Document Title	Main Requirements
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	054
Document Classification	Auxiliary

Document Version	2.1.0
Document Status	Final
Part of Release	3.0
Revision	7

Document Change History

Date	Version	Changed by	Change Description
15.09.2010	2.1.0	AUTOSAR Administration	• Updated Main270 • Legal disclaimer revised
05.12.2007	2.0.3	AUTOSAR Administration	• Document meta information extended • Small layout adaptations made
24.01.2007	2.0.2	AUTOSAR Administration	• “Advice for users” revised • “Revision Information” added
28.11.2006	2.0.1	AUTOSAR Administration	Legal disclaimer revised
06.12.2005	2.0.0	AUTOSAR Administration	Removed section “2.1 Recipients” Update of section 3.1.1 Changed [Main11], [Main60], [Main300], [Main310], [Main320], [Main330], [Main340], [Main350], [Main360], [Main370], [Main380] • Use Case added Changed [Main20] • Rationale extended Changed [Main10], [Main50], [Main80], [Main90], [Main130], [Main230], [Main240] • Rationale added Changed [Main160], [Main280] • Rationale and Use Case added Changed [Main300], [Main310] • Headline and Short description written in active Update of section 3.3 according to changes of 3.1.1
09.05.2005	1.0.0	AUTOSAR Administration	Initial release

Disclaimer

Advice for users

AUTOSAR Specification Documents 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 Specification Documents for illustration purposes only, and they themselves are not part of the AUTOSAR Standard. Neither their presence in such Specification Documents, 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

1 Scope of the document

Each partner has committed to the overall project objectives (PO) of AUTOSAR. The objectives are listed in the AUTOSAR Standard Info Pack V3.3 or in subsequent documents. AUTOSAR Standard Info Pack is an official communication paper of development partnership.

These objectives are not directly usable and have to be refined in order to generate the specific technical requirements. For this purpose, the AUTOSAR Main Requirements are established as a fundamental base to derive these specific requirements.
The goal of this document is to define the main requirements of AUTOSAR including its link to the AUTOSAR objectives.
The term AUTOSAR is used as a synonym of the development partnership and the technical product AUTomotive Open System ARchitecture.

Besides the technical requirements also non-technical requirements (i.e. business model, legal issues) exist, which are not covered here.

The project objectives are listed as follows:

No.	*Project objectives*	*Abbreviation*	*Priority*
1	Consideration of availability and safety requirements	AUTOSAR PO1	1
2	Redundancy activation	AUTOSAR PO2	2
3	Scalability to different vehicle and platform variants	AUTOSAR PO3	1
4	Implementation and standardization of basic system functions as an OEM wide Standard Core solution	AUTOSAR PO4	1
5	Transferability of functions throughout the network	AUTOSAR PO5	1
6	Integration of functional modules from multiple suppliers	AUTOSAR PO6	1
7	Maintainability throughout the whole product life cycle	AUTOSAR PO7	2
8	Increased use of commercial off the shelf hardware (COTS)	AUTOSAR PO8	3
9	Software updates and upgrades over vehicle lifetime	AUTOSAR PO9	2

For this document the project objectives are given.
The prioritization of the objectives has following levels:

1: High, required
2: Medium, recommended
3: Low, optional

2 How to read this document

Each requirement has its unique identifier starting with the prefix “Main” (for “Main Requirement”). For any review annotations, remarks or questions, please refer to this unique ID rather than chapter or page numbers!

2.1 Conventions used

In requirements, the following specific semantics are used (taken from Request for Comment RFC 2119 from the Internet Engineering Task Force IETF)

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 described in RFC 2119. Note that the requirement level of the document in which they are used modifies the force of these words.

- MUST: This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase „SHALL NOT“, means that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective "RECOMMENDED", mean 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" mean 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, MUST 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, MUST be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides.)

3 The AUTOSAR main requirements

This chapter describes the main requirements of AUTOSAR. These main requirements shall be used as a basis for the work in the work packages. Besides these technical requirements, there are non-technical requirements, such as new business model etc., which are not considered here.

3.1 The AUTOSAR project objectives and their concretization by the main requirements

The following shows the main requirements of each project objectives. The main requirements are described below in chapter 3.2.

3.1.1 Requirements to achieve the AUTOSAR PO1 (CONSIDERATION OF AVAILABILITY AND SAFETY REQUIREMENTS)

- Using AUTOSAR system reliability with a probability of failure per system down time shall be achievable down to 10^{-8} per hour [Main10].
- AUTOSAR shall provide means to reduce system down-time [Main11].
- AUTOSAR shall provide mechanisms to support redundancy paths [Main20].
- A SIL-3-Level development must be possible with AUTOSAR [Main30].
- AUTOSAR shall support inter- and intra-ECU communication mechanisms with high reliability [Main50].
- AUTOSAR shall provide means to clearly check the conformance of an AUTOSAR-implementation with its AUTOSAR-specification [Main120].
- AUTOSAR shall provide an abstraction of the application software from hardware [Main130].
- AUTOSAR shall provide an independency of application software from in-vehicle communication technologies [Main140].
- AUTOSAR should provide an independency of application software from operating systems [Main141].
- AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure [Main150].
- AUTOSAR shall provide means to protect SW-components from malicious SW-components [Main240].
- AUTOSAR should provide means to achieve compositionality [Main250].
- AUTOSAR shall provide diagnostics means during runtime, for production and service purposes [Main260].
- AUTOSAR shall ensure the verification of all processes and products developed within AUTOSAR [Main290].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Definitions of relations between SW components are exhaustive and formal [Main320].
- SW components are protected from illegal access [Main330].

- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR process shall provide a predefinition of typical roles and activities in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

3.1.2 Requirements to achieve the AUTOSAR PO2 (REDUNDANCY ACTIVATION)

- AUTOSAR shall provide mechanisms to support redundancy paths [Main20].
- AUTOSAR shall support inter- and intra-ECU-communication mechanisms with high reliability [Main50].
- Definitions of relations between SW components are exhaustive and formal [Main320].

