Document Title	Requirements on Diagnostic
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	004

Document Status	Final
Part of AUTOSAR Standard	Foundation
Part of Standard Release	1.3.0

Document Change History

Date	Release	Changed by	Description
2017-12-08	1.3.0	AUTOSAR Release Management	• Minor corrections • Update of requirements tracing
2017-10-27	1.2.0	AUTOSAR Release Management	• Restructured document • New requirments for CP and AP • Common requirements for CP and AP
2017-03-31	1.1.0	AUTOSAR Release Management	• Merge and alignment with AP requirements • Restructured chapter 4 • Removed reference to HIS
2016-11-30	1.0.0	AUTOSAR Release Management	• –Migration of document to standard "Foundation"– • Additional requirements for ISO14229-1 conformance • Parallel access for DEM • Parallel processing of OBD and UDS services • Independent fault memory access for virtual ECUs
2015-07-31	4.2.2	AUTOSAR Release Management	• Clarification of bootloader interaction • Interfaces for DCM communication via PDU router • Rework of document structure

2014-10-31	4.2.1	AUTOSAR Release Management	• Support of WWH-OBD (Major change) • Support of UDS service $38 (”RequestFileTransfer”), (Change) • Added new requirements for runtime errors and transient errors (Change) • Aging of events (Change)
2014-03-31	4.1.3	AUTOSAR Release Management	• New requirement for processing a new request in DEM • New requirement for event management mechanisms in DEM
2013-03-15	4.1.1	AUTOSAR Release Management	• OBD-specific configuration capabilities in DCM and DEM • Event de-bouncing in DEM • Freeze Frame and Extended Data Record handling in DEM • Support of SAE J1939 • Link Requiriement with BSW Feature Document • Updating format of requirements according to TPS_StandardizationTemplate
2011-12-22	4.0.3	AUTOSAR Release Management	• Clarification of DET functionality • Formal Rework for Requirements Tracing
2011-04-15	4.0.2	AUTOSAR Release Management	• Clarification of DET functionality (remove BSW04088)
2010-09-30	3.1.5	AUTOSAR Release Management	• Document structure reworked and extended • Improvement of DEM behavior description • Introduce the approach for functional diagnostics of SW-Cs • Added requirements for further diagnostic modules (DLT/DET) • Legal disclaimer revised

2008-08-13	3.1.1	AUTOSAR Release Management	• Remove requirement BSW04062 • Added requirement [SRS_Diag_04082] for OBDII support • Legal disclaimer revised
2007-12-21	3.0.1	AUTOSAR Release Management	• Document meta information extended • Small layout adaptations made
2007-01-24	2.1.15	AUTOSAR Release Management	• ”Advice for users” revised • ”Revision Information” added
2006-11-28	2.1	AUTOSAR Release Management	• Legal Disclaimer revised
2006-05-16	2.0	AUTOSAR Release Management	• Minor formal changes
2005-05-31	1.0	AUTOSAR Release Management	• Initial Release

Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

Table of Contents

1 Scope of the Document

This document specifies system requirements of the Diagnostic Manager. It is meant to be independent of any particular implementation and it contains foundation requirements, common to AUTOSAR classical and adaptive platform, as well as requirements specific to the AUTOSAR classic and Adaptive Platform .

In the Classic Platform chapter the handling of the legislated OBD and enhanced Diagnostics shall be achieved. As far as possible the set of diagnostic basic software elements should consist of already existing elements of modules of automotive software. Only in case of good reasons valid elements of basic software should be part of the set. If such the definition of these valid elements is not part of this work package. Nevertheless the information about basic software elements additionally required shall be given to related work groups.

In the Adaptive Platform chapter, some constraints should be notify related to the Adaptive environment : - only support for Ethernet as physical communication infrastructure will be provided, and no other typical bus communication is planned for release 1.0; on these grounds, all classical SRS Diagnostics requirements referring to standards (i.e. J1939) considering other bus protocols (i.e. FlexRay, CAN ..) were not considered in this specification
- due to insufficient information about the car domains where the AUTOSAR Adaptive Platform will apply, OBD protocol (standardized as ISO 15031) is also not subject of this specification
- Release 1.0 of AUTOSAR Adaptive Platform is planned to be a learning environment for future development as a consequence its interfaces are described with ICC1 (Interface Conformance Class) granularity level, meaning that no internal DM interfaces are to be specified

2 Acronyms and Abbreviations

Abbreviation / Acronym:	Description:
CAN	Controller Area Network (communication bus)
Dem	Diagnostic Event Manager
DID	Diagnostic Identifier
DM	Diagnostic Management
DoIP	Diagnostic over IP - transport protocol for diagnostic services standardized as ISO 13400

DTC	Diagnostic Trouble Code
ECU	Electronic Control Unit
IDL	Interface Description Language
OBD	On-board Diagnostic (standardized as ISO 15031)
RTE	Runtime Environment
SA	Source Address (diagnostics address of the tester)
SID	Service Identifier (hexa number to uniquely identify UDS services) 0x22 for Read Data by Identifier service 0x2E for Write to Non-Volatile memory service
SWC	Software Component (could refer either to classical Autosar SW-C or to dynamic SW-C)
TA	Target Address (diagnostic address of the ECU)
UDS	Unified Diagnostic Specification standardized as ISO 14229

Table 2.1: table:acronyms

3 Conventions to be used

In requirements, the following specific semantics are used :

The key words ”MUST”, ”MUST NOT”, ”REQUIRED”, ”SHALL”, ”SHALL NOT”, ”SHOULD”, ”SHOULD NOT”, ”RECOMMENDED”, ”MAY” and ”OPTIONAL” in this document are to be interpreted . Note that the requirement level of the document in which they are used modifies the force of these words.

- SHALL: This word means that the definition is an absolute requirement of the specification.
- SHALL NOT: This phrase means that the definition is an absolute prohibition of the specification.
- 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 inter operate 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 inter operate with another implementation, which does not include the option (except, of course, for the feature the option provides).

4 Requirements Specification

4.1 Common Diagnostic requirements for Classic and Adaptive Platform

[SRS_Diag_04200] Support event combination ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall allow combining several individual events to trigger a single DTC.
Rationale:	Advanced fault analysis
Applies to:	CP, AP
Dependencies:	–
Use Case:	Improved clustering and judging of events/faults. Several internal hardware faults of an electronic control unit can be mapped onto a single "ECU internal" failure to reduce the number of Diagnostic Trouble Codes shown to the technician in the service workshop.

⌋(*RS_Main_00260*)

[SRS_Diag_04150] Support the primary fault memory defined by ISO 14229-1 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the primary fault memory defined by ISO 14229-1.
Rationale:	Storage of fault information for workshops.
Applies to:	CP, AP
Dependencies:	Production line, garage after reparation,...

Use Case:	The primary fault memory is used to store fault information that is related to defects in the vehicle and helps the workshops to identify the fault and repair it.
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04214] Support the user defined fault memories defined by ISO 14229-1 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the user defined fault memories defined by ISO 14229-1.
Rationale:	Independent storage of fault information.
Use Case:	User defined fault memories are used by OEM and Tier1 during development or for storing warranty relevant information inside. This information is not relevant for workshops or repairing the vehicle.
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO 14229-1 v.2013

⌋(*RS_Main_00260*)

[SRS_Diag_04068] Event specific debounce algorithms ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support event specific debounce counters to improve signal quality internally. The following types of debounce mechanisms shall be supported: According to ISO 14229-1 Appendix D, the diagnostic in AUTOSAR module shall provide the ability to configure the jump behavior including jump up and jump down threshold value of the debounce counter in case of pre-passed or pre-failed event reporting. If failure detection jitters (e.g. sporadically reported pre-passed events), failure detection must not be delayed or prevented. For example, a monitoring configuration does NOT use jumpdown to avoid losing an event reporting a pre-failed status. The provision of jumping behavior of the debounce counter shall ensure the failure detection time because debouncing always starts from a defined starting point. The time based debouncing use a configurable time instead of counter threshold. The time is reloaded and running after the last monitor result/event status is different to the previous. After the time is exceeded the event has qualified. The following debouncing mechanisms shall be supported: • counter based (According to ISO 14229-1 Appendix D); • time based; • handling of external debouncing.
Rationale:	Advanced fault analysis
Use Case:	All applications and system modules can report events. The diagnostic module processes all these events and is able to provide a central de-bounce behavior for event classification and status management.
Applies to:	CP

Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04115] The optional parameter DTCSettingControlOptionRecord as part of UDS service ControlDTCSetting shall be limited to GroupOfDTC ⌈

Type:	Valid
Description:	ISO14229-1 does not specify how the parameter DTCSettingControlOptionRecord needs to be used. Therefore, the usage of the parameter shall be limited to GroupOfDTC.
Rationale:	Currently, no other use case for parameter DTCSettingControlOptionRecord is known than the usage for GroupOfDTC.
Use Case:	Fault storage is activated and deactivated for one specific DTC or for all DTCs.
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00260*)

[SRS_Diag_04164] Independent event memories for multiple diagnostic server instances (virtual ECUs) ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide multiple sets of independent event memories that can store information independently from each other.
Rationale:	Individual assignment of fault memories to dedicated diagnostic servers.
Use Case:	ECUs with multiple independent diagnostic servers. Common faults of the host ECU shall be stored in each of the virtual ECU which is affected by such a fault. Common faults need to be stored in each virtual ECU to ensure that storing and clearing of fault entries has no or little side-effects with the information stored in other virtual ECUs. This use-case assumes that the cost to store a common fault in multiple event memory entries is accepted because sharing of a single event memory entry may have unintended side-effects.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04064] Buffers of scalable sizes for the storage of the events, status information and environmental data ⌈

Type:	Valid

Description:	0. For the internal administration the diagnostic in AUTOSAR needs an Event buffer which shall be configurable depending on the number of the possible events in the system i.e. related to all SW components which are assigned to the diagnostic in AUTOSAR ; 0. The fault storage [event buffer] shall provide enough space to store all high priority failures.
Rationale:	Processor resource constraints
Use Case:	In case of large systems with many events a selection of events shall take place to fulfill NVRAM / RAM constraints of smaller processors.
Applies to:	CP, AP
Dependencies:	–
Supporting Material:	

⌋(*RS_Main_00011*)

[SRS_Diag_04172] Inform external service processors about outcome of the final response ⌈

Type:	Valid
Description:	For each UDS service which diagnostic in AUTOSAR delegates to a application for processing, it shall inform the application, whether a response has been successfully sent out or not.
Rationale:	For long running service processing, which delegate the processing to separate threads, the asynchronous callback model is more efficient, while for simple service processors the strict synchronous model is easier to implement.
Applies to:	AP
Dependencies:	SRS_Diag_04169
Use Case:	Flexibility for service processor implementations.

