Document Title	Requirements on Safety Extensions
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	670
Document Classification	Auxiliary

Document Status	Final
Part of AUTOSAR Standard	Classic Platform
Part of Standard Release	4.3.0

Document Change History			
Date	**Release**	**Changed by**	**Description**
2016-11-30	4.3.0	AUTOSAR Release Management	minor corrections / clarifications / editorial changes; For details please refer to the ChangeDocumentation
2015-07-31	4.2.2	AUTOSAR Release Management	minor corrections / clarifications / editorial changes; For details please refer to the ChangeDocumentation
2014-10-31	4.2.1	AUTOSAR Release Management	Initial release based on Concept "'Safety Extensions"'

Disclaimer

Advice for users

AUTOSAR specifications may contain exemplary items (exemplary reference models, "use cases", and/or references to exemplary technical solutions, devices, processes or software).

Any such exemplary items are contained in the specifications for illustration purposes only, and they themselves are not part of the AUTOSAR Standard. Neither their presence in such specifications, nor any later documentation of AUTOSAR conformance of products actually implementing such exemplary items, imply that intellectual property rights covering such exemplary items are licensed under the same rules as applicable to the AUTOSAR Standard.

Table of Contents

Bibliography

[1] ISO 26262 (Part 1-10) – Road vehicles – Functional Safety, First edition
http://www.iso.org

[2] Specifications of Safety Extensions
AUTOSAR_TPS_SafetyExtensions

[3] Standardization Template
AUTOSAR_TPS_StandardizationTemplate

[4] Requirements on AUTOSAR Features
AUTOSAR_RS_Features

[5] Methodology
AUTOSAR_TR_Methodology

1 Introduction

1.1 Scope

This document collects the requirements on the Safety Aspects of AUTOSAR models and its incorporation into the AUTOSAR templates.

The main goal of the Safety Extensions is to enable the exchange of safety related information for an AUTOSAR system as part of the AUTOSAR templates. This will pave the ground for the necessary traceability of safety requirements to AUTOSAR elements, safety measures and AUTOSAR safety mechanisms. It will also ensure, that the appropriate Safety Integrity Levels for AUTOSAR elements are available during system design, realization and configuration and that they can be subject for constraint checking.

In the context of this document, functional safety mechanisms are a concrete product part, such as memory protection. They are considered as specialization of functional safety measures, which also include process steps, like a review. This definition is inline with the definition given in ISO 26262-1 [1] for these terms.

The requirements collected in this document will be satisfied by the AUTOSAR Specification of Safety Extensions [2].

1.2 Document Conventions

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([3]).

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 ([3]).

1.3 Guidelines

Existing specifications shall be referenced (in form of a single requirement). Differences to these specifications are specified as additional requirements. All Requirements shall have the following properties:

- Redundancy
  Requirements shall not be repeated within one requirement or in other requirements.
- Clearness
  All requirements shall allow one possibility of interpretation only. Used technical terms that are not in the glossary must be defined.
- Atomicity
  Each Requirement shall only contain one requirement. A Requirement is atomic if it cannot be split up in further requirements.
- Testability
  Requirements shall be testable by analysis, review or test.
- Traceability
  The source and status of a requirement shall be visible at all times.

2 Use Case Tracing

Following table references the use cases specified in 5 and links to the related requirements.

Use Case	Description	Satisfied by
[UC_SAFEX_00001]	Exchange of safety information in case of a distributed development of an AUTOSAR system	[RS_SAFEX_00001] [RS_SAFEX_00002] [RS_SAFEX_00003] [RS_SAFEX_00004] [RS_SAFEX_00005] [RS_SAFEX_00006] [RS_SAFEX_00007] [RS_SAFEX_00008] [RS_SAFEX_00009] [RS_SAFEX_00010] [RS_SAFEX_00011] [RS_SAFEX_00015] [RS_SAFEX_00016] [RS_SAFEX_00017] [RS_SAFEX_00023] [RS_SAFEX_00018] [RS_SAFEX_00012] [RS_SAFEX_00013] [RS_SAFEX_00014] [RS_SAFEX_00022]
[UC_SAFEX_00002]	Manage Safety Requirements in AUTOSAR	[RS_SAFEX_00001] [RS_SAFEX_00002] [RS_SAFEX_00003] [RS_SAFEX_00004] [RS_SAFEX_00005] [RS_SAFEX_00006] [RS_SAFEX_00007] [RS_SAFEX_00008] [RS_SAFEX_00009] [RS_SAFEX_00010]
[UC_SAFEX_00003]	ASIL constraint checking	[RS_SAFEX_00008] [RS_SAFEX_00010] [RS_SAFEX_00011] [RS_SAFEX_00018] [RS_SAFEX_00012] [RS_SAFEX_00013] [RS_SAFEX_00014] [RS_SAFEX_00022]