3.1.3 Requirements to achieve the AUTOSAR PO3 (SCALABILITY TO DIFFERENT VEHICLE AND PLATFORM VARIANTS)

- AUTOSAR shall provide open and standardized SW interfaces for intra- and inter-ECU communication [Main60].
- AUTOSAR shall provide complete interfaces to application software and basic software modules [Main70].
- AUTOSAR shall ease the reusability of software and its concepts and implementations [Main80].
- AUTOSAR shall provide interoperability with legacy software [[Main190].
- AUTOSAR shall imply only small memory and performance impacts when used in today's micro controllers [Main200].
- AUTOSAR shall provide means to integrate AUTOSAR ECU's in non-AUTOSAR networks [Main210].
- AUTOSAR shall support networks of networks including sub networks [Main230].
- AUTOSAR shall provide means to achieve compositionality [Main250].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- The AUTOSAR architecture must provide dynamic communication pattern [Main280].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Definitions of relations between SW components are exhaustive and formal [Main320].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to Change process in design are predefined and supported by AUTOSAR [Main380].

Remark: Intra-ECU: AUTOSAR and OS-interface; Inter-ECU: CAN, MOST, LIN, FlexRay.

3.1.4 Requirements to achieve the AUTOSAR PO4 (IMPLEMENTATION AND STANDARDIZATION OF BASIC SYSTEM FUNCTIONS AS AN OEM WIDE STANDARD CORE SOLUTION)

- All AUTOSAR standard software functions shall be standardized across OEM- and Supplier [Main100].
- AUTOSAR shall provide a software architecture that is applicable across different functional domains [Main110].
- AUTOSAR shall provide means to clearly check the conformance of an AUTOSAR-implementation with its AUTOSAR-specification [Main120].
- AUTOSAR shall imply only small memory and performance impacts when used in today's micro controllers [Main200].
- AUTOSAR shall support following programming languages: C, C++, Java [Main220].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Definitions of relations between SW components are exhaustive and formal [Main320].
- SW components are protected from illegal access [Main330].
- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

Note: This objective is more precisely with the formulation "… system functions as an OEM and Supplier wide Standard …".

3.1.5 Requirements to achieve the AUTOSAR PO5 (TRANSFERABILITY OF FUNCTIONS THROUGHOUT THE NETWORK)

- AUTOSAR shall provide open and standardized software interfaces for inter- and intra-ECU communication [Main60].
- AUTOSAR shall ease the reusability of software and its concepts and implementations [Main80].
- Tool-chains, which are developed or adapted to AUTOSAR, must be compatible with the AUTOSAR-process [Main90].
- AUTOSAR shall provide an abstraction of the application software from hardware [Main130].

- AUTOSAR shall provide an independency of application software from in-vehicle communication technologies [Main140].
- AUTOSAR should provide an independency of application software from operating systems [Main141].
- AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure [Main150].
- AUTOSAR shall support networks of networks including sub networks [Main230].
- AUTOSAR shall provide means to achieve compositionality [Main250].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- The AUTOSAR architecture must provide dynamic communication pattern [Main280].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Definitions of relations between SW components are exhaustive and formal [Main320].
- SW components are protected from illegal access [Main330].
- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

3.1.6 Requirements to achieve the AUTOSAR PO6 (INTEGRATION OF FUNCTIONAL MODULES FROM MULTIPLE SUPPLIERS)

- AUTOSAR shall provide open and standardized software interfaces for intra-ECU- and inter-ECU communication [Main60].
- AUTOSAR shall provide complete interfaces to application software and basic software modules [Main70].
- AUTOSAR shall ease the reusability of software and its concepts and implementations [Main80].
- Tool-chains, which are developed or adapted to AUTOSAR, must be compatible with the AUTOSAR-process [Main90].
- AUTOSAR shall provide means to clearly check the conformance of an AUTOSAR-implementation with its AUTOSAR-specification [Main120].
- AUTOSAR shall provide an abstraction of the application software from hardware [Main130].
- AUTOSAR shall provide an independency of application software from in-vehicle communication technologies [Main140].
- AUTOSAR should provide an independency of application software from operating systems [Main141].
- AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure [Main150].

- AUTOSAR shall consider protection/unlock mechanisms for software through appropriate services in the infrastructure [Main180].
- AUTOSAR shall provide means to protect SW-Components from malicious SW-components [Main240].
- AUTOSAR shall provide means to achieve compositionality [Main250].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- The AUTOSAR architecture must provide dynamic communication pattern [Main280].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Definitions of relations between SW components are exhaustive and formal [Main320].
- SW components are protected from illegal access [Main330].
- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

3.1.7 Requirements to achieve the AUTOSAR PO7 (MAINTAINABILITY THROUGHOUT THE WHOLE PRODUCT LIFE CYCLE)

- AUTOSAR shall provide complete interfaces to application software and basic software modules [Main70].
- Tool-chains, which are developed for or adapted to AUTOSAR, must be compatible with the AUTOSAR-process [Main90].
- AUTOSAR shall provide an abstraction of the application software from hardware [Main130].
- AUTOSAR shall provide an independency of application software from in-vehicle communication technologies [Main140].
- AUTOSAR should provide an independency of application software from operating systems [Main141].
- AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure [Main150].
- AUTOSAR shall provide a functional interface view of the entire system [Main160].
- AUTOSAR shall provide means to integrate AUTOSAR ECU's in non-AUTOSAR networks [Main210].
- AUTOSAR shall support following programming languages: C, C++, Java [Main220].
- AUTOSAR shall provide diagnostics means during runtime, for production and service purposes [Main260].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- The AUTOSAR architecture must provide dynamic communication pattern [Main280].

- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

3.1.8 Requirements to achieve the AUTOSAR PO8 (INCREASED USE OF COMMERCIAL OFF THE SHELF HARDWARE (COTS))

- AUTOSAR shall provide open and standardized software interfaces for intra-ECU and inter-ECU communication [Main60].
- AUTOSAR shall provide complete interfaces to application software and basic software modules [Main70].
- Tool-chains, which are developed for or adapted to AUTOSAR, must be compatible with the AUTOSAR-process [Main90].
- AUTOSAR shall provide an abstraction of the application software from hardware [Main130].
- AUTOSAR shall provide an independency of application software from in-vehicle communication technologies [Main140].
- AUTOSAR should provide an independency of application software from operating systems [Main141].
- AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure [Main150].
- AUTOSAR shall imply only small memory and performance impacts when used in today's small micro controllers [Main200].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

Remark:
The listed requirements fulfill also the increase of commercial off the shelf software. Especially the bullet encapsulation is essential for commercial off the shelf software (COTS-SW).