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04127] Configurable record numbers and trigger options for DTCSnapshotRecords and DTCExtendedDataRecords ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR module shall provide the capability to configure record numbers and trigger options for the storage of DTCSnapshotRecords and DTCExtendedDataRecords.
Rationale:	Advanced fault analysis
Use Case:	Flexible handling of DTCSnapshotRecords and DTCExtendedDataRecords
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04177] Custom diagnostic services ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the configuration of custom diagnostic services.
Rationale:	In some cases diagnostic services beyond the set of services standardized in ISO 14229-1 are needed.
Applies to:	CP, AP
Dependencies:	RS_DEXT_00047

⌋*(RS_Main_00260)*

[SRS_Diag_04059] Configuration of timing parameters ⌈

Type:	Valid
Description:	Every physical layer requires specific timing parameter values therefore it is necessary to include the ability to configure the timing constraints depending on the used network. The timing parameters are set to default values when a communication starts and shall be changeable at runtime.
Rationale:	Usability with different networks.
Use Case:	The diagnostic communication can be done at different networks (e.g. CAN/LIN/FlexRay/Ethernet).
Applies to:	CP, AP
Dependencies:	–
Supporting Material:	

⌋*(RS_Main_00011, RS_Main_00260)*

[SRS_Diag_04033] Support the upload/download services for reading/writing data in an ECU in an extended and manufacturer specific diagnostic session ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the UDS services RequestDownload, RequestUpload, TransferData, RequestTransferExit (0x34-0x37) according to ISO 14229-1:2013. Note that in the Classic Platform these services are usually also implemented inside the bootloader which is out of scope of this requirement.
Rationale:	Provide means to upload and download data blocks.
Use Case:	Downloading configuration or application data during end of line or development. Another use case is uploading data blocks from the ECU for evaluation or verification purposes.
Applies to:	CP
Dependencies:	
Supporting Material:	ISO14229-1 v.2013

⌋*(RS_Main_00011)*

[SRS_Diag_04020] Suppress responses to diagnostic tool requests ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the suppressPosRspMsgIndicationBit and the defined behavior according to ISO 14229-1:2013.
Rationale:	The tester is not interested in the positive response in certain situations. It prevents bus burst as result of a functional request.
Use Case:	In most cases, the positive responses are not relevant for functional requests to set the vehicle in a certain state. This can be a sequence of service 0x85, 0x28 and functional 0x3E during reprogramming to keep the vehicle in a 'silent' state without normal bus communication and DTC setting switched off.
Applies to:	CP
Dependencies:	
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00011*)

[SRS_Diag_04119] Handle the execution of diagnostic services according to the assigned diagnostic session ⌈

Type:	Valid
Description:	If a diagnostic session transition occurs (initiated by UDS Service 0x10), the diagnostic in AUTOSAR shall only maintain active diagnostic functionality if supported in the new session and if not prohibited by security access.
Rationale:	No interruption of diagnostic functionality
Use Case:	Deactivation of fault management and normal communication during ECU reprogramming
Applies to:	CP
Dependencies:	
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00011*)

[SRS_Diag_04016] Support "Busy handling" by sending a negative response 0x78 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the sending of the negative response 0x78 in order get more time to build up the final positive or negative response.
Rationale:	Ensure a steady and save communication link and guarantee specified timing conditions.
Use Case:	When an application cannot provide the response in the protocol specific time
Applies to:	CP
Dependencies:	
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00011*)

[SRS_Diag_04006] Manage session handling ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the transition from a default session to any other session, also back to the default session. (A diagnostic session enables a specific set of diagnostic services and/or functionality).
Rationale:	Some diagnostic services are not available in the default session. Therefore it is necessary to have information about the current session and no service which is connected to a non default session will be processed in the default session.
Use Case:	Special services need a different session than the default session, e.g. Reduction of communication traffic on the network in order to get more performance for the flash programming.
Applies to:	CP
Dependencies:	[SRS_Diag_04005] SecurityAccess level handling
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04005] Manage Security Access level handling ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall manage the handling of the UDS-service 0x27 (SecurityAccess) and also the Security level handling. The accessibility of the services (service identifier) in the actual security level shall be checked.
Rationale:	Some diagnostic services are in dependence to a security access level. Therefore it is necessary to have information about the current level and no service which is restricted by security will be processed without authorization.
Use Case:	Not all diagnostic services are allowed in each security level.
Applies to:	CP
Dependencies:	
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04135] Support UDS service $38 (RequestFileTransfer) ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support UDS service 0x38 ("RequestFileTransfer").
Rationale:	The requestFileTransfer service is used by the client to initiate a file data transfer from either the client to the server or from the server to the client (download or upload). Additionally, this service has capabilities to retrieve information about the file system
Use Case:	Upload of files (e.g. data files, graphics, navigation data...)
Applies to:	CP
Dependencies:	[SRS_Diag_04059] Configuration of timing parameter
Supporting Material:	ISO 14229-1 v.2013

⌋(*RS_Main_00011*)

[SRS_Diag_04100] Interface for logging and tracing ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide an interface for DLT to transport log and trace data using a diagnostic service. Logging and tracing data are sent via this service and control requests from the logging and tracing modules are received. For this purpose the ResponseOnEvent service is implemented. The diagnostic in AUTOSAR should provide an interface for DLT to send data and receive control requests.
Rationale:	Logging and trace needs an interface to send LogAndTrace data out of the ECU. A bus independent access to the ECU over standardized diagnostic is provided. This is available during production phase and provides a secured session control. Because log and trace messages are event triggered and the storage on the ECU is limited, these messages must be sent when they occur.
Use Case:	• Transmitting log and trace data during a diagnostic session • Advanced Diagnostic Tracing, optional via telematics services
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04098] Interact with standard bootloader ⌈

Type:	Valid
Description:	Integration of a standard bootloader into the AUTOSAR architecture. • If the diagnostic in AUTOSAR is requested to change into the programming session ($1002), it shall either send the final response and then activate the bootloader or it shall not send the final response and activate the bootloader where the activate the bootloader and the final response shall be sent by the bootloader (according HIS [FL-504]). • The diagnostic in AUTOSAR shall be able to check environmental conditions (e.g. engine speed) before activating the bootloader. • The diagnostic in AUTOSAR shall provide a configurable NRC 0x78 (RCRRP, retrigger the timeout supervision of the diagnostic client) response during transition to the bootloader.
Rationale:	Bootloader concept has to be standardized within AUTOSAR.
Use Case:	Usage of ”off-the-shelf” bootloader
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04159] Control of DTC storage ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support control of DTC storage via UDS service 0x85.
Rationale:	Avoiding unwanted storage of DTCs.
Use Case:	No DTCs storage when functional communication is deactivated during ECU reprogramming.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04157] Reporting of DTCs and related data ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the reporting of DTCs and related data.
Rationale:	Report failure memory data to the requester.
Use Case:	All services reporting fault memory data.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04156] Support DTCFunctionalUnit ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support DTCFunctionalUnit according to ISO 14229-1.
Rationale:	Compliance to ISO 14229-1.
Use Case:	OEM-specific use of DTCs.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04077] Uses standard mechanisms provided by persistency modules ⌈

Type:	Valid
Description:	–

Rationale:	Non volatile data storage
Use Case:	Triggered data storage during normal ECU operation to avoid loss of volatile data / event information.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00130*, *RS_Main_00440*)

[SRS_Diag_04131] Consistent event management mechanisms ⌈

Type:	Valid
Description:	All memory locations except mirror memory shall use the same event management mechanisms.
Rationale:	Ensure identical event management behavior.
Use Case:	–
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04117] Configurable behavior for DTC deletion ⌈

Type:	Valid
Description:	Usually, only ClearAllDTCs is used for the deletion of DTCs. Therefore, a configurable behavior which optionally limits the deletion of DTCs to ClearAllDTCs.
Rationale:	OEM specific behavior
Use Case:	Allow only ClearAllDTCs and therefore optimization of ClearDTC behavior.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04107] Provide defensive behavior ⌈

Type:	Valid
Description:	For safety-related applications, the diagnostic in AUTOSAR shall ensure data integrity of fault information stored in non-volatile memory.
Rationale:	Error protection of fault memory is needed for safety-related applications
Use Case:	Fault memory could have been corrupted
Applies to:	CP
Dependencies:	–

