [RS_SAF_00002] [RS_SAF_00003] [RS_SAF_00004]
[RS_Main_00150]	AUTOSAR shall support the deployment and reallocation of AUTOSAR Application Software	[RS_SAF_00003]
[RS_SAF_00001]	Safe Execution	[RS_SAF_10001] [RS_SAF_10005] [RS_SAF_10008] [RS_SAF_10028] [RS_SAF_10030] [RS_SAF_10031]
[RS_SAF_00002]	Safe Configuration	[RS_SAF_10001] [RS_SAF_10002] [RS_SAF_10008] [RS_SAF_10027] [RS_SAF_10028] [RS_SAF_10037]
[RS_SAF_00003]	Safe Update or Safe Upgrade	[RS_SAF_10002] [RS_SAF_10005] [RS_SAF_10037] [RS_SAF_10038]
[RS_SAF_00004]	Safe Exchange of Information	[RS_SAF_10008] [RS_SAF_10014] [RS_SAF_10037]
[RS_SAF_10001]	AUTOSAR shall provide mechanisms to support safe initialization of software components.	[RS_SAF_21201] [RS_SAF_21301] [RS_SAF_21702] [RS_SAF_31101] [RS_SAF_31302]
[RS_SAF_10002]	AUTOSAR shall provide mechanisms to support safe verification mechanisms of platform basic software modules, functional-clusters, software components, applications, services and their respective configuration data.	[RS_SAF_21101] [RS_SAF_21702]

[RS_SAF_10005]	AUTOSAR shall provide mechanisms to support safe shutdown and termination of applications, software components, basic software modules and services.	[RS_SAF_21102] [RS_SAF_21103] [RS_SAF_21105] [RS_SAF_21107] [RS_SAF_21202] [RS_SAF_21302] [RS_SAF_21702] [RS_SAF_31103]
[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_SAF_21102] [RS_SAF_21103] [RS_SAF_21105] [RS_SAF_21107] [RS_SAF_21302] [RS_SAF_21702] [RS_SAF_31103]
[RS_SAF_10008]	AUTOSAR shall provide mechanisms to support safe resource management for the AUTOSAR Adaptive Platform functional-clusters, applications and services and AUTOSAR Classic Platform basic software modules and software components.	[RS_SAF_21401] [RS_SAF_21402] [RS_SAF_21403] [RS_SAF_21702]
[RS_SAF_10014]	AUTOSAR shall provide an interface to support safe communication for basic software module, software component, application or services.	[RS_SAF_21601] [RS_SAF_21602] [RS_SAF_31301]
[RS_SAF_10027]	AUTOSAR shall provide mechanisms to prevent the loss of a valid configuration.	[RS_SAF_21704]
[RS_SAF_10028]	AUTOSAR shall provide mechanisms to support dependable scheduling of AUTOSAR Adaptive Platform functional-clusters, applications and services and AUTOSAR Classic Platform basic software modules and software components.	[RS_SAF_21202] [RS_SAF_21401] [RS_SAF_21702]
[RS_SAF_10030]	AUTOSAR shall provide mechanisms to support safe program execution.	[RS_SAF_21101] [RS_SAF_21102] [RS_SAF_21103] [RS_SAF_21105] [RS_SAF_21202] [RS_SAF_31103]
[RS_SAF_10031]	AUTOSAR shall provide mechanisms to detect program execution time violation	[RS_SAF_21101] [RS_SAF_21104] [RS_SAF_21106] [RS_SAF_21202] [RS_SAF_21401] [RS_SAF_31102] [RS_SAF_31104] [RS_SAF_31202]
[RS_SAF_10037]	AUTOSAR shall provide mechanisms to prevent unintended alteration of data.	[RS_SAF_21501] [RS_SAF_21502] [RS_SAF_21601] [RS_SAF_21602] [RS_SAF_31201] [RS_SAF_31301]
[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_SAF_21701] [RS_SAF_21703]

6 References

[1] ISO 26262:2018 (all parts) – Road vehicles – Functional Safety
http://www.iso.org

[2] Standardization Template
AUTOSAR_TPS_StandardizationTemplate

[3] Glossary
AUTOSAR_TR_Glossary

[4] Explanation of Safety Overview
AUTOSAR_EXP_SafetyOverview

[5] Main Requirements
AUTOSAR_RS_Main