3.1.9 Requirements to achieve the AUTOSAR PO9 (Software updates and upgrades over vehicle lifetime)

- AUTOSAR shall provide open and standardized software interfaces for intra-ECU and inter-ECU communication [Main60].
- AUTOSAR shall ease the reusability of software and its concepts and implementations [Main80].
- AUTOSAR shall provide an abstraction of the application software from hardware [Main130].
- AUTOSAR shall provide an independency of application software from in-vehicle communication technologies [Main140].
- AUTOSAR should provide an independency of application software from operating systems [Main141].
- AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure [Main150].
- AUTOSAR shall provide secure access to ECU [Main170].
- AUTOSAR shall imply only small memory and performance impacts when used in today's micro controllers [Main200].
- AUTOSAR shall provide diagnostics means during runtime, for production and service purposes [Main260].
- Releases of AUTOSAR shall be forward and backward compatible [Main270].
- The AUTOSAR architecture must provide dynamic communication pattern [Main280].
- AUTOSAR shall support work-share in large inter-company development groups [Main300].
- AUTOSAR shall support hierarchical design methods [Main310].
- Protection of timing requirements is supported by AUTOSAR [Main340].
- AUTOSAR methods shall be FMEA compatible [Main350].
- Management of vehicle diversity is supported by AUTOSAR [Main360].
- AUTOSAR method shall provide a predefinition of typical roles in work-share method [Main370].
- Basic requirements to change process in design are predefined and supported by AUTOSAR [Main380].

In 3.3 a table is shown, which gives the links from the objectives to the Main Requirements.

3.2 Refinement of the Main Requirements

In the following the Main Requirements are refined.
Note:

1. The Importance Level have following meanings:
   High: Required,
   Medium: Recommended,
   Low: Optional.

2. The use cases in the requirements are given as examples.

3.2.1 [Main10] Using AUTOSAR a system reliability shall be achievable with a failure rate down to 10^{-8} per hour

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	Using AUTOSAR a system reliability shall be achievable with a failure rate down to 10^{-8} per hour.
Type:	New
Importance:	High
Description:	Reliability and availability are defined in [Glossary]. The value of the failure rate $\lambda = 10^{-8}$ per hour is related to safety objectives. AUTOSAR shall provide the means to achieve this target failure rate applying the best current practice.
Rationale:	High reliable systems are necessary in order to run safety-relevant applications.
Use Case:	Steering angle sensor signal has to have a high reliability for the use in the electronic stability program or in active steering. Erroneous signals must be detected that those systems can fall back into a degraded, safe mode.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1)

3.2.2 [Main11] AUTOSAR shall provide means to reduce system down-time

Initiator:	BMW/PSA
Date:	Feb. 7th, 2005
Short Description:	AUTOSAR shall provide means to reduce system down-time.
Type:	New
Importance:	Medium
Description:	Reducing the system down-time increases the availability of a vehicle (see [IEEEElecEng]). Thus, AUTOSAR shall provide to enhance availability during operation or by reducing repair-time to achieve this purpose. Possible examples are: • self-reset, • memory protection, • HW and SW watchdog management, • state management on ECU and system architecture level, • error management, • self-diagnostics, • fast diagnostics in field service based on standardized communications protocols.
Rationale:	Availability of the functionality of a vehicle is highly customer-relevant.
Use Case:	Reduction of repair-time of a vehicle in field-service.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1)

3.2.3 [Main20] AUTOSAR shall provide mechanisms to support redundancy paths

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide mechanisms to support redundancy paths.
Type:	New
Importance:	High
Description:	AUTOSAR shall provide following mechanisms to support redundancy paths: • redundant data handling in SW and/or HW, • agreement, • voting, • activation of redundant units. Redundancy is a solution to achieve reliable, available and safe systems.
Rationale:	Establishing redundancy paths can enhance reliability, availability, and safety at the same time. Note: Redundancy is related to HW, SW, time and value and enables to detect and overcome faults of SW and HW according to the fault hypothesis.
Use Case:	Steering Angle: steering angle-value-signal comes from two independent sensors. The handling of the steering angle signal implies agreement of data.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO2 (3.1.2)

3.2.4 [Main30] A SIL-3-Level compatible development process must be possible with AUTOSAR

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	A development process comparable to IEC 61508 SIL 3 process shall be possible with AUTOSAR.
Type:	New
Importance:	Medium
Description:	AUTOSAR has to deal with E/E-functionalities and their development up to a level of SIL 3 (see [IEC61508-4]). Minimal requirement is that AUTOSAR shall not prevent a SIL 3 development. AUTOSAR should ease a SIL 3 development. AUTOSAR must be compatible with concepts, mechanisms, tools, and processes to handle safety-related systems like IEC61508 (see [IEC61508-4], [IEC61508-7]).
Rationale:	Currently SIL-3-Systems begin to penetrate in vehicle architecture. Caveat: AUTOSAR does not help from itself to master hazards caused outside AUTOSAR. AUTOSAR delivers no support for control hazards coming from outside. E.g. functionality with very poor quality cannot expect help from AUTOSAR to significantly improve its quality if it is integrated into the open environment and architecture. In the best case, AUTOSAR can encapsulate this functionality that other functionalities are not (heavily) affected or damaged.
Use Case:	Active Front Steering is a SIL-3-functionality.
Dependencies:	--

Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1)

3.2.5 [Main50] AUTOSAR shall support inter- and intra-ECU-communication mechanisms with high reliability

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall support inter- and intra-ECU-communication mechanisms with high reliability.
Type:	New
Importance:	High
Description:	To achieve high reliability in communication AUTOSAR shall support concepts to handle erroneous communication channels (e.g. repeat messages or redundant communication paths, see [Main20]) and communication mechanisms like alive-counter, CRC and so on. Note: HW development is not in the focus of AUTOSAR. To ensure [Main50] high quality of HW is a necessary precondition.
Rationale:	Reliable communication is a key-factor for safe operation of E/E-systems.
Use Case:	FlexRay continuation of communication despite erroneous communication channel by switching to a redundant channel.
Dependencies:	--
Conflicts:	Hardware is not in the scope of AUTOSAR. AUTOSAR by itself cannot provide high availability, this must be implemented in the concepts of the functional SW.
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO2 (3.1.2)