Supporting Material:	Use the optional CRC and redundancy capabilities provided by the AUTOSAR persistency modules for stored fault memory blocks. Only blocks assigned to error events of high severity can be protected. These blocks can be stored in non-volatile memory when the error event is confirmed (before shutdown of the ECU)

⌋(*RS_Main_00011*)

[SRS_Diag_04105] Event memory management ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall be able to handle valid events, update existing event memory entries or replace events in case of a full event memory. The processing is triggered externally (e.g. by the reported event status) or depends on internal information (e.g. value of debounce counter \timer,occurrence counter, ...)
Rationale:	Support of fault storage and analysis
Use Case:	Support of fault storage and analysis
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO 14229-1 v.2013

⌋(*RS_Main_00420*)

[SRS_Diag_04091] Notification about valid freeze frame data to applications ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall be enabled to notify other applications (or system modules) about valid freeze frame data (e.g. time stamp). If this functionality is configured for an event, it shall be executed every time a valid freeze frame is stored in the event memory.
Rationale:	Providing freeze frame data (like time stamp) to applications or system modules. Additionally this functionality provides a simple way for providing this data to other components (every time valid data is available) to avoild cyclic polling.
Use Case:	The information provided by this functionality is needed by modules like a special 'Diagnostic active response handler'.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04151] Event status handling ⌈

Type:	Valid
Description:	Diagnostics shall support event status handling.
Rationale:	Support OEM specific event status handling

Use Case:	Evaluation of monitor results and deriving corresponding actions from them
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04071] Process events according to their defined importance like priority and/or severity ⌈

Type:	Valid
Description:	The events shall be sorted or assigned to a specific priority (e.g. Severity Mask - ISO14229-1 v.2013,Annex D3) representing their importance like: • Healed events can be overwritten; • Privileged storing in case of Event Buffer filled up with less privileged events.
Rationale:	ISO14229-1 v.2013
Use Case:	Improved clustering and judging of events.
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00260*)

[SRS_Diag_04125] Event debounce counter shall be configurable ⌈

Type:	Valid
Description:	It shall be configurable if the debounce counter shall be frozen or reset, when at least one enable condition for the event is set to ”not fulfilled” or when ControlDTCSetting is set to ”disabled”. In case of switching the enable conditions to ”fulfilled” the monitor needs to be informed to restart the event detection. In case of switching ControlDTCSetting to ”re-enabled” the monitor needs to be informed to restart the event detection.
Rationale:	Flexible usage of internal debouncing
Use Case:	–
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00420*)

[SRS_Diag_04136] Configurable ”confirmed” threshold ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support a postbuild configurable ”confirmed” threshold.
Rationale:	Flexible usage of local legislated requirements.
Use Case:	Support different legislated requirements in different markets (US/EURO). For the US market the MIL and the ConfirmedDTC is activated after 2 DCY (Driving Cycles). For the EUR market the MIL and the ConfirmedDTC is activated after 3 DCY (Driving Cycles).
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04140] Aging for UDS status bits ”confirmedDTC” and ”testFailedSinceLastClear” ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the capability to age both the confirmedDTC bit and the testFailedSinceLastClear bit after a configurable number of aging cycles has been reached. The value at which each bit is aged may be different between the two.
Rationale:	–
Use Case:	–
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04133] Aging for event memory entries ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support aging for event memory entries to remove entries from the event memory which have not failed for a specific number of operating cycles.
Rationale:	Remove information from fault memory that is not relevant for a repair action.
Use Case:	Network timeout fault that has been detected, but is not in active state any more.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04063] Process a dedicated event identifier for each monitoring path to support an autonomous handling of different events/faults ⌈

Type:	Valid
Description:	For the internal administration the diagnostic in AUTOSAR needs a unique identification of each monitoring path. This identification shall be handled via an event ID value (Integer).
Rationale:	A monitoring path shall be uniquely identified by its unique event ID value.
Use Case:	Unique fault identification which can be used for enhanced debugging.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04148] Provide capabilities to inform applications about diagnostic data changes ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR modules shall provide capabilities to inform applications about diagnostic data changes. The capabilities shall cover the provision of corresponding interfaces and configuration options for data elements and associated triggers.
Rationale:	Applications requires information about data changes).
Use Case:	Applications needs to be informed about a status change of a DTC to be able to react on this DTC status.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04097] Decentralized and modular diagnostic configuration in applications ⌈

Type:	Valid
Description:	Applications can provide diagnostic information. The diagnostic in AUTOSAR module shall be able to generate ports to be connected to these applications in order access this diagnostic data.
Rationale:	Because of decentralized configuration and interface requirements each application shall provide and implement diagnostic interfaces to allow code generation and port connection

Use Case:	Use-case example: • As of today functions and associated diagnostics are developed by several parties. Thus for each function and its diagnostic monitors (e.g. torque management in an engine controller)the diagnostic capabilities are defined separately and will not necessarily be coordinated during development. • System integration and combination of diagnostics for accessibility through diagnostic in AUTOSAR requires that the individual functions and diagnostic features are connected to be compiled as a complete diagnostic system (which is in case of OBD2 certification relevant). Use-case summary: 0. develop decentralized modular software and its diagnostics without permanent interaction with other application developers. 0. Combine modules and extract module-specific diagnostic data. 0. link diagnostic data from applications to the diagnostic in AUTOSAR.
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO 14229-1 v.2013

⌋(*RS_Main_00420*, *RS_Main_00260*)

[SRS_Diag_04067] Provide the diagnostic status information according to ISO 14229-1 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the diagnostic status information according to the DTCStatusMask, ISO 14229-1 v.2013 (refer to DTC status mask), Annex D5
Rationale:	Advanced fault analysis
Use Case:	Improved fault and event tracking and analysis
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO 14229-1 v.2013

⌋(*RS_Main_00420*, *RS_Main_00260*)

[SRS_Diag_04179] Provide interfaces for diagnostic monitors. ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide an interface to monitoring application for reporting and processing monitor results. The reported result shall uniquely be identified by an EventID.
Rationale:	Test results reported by monitoring applications are handled diagnostic in AUTOSAR internally. The interaction between diagnostic in AUTOSAR and the application is realized using a dedicated interface.
Applies to:	CP, AP

Dependencies:	–
Use Case:	Monitoring applications report test results as soon as valid results are available by using the provided interface.

⌋(*RS_Main_00260*)

[SRS_Diag_04178] Support operation cycles according to ISO 14229-1 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide a configurable set of system cycles that may qualify the event in an additional manner.
Rationale:	Operation cycles are essential for event status management.
Applies to:	CP, AP
Dependencies:	–
Use Case:	Starting of an operation cycle triggers many types of system reactions.
Supporting Material:	ISO 14229-1 v.2013 and ISO 15031-5

⌋(*RS_Main_00260*)

[SRS_Diag_04201] Support a configuration to assign specific events to a customer specific DTC ⌈

Type:	Valid
Description:	Assignment of events to customer specific or standardized DTCs.
Rationale:	Events are used diagnostic in AUTOSAR internally only. An external scan tool requests a DTC number which was assigned to one or multiple events/monitors.
Applies to:	CP, AP
Dependencies:	–
Use Case:	Internal monitor results (e.g. driver can be experienced) are observable via a scan tool enabling external fault analysis.

⌋(*RS_Main_00260*)

[SRS_Diag_04180] Process all UDS Services related to diagnostic fault memory of ISO 14229-1 internally ⌈

Type:	Valid
Description:	Service implementation of all UDS services, which are related to fault memory (ClearDiagnosticInformation and ReadDTCInformation from 'Stored Data Transmission functional unit'), shall be implemented internally within diagnostic in AUTOSAR without delegating the processing/part of the processing to external modules. The MirrorMemory is not supported, wherefore the services for MirrorMemory shall be excluded (0x19 10 and 0x19 11).
Rationale:	Since diagnostic in AUTOSAR is also responsible fault memory management, all fault memory related UDS services (0x85, 0x14, 0x19) have to be processed internally.
Applies to:	CP, AP
Dependencies:	–
Use Case:	General diagnostic protocol processing.

Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*)

[SRS_Diag_04182] Provide an application interface to change operation cycles states ⌈

Type:	Valid
Description:	Operation cycles handled by the diagnostic in AUTOSAR can be started, stopped or restarted by application.
Rationale:	Operation cycle state transitions are trigger conditions for event status management according to ISO 14229-1.
Applies to:	CP, AP
Dependencies:	SRS_Diag_04178
Use Case:	Monitoring application starts an operation cycle. This triggers some status changes for the relevant events.

⌋(*RS_Main_00060*)

[SRS_Diag_04183] Notify interested parties about event status changes ⌈

Type:	Valid
Description:	Event status change report shall be available for application subscribing for the notification.
Rationale:	Event specific status information is handled diagnostic in AUTOSAR internally, the change of the status might be relevant for monitoring or other applications.
Applies to:	CP, AP
Dependencies:	–
Use Case:	The application gets informed about relevant event status change.

⌋(*RS_Main_00060*)

[SRS_Diag_04185] Notify applications about the clearing of an event ⌈

Type:	Valid
Description:	Interested monitoring application shall be notified about the clearing of event status information and event related data.
Rationale:	Monitor reinitialization can be triggered by the clear notification.
Applies to:	CP, AP
Dependencies:	–
Use Case:	After the event status is cleared diagnostic in AUTOSAR informs the relevant monitoring application which can be reinitialized.

