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

Document Version	2.2.0
Document Status	Final
Part of Release	3.2
Revision	2

Document Change History

Date	Version	Changed by	Change Description
07.03.2012	2.2.0	AUTOSAR Administration	Added requirement BSW04083
23.03.2011	2.1.1	AUTOSAR Administration	Legal disclaimer revised
24.07.2008	2.1.0	AUTOSAR Administration	• Remove requirement BSW04062 • Added requirement BSW04082 for OBDII support • Legal disclaimer revised
31.10.2007	2.0.3	AUTOSAR Administration	• Document meta information extended • Small layout adaptations made
24.01.2007	2.0.2	AUTOSAR Administration	• “Advice for users” revised • “Revision Information” added
28.11.2006	2.0.1	AUTOSAR Administration	Legal Disclaimer revised
06.04.2006	2.0.0	AUTOSAR Administration	Minor formal changes
30.06.2005	1.0.0	AUTOSAR Administration	Initial Release

Disclaimer

Advice for users

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

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

Table of Contents

1 Scope of this document

The goal of AUTOSAR WP4.2.2.1.4 and this document is to define to what extent elements of the diagnostic basic software have to be configurable and what preliminaries they shall comply with to meet the tailoring requirements. The handling of the legislated OBD and enhanced Diagnostics shall also 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’ new elements of basic software should be part of the set.

If such the definition of these new elements is not part of this work package. Nevertheless the information about basic software elements additionally required shall be given to related work groups.

Constraints

First scope for specification of requirements on basic software modules are systems which are not safety relevant. For implementation of the basic software modules in safety relevant systems, it shall be checked if additional requirements are necessary.

For this document we refer to ISO 15031-5. The equivalent SAEJ1979 is not mentioned explicitly but is covered accordingly.

2 How to read this document

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

2.1 Conventions used

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

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. Note that the requirement level of the document in which they are used modifies the force of these words.

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

2.2 Requirements structure

Each module specific chapter contains a short functional description of the Basic Software Module. Requirements of the same kind within each chapter are grouped under the following headlines (where applicable):

Functional Requirements:
- Configuration (which elements of the module need to be configurable)
- Initialisation
- Normal Operation
- Shutdown Operation
- Fault Operation
- ...

Non-Functional Requirements:
- Timing Requirements
- Resource Usage
- Usability
- Output for other WPs (e.g. Description Templates, Tooling,...)
- ...

3 Acronyms and abbreviations

Acronym:	*Description:*
External diagnostic tool	It is a device which is NOT permanently connected within the vehicle communication network. This device could be connected to the vehicle for various purposes, as e.g. • development • manufacturing • service (garage) Know devices are e.g. • a diagnostic tester • an OBD scan tool The external diagnostic tool is to be connected by a mechanic to gather information from “inside” the car.
Internal diagnostic tool	It is a device/ECU which could be connected permanently within the vehicle communication network. The purpose of this device/ECU could be a functionality as e.g. • advanced event tracking • advanced analysis’s for service mechanics. The behavior of the device/ECU could be the same as if it is an external diagnostic tool. The meaning of ´internal diagnostic tool´ is NOT that it is included in each ECU as a AUTOSAR SW-Component.
AUTOSAR application	A SW-application above the RTE which is using the API’s defined by DCM and DEM
Monitoring path	A monitoring path represents a diagnostic symptom and it is assigned to a unique event ID.
Event	In case of the use of the term Event a Diagnostic event is meant.
Diagnostic test results	De-bounced and qualified test result provided by a monitoring function.