3.2.6 [Main60] AUTOSAR shall provide open and standardized software interfaces for intra-ECU and inter-ECU communication

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide open and standardized software interfaces for intra-ECU and inter-ECU communication.
Type:	New
Importance:	High
Description:	The following interfaces shall be standardized: • align the SW architecture to ISO/OSI layered model, • from SW components to AUTOSAR Runtime Environment, • from AUTOSAR RTE to different SW layers below the AUTOSAR RTE. "Open" means here: The specification of a component is open if (1) its interface specification is fully defined and available to the public, and (2) this specification is maintained by a group consensus process.
Rationale:	Using a standardized Software architecture with standardized APIs (see [Glossary]) between the layers supports abstraction of SW components from the hardware. This abstraction leads to an easy integration of different functional modules and the possibility of relocatability of these modules. Furthermore, it is intended to shift parts of AUTOSAR in the future to ISO

	or other standardization bodies. Any misalignment would make this shift futile.
Use Case:	Application SW is developed independently from the underlying infrastructure.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.7 [Main70] AUTOSAR shall provide complete interfaces to application software and basic software modules

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide complete interfaces to application software and basic software modules.
Type:	New
Importance:	Medium
Description:	Due to compatibility and extensibility reasons the interfaces of the software module have to be complete. Complete means that all elements of the interface shall be defined during design time. But this doesn't mean that e.g. all ports must have access to internal (software) functionalities. A remaining number of ports can only be declared (for example as proxies) in this way that extensions to the functionality are easily achieved – without redefinition of the interface. Otherwise this leads regularly to compatibility problems. In some senses the situation can be compared with an ECU-connector where only 8 pins of a 20-pin connector are assigned with electrical wires. The remaining 12 pins are free for further extensions.
Rationale:	Controlling compatibility of interfaces during extension of functionality of SW.
Use Case:	Compatibility handling of all SW-components.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8)

3.2.8 [Main80] AUTOSAR shall ease the reusability of software and its concepts and implementations

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall ease the reusability of software and its concepts and implementations.
Type:	New
Importance:	High
Description:	AUTOSAR shall provide a meta-model of elements to be used for SW

	description. With using the meta model, a reuse of SW components provided as description, simulation model, source code and in a second step object code should be eased. Further on SW components below the AUTOSAR RTE should easily be reusable as well. AUTOSAR should provide for the car domains a partitioning of the functionality into reusable SW-components. A tool to check the compatibility of the SW components shall be provided.
Rationale:	SW Reuse is one of the major aims of AUTOSAR. SW what shall be transferred to another ECU must be reusable. Otherwise integration into to the new environment is impossible.
Use Case:	Momentum control in different ECU.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO9 (3.1.9)

3.2.9 [Main90] Tool-chains, which are developed for or adapted to AUTOSAR, must be compatible with the AUTOSAR process

Initiator:	PL Team
Date:	Jan. 24th, 2004
Short Description:	Tool-chains, which are developed for or adapted to AUTOSAR, must be compatible with the AUTOSAR process.
Type:	New
Importance:	High
Description:	New tools shall be developed to implement the AUTOSAR process. Existing tools must be adapted in this way that they are conformant with the AUTOSAR process (input data consumption, and output data production) AUTOSAR shall provide standards for data exchange formats covering information needed during the AUTOSAR generation process. Those tools are modeling tools, simulation tools, compilers, linkers, debugging tools, configurators, and generators.
Rationale:	It is to be expected that AUTOSAR needs a good tool support in each activity of the process. Thus, tool-chains must follow the AUTOSAR process.
Use Case:	Tools must be able to utilize the AUTOSAR input data and produce the AUTOSAR output data for a specific activity in the process.
Dependencies:	[Main370] requires the description of a uniform AUTOSAR process within the AUTOSAR standardization.
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8)

3.2.10 [Main100] All AUTOSAR standard software functions shall be standardized across OEM and Supplier

Initiator:	PL Team
Date:	Nov. 19th, 2003

Short Description:	All AUTOSAR standard software functions shall be standardized across OEM and Supplier.
Type:	New
Importance:	High
Description:	The Basic Software provides the infrastructural (schematic dependent and schematic independent) functionalities of an ECU. It consists of ECU Firmware (see [Glossary]) and Standard Software (see [Glossary]). Standard software does not implement functionality, which can be recognized by the customer. This kind of services is needed in all ECU. The APIs and the content/functionality shall be standardized. Common implementations should be used.
Rationale:	Hence, it makes sense to define, implement, and test the basic software once but integrating this in many ECU's of an E/E-architecture. Achieving this for many OEMs one reaches an OEM-wide standard for the purpose of interchangeability. The suppliers then have stable foundation for implementing their application without bothering about details of the basic software. Standardization leads in general to higher quality und lower costs (development, marketing, maintenance) of the regarded elements with defined and well-known properties.
Use Case:	Compatibility of the basic SW with defined quality and maintenance is achieved. The BMW, DC, VW Standard Core were introduced for the purpose of company internal standardization.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO4 (3.1.4)

3.2.11 [Main110] AUTOSAR shall provide a software architecture that is applicable across different functional domains

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide a software architecture that is applicable across different functional domains.
Type :	New
Importance:	Medium
Description:	The AUTOSAR software architecture shall be defined as a general architecture across the functional domains, which can be found in vehicles. The functional domains are: • body/comfort, • power train, • chassis, • safety, • multimedia/telematics, • human-machine-interface. In a first AUTOSAR release the architecture shall be applicable in the functional domains body/comfort, power train, chassis, and safety. The architecture may be applicable in the functional domains multimedia/telematics MM/T and human-machine-interface HMI.
Rationale:	A common architecture across the functional domains allows the relocatability of software components across domains.