⌋(*RS_Main_00060*)

[SRS_Diag_04186] Notify applications about the start or restart of an operation cycle ⌈

Type:	Valid

Description:	Interested monitoring application shall be informed about the start or restart of operation cycles.
Rationale:	Monitor reinitialization can be triggered by the start of an operation cycle.
Applies to:	CP, AP
Dependencies:	–
Use Case:	A monitor application gets initialized after diagnostic in AUTOSAR informs it about the start of a relevant operation cycle.

⌋(*RS_Main_00060*)

[SRS_Diag_04204] Provide the current status of each warning indicator. ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall derive the current warning indicator status from the assigned events according to ISO 14229-1. The warningIndicatorRequested bit shall be set according to ISO 14229-1.
Rationale:	The warning indicator status is used to activate or deactivate indicators like lamps, text message or a beep. The state is calculated in diagnostic in AUTOSAR wherefore the information needs to be distribution to the application.
Applies to:	CP, AP
Dependencies:	–
Use Case:	Indications of certain malfunctions to the driver (e.g. Malfunction Indicator Lamp (MIL)).

⌋(*RS_Main_00060*, *RS_Main_00420*)

[SRS_Diag_04202] Report DTCs getting active to the error logging module/system ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall report DTCs getting active to the error logging module/system
Rationale:	To have an overview of all log, trace error messages and to set all of them in the correct context with the error events reported to the diagnostic in AUTOSAR, it is important to have all this messages and events in one list (context). This makes an analysis of the reported errors more efficient and gives a correct picture of the ongoing sequences, which report an error.
Applies to:	CP, AP
Dependencies:	–
Use Case:	The application sets an event status diagnostic in AUTOSAR forwards it to the logging system The logging system inserts the action to the log list

⌋(*RS_Main_00260*)

[SRS_Diag_04205] Support of SnapshotRecords ⌈

Type:	Valid

Description:	The diagnostic in AUTOSAR shall support SnapshotRecords according to ISO 14229-1. Each DTC can optionally have one or more SnapshotDataRecords. The supported record numbers shall be configurable. Only a atomic update of the whole record shall be supported. The storage trigger shall be configurable per snapshot record number. The configurable trigger is based on the following DTC status bit transitions: TestFailed_Set; Confirmed_Set; Pending_Set FaultDetectionCounterThreshold_Reached. The environmental data shall be captured from external applications.
Rationale:	Advanced fault analysis.
Applies to:	CP, AP
Dependencies:	[SRS_Diag_04189]
Use Case:	Improved clustering and judging of events/faults.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260, RS_Main_00011*)

[SRS_Diag_04206] Support of ExtendedDataRecords ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support ExtendedDataRecords according to ISO 14229-1. Each DTC can optionally have one or more ExtendedDataRecords. The record numbers shall be configurable. Only a atomic update of the whole record shall be supported. The storage trigger shall be configurable per Extended data number. The configurable trigger is based on the following DTC status bit transitions: TestFailed_Set; Confirmed_Set; Pending_Set FaultDetectionCounterThreshold_Reached.
Rationale:	Advanced fault analysis.
Applies to:	CP, AP
Dependencies:	[SRS_Diag_04189]
Use Case:	Improved clustering and judging of events/faults.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260, RS_Main_00011*)

[SRS_Diag_04189] Support a fine grained configuration for SnapshotRecords and ExtendedDataRecords ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall be able to handle fine grained layout configurations for event related data. Data elements might be collected from different applications and merged to different DIDs or ExtendedDataRecords.
Rationale:	Advanced fault analysis.
Applies to:	CP, AP
Dependencies:	–

Use Case:	diagnostic in AUTOSAR collects SnapshotRecord data from different application and merges diagnostic information into one DID.

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04190] Usage of internal data elements in SnapshotRecords and ExtendedDataRecords ⌈

Type:	Valid
Description:	It shall be possible to assign the diagnostic in AUTOSAR internal data elements like Operation Cycle Counter, Fault Detection Counter (FDC) and Occurrence Counter to Snapshot- and ExtendedDataRecords. While reading the Snapshot- or ExtendedDataRecord the current value of the diagnostic in AUTOSAR internal data element shall be reported.
Rationale:	Some data objects that are internally generated by the diagnostic in AUTOSAR can be retrieved by UDS service 0x19 ReadDTCInformation.
Applies to:	CP, AP
Dependencies:	SRS_Diag_04205
Use Case:	Reading Operation Cycle Counter, Fault Detection Counter and Occurrence Counter.

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04192] Provide the ability to handle event specific enable and storage conditions ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall accept event status reporting if event-specific enable conditions are currently valid. Otherwise the reporting shall be rejected. In case the event-specific storage condition(s) are not fulfilled, the DTC will fail but not added to or updated in the fault memory (Pending and Confirmed are not set set).
Rationale:	Support mechanisms to avoid reams of event memory entries in case of specific ECU conditions.
Applies to:	CP, AP
Dependencies:	–
Use Case:	Depending on environmental data or the current status of an ECU the diagnostic in AUTOSAR considers a certain number of conditions/checks before the event get qualified. - Enable conditions affects the ability of a diagnostic monitor to report events - Storage conditions affects the qualification of the reported event before the event is stored in its configured event memory For specific fault groups (e.g. network faults) it is necessary to evaluate the current status of an ECU (e.g. under voltage) before the reported events are qualified by the diagnostic in AUTOSAR.

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04194] ClearDTC shall be accessible for applications ⌈

Type:	Valid

Description:	The service ClearDTC provided by the diagnostic in AUTOSAR supports the functionality of clearing the DTCs of a specified memory origin. This service shall be available not only inside the diagnostic in AUTOSAR, but also for the application.
Rationale:	The UDS job 0x14 ClearDiagnosticInformation supports only the clearing of primary memory. Clearing of user defined memory origins is usually handled by the application, that is why the ClearDTC service shall be provided.
Applies to:	CP, AP
Dependencies:	–
Use Case:	A routine control UDS job activates application, which clears the DTCs of a user defined memory using the ClearDTC service in diagnostic in AUTOSAR.

⌋(*RS_Main_00260, RS_Main_00060*)

[SRS_Diag_04195] Chronological reporting order of the DTCs located in the configured event memory ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall be able to handle the order of event occurrences (e.g. represented by a time stamp or odometer value).
Rationale:	Advanced fault analysis.
Applies to:	CP, AP
Dependencies:	–
Use Case:	When processing 0x19 UDS job, DTCs are returned in the chronological order.

⌋(*RS_Main_00260, RS_Main_00011*)

[SRS_Diag_04211] Persistent storage of DTC status and environmental data ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the non-volatile storage for event status and environmental data parameters required by ISO 14229-1.
Rationale:	According to the ISO 14229-1 UDS specification a set of status information and environmental data shall be stored non-volatile.
Applies to:	CP, AP
Dependencies:	–
Use Case:	Status information is stored non-volatile over power cycles.
Supporting Material:	ISO 14229-1 Appendix D

⌋(*RS_Main_00011*)

[SRS_Diag_04196] UDS Service handling for all diagnostic services defined in ISO 14229-2 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall implement the protocol handling for all UDS services defined in ISO 14229-2.
Rationale:	The diagnostic in AUTOSAR shall be the central service handler for UDS diagnostics.

Applies to:	CP, AP
Dependencies:	–
Use Case:	Interaction with UDS compliant tester on Ethernet.
Supporting Material:	ISO 14229

⌋(*RS_Main_00260*)

[SRS_Diag_04203] Common checks on all supported UDS Services Requests ⌈

Type:	Valid
Description:	The following checks shall be implemented by diagnostic in AUTOSAR on all supported UDS services: SID and sub-function format - Diagnostic session level - Diagnostic security level - Message length
Rationale:	The diagnostic in AUTOSAR shall be UDS compliant and shall do general checks, which can be done on UDS protocol level centrally, independently whether the service is processed internally or externally by a applications as service processor.
Applies to:	CP, AP
Dependencies:	–
Use Case:	General diagnostic protocol processing.
Supporting Material:	ISO 14229

⌋(*RS_Main_00260*)

[SRS_Diag_04197] Clearing the user defined fault memory ⌈

Type:	Valid
Description:	The clearance of user defined fault memory shall be possible according to the ISO 14229 draft document: “02_ISO_14229-1_Comments-Summary_2016-09-13.docx” via diagnostic requests.
Rationale:	Provide a standardized way to clear user defined fault memory.
Applies to:	CP, AP
Dependencies:	–
Use Case:	OEM and TIER1 using the user defined fault memory need to clear the user defined memory. A standardized way make OEM or TIER1 specific solutions obsolete, which were incompatible to each.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*)

[SRS_Diag_04198] Process all UDS Services related to session and security management of ISO 14229 internally ⌈

Type:	Valid

Description:	Service implementation of all UDS services, which are related to session and security management (DiagnosticSessionControl, SecurityAccess and TesterPresent from 'Diagnostic and Communication Management functional unit'), shall be implemented internally within diagnostic in AUTOSAR without delegating the processing/part of the processing to external modules. This does NOT exclude, that diagnostic in AUTOSAR does callout to external application for instance to get/check certain security keys. But the state machine/protocol is handled internally by diagnostic in AUTOSAR.
Rationale:	Session and security management is an integral part of general UDS service handling and has therefore to be implemented internally.
Applies to:	CP, AP
Dependencies:	–
Use Case:	General diagnostic protocol processing.
Supporting Material:	ISO 14229

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04199] Provide a configurable UDS service execution mechanism at runtime to decide if a UDS request shall be processed or not ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support to query configured application, whether a received UDS service request shall be processed or rejected.
Rationale:	Infrastructural/OEM specific supervisor components decide about service execution on a basis of ECU/vehicle state.
Applies to:	CP, AP
Dependencies:	–
Use Case:	Control of service access centrally done in one application.