Use Case	Description	Satisfied by
[UC_SAFEX_00004]	AUTOSAR SEooC development	[RS_SAFEX_00001] [RS_SAFEX_00002] [RS_SAFEX_00003] [RS_SAFEX_00004] [RS_SAFEX_00005] [RS_SAFEX_00006] [RS_SAFEX_00007] [RS_SAFEX_00008] [RS_SAFEX_00009] [RS_SAFEX_00010] [RS_SAFEX_00011] [RS_SAFEX_00015] [RS_SAFEX_00016] [RS_SAFEX_00017] [RS_SAFEX_00023] [RS_SAFEX_00018] [RS_SAFEX_00012] [RS_SAFEX_00013] [RS_SAFEX_00014] [RS_SAFEX_00022]
[UC_SAFEX_00005]	Provision of Safety documentation for an AUTOSAR system	[RS_SAFEX_00001] [RS_SAFEX_00002] [RS_SAFEX_00003] [RS_SAFEX_00004] [RS_SAFEX_00005] [RS_SAFEX_00006] [RS_SAFEX_00007] [RS_SAFEX_00008] [RS_SAFEX_00009] [RS_SAFEX_00010] [RS_SAFEX_00011] [RS_SAFEX_00015] [RS_SAFEX_00016] [RS_SAFEX_00017] [RS_SAFEX_00023] [RS_SAFEX_00018] [RS_SAFEX_00012] [RS_SAFEX_00013] [RS_SAFEX_00014] [RS_SAFEX_00022]
[UC_SAFEX_00006]	Provision of appropriate safety mechanisms for an AUTOSAR system	[RS_SAFEX_00008] [RS_SAFEX_00009] [RS_SAFEX_00010] [RS_SAFEX_00011] [RS_SAFEX_00015] [RS_SAFEX_00016] [RS_SAFEX_00017] [RS_SAFEX_00023] [RS_SAFEX_00018] [RS_SAFEX_00012] [RS_SAFEX_00013] [RS_SAFEX_00014] [RS_SAFEX_00022]

Use Case	Description	Satisfied by
[UC_SAFEX_00007]	Observation of constraints resulting from an applied ASIL decomposition	[RS_SAFEX_00008] [RS_SAFEX_00009]
[UC_SAFEX_00008]	Obtaining ASIL information for an AUTOSAR element	[RS_SAFEX_00011]

3 Requirements Tracing

The following table references the requirements specified in [4] and links to the fulfillment of these.

Requirement	Description	Satisfied by
[RS_BRF_02068]	AUTOSAR methodology shall allow to allocate safety properties to model elements	[RS_SAFEX_00001] [RS_SAFEX_00002] [RS_SAFEX_00003] [RS_SAFEX_00004] [RS_SAFEX_00005] [RS_SAFEX_00006] [RS_SAFEX_00007] [RS_SAFEX_00008] [RS_SAFEX_00009] [RS_SAFEX_00010] [RS_SAFEX_00011] [RS_SAFEX_00012] [RS_SAFEX_00013] [RS_SAFEX_00014] [RS_SAFEX_00015] [RS_SAFEX_00016] [RS_SAFEX_00017] [RS_SAFEX_00018] [RS_SAFEX_00020] [RS_SAFEX_00021] [RS_SAFEX_00022] [RS_SAFEX_00023] [RS_SAFEX_00024]

4 Requirements

This chapter describes all requirements driving the work to define the `Safety Extensions` specification [2].