	It increases the degree of freedom at generating the E/E system.
Use Case:	Apply the software architecture at least to one ECU at each functional domain.
Dependencies:	--
Conflicts:	The integration of all needs, which are required in MM/T and HMI domain, seems to be not achievable in the 1st phase of AUTOSAR, because in these domains more powerful OS and multiprocessor ECU's are convenient. In any case, the AUTOSAR architecture shall provide a stable interface to the domains MM/T and HMI.
Supporting Material:	AUTOSAR PO4 (3.1.4)

3.2.12 [Main120] AUTOSAR shall provide means to clearly check the conformance of an AUTOSAR-implementation with its AUTOSAR-specification

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide means to clearly check the conformance of an AUTOSAR-implementation with its AUTOSAR-specification.
Type:	New
Importance:	High
Description:	AUTOSAR shall develop criteria that define AUTOSAR conformance. Criteria shall be developed for implementations of AUTOSAR basic software functionalities and application SW components. Difference between both: application software components have only to be AUTOSAR conformant by its interface definition and description methodologies; in addition basic software shall be AUTOSAR conformant by its functional behavior. Criteria shall be developed for tools, which support the AUTOSAR process. AUTOSAR shall provide mechanisms to ensure that implementations are AUTOSAR conformant.
Rationale:	This requirement is a basic assumption of AUTOSAR: each product that is called AUTOSAR conformant shall be conformant to the specification from which is implemented/produced. Thus, there is a strong need for conformance methods/testing/specification i.e. the conformance ensures a certain behavior of the regarded elements.
Use Case:	Integration of the infrastructure SW into a specific ECU, bring it into the E/E-architecture without backlashes on the system. Example from real world: OSEK (NM, COM, OS) as the kernel of the basic software did compile conformance specification and test suites.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO6 (3.1.6)

3.2.13 [Main130] AUTOSAR shall provide an abstraction of the application software from hardware

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide an abstraction of the application software from hardware.
Type:	Change Main130
Importance:	High
Description:	The application SW shall be abstracted from the hardware. Thus, the SW-layers below the applications shall guarantee the abstraction from the HW.
Rationale:	Today's ECU's in the automotive domain in general have no abstraction from the hardware. This leads to at least reengineering of the SW if the HW is changed (e.g. new microcontroller family). This effort is not longer acceptable.
Use Case:	Relocate SW application from one ECU with hardware A to ECU with hardware B without changes of the SW application.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.14 [Main140] AUTOSAR shall provide an independency of application software from in-vehicle communication technologies

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide an independency of application software from in-vehicle communication technologies.
Type:	New
Importance:	High
Description:	AUTOSAR shall support different communication technologies. Considered communication systems are CAN, MOST, LIN, FlexRay for the purpose of inter-ECU communication. Others like IEEE1394 (see [IEEE1394]) or MML can follow later. Communication systems have to be at least industry standard solutions. Communication from the in-car network to the outside world is currently not in the focus of AUTOSAR. With respect to its openness an integration of e.g. GSM, WLAN, Bluetooth or IrDA is expected to achieve much easier with AUTOSAR architecture.
Rationale:	The relocatability of application SW is one of the most important objectives of AUTOSAR. For this purpose the application must be independent from communication technologies and operating systems.
Use Case:	Relocation of SW component from ECU A with CAN-Bus to ECU B with MOST.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6)

	▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.15 [Main141] AUTOSAR should provide an independency of application software from operating systems

Initiator:	PL Team
Date:	Sept. 14th, 2004
Short Description:	AUTOSAR should provide an independency of application software from operating systems.
Type:	New
Importance:	Medium
Description:	AUTOSAR should support several operating systems. Operating systems are OSEK, OSEK^{Time}, QNX, VxWorks, Win CE, Embedded Linux, and uITRON (the list is not exhaustive).
Rationale:	The relocatability of application SW is one of the most important objectives of AUTOSAR. For this purpose the application must be independent from operating systems.
Use Case:	Relocation of SW component from ECU A with OSEK to ECU B with QNX.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.16 [Main150] AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide mechanisms, methods, processes, and tools to encapsulate application software from the infrastructure.
Type:	Change Main150
Importance:	High
Description:	Encapsulation of the functional software supports the relocatability and reuse of the functional software. Thus, AUTOSAR has to deal deeply with mechanisms, methods, tools, and processes to achieve this. In difference to the requirements [Main140] and [Main141] this requirement [Main150] gives an requirement how to handle encapsulation of application SW.
Rationale:	In addition to the standardized APIs mentioned in other requirements AUTOSAR shall provide scheduling mechanisms, etc that allow integration of separate SW components into one ECU.
Use Case:	Relocation of yaw rate control from one ECU to another. Current situation is: more or less each component implements its own one. The encapsulation of this functionality gives the opportunity to relocate a valuable solution to another company for integration into its ECU.
Dependencies:	--
Conflicts:	--

Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.17 [Main160] AUTOSAR shall provide a functional interface view of the entire system

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide a functional interface view of the entire system.
Type:	New
Importance:	Medium
Description:	A functional decomposition is essential for an appropriate functional clustering and partitioning in the SW-components. This leads to a logical architecture of the entire system and the functional interfaces.
Rationale:	Appropriate SW/SW-partitioning bases on functional decomposition.
Use Case:	SW/SW-partitioning.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO7 (3.1.7)

3.2.18 [Main170] AUTOSAR shall provide secure access to ECU

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide secure access to ECU.
Type:	New
Importance:	Medium
Description:	AUTOSAR shall provide secure access to ECU, (e.g. by user authentication), including standardized up- and download of data and software. For this mechanisms and methods shall be defined.
Rationale:	The update and upgrade feasibility provided by AUTOSAR includes technical challenges (e.g. standardized up-/download protocol, partly update of the software) and mechanisms (e.g. how to authorize the user).
Use Case:	Download of dedicated SW-components in ECU.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO9 (3.1.9)

3.2.19 [Main180] AUTOSAR shall provide protection/unlock mechanisms for software through appropriate services in the infrastructure

Initiator:	PL Team
Date:	Nov. 19th, 2003
Short Description:	AUTOSAR shall provide protection/unlock mechanisms for software through appropriate services in the infrastructure.
Type:	New

Importance:	High
Description:	Integration of software of different suppliers requires exchange of software (esp. source code) between the different parties involved. Thus, AUTOSAR shall provide mechanisms to safe-guard software. AUTOSAR shall ensure a smooth integration process that at the same time protects intellectual property of the companies involved.
Rationale:	Integration of third party solutions requires dealing with intellectual property issues.
Use Case:	1) SW sale of split-screen software for navigation. 2) Integration of BSW modules of different suppliers.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO6 (3.1.6)