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04208] Inform the application about diagnostic session and diagnostic security level changes on each tester connection. ⌈

Type:	Valid
Description:	In case the currently active UDS session or security level change on a tester conversation, the diagnostic in AUTOSAR shall provide a notification mechanism for the application, to inform the applications about the new session or security level and the affected tester connection.
Rationale:	Session changes happen asynchronously to service processor implementations. But there exists functionality that needs to react on session changes.
Applies to:	CP, AP
Dependencies:	SRS_Diag_04169
Use Case:	Flexibility for service processor implementations.

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04218] Support of UDS service 0x2F InputOutputControlByIDentifier. ⌈

Type:	Valid
Description:	The Diagnostic Management shall support the ISO 14229-1 service 0x2F InputOutputControlByIDentifier.
Rationale:	Allow to simulate input values and to control output values.
Applies to:	CP, AP
Use Case:	In workshop or production checks with the input and output channels of the ECU is needed.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*, *RS_Main_00011*)

4.2 Diagnostic requirements for the Classic Platform

4.2.1 Functional Requirements

[SRS_Diag_04213] Support the mirror fault memory defined by ISO 14229-1 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the mirror fault memory defined by ISO 14229-1.
Rationale:	Extended storage of fault information independent from the primary fault memory.
Use Case:	Mirror fault memory is used by OEM and Tier1 during development or for storing warranty relevant information inside. DTCs in the mirror memory are triggered along with a DTC in the primary fault memory, but it has different event related data stored and it is not cleared by clearing the primary fault memory. The information stored in the mirror memory is not relevant for workshops or to repair the vehicle.
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO 14229-1 v.2013

⌋(*RS_Main_00260*)

[SRS_Diag_04112] The DEM module shall support DTCs according to SAE J1939 ⌈

Type:	Valid
Description:	The DEM module shall support DTCs according to SAE J1939-73.
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HD-OBD
Applies to:	CP
Dependencies:	DEM, J1939DCM
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04139] Support subfunction 0x42 of UDS service 0x19 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support subfunction 0x42 of UDS service 0x19 to retrieve WWH-OBD-specific DTCs matching the requested DTC status mask and severity mask record.
Rationale:	Support of WWH-OBD
Use Case:	Improved fault and event tracking and analysis
Applies to:	CP
Dependencies:	–
Supporting Material:	Support of WWH-OBD

⌋(*RS_Main_00260*)

[SRS_Diag_04129] Provide OBD-specific configuration capabilities ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the following configuration capabilities: • OBD- ECU kind 1: ECU acts as OBD Master ECU (Master or Primary ECU) • OBD- ECU kind 2: ECU acts as OBD Slave ECU (Dependent / Secondary ECU) • OBD- ECU kind 3: ECU acts as non-OBD ECU The diagnostic in AUTOSAR shall both provide corresponding configuration parameters to switch on/switch off module-specific OBD functionality. Depending on the configured use case, the associated application interfaces shall be provided to connect different OBD-ECU kinds on application level (via bus communication).
Rationale:	UseCase-specific module configuration.
Use Case:	Optimization of RAM/ROM consumption.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04163] Parallel OBD and UDS processing ⌈

Type:	Valid
Description:	Diagnostics shall support the parallel processing of OBD and UDS protocols.
Rationale:	Vehicles can be equipped with On-board testers which send diagnostic requests at any arbitrary point in time. Legislative OBD requests need to be processed independently from a UDS requests from On-board testers.
Use Case:	Parallel reception of diagnostic requests from multiple testers.

Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04161] Provide support for the ASMIP algorithm ⌈

Type:	Valid
Description:	The diagnostic in AUTOSARs shall consider the ASMIP algorithm (Alternative Statistical MIL Illumination Protocol) according to the Californian Code of Regulation 13 CCR section 1968.2.
Rationale:	Supporting OBD use cases.
Use Case:	Dynamical threshold modification.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

4.2.2 Fault Memory Management

[SRS_Diag_04002] The Diagnostic event (fault) management shall be established as Basic SW Module ⌈

Type:	Valid
Description:	The Diagnostic event (error) management shall be a Basic SW Module described in the Diagnostic WP. Diagnostic event (error) management is out of scope for Mode Management.
Rationale:	SW Architecture
Use Case:	Improved fault and event tracking and analysis for Service, assembly line, OBD-SCAN-Tool
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04057] Classification of events for series production, OBD and expert usage ⌈

Type:	Valid

Description:	The diagnostic in AUTOSAR shall support a classification of events for the following types of events: • Events that are defined for error analysis in the service station shall be stored in the primary event memory. • Events that are defined for detailed error analysis by experts in the after sale department are stored in the secondary error memory. Errors that occur during the development process shall be reported to the debugging modules. Therefore, debugging module APIs shall be used which (are not provided by the diagnostic in AUTOSAR).
Rationale:	After sales analysis
Use Case:	Distinction between service station relevant and after sales relevant events.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04124] Store the current debounce counter value nonvolatile to over a powerdown cycle ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall be able to store the current debounce counter value non-volatile to over a power-down cycle.
Rationale:	Support of DTC de-bouncing within several power cycles.
Use Case:	While the typical DTC operation cycle for a DTC is to start at power up and end at power down, there are different situations, when a particular DTC must define its operation cycle to span multiple ECU power up/down cycles. In this case, the FDC would need to be stored in NVM as it may never make it to 127 during a single power up.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04118] Optionally support event displacement ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall optionally support event displacement. The following sequence of different displacement criteria shall be possible: 0. Priority; 0. Active/passive status (optional); 0. Occurrence.
Rationale:	Limited hardware (memory resources) in ECU.
Use Case:	Error memory is full and Valid event is reported to diagnostic in AUTOSAR.

Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04123] Harmonized Driving//WarmUp cycles ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support harmonized Driving-/WarmUp cycles. The calculation of Driving-/WarmUp cycles is based on legal requirements.
Rationale:	OBD certification requires vehicle consistent calculations based on a harmonized Driving-/WarmUp cycle in the centralized OBD Master ECU.
Use Case:	Qualification of OBD-relevant DTCs
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04093] Memory overflow indication ⌈

Type:	Valid
Description:	For each Event Memory it shall be indicated if the related event memory (e.g. primary, secondary, mirror) is full and the next event occurs to be stored in this event memory.
Rationale:	The information that an event memory overflow occurred is very important for fault analysis.
Use Case:	• Triggering further internal behavior (e.g displacement strategies) • Linking this information to a dedicated Extended Data Record • Vendor specific UDS-Service
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04109] Provide an interface to retrieve the number of event memory entries ⌈

Type:	Valid

Description:	The diagnostic in AUTOSAR shall provide an interface to retrieve the number of event memory entries currently stored in Primary, Secondary and Mirror Memory to the application. Additionally, the corresponding Client Server Interface shall be provided.
Rationale:	The interface is required from application, to check if event memory entries exist that influence the ECU behavior.
Use Case:	There is an application message where a status bit must be set as soon as events are stored in the event memory. Therefore, the application needs to know how many event memory entries exist.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00420*)

[SRS_Diag_04126] Configurable suppression of events ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide a postbuild/loadable boolean configuration option per event. If this configuration is set to true the event behaves the same as if it is suppressed by API call. An event suppressed by configuration can not be activated via API call.
Rationale:	Use case-specific configuration of fault memory, only required events are visible and usable in ECU.
Use Case:	Variant coding
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04110] SAE J1939 lamp status ⌈

Type:	Valid
Description:	The composite and DTC-specific lamp status of the following lamps shall be supported: Malfunction Indicator Lamp, Red Stop Lamp, Amber Warning Lamp and Protect Lamp.
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HDOBD
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04111] SAE J1939 Expanded-FreezeFrame ⌈

Type:	Valid
Description:	The composite and DTC-specific lamp status of the following lamps shall be supported: Malfunction Indicator Lamp, Red Stop Lamp, Amber Warning Lamp and Protect Lamp.
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HDOBD
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04113] Support a set of SAE J1939 DM-messages ⌈

Type:	Valid
Description:	The following DM-messages shall be supported: **Name** **Description** DM01 Active Diagnostic Trouble Codes DM02 Previously Active Diagnostic Trouble Codes DM03 Diagnostic Data Clear/Reset for Previously Active DTCs DM04 Freeze Frame Parameters DM05 Diagnostic Readiness 1 DM06 Emission Related Pending DTCs DM11 Diagnostic Data Clear/Reset for Active DTCs DM12 Emissions Related Active DTCs DM13 Stop Start Broadcast DM19 Calibration Information DM20 Monitor Performance Ratio SAE J1939-73 Revised SEP2006 DM21 Diagnostic Readiness 2 DM23 Previously Active Emission Related Faults DM24 SPN Support DM25 Expanded Freeze Frame DM26 Diagnostic Readiness 3 DM28 Permanent DTCs DM29 Regulated DTC Counts (Pending, Permanent, MIL-On, PMIL-On) DM31 DTC to Lamp Association DM35 Immediate Fault Status
Rationale:	Support of SAE J1939-73
Use Case:	Diagnostics in HDV, HD-OBD
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04137] Definition of replacement failure ⌈

Type:	Valid

Description:	Upon filtering the storage of failure reports by central conditions (Storage Condition), it shall be possible to define and store a replacement failure info which then can be stored to the event memory. This replacement failure will represent the actual failure reason.
Rationale:	Improvement of failure analysis.
Use Case:	–
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04155] Notify applications and BSW modules about updates of event related data ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall notify other applications / BSW modules about updates of the event-related data in the event memory.
Rationale:	Changes to the event related data are done internally while evaluating event information passed from the diagnostic monitors. Third parties interested in the change of event related data need to get notified.
Use Case:	Allow OEM specific reaction on updates of the event related data.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04160] ResponseOnEvent according to ISO 14229-1 ⌈

Type:	Valid
Description:	Diagnostics shall support ResponseOnEvent according to ISO 14229-1.
Rationale:	Needed for failure analysis and fault memory tracking.
Use Case:	Inform diagnostic tooling about certain runtime conditions.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04215] Support of UDS service ReadDataByPeriodicIdentifier (0x2A) ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support UDS service ReadDataByPeriodicIdentifier (0x2A) with all supported sub-functions according to ISO 14229-1.