4.1 Safety Requirements

[RS_SAFEX_00001] Safety Requirements expressible within AUTOSAR Models ⌈

Type:	valid
Description:	Safety requirements shall be expressed within AUTOSAR models and documents by means of the AUTOSAR meta-model.
Rationale:	Consistent specification and representation of all requirements including safety requirements and their specification items in AUTOSAR.
Use Case:	[UC_SAFEX_00002],[UC_SAFEX_00001]
Dependencies:	–
Supporting Material:	see ISO 26262-8 [1].

⌋*(RS_BRF_02068)*

[RS_SAFEX_00002] Safety Requirements at least as expressive as other Requirements ⌈

Type:	valid
Description:	Safety requirements shall at least be able to carry the same kind of information as other requirements in AUTOSAR. In addition, follow the requirements upon requirements management of ISO 26262-8, see [1].
Rationale:	Safety standards like ISO 26262 [1] define the minimum requirements towards the definition of safety requirements. Furthermore, a harmonized definition using a similar structure for safety and non-safety requirements in AUTOSAR is desired.
Use Case:	[UC_SAFEX_00001],[UC_SAFEX_00002]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	–

⌋*(RS_BRF_02068)*

[RS_SAFEX_00003] Safety Requirements Description by an URI ⌈

Type:	valid
Description:	It shall be possible to relate a safety requirement definition within an AUTOSAR model with a specification of that requirement outside of that AUTOSAR model by an URI.

Rationale:	There are several technical approaches of exchanging requirements used in practice. This includes the Requirements Interchange Format (ReqIF) or proprietary tool based interchange. By the possibility to refer to an external requirement definition via an URI, the traceability can be established within AUTOSAR models while the duplication of data with its typical negative effects is avoided.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	–

⌋(*RS_BRF_02068*)

[RS_SAFEX_00004] Safety Requirements distinguishable ⌈

Type:	valid
Description:	Safety requirements shall be distinguishable from other requirements in AUTOSAR models
Rationale:	Regulations of safety standards need to be applied solely to safety requirements. This holds e.g. for the traceability or ASIL dependent measures or constraints. It is therefore necessary to clearly identify the safety requirements.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-8 [1].

⌋(*RS_BRF_02068*)

[RS_SAFEX_00005] Safety Requirements uniquely identifiable ⌈

Type:	valid
Description:	Safety requirements shall be uniquely identifiable.
Rationale:	This is necessary to fulfill the requirements of safety standards.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-8 [1].

⌋(*RS_BRF_02068*)

[RS_SAFEX_00006] Status Information for Safety Requirements ⌈

Type:	valid
Description:	It shall be possible to specify the status of a safety requirement.
Rationale:	This is necessary to fulfill the requirements of safety standards.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00004]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-8 [1].

⌋(*RS_BRF_02068*)

[RS_SAFEX_00007] Hierarchy of Safety Requirements ⌈

Type:	valid
Description:	It shall be possible to specify a hierarchy of safety requirements
Rationale:	This is necessary to fulfill the requirements of safety standards.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-8 [1].

⌋(*RS_BRF_02068*)

[RS_SAFEX_00008] Decomposition of Safety Requirements ⌈

Type:	valid
Description:	It shall be possible to express the decomposition of a safety requirement into two independent safety requirements.
Rationale:	ASIL decomposition is a concept provided in ISO 26262 to reduce the ASIL of a safety requirement by splitting it into independent safety requirements. ASIL decomposition should also be available for AUTOSAR systems.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00007]
Dependencies:	[RS_SAFEX_00010], [RS_SAFEX_00001]
Supporting Material:	see ISO 26262-9 [1]

⌋(*RS_BRF_02068*)

[RS_SAFEX_00009] Specification of Independence Requirements ⌈

Type:	valid
Description:	It should be possible to specify an independence requirement which is a special safety requirement and relate it to a decomposition of a safety requirement.
Rationale:	ASIL decomposition is only allowed if the independence of the resulting safety requirements with lower ASILs can be ensured. This results in requirements for independence which clearly relate to the decomposition.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00007]
Dependencies:	[RS_SAFEX_00001], [RS_SAFEX_00008]
Supporting Material:	see ISO 26262-9 [1]