3.2.20 [Main190] AUTOSAR shall provide interoperability with legacy software

Initiator:	PL Team
Date:	Feb 13th, 2004
Short Description:	AUTOSAR shall provide interoperability with legacy software.
Type:	New
Importance:	High
Description:	AUTOSAR must not require that all E/E functionality of a car be developed with AUTOSAR technology. Integration of legacy software blocks (ECU abstraction and/or Complex Device Drivers) in an ECU that is developed according to the AUTOSAR process shall be supported. For this purpose, a minimum set of imported interfaces shall be given to ensure that an OS scheduler does not exist twice. Note: It is important to clarify that the interface definitions of the AUTOSAR architecture are not touched by the integration of legacy software. Otherwise the interoperability cannot be achieved.
Rationale:	A smooth integration of the AUTOSAR process requires that software from existing cars can be reused.
Use Case:	Reuse of existing complex device drivers for a new ECU that is developed according to AUTOSAR.
Dependencies:	--
Conflicts:	Conflict with [Main100]: Legacy SW may have other interfaces than the AUTOSAR architecture. In this case the legacy SW has to be redesigned in accordance to the rules of AUTOSAR.
Supporting Material:	▪ AUTOSAR PO3 (3.1.3)

3.2.21 [Main200] AUTOSAR shall imply only small memory and performance impacts when used in today's micro controllers

Initiator:	DC
Date:	Mar 18th, 2004
Short Description:	AUTOSAR shall imply only small memory and performance impacts when used in today's micro controllers.
Type:	New
Importance:	Medium
Description:	AUTOSAR shall support 16 bit controllers/processors and bigger ones. All Basic Software including Runtime Environment and a small

	application should fit into 64KByte of ROM.
Rationale:	It can be expected that concerns over a potentially unacceptable overhead in terms of processing and memory needs implied by AUTOSAR will occur. The acceptance and utilization of AUTOSAR does such depend heavily on these resource needs and the possibilities for optimization.
Use Case:	Integration of the AUTOSAR architecture and a single application in an 16-bit microcontroller and with memory amount less than 64KByte ROM.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO9 (3.1.9)

3.2.22 [Main210] AUTOSAR shall provide means to integrate AUTOSAR ECU's in non-AUTOSAR networks

Initiator:	DC
Date:	Mar 18th, 2004
Short Description:	AUTOSAR shall provide means to integrate AUTOSAR ECU's in non-AUTOSAR networks.
Type:	New
Importance:	High
Description:	Integration of AUTOSAR ECU in non-AUTOSAR network shall be possible and supported during the development process. Note: A mix-up of AUTOSAR ECU and non-AUTOSAR ECU may lead to conflicts in the infrastructure functionalities like network management, COM or diagnostics.
Rationale:	This opens a migration path for the application of AUTOSAR into existing non-AUTOSAR architectures.
Use Case:	Integration of an AUTOSAR-ECU into a non-AUTOSAR network.
Dependencies:	--
Conflicts:	Conflict with [Main100]. Ability to relocate SW-Components might be limited in this use case. One option is to modify the AUTOSAR-ECU to make it fit into the non-AUTOSAR network. Modification can mean either leaving out some modules, or replacing them with OEM-specific modules (i.e. compliant to the interfaces but with specific behavior).
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO7 (3.1.7)

3.2.23 [Main220] AUTOSAR shall support following programming languages: C, C++, Java

Initiator:	DC
Date:	Mar 18th, 2004
Short Description:	AUTOSAR shall support following programming languages: C, C++, Java.
Type:	New
Importance:	Medium
Description:	In today's embedded systems only a small range of programming languages are used: C, C++, and Java. Due to its differences the

	methods, mechanisms, processes and tools in AUTOSAR shall take this into account (independency where possible, some dependencies where necessary). To ensure flexibility / extensibility for the future AUTOSAR should support object-oriented techniques.
Rationale:	A useful reduction of programming languages to current programming languages reduces the impacts on AUTOSAR definitions and specifications due to logical and/or technical differences of different programming languages.
Use Case:	AUTOSAR implementation in C, C++, or Java.
Dependencies:	--
Conflicts:	Usage of C++ and in particular Java may not be appropriate for some lower performing and legacy ECU platforms.
Supporting Material:	▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO7 (3.1.7)

3.2.24 [Main230] AUTOSAR shall support networks of networks including sub networks

Initiator:	DC
Date:	Mar 18th, 2004
Short Description:	AUTOSAR shall support networks of networks including sub networks.
Type:	New
Importance:	High
Description:	AUTOSAR shall handle net topologies with multiple networks and different in-vehicle network technologies. These networks shall be connected via bridges, repeaters or gateways.
Rationale:	See Use Case.
Use Case:	Today's network topologies of E/E-architectures in series production.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO5 (3.1.5)

3.2.25 [Main240] AUTOSAR shall provide means to protect SW-Components from malicious SW-components

Initiator:	DC
Date:	Mar 18th, 2004
Short Description:	AUTOSAR shall provide means to protect SW-Components from malicious SW-components.
Type:	New
Importance:	High
Description:	A malicious SW component shall not have serious impacts on other SW components due to single point of failure and/or error propagation.
Rationale:	Protection of SW-components is necessary because the integration of third-party SW is one of the most important use cases of AUTOSAR.
Use Case:	Corrupted SW component is integrated into ECU. The ECU remains stable and the environment of this SW component is not affected due to intra-ECU and/or inter-ECU communication.
Dependencies:	--
Conflicts:	--

Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO6 (3.1.6)

3.2.26 [Main250] AUTOSAR shall provide means to achieve compositionality

Initiator:	BMW
Date:	Mar 25th, 2004
Short Description:	AUTOSAR shall provide means to achieve compositionality
Type:	New
Importance:	High
Description:	Compositionality helps to decouple functionalities within the architecture during designing, testing and integration. A SW component or system shall meet its timing requirements independent of the overall load and configuration.
Rationale:	The easy integration of new functions without changing the interface definitions.
Use Case:	A new component or subsystem can be added to a system without changing the behavior of the original components or system.
Dependencies:	Compositionality as a whole can only be achieved by using e.g. time triggered protocols, specific OS services.
Conflicts:	Using CAN or MOST compositionality can not (strictly) be achieved (needs to consider acceptable tolerances in timing aspects).
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6)