Rationale:	Periodic transmission of measurements/data by the diagnostic server (ECU), instead of frequent polling by re-requesting the same data via ReadDataByIdentifier. Further it is possible to reach higher update rates of measurements (e.g. 2ms).
Use Case:	Monitor measurement values over time by diagnostics.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04217] Adding the Lamp status pertinent to a specific Fault Event/DTC available as DemInternalDataClass shall be codified in the same format of DM31 ⌈

Type:	Valid
Description:	when a Fault Event memory entry is coming, the related FreezeFrame includes the pertinent DTC lamp status with the SPN number for each kind of lamp. In fact, the format of this data shall also be compliant to the content of the DM31 with the same codification/format and SPNs identification. In other word this solution would ensure that the user is able to retrieve the pertinent lamp status as it becomes a memory entry even if the DM31 request is not done in the same moment.
Rationale:	After sales analysis.
Use Case:	Provide lamp status per DTC to diagnostic testers.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04165] Triggering of multiple events upon a master event is reported ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the capability to trigger multiple events upon an event is reported.
Rationale:	From one unique fault source, multiple events shall be derived and each derived event can trigger an own DTC and event memory entry.
Use Case:	Storing DTCs from one unique source into different event memories without changing and recompiling the reporting software. A given software can report event status information and depending on configuration multiple DTCs and event related data in different fault memories can be stored.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04031] Notify the Function Inhibition Manager (FIM) upon changes of the event status in order to process them according to the SW components dependencies ⌈

Type:	Valid
Description:	Control (enable/disable) of functionalities of SW components based on the following inhibit condition: - faults
Rationale:	Event status information for function inhibition
Use Case:	Usage of event status information for function inhibition
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

4.2.2.1 DTC and event-related data

[SRS_Diag_04162] Parallel fault memory access ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide parallel access to the fault memory to various clients. Each client shall be able to access the fault memory independent from other clients. Conflicts occurring during parallel access to shared resources shall be resolved.
Rationale:	OEMs require parallel access to diagnostics.
Use Case:	• Support of OBD and UDS in parallel • Software interacting with secondary ECUs in OBD • Software components accessing event memory data
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

4.2.3 Diagnostic Communication

[SRS_Diag_04007] Provide a diagnostic service handling for the applications involved in diagnostic functionality ⌈

Type:	Valid

Description:	The diagnostic in AUTOSAR shall provide the diagnostic service handling, according to ISO14229-1 v.2013, ISO 15031-5 and ISO 15765-3 for the communication between an AUTOSAR conform ECU and an internal tester or an external diagnostic tool).
Rationale:	Only one diagnostic service instance in an ECU.
Use Case:	Communication with an external diagnostic tools in : • development • manufacturing • service (garage) • OBD scan tools Communication with an internal tester.
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO14229-1 v.2013, ISO 15031-5, ISO 15765-3

⌋(*RS_Main_00011*)

[SRS_Diag_04021] Handling of different diagnostic sessions in parallel ⌈

Type:	Valid
Description:	Handle an established diagnostic communication and a parallel diagnostic access request in parallel. This is necessary to open a diagnostic access with high priority and the controlled shutdown of the established diagnostic access with low priority.
Rationale:	To prioritize handling of different diagnostic protocols e.g. OBD and normal diagnostic communication as UDS.
Use Case:	An internal vehicle diagnostic tester communication is interrupted by OBD diagnostic access request.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04032] Different diagnostic addresses shall be supported by multiple (physical) channels ⌈

Type:	Valid
Description:	Modern ECUs contain more than one functionality (e.g. board computer, instrument cluster). Each functionality shall be addressable by a diagnostic tool with a different diagnostic address. This does not imply that those multiple requests are allowed in parallel.
Rationale:	High flexibility and granularity for addressing of applications
Use Case:	At the service (garage) a fault symptom is based on functionality. The service only wants to address this functionality.
Applies to:	CP
Dependencies:	[SRS_Diag_04021] Switch diagnostic communication access

Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04058] Ability to access different event memories ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support diagnostic services to read or remove event entries from the configured event memory seperatly.
Rationale:	Advanced fault analysis
Use Case:	The development departments of the OEMs and Suppliers need as much as possible deeper fault/event analysis although the mechanics may have deleted the faults or may not need to know if there are more detailed root causes for an event or fault.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04024] Access and handle specific data elements and data element groups if requested by an external scan tool ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide interfaces for applications to access diagnostic data and to process diagnostic services. The size of a diagnostic data element is derived by the interface or provided as an attribute of the API call itself.
Rationale:	Optimized usage of resources
Use Case:	Transfer environmental / FreezeFrame data of the diagnostic in AUTOSAR.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04015] Timing handling according to ISO15765-3 ⌈

Type:	Valid
Description:	In ISO15765-3 timing handling for physical and functional communication and error reaction is described. The diagnostic in AUTOSAR shall work according this specification. Timing parameters shall be configurable (see dependencies).
Rationale:	Ensure a steady and save communication link and guarantee specified timing conditions.
Use Case:	Optimizing of timing for high performance during reprogramming.
Applies to:	CP

Dependencies:	[SRS_Diag_04059] Configuration of timing parameter
Supporting Material:	ISO15765-3

⌋(*RS_Main_00011*)

[SRS_Diag_04019] Confirm transmitting if complete to continue processing ⌈

Type:	Valid
Description:	In some cases it is necessary that the application starts execution of the requested functionality after the positive response is completely transmitted. The application needs the callback functionality to get the information that the positive response is complete transmitted. After this callback the application can execute the requested functionality.
Rationale:	This behavior is specified by ISO 14229-1 v.2013.
Use Case:	E.g. call of the reset function. This call needs to be done after transmission of the positive response is over.
Applies to:	CP
Dependencies:	
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00011*)

[SRS_Diag_04120] Support a predefined AddressAndLengthFormatIdentifier ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support a predefined AddressAndLengthFormatIdentifier for UDS service $23 (ReadMemoryByAddress), UDS service 0x2C (DynamicallyDefineDataIdentifier with subservice DefineByMemoryAddress), UDS service 0x3D (WriteMemoryByAddress), UDS service 0x34 (RequestDownload) and UDS service 0x35 (RequestUpload).
Rationale:	AddressAndLengthFormatIdentifier is defined once and afterwards used in corresponding UDS services.
Use Case:	Static configuration of AddressAndLengthFormatIdentifier
Applies to:	CP
Dependencies:	–
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00011*, *RS_Main_00260*)

[SRS_Diag_04121] Provide the handling of service DynamicallyDefineDataIdentifier according to ISO 14229-1 ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide the handling of service DynamicallyDefineDataIdentifier according to ISO 14229-1 v.2013.
Rationale:	Standardized ISO 14229-1 v.2013 behavior
Use Case:	–

Applies to:	CP
Dependencies:	–
Supporting Material:	ISO14229-1 v.2013

⌋(*RS_Main_00011*, *RS_Main_00260*)

[SRS_Diag_04153] Support generic connections ⌈

Type:	Valid
Description:	Diagnostics shall support generic connections. Addressed information is then using MetaData.
Rationale:	Channel and connection configuration optimization through the layers.
Use Case:	Limit the request execution due to vehicle- or ECU states/-conditions.
Applies to:	CP
Dependencies:	Generic connections are supported for CAN diagnostics using normal fixed or mixed 29 bit addressing formats according to ISO15765-2. Depending on the actual layout of the CAN IDs, generic connections could also be used for extended or normal and mixed 11 bit addressing formats.
Supporting Material:	–

⌋(*RS_Main_00260*)

[SRS_Diag_04011] Provide diagnostic state information to applications ⌈

Type:	Valid
Description:	Applications need to know about the actual session and security state, because it is not predictable if the information's lead to a different functional diagnostic behavior.
Rationale:	Functional requirement
Use Case:	With the diagnostic session which the garage is using, it is allowed to switch between different sets of parameters. With an enhanced diagnostic session which could be used in development and a corresponding security level, it is allowed to change the data within the set of parameters.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04003] Network independent design ⌈

Type:	Valid
Description:	All network (CAN, LIN, FlexRay, MOST, Ethernet) dependent parts shall be done outside the diagnostic in AUTOSAR. That means that all interfaces to the transport protocol modules shall be network independent.

Rationale:	The diagnostic in AUTOSAR describes only the services for communication and the behavior of network is out of scope. Highest granularity and best option to adapt upcoming networks.
Use Case:	The diagnostic in AUTOSAR has to be network independent. The interface to the transport protocol shall be network independent.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00260*)

[SRS_Diag_04147] Communication with the transport layers to receive and send diagnostic data ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall communicate with the transport layer modules to receive and send diagnostic data.
Rationale:	Ensure diagnostic communication.
Use Case:	Support of various transport protocols (ISO-15765-2, ...).
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00260*)

4.2.4 Function Inhibition Manager (FIM)

The specification of Software requirements of the function inhibition manager is not a part of this specification. For details, please refer to the AUTOSAR_FIM_SRS.