⌋(*RS_BRF_02068*)

4.2 Safety Integrity Level

[RS_SAFEX_00010] ASIL Attribute for Safety Requirements ⌈

Type:	valid

Description:	It shall be possible to specify an ASIL attribute for safety requirements. The values of the attribute shall at least carry values for the possible ASILs as listed in ISO 26262 in an unambiguous manner.
Rationale:	The necessary measures for ensuring functional safety of a system depend on the applicable ASIL. The assignment of the ASIL to system elements is done via the safety requirements. Failure to respect the ASIL could lead to unsafe systems.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00008]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-3 [1]

⌋(*RS_BRF_02068*)

[RS_SAFEX_00011] ASIL Attribute for AUTOSAR Elements ⌈

Type:	valid
Description:	It shall be possible to specify an ASIL attribute for any AUTOSAR element which is part of an AUTOSAR model. The values of the attribute shall at least carry values for the possible ASILs as listed in ISO 26262 in an unambiguous manner.
Rationale:	This allows for cross checks of ASIL values between safety requirements and AUTOSAR elements. It is important for using e.g. a safety element out of context approach (SEooC), see ISO 26262-10 [1].
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00008]
Dependencies:	
Supporting Material:	see ISO 26262-4 and ISO 26262-6 [1]

⌋(*RS_BRF_02068*)

4.3 Safety Measures and Safety Mechanisms

[RS_SAFEX_00015] Safety Measures expressible within AUTOSAR Models ⌈

Type:	valid
Description:	Safety Measures shall be expressible within AUTOSAR models.
Rationale:	AUTOSAR provides a number of safety mechanisms. They should be related to the safety requirements in AUTOSAR models to demonstrate the proper realization of the safety requirements. Furthermore, it is important to also be able to address safety measures that are external to AUTOSAR, but which are important for the AUTOSAR system. By modeling a safety measure it can be used as a proxy and end point for traceability within an AUTOSAR model.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00006]
Dependencies:	–
Supporting Material:	–

⌋(*RS_BRF_02068*)

[RS_SAFEX_00016] Textual Description of Safety Measures ⌈

Type:	valid
Description:	Safety Measures shall have at least a textual description.
Rationale:	The textual description provides an informal way of describing a safety measure. Additional formal properties may be defined in the future.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00005], [UC_SAFEX_00006]
Dependencies:	[RS_SAFEX_00015]
Supporting Material:	–

⌋(*RS_BRF_02068*)

[RS_SAFEX_00017] Safety Measures uniquely identifiable ⌈

Type:	valid
Description:	Safety Measures shall be uniquely identifiable.
Rationale:	The safety measures are subject for traceability to safety requirements. Without a unique identifier it is not possible to establish such traceability.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00005], [UC_SAFEX_00006]
Dependencies:	[RS_SAFEX_00015]
Supporting Material:	–

⌋(*RS_BRF_02068*)

[RS_SAFEX_00023] Safety Mechanisms as special Safety Measures ⌈

Type:	valid
Description:	Safety Mechanisms shall be expressible within AUTOSAR models as specialization of safety measures
Rationale:	ISO 26262 distinguishes between safety measures and safety mechanisms whereas safety measures are including safety mechanisms. This terminology should be reflected in the safety extensions. (see ISO 26262-1, clause 1.110 [1])
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00005], [UC_SAFEX_00006]
Dependencies:	[RS_SAFEX_00015]
Supporting Material:	–

⌋(*RS_BRF_02068*)

[RS_SAFEX_00018] Relation between Safety Requirements and Safety Measures ⌈

Type:	valid
Description:	It shall be possible to relate safety requirements to safety measures. Such relations shall be clearly distinguishable from any other relations in AUTOSAR models.