3.2.27 [Main260] AUTOSAR shall provide diagnostics means during runtime, for production and services purposes

Initiator:	BMW
Date:	May 7th, 2004
Short Description:	AUTOSAR shall provide diagnostics means during runtime, for production and service purposes.
Type:	New
Importance:	High
Description:	AUTOSAR shall at least support diagnostics standards like ISO14229 or OBD. Specifications of error handling must be developed. Furthermore, AUTOSAR shall reflect the invention of encapsulated SW in its diagnostics specifications.
Rationale:	Standardized diagnostics is necessary for field service and admission.
Use Case:	Diagnosis of an encapsulated SW function or a ECU.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO9 (3.1.9)

3.2.28 [Main270] Releases and revisions of AUTOSAR shall be backward compatible

Initiator:	BMW
Date:	May 7th, 2004
Short Description:	Releases and revisions of AUTOSAR shall be backward compatible.
Type:	New
Importance:	High
Description:	Migration from a previous AUTOSAR release/revision to the latest release/revision shall be supported well. Backward compatibility shall be managed throughout the development of a new release/revision in relation to the previous release/revision.
Rationale:	Backward compatibility ensures a long time usage of the AUTOSAR standard.
Use Case:	Integration of ECU's using infrastructure software of the latest AUTOSAR release /revision in a network built from ECU's using a former release/revision. Re-use of SW-Cs being developed for a previous release/revision in the latest release/revision of AUTOSAR.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.29 [Main280] The AUTOSAR architecture must provide dynamic communication pattern

Initiator:	BMW
Date:	May 17th, 2004
Short Description:	The AUTOSAR architecture must provide dynamic communication pattern.
Type:	New
Importance:	Low
Description:	Communication mechanisms must support a certain amount of dynamic behavior. This means that during design time all potential communication partners have to be specified and declared. Note: In the first release for the purpose of commercial exploitation Dynamical reconfiguration of the architecture and/or dynamical relocation of software during runtime shall not be part of the AUTOSAR architecture.
Rationale:	Dynamic communication patterns are well known in the MOST technology.
Use Case:	A SW component can establish communication connections to another SW component during run-time as long this was already defined in the design process.
Dependencies:	--
Conflicts:	Dynamical reconfiguration/relocation is an important issue for the multimedia/telematics and man-machine-interface domain. Thus, [Main280] is in conflict with requirement [Main110]. On the other hand dynamical reconfiguration/relocation is not allowed

	within a SIL-Level3 System. In further releases of AUTOSAR careful observation of [Main280] and [Main30] must take into account.
Supporting Material:	▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO9 (3.1.9)

3.2.30 [Main290] AUTOSAR shall ensure the verification of all processes and products developed within AUTOSAR

Initiator:	BMW
Date:	May 20th, 2004
Short Description:	AUTOSAR shall ensure the verification of all methods, processes and products developed within AUTOSAR.
Type:	New
Importance:	Medium
Description:	To enable a SIL3 development all processes and products, which are developed within the partnership must be at least verifiable. Verification is here defined by: The act of reviewing, inspecting, testing, checking, auditing, or otherwise establishing and documenting whether items, processes, services, or documents conform to specified requirements (see [IEEEElecEng]). AUTOSAR shall support a certification of all processes and products following accepted standards (e.g. IEC61508).
Rationale:	Verification of all processes and products is a must of SIL3 development.
Use Case:	Verification of Active Front Steering (SIL3 development).
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1)

3.2.31 [Main300] AUTOSAR shall support work-share in large inter-company development groups

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	AUTOSAR shall support work-share in large inter- company development groups.
Type:	New
Importance:	Medium
Description:	Requirement comprises sub-requirements: hierarchical design methods supported, interface definitions supported, encapsulation of variables supported, protected scheduling definitions supported, FMEA compatible design methods supported, support of car diversity, definition of roles in work share, change process in design, protection of intellectual property.
Rationale:	The AUTOSAR virtual functional bus VFB is expected to carry 10 000 to 30 000 signals per vehicle. To develop vehicle descriptions in this size a good organization of work-share is needed. AUTOSAR tools support this work-sharing process.
Use Case:	Data sharing between OEM and 1st Tier supplier.
Dependencies:	--
Conflicts:	--

Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.32 [Main310] AUTOSAR shall support hierarchical design methods

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	AUTOSAR shall support hierarchical design methods.
Type:	New
Importance:	High
Description:	It must be possible to structure SW components in a hierarchical way, so that only links to outside SW components need to be treated / adapted / changed in the next hierarchical level.
Rationale:	Objective is to allow each actor in the development chain to focus on the required level and tasks.
Use Case:	SW development of an engine management system can only be achieved by using hierarchical strategies.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO9 (3.1.9)

3.2.33 [Main320] Definitions of relations between SW components are exhaustive and formal

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	Definitions of relations between SW components are exhaustive and formal.
Type:	New
Importance:	High
Description:	In AUTOSAR it is possible to describe all requirements of SW components / SW- compositions to their outside links, such that subsequent engineering can check their work result against these requirements.
Rationale:	It has to be defined, which requirements need to be described and where these requirements need to be described. Potential requirements are timing requirements, max delay requirements, requirement of availability of specific other SW components in specific release states etc. Potential solutions for the requirements locations are the attributes of the connectors, as well in the class, group or instance requirements.
Use Case:	SW component is designed by OEM and a 1st Tier Supplier shall integrate this SW component into an ECU. In this case exhaustive and

	formal description of the API is necessary
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO2 (3.1.2) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6)

3.2.34 [Main330] SW components are protected from illegal access

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	SW components are protected from illegal access.
Type:	New
Importance:	Medium
Description:	AUTOSAR method supports SW component protection in the way that write-access to inner variables of a SW component is impossible. Write access to exported variables (e.g. provide ports) is possible only from the variable owning component. One potential solution is encapsulation. Here only the way how to deal with variables within a SW component shall be protected.
Rationale:	Need to ensure responsibility for the SW component by component author.
Use Case:	Changes of inner variables of a SW component can only by performed by the component author.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6)