4.2.5 Defaut Error Tracer (DET)

[SRS_Diag_04090] A configurable list of error report receivers shall be provided ⌈

Type:	Valid
Description:	The Default Error Tracer shall support a configurable list of functions for fan-out of received error reports. This list can be empty.
Rationale:	This implements the debugging concept in R4.0 (DocumentId 298).
Use Case:	Even development errors shall be captured by the Log and Trace functionality. Error Handling shall be enabled to react on development errors
Applies to:	CP
Dependencies:	–

Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04086] Report errors shall contain a dedicated set of information ⌈

Type:	Valid
Description:	Error reports, which the Default Error Tracer receives, shall consist of the ID of the reporting module, the ID of reporting instance, the ID of the API service in which the error has been detected and the error ID itself.
Rationale:	For optimal support of the error tracing some tracing information is necessary.
Use Case:	During software development phase a BSW module has been called using wrong parameters. Due to communication of some tracing information the location of the error source will be supported.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04087] The Default Error Tracer shall provide a development error report reception service ⌈

Type:	Valid
Description:	The Default Error Tracer shall be accessible by applications to report development error.
Rationale:	It shall be possible to perform error tracing during development of applications.
Use Case:	During software development phase a applictaion has received an unexpected response by a BSW module. By generating a development error and reporting it to the DET, configuration errors can be detected.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04089] The DET module shall support fan-out of received error reports ⌈

Type:	Valid
Description:	The Default Error Tracer shall forward each received error report by calling each element of a configurable list of functions.
Rationale:	This implements the debugging concept in R4.0 (DocumentId 298)
Use Case:	Even development errors shall be captured by the Log and Trace functionality. Error Handling shall be enabled to react on development errors
Applies to:	CP
Dependencies:	–

Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04085] The Default Error Tracer shall provide an interface to receive error reports ⌈

Type:	Valid
Description:	The Default Error Tracer shall provide an interface to get a development error report.
Rationale:	An interface will be needed to enable handling of development errors
Use Case:	During software development phase a BSW module has been called using wrong parameters. By generating a development error and reporting it to the DET, configuration errors can be detected.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00100*)

[SRS_Diag_04101] The DET module shall forward its trace events to the DLT ⌈

Type:	Valid
Description:	The DET receives trace events from errors from the BSW and application during debugging time. If a DLT module exists, these events should be forwarded to the DLT to collect logs and traces only in one instance.
Rationale:	To have an overview of all log, trace and error messages and to set all of them in the correct context, it is important to have all these messages and events in one list (context). Also it is not practicable to use more than one mechanism to report errors, logs and traces to a debugging interface. So all these sources should be routed to the DLT.
Use Case:	• A debugging scenario, an application or BSW Module uses the DET interface to trace an error • This error is forwarded by the DET to the DLT • The DLT turns these events in the DLT format and sends it over the debugging interface, together with all the other logs and traces
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*)

[SRS_Diag_04143] The Default Error Tracer shall provide an interface to receive runtime error reports ⌈

Type:	Valid

Description:	The Default Error Tracer shall provide an interface to get a runtime error report, issued by BSW modules. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	An interface will be needed to enable handling of runtime errors, caused by seldom occurring systematic faults. The caller will handle the error and continue appropriate in a deterministic manner.
Use Case:	CANNM_E_NET_START_IND: Reception of NM PDUs in Bus-Sleep Mode
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00100*)

[SRS_Diag_04144] The Default Error Tracer shall provide an interface to receive transient fault reports ⌈

Type:	Valid
Description:	The Default Error Tracer shall provide an interface to get a transient fault report, issued by BSW modules. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	An interface will be needed to enable handling of transient faults, caused by seldom occurring transient hardware faults.
Use Case:	• CAN controller goes offline due to bit-flip in its control register • Peripheral action lasts accidentally longer than expected (and specified)
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00100*)

[SRS_Diag_04145] The Default Error Tracer shall forward received runtime error reports to configured integrator code ⌈

Type:	Valid
Description:	The Default Error Tracer shall propagate all received runtime error reports using configurable callout. The received callout return value shall be returned to the reporter of the runtime error. If no callout has been configured, a default return value shall be provided. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	Integrator shall be able to recognize runtime errors and to handle in an appropriate manner.
Use Case:	CANNM_E_NET_START_IND: Reception of NM PDUs in Bus-Sleep Mode
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00100*)

[SRS_Diag_04146] The Default Error Tracer shall forward received transient fault reports to configured integrator code ⌈

Type:	Valid
Description:	The Default Error Tracer shall propagate all received transient fault report using configurable callout. The received callout return value shall be returned to the reporter of the transient fault. If no callout has been configured, a default return value shall be provided. The Default Error Tracer returns to the caller in order to allow continuation of intended program flow.
Rationale:	Integrator shall be able to recognize transient faults and to handle in an appropriate manner and to advice the reporter.
Use Case:	• CAN controller goes offline due to bit-flip in its control register. Integrator decides that reporting CAN driver shall re-initialize the CAN controller. • CAN controller goes offline due to bit-flip in its control register. Integrator decides that reporting CAN driver shall treat offline state of CAN controller as intended.
Applies to:	CP
Dependencies:	–
Supporting Material:	–

⌋(*RS_Main_00011*, *RS_Main_00100*)

4.3 Diagnostic requirements for the Adaptive Platform

[SRS_Diag_04166] Several tester conversations in parallel with assigned priorities ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall generally support a configurable amount of tester conversations/connections in parallel. Per tester connection, a priority shall be configurable. The priority is assigned to the tester address (SA of the UDS request), which identifies the connection.
Rationale:	ECUs in the Adaptive Platform generally have enough resources to handle multiple tester conversations in parallel.
Applies to:	AP
Dependencies:	–
Use Case:	Support for vehicle internal and external testers in parallel, which can not be easily synchronized.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04209] Pseudo parallel client interaction according to ISO ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the parallelism defined by the ISO as pseudo parallel concept, which is defined in ISO 14229-1 under Figure J.2.
Applies to:	AP
Dependencies:	–
Use Case:	Support of scenarios, where testers in parallel is only allowed, when in default session.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04210] Fully parallel client interaction ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support fully parallel client interaction, where clients are fully shielded from each other and can have different non-default sessions.
Rationale:	ECUs in the Adaptive Platform generally have enough resources to handle multiple tester conversations in parallel.
Applies to:	AP
Dependencies:	–
Use Case:	Support of scenarios, where maximum of testers in parallel shall be allowed
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*, *RS_Main_00011*)

[SRS_Diag_04167] Conversation preemption/abortion ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall generally support the preemption of a tester conversation in case all configured tester connections are currently active and a new connection of a tester with higher priority than an existing one takes place, it shall abort the lowest priority conversation and accept the new connection/conversation.
Rationale:	A ECU will have limited resources for parallel processing of diagnostic requests and different requests will have different priorities therefore the need for abortion.
Applies to:	AP
Dependencies:	–
Use Case:	Support for vehicle internal and external testers in parallel, which can not be easily synchronized.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*)

[SRS_Diag_04168] Adding of user-defined transport layers ⌈

Type:	Valid

Description:	The diagnostic in AUTOSAR shall support adding of user-defined transport layers.
Rationale:	Although the Adaptive Platform starts out with Ethernet support, later extension to other networks (CAN, Fr) should already be prepared. Additionally there is at least one OEM, which has its own DoIP implementation, which differs from ISO 13400. It should be possible to integrate this DoIP implementation with manageable effort/costs.
Applies to:	AP
Dependencies:	–
Use Case:	Plugability of UDS transport layers, to support different networks.

⌋(*RS_Main_00260*)

[SRS_Diag_04169] Provide an interface for external UDS service processors. ⌈

Type:	Valid
Description:	For all UDS services, which are NOT processed/implemented internally by diagnostic in AUTOSAR (either by configuration or generally not supported internally), but by external service processors, the diagnostic in AUTOSAR has to delegate the processing to the external application.
Rationale:	The majority of diagnostic services is implemented by the application, where the diagnostic in AUTOSAR has to delegate the service processing to.
Applies to:	AP
Dependencies:	SRS_Diag_04097, SRS_Diag_04007
Use Case:	Service processing by software components.
Supporting Material:	ISO 14229-1

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04170] Provide connection specific meta information to external service processors ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide connection specific meta-information to the external service processor, which is processing the UDS service request. At least DoIP shall be supported and the meta-information shall contain Src-IP-Adr/Port and Target-IP-Adr/Port of the request. The meta-information should be designed, that it can later easily extended to also cover connection information of other network technologies (like CAN, Flexray).
Rationale:	Sometimes the reaction of service processor implementations on a UDS request depend on the connection properties of the tester.
Dependencies:	SRS_Diag_04169
Use Case:	Flexibility for service processor implementations.
Applies to:	AP
Dependencies:	–

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04171] Synchronous and asynchronous interaction with external service processors ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support both types of interaction: • Calling a service processor synchronously, which means a blocking call until the service processor returns the final result (pos./neg. response, optional out parameters). • Calling a service processor asynchronously, which means a call to the service processor, where the service processor returns, that the job is not yet finished and later reports back to diagnostic in AUTOSAR via a separate callback, that the service processing has finished.
Rationale:	For long running service processing, which delegate the processing to own worker threads, the asynchronous callback model is more efficient, while for simple service processors the strict synchronous model is easier to implement.
Applies to:	AP
Dependencies:	SRS_Diag_04169
Use Case:	Flexibility for service processor implementations.