4 Requirement Specification

4.1 Functional Requirements

4.1.1 General

4.1.1.1 [BSW04010] Interface between Diagnostic service handling and Diagnostic event (error) management

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	DEM and DCM shall ensure interaction in order to fulfill ISO 14229-1 and 15031-5
Type:	New
Importance:	High
Description:	The interface between the ´Diagnostic Service Handling´ (DCM) and the ´Diagnostic Event (error) Management´(DEM) shall ensure a interaction according to the ISO14229-1. The DCM shall use the interface provided by the DEM to process the required diagnostic service send by a diagnostic tester.
Rationale:	ISO14229-1
Use Case:	Improved fault and event tracking and analysis for Service, assembly line, OBD-SCAN-Tool
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.1.2 [BSW04082] Support of ISO15031-5 and SAE J1979

Initiator:	WPII-2.1.4
Date:	27.03.2008
Short Description:	The diagnostic modules DCM and DEM shall provide standardized interfaces to support OBD services as defined in ISO15031-5 and SAE J1979.
Type:	New
Importance:	High
Description:	The DCM and the DEM provide interface to support OBD services $01 to $0A to access Parameter Identifiers (PIDs), Diagnostic Test Results and further OBDII specific data.
Rationale:	--
Use Case:	--
Dependencies:	Configuration
Conflicts:	--
Supporting Material:	--

4.1.2 Diagnostic Event Manager (DEM)

4.1.2.1 [BSW04002] Basic SW Module for Diagnostic event (error) management

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The Diagnostic event (error) management shall be established as Basic SW Module.
Type:	New
Importance:	High
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
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.2 [BSW04057] Classification of event

Initiator:	WP4.2.2.1.4
Date:	17.06.2004
Short Description:	The DEM shall support a classification of events for series production, OBD and expert usage.
Type:	New
Importance:	High
Description:	The DEM 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 stored in the DET. Therefore, a special DET API shall be used which is not provided by the DEM.
Rationale:	After sales analysis
Use Case:	Distinction between service station relevant and after sales relevant events.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.3 [BSW04061] Distinction between different function groups

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall provide mechanisms to distinguish between different applications.
Type:	New
Importance:	High
Description:	The DEM shall process event information of different applications, i.e. Software components.
Rationale:	Unique Event IDs in DEM
Use Case:	Distinction between different applications using the same DEM by their application function group in case of merged applications on one single ECU.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.4 [BSW04063] Single Event ID for each monitoring path

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall process a dedicated Event ID for each monitoring path.
Type:	New
Importance:	High
Description:	For the internal administration the DEM needs a unique identification of each monitoring path. This identification shall be handled via an Event ID value (Integer).
Rationale:	Unique Event IDs in DEM
Use Case:	Unique fault identification which can be used for enhanced debugging
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.5 [BSW04065] Clearing of events or event groups

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM and DCM shall process the deletion of events or event groups.
Type:	New
Importance:	High
Description:	The DEM and DCM shall process the deletion of events or event groups according to ISO14229 AnnexD1 and ISO15031-5.
Rationale:	ISO 14229, ISO15031-5
Use Case:	Single Event deletion a) Support of ´mechanics´ which can follow step by step (DTC by DTC) the repair process Event Group deletion: a) Support of ´mechanics´ who can delete areas of faults which are subsequent faults of the first one. b) OBD faults
Dependencies:	[BSW111], [BSW113]

Conflicts:	--
Supporting Material:	--

4.1.2.6 [BSW04066] Provision of a ´Secondary Event Memory´

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall support the distinction of Primary and Secondary Event Memory.
Type:	New
Importance:	High
Description:	Provision of a Secondary Event Memory is optional and for internal usage by OEM and supplier, e.g. only used for development and product improvements. a) The ´service station workers´ have only access to the ´Primary Event Memory´ b) The development departments of the OEMs and Suppliers have access to the ´Primary Event Memory´ and ´Secondary Event Memory´ The secondary event memory allows storage of development events. It is not a trace tool.
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
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.7 [BSW04058] Support deletion and reading services for ´Secondary Event Memory´

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	Deletion and reading services shall be supported for Secondary Event Memory.
Type:	New
Importance:	High
Description:	The DEM shall support event deletion and reading services separately for Primary and Secondary Event Memory.
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.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.8 [BSW04067] Counting and evaluation of events according to ISO 14229-1 DTCStatusMask

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DCM and DEM shall provide the diagnostic status information according to the DTCStatusMask, ISO 14229-1
Type:	New
Importance:	High
Description:	The DCM and DEM shall provide the diagnostic status information according to the DTCStatusMask, ISO 14229-1, Annex D5