3.2.35 [Main340] Protection of timing requirements is supported by AUTOSAR

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	Protection of timing requirements is supported by AUTOSAR.
Type:	New
Importance:	Medium
Description:	AUTOSAR method and mechanisms allow describing exhaustively and protect timing requirements of SW components / compositions and complex device drivers. This includes dataflow and control flow related requirements.
Rationale:	E.g. complex device drivers have specific timing requirements, which are not to be overwritten by higher level changes.
Use Case:	Real time control of today's gasoline injection systems.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO4 (3.1.4)

	▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.36 [Main350] AUTOSAR methods shall be FMEA compatible

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	AUTOSAR methods shall be FMEA compatible.
Type:	New
Importance:	High
Description:	Boundary conditions to FMEA or fault tree analysis per function, atomic SW component and composition is documented with the related class, group and instance such that the non-fulfillment of these conditions is likely to be recognized and submitted to the related change process.
Rationale:	Shifting a SW component from one ECU to another is typically changing the FMEA related assumptions. Same holds true related to changes in signal timing etc. These changes might be necessary to achieve efficient implementations. It is however by no means acceptable that these changes happen accidentally and unmanaged.
Use Case:	FMEA is very common in the automotive industry.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.37 [Main360] Management of vehicle diversity is supported by AUTOSAR

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	Management of vehicle diversity is supported by AUTOSAR.
Type:	New
Importance:	Medium
Description:	Diversity management is introduced on vehicle level. This enables formal check of compatibility of SW components, management of availability of partner SW components in vehicle versions their release state etc. Also the number of required SW versions per ECU integration can be evaluated and tracked with reasonable effort.
Rationale:	Diversity of e.g. a wiring harness is reaching the amount of 10 000 to 1.000.000 different versions for the same vehicle platform. Same diversity requirements multiplied with the version management per SW component applies for the entity of the SW on the vehicle level. Unmanaged this effect can lead to deadlock situations in the logistic of vehicle SW. Potential implementations are e.g. "existence" property matrix per class,

	group and instance of SW components and connections.
Use Case:	Integration of SW components in different ECUs and/or E/E-architectures.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.38 [Main370] AUTOSAR process shall provide a predefinition of typical roles and activities in work-share method

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	AUTOSAR process shall provide a predefinition of typical roles and activities in work-share method.
Type:	New
Importance:	High
Description:	Work-share requires visibility and common understanding of specific roles and activities in the design process. Roles could be e.g. vehicle architect, domain architect, ECU integrator, function designer. Roles could also be found related to different disciplines like static architecture, dynamic architecture, communication architect, etc. Typical activities could be e.g. SW/SW partitioning, mapping of SW to ECU, configuration of Basic Software.
Rationale:	This definition serves the understanding of workflow for the design of the tools. Individual roles and activities might be combined to one person in the later application, or distributed differently. This also does not assign tasks to OEM or Tier1 suppliers. Application of later work-share-distribution is matter of individual contracts between the parties.
Use Case:	System architect or SW component developer are such roles which shall be predefined.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.2.39 [Main380] Basic requirements to change process in design are predefined and supported by AUTOSAR

Initiator:	SiemensVDO
Date:	May 2004
Short Description:	Basic requirements to change process in design are predefined and

	supported by AUTOSAR.
Type:	New
Importance:	Medium
Description:	Change process in its basic requirements is defined such that SW component providers can take warrant for their deliverables.
Rationale:	Changes in each hierarchical level on the VFB can influence timing, FMEA assumptions, FMEA related requirements of the under laying SW components as well as of those SW components which communicate directly or indirectly with the directly affected SW component. A change process has to be defined such that designers of SW components are responsible to release these changes. This process might need some formal support by the AUTOSAR tools.
Use Case:	Change of SW component designed by OEM and its integration in 1st Tier Supplier ECU.
Dependencies:	--
Conflicts:	--
Supporting Material:	▪ AUTOSAR PO1 (3.1.1) ▪ AUTOSAR PO3 (3.1.3) ▪ AUTOSAR PO4 (3.1.4) ▪ AUTOSAR PO5 (3.1.5) ▪ AUTOSAR PO6 (3.1.6) ▪ AUTOSAR PO7 (3.1.7) ▪ AUTOSAR PO8 (3.1.8) ▪ AUTOSAR PO9 (3.1.9)

3.3 Mapping of the Project Objectives and the Main Requirements

The following table shows the relationship of the project objectives with the main requirements. The symbol "+" is used for compliant requirements. The symbol "-" indicates contradictory requirements.

	Project Objectives								
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9
Main Requirements									
Main10	+								
Main11	+								
Main20	+	+							
Main30	+								
Main50	+								
Main60			+		+			+	+
Main70			+						
Main80			+		+	+			+
Main90						+	+	+	
Main100				+					
Main110				+					
Main120	+			+		+			
Main130	+				+	+	+	+	+
Main140	+				+	+	+	+	+
Main141	+				+	+	+	+	+
Main150	+				+	+	+	+	+
Main160							+		
Main170									+
Main180						+			
[Main190			+						
Main200			+	+					+
Main210			+				+		
Main220				+			+		
Main230			+		+				
Main240	+					+			
Main250	+				+	+			
Main260	+						+		+
Main270			+	+	+	+	+	+	+
Main280			+		+	+	+		+
Main290	+								
Main300	+		+	+	+	+	+	+	+
Main310	+		+	+	+	+	+		+
Main320	+	+	+	+	+	+			
Main330	+			+	+	+			
Main340	+			+	+	+	+	+	+
Main350	+		+	+	+	+	+	+	+
Main360	+		+	+	+	+	+	+	+
Main370	+		+	+	+	+	+	+	+
Main380	+		+	+	+	+	+	+	+

4 References

[Glossary] Glossary,
AUTOSAR_Glossary.pdf

[IEC61508-4] Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 4: Definitions and abbreviations,
International Electrotechnical Commission

[IEC61508-7] Functional safety of electrical/electronical/programmable electronic safety-related systems – Part 7: Overview of techniques and measures,
International Electrotechnical Commission

[IEEE1394] FireWire Bus,
standardized by IEEE

[IEEEElecEng] The Electrical Engineering Handbook,
Editor R. C. Dorf, CRC Press