Rationale:	For demonstrating the system safety, it is an advantage to have the relation between safety requirements and safety measures explicitly modeled. That eases documentation and enables consistency checks (e.g. observing applicable ASIL related rules).
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00006], [UC_SAFEX_00005], [UC_SAFEX_00004]
Dependencies:	[RS_SAFEX_00015], [RS_SAFEX_00001]
Supporting Material:	–

⌋(*RS_BRF_02068*)

4.4 Traceability and Allocation

[RS_SAFEX_00012] Safety Requirements traceability ⌈

Type:	valid
Description:	Safety Requirements shall be traceable according to ISO 26262 [1].
Rationale:	Traceability of safety requirements is a main requirement of safety standards like ISO 26262 [1]. Establishing traceability directly within AUTOSAR models increases consistency and reduces effort.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00005]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-8 [1]

⌋(*RS_BRF_02068*)

[RS_SAFEX_00013] Safety Measures traceability ⌈

Type:	valid
Description:	Safety Measures shall be traceable according to ISO 26262 [1].
Rationale:	Traceability is a main requirement of safety standards (see ISO 26262-8 clause 6.4.3.2. [1]). Safety measures are activities or technical solutions that support the fulfillment of safety requirements which includes safety mechanisms provided by AUTOSAR. Establishing traceability directly within AUTOSAR models increases consistency and reduces effort for the provision of safety documentation.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00004], [UC_SAFEX_00005]
Dependencies:	[RS_SAFEX_00015]
Supporting Material:	–

⌋(*RS_BRF_02068*)

[RS_SAFEX_00014] Safety Requirements Allocation ⌈

Type:	valid

Description:	It shall be possible to allocate technical safety requirements to elements of an AUTOSAR model. Such allocation shall be distinguishable from other relations in AUTOSAR models.
Rationale:	All Safety Requirements must be allocated to hardware, software or both. Those safety requirements that are to be realized by the AUTOSAR system should be allocated to the corresponding AUTOSAR elements. This is the base for e.g. checking constraints regarding the ASIL or to perform appropriate safety analysis.
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00002], [UC_SAFEX_00005]
Dependencies:	[RS_SAFEX_00001]
Supporting Material:	see ISO 26262-4 and ISO 26262-6 [1]

⌋(*RS_BRF_02068*)

[RS_SAFEX_00022] Safety Measures Allocation ⌈

Type:	valid
Description:	It shall be possible to allocate safety measures to elements of an AUTOSAR model. Such allocation shall be distinguishable from other relations in AUTOSAR models.
Rationale:	A safety measure information element describes a safety measure, that can be realized by the AUTOSAR system (e.g. an AUTOSAR safety mechanism like E2E communication protection). In such a case, it is necessary to relate the AUTOSAR elements that realize the safety measure to the safety measure information element. The presence of such relation will ease the required verification process (of the safety requirements related to the safety measure) and also enable constraint checking (e.g. ASIL obligations.)
Use Case:	[UC_SAFEX_00001], [UC_SAFEX_00005]
Dependencies:	[RS_SAFEX_00015]
Supporting Material:	see ISO 26262-4 and ISO 26262-6 [1]

⌋(*RS_BRF_02068*)

4.5 Methodology and Usage

[RS_SAFEX_00024] AUTOSAR Methodology explains Usage of Safety Extensions ⌈

Type:	valid
Description:	The usage of the safety extensions shall be explained by the AUTOSAR Methodology.
Rationale:	The safety extensions can be facilitated for a number of activities that are typically performed during the development of an AUTOSAR system. The AUTOSAR methodology describes such activities. If safety information is necessary for performing existing activities or if new activities or tasks are necessary to consume or produce safety information, then they should be explained by the methodology.

Use Case:	–
Dependencies:	[5]
Supporting Material:	

⌋(*RS_BRF_02068*)

[RS_SAFEX_00020] Safety Extensions do not break AUTOSAR Model Processing ⌈

Type:	valid
Description:	The usage of Safety Extensions shall not break the processing of existing AUTOSAR models.
Rationale:	The safety extensions are provided as extensions that can be used in addition to the existing models. This ensures backward compatibility. For some generation purposes, it might not be necessary to include the safety extensions into the generation process to save resources.
Use Case:	–
Dependencies:	–
Supporting Material:	

⌋(*RS_BRF_02068*)

[RS_SAFEX_00021] Safety Extensions for existing AUTOSAR Models ⌈

Type:	valid
Description:	It shall be possible to specify Safety Extensions for existing AUTOSAR model.
Rationale:	This would allow to extend existing AUTOSAR models by safety extensions as a lot of AUTOSAR systems are safety relevant.
Use Case:	–
Dependencies:	–
Supporting Material:	

⌋(*RS_BRF_02068*)

5 Supported Use Cases

[UC_SAFEX_00001] Exchange of safety information in case of a distributed development of an AUTOSAR system ⌈

Distributed development is typical for an AUTOSAR based system. For the final system (item) it has to be demonstrated that it fulfills the needs of functional safety.