⌋(*RS_Main_00260, RS_Main_00420*)

[SRS_Diag_04173] Different signature types, when delegating processing of UDS service to the application ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall support the following signatures, when delegating processing of UDS service to the application: • Untyped interface, where the entire payload including SID and sub-service is given as a byte array to service processors • Typed interface per SID, sub-service and data element, where a mapping from the UDS parameters/data stream to datatypes is described in the configuration.
Rationale:	Depending on the use case/complexity of the UDS service and its parameters, it is much more efficient to do the parsing/interpretation in the implementation of the service processor. On the other hand, there are use cases, where the description of mapping from UDS data stream to interface type has the benefit, that the service processor implementation may stay unchanged, where the mapping description may be adapted to an altered on the wire representation.
Applies to:	AP
Dependencies:	SRS_Diag_04169
Use Case:	Flexibility for service processor implementations.

⌋(*RS_Main_00260, RS_Main_00420*)

[SRS_Diag_04174] Provide SA and TA to external service processors ⌈

Type:	Valid
Description:	The diagnostic in AUTOSAR shall provide source and target address to the external service processor, which is processing the UDS service request.

Rationale:	Sometimes the reaction of service processor implementations on a UDS request depend on the tester (SA) or on the target.
Applies to:	AP
Dependencies:	SRS_Diag_04169
Use Case:	Flexibility for service processor implementations.

⌋(*RS_Main_00260*, *RS_Main_00420*)

[SRS_Diag_04216] Support for multiple Diagnostic Server Instances ⌈

Type:	Valid
Description:	The Diagnostics in AUTOSAR shall be able to handle multiple Diagnostic Server Instances. Each Diagnostic Server Instance shall be addressable by its own set of target address and they shall be almost independent of each other. Exceptions like EcuReset needs to be coordinated between the server instances.
Rationale:	Software on AP is grouped in so called SoftwareClusters, and each cluster shall be diagnosed on its own.
Applies to:	AP
Dependencies:	–
Use Case:	Multiple SoftwareClusters deployed on single AP and each SoftwareCluster is diagnosed separately.

⌋(*RS_Main_00260*, *RS_Main_00420*)

4.4 Configuration

5 Requirements Tracing

The following tables reference the requirements specified in [**?**,] and links to the fulfillment of these. Please note that if column ”Satisfied by” is empty for a specific requirement this means that this requirement is not fulfilled by this document.

Requirement	Description	Satisfied by
[RS_Main_00011]	AUTOSAR shall support the development of reliable systems	[SRS_Diag_04003] [SRS_Diag_04005] [SRS_Diag_04006] [SRS_Diag_04007] [SRS_Diag_04011] [SRS_Diag_04015] [SRS_Diag_04016] [SRS_Diag_04019] [SRS_Diag_04020] [SRS_Diag_04021] [SRS_Diag_04024] [SRS_Diag_04031] [SRS_Diag_04032] [SRS_Diag_04033] [SRS_Diag_04057] [SRS_Diag_04058] [SRS_Diag_04059] [SRS_Diag_04063] [SRS_Diag_04064] [SRS_Diag_04085] [SRS_Diag_04086] [SRS_Diag_04087] [SRS_Diag_04089] [SRS_Diag_04090]

Requirement	Description	Satisfied by
		[SRS_Diag_04100] [SRS_Diag_04101] [SRS_Diag_04107] [SRS_Diag_04119] [SRS_Diag_04120] [SRS_Diag_04121] [SRS_Diag_04135] [SRS_Diag_04143] [SRS_Diag_04144] [SRS_Diag_04145] [SRS_Diag_04146] [SRS_Diag_04147] [SRS_Diag_04156] [SRS_Diag_04157] [SRS_Diag_04159] [SRS_Diag_04162] [SRS_Diag_04166] [SRS_Diag_04189] [SRS_Diag_04190] [SRS_Diag_04195] [SRS_Diag_04198] [SRS_Diag_04199] [SRS_Diag_04205] [SRS_Diag_04206] [SRS_Diag_04208] [SRS_Diag_04209] [SRS_Diag_04210] [SRS_Diag_04211] [SRS_Diag_04218]
[RS_Main_00060]	AUTOSAR shall provide a standardized software interface for communication between Applications	[SRS_Diag_04182] [SRS_Diag_04183] [SRS_Diag_04185] [SRS_Diag_04186] [SRS_Diag_04194] [SRS_Diag_04204]
[RS_Main_00100]	AUTOSAR shall provide standardized Basic Software	[SRS_Diag_04085] [SRS_Diag_04143] [SRS_Diag_04144] [SRS_Diag_04145] [SRS_Diag_04146]
[RS_Main_00130]	AUTOSAR shall provide an abstraction from hardware	[SRS_Diag_04077]
[RS_Main_00260]	AUTOSAR shall provide diagnostics means during runtime, for production and services purposes	[SRS_Diag_04002] [SRS_Diag_04003] [SRS_Diag_04059] [SRS_Diag_04067] [SRS_Diag_04068] [SRS_Diag_04071] [SRS_Diag_04091] [SRS_Diag_04093] [SRS_Diag_04097] [SRS_Diag_04098] [SRS_Diag_04110] [SRS_Diag_04111] [SRS_Diag_04112] [SRS_Diag_04113] [SRS_Diag_04115] [SRS_Diag_04117] [SRS_Diag_04118] [SRS_Diag_04120] [SRS_Diag_04121] [SRS_Diag_04123] [SRS_Diag_04124] [SRS_Diag_04126] [SRS_Diag_04127] [SRS_Diag_04129] [SRS_Diag_04131] [SRS_Diag_04133] [SRS_Diag_04136] [SRS_Diag_04137] [SRS_Diag_04139] [SRS_Diag_04140] [SRS_Diag_04147] [SRS_Diag_04148] [SRS_Diag_04150] [SRS_Diag_04151] [SRS_Diag_04153] [SRS_Diag_04155] [SRS_Diag_04160] [SRS_Diag_04161] [SRS_Diag_04163] [SRS_Diag_04164] [SRS_Diag_04165] [SRS_Diag_04166] [SRS_Diag_04167] [SRS_Diag_04168] [SRS_Diag_04169] [SRS_Diag_04170] [SRS_Diag_04171] [SRS_Diag_04172]

Requirement	Description	Satisfied by
		[SRS_Diag_04173] [SRS_Diag_04174] [SRS_Diag_04177] [SRS_Diag_04178] [SRS_Diag_04179] [SRS_Diag_04180] [SRS_Diag_04189] [SRS_Diag_04190] [SRS_Diag_04192] [SRS_Diag_04194] [SRS_Diag_04195] [SRS_Diag_04196] [SRS_Diag_04197] [SRS_Diag_04198] [SRS_Diag_04199] [SRS_Diag_04200] [SRS_Diag_04201] [SRS_Diag_04202] [SRS_Diag_04203] [SRS_Diag_04205] [SRS_Diag_04206] [SRS_Diag_04208] [SRS_Diag_04209] [SRS_Diag_04210] [SRS_Diag_04213] [SRS_Diag_04214] [SRS_Diag_04215] [SRS_Diag_04216] [SRS_Diag_04217] [SRS_Diag_04218]
[RS_Main_00420]	AUTOSAR shall use established software standards and consolidate de-facto standards for basic software functionality	[SRS_Diag_04067] [SRS_Diag_04068] [SRS_Diag_04097] [SRS_Diag_04105] [SRS_Diag_04109] [SRS_Diag_04110] [SRS_Diag_04111] [SRS_Diag_04113] [SRS_Diag_04124] [SRS_Diag_04125] [SRS_Diag_04169] [SRS_Diag_04170] [SRS_Diag_04171] [SRS_Diag_04172] [SRS_Diag_04173] [SRS_Diag_04174] [SRS_Diag_04192] [SRS_Diag_04204] [SRS_Diag_04216]
[RS_Main_00440]	AUTOSAR shall standardize access to non-volatile memory	[SRS_Diag_04077]

6 References

6.1 Deliverables of AUTOSAR

1. General Requirements of Basic Software Modules: *AUTOSAR_SRS_BSWGeneral.pdf*
2. Specification of the Virtual Functional Bus : *AUTOSAR_EXP_VFB.pdf*
3. Software Standardization Template : *AUTOSAR_TPS_StandardizationTemplate.pdf*

6.2 Related standards and norms

6.2.1 ITEA-EAST

4. D1.5-General Architecture; ITEAEAST-EEA, Version 1.0; chapter 3, page 72 et seq.

5. D2.1-Embedded Basic Software Structure Requirements; ITEAEAST-EEA, Version 1.0 or higher
6. D2.2-Description of existing solutions; ITEA/EAST-EEA, Version 1.0 or higher.

6.2.2 ISO

7. ISO 14229-1 Unified diagnostic services (UDS) Part 1: Specification and Requirements (v.2013)
8. ISO 15031-5 Communication between vehicle and external equipment for emissions related diagnostics Part 5: Emissions related diagnostic services (2005-01-13)
9. ISO 15765-3 Diagnostics on controller area network (CAN) Part 3: Implementation of unified diagnostic services (UDS on CAN) (2004-10-06)
10. ISO 15765-4 Diagnostics on controller area network (CAN) Part 4: Requirements for emissions-related systems (2005-01-04)