The safety requirements relevant for the AUTOSAR system are exchanged as part of AUTOSAR models among the organizations taking part in the distributed development. The safety requirements contain also ASIL attributes and their allocation to AUTOSAR elements is explicitly specified. It is ensured, that safety related information cannot be lost. Traceability is established whenever it is appropriate. At the end, a lot of information for the documentation of system safety is contained in the AUTOSAR model and can be facilitated.

⌋()

[UC_SAFEX_00002] Manage Safety Requirements in AUTOSAR ⌈

In AUTOSAR all requirements are formally captured in requirement documents (RS/Feature/SRS) with a unique id. Specification documents (SWS) contain specification items that formally trace to requirements. Dependencies between requirements on the same level are expressed in the requirement block itself by providing references to the related requirements. Safety requirements (potentially including safety goals) are captured in a separate safety requirements document or in the same document as other requirements. In both cases, traceability is established between such safety requirements and safety related specification elements.

⌋()

[UC_SAFEX_00003] ASIL constraint checking ⌈

The ASIL of AUTOSAR (i.e. used for their development) must match the ASIL of the allocated safety requirements for these elements. Match means that the ASIL of the element is equal or higher then that of the allocated safety requirement(s). Having all information in the AUTOSAR model (safety requirements, ASIL, allocation) a constraint check can be performed to find invalid allocations. This is especially useful in a context where the development is distributed or existing components are to be integrated.

⌋()

[UC_SAFEX_00004] AUTOSAR SEooC development ⌈

According to ISO 26262-10 ([1]) the development of a Safety Element out of Context is characterized by the fact that the assumptions on the environment of the SEooC are made without knowing the actual context (item) into which the SEooC is integrated. A developer of such an SEooC will provide the assumptions in form of safety requirements with appropriate ASILs and status information in the AUTOSAR model of the SEooC. Furthermore, the safety measures/safety mechanisms will be described and provided. The integrator will facilitate this information to perform the analysis that the

assumptions are met by the environment into which the SEooC is embedded. Again, traceability, allocation and mapping relations are used in the AUTOSAR model.

⌋()

[UC_SAFEX_00005] Provision of Safety documentation for an AUTOSAR system ⌈

An OEM can use the AUTOSAR model of an AUTOSAR system and extract the information in the model on safety requirements, safety measures, their allocation to AUTOSAR elements and the mapping between safety requirements and safety measures to create Safety Documentation as required by ISO 26262-8 ([1]).

⌋()

[UC_SAFEX_00006] Provision of appropriate safety mechanisms for an AUTOSAR system ⌈

The OEM can specify requirements for safety mechanisms on the system level. The supplier working on an ECU level can provide such appropriate safety mechanisms and establish required traceability. It is also possible, that the vendor of the AUTOSAR stack (BSW components) provides and describes vendor specific safety mechanisms. The information on safety mechanisms is available for the verification process as it is exchanged as part of the AUTOSAR model.

⌋()

[UC_SAFEX_00007] Observation of constraints resulting from an applied ASIL decomposition ⌈

The OEM applies an ASIL decomposition as part of his technical safety concept. This has implications on the independence of software components of the intended system. Both the information on the applied decomposition as well as the independence requirements are submitted by the supplier as part of the AUTOSAR model. The supplier is able to fulfill the independence requirements as they are explicitly known and the verification of that is much easier due to traceability.

⌋()

[UC_SAFEX_00008] Obtaining ASIL information of an AUTOSAR element ⌈

A supplier that is asked to implement a software component needs to know the ASIL of that component in order to apply appropriate development process. Furthermore, the safety requirements that need to be implemented should be known. Both information is exchanged as part of the AUTOSAR model using the safety extensions.

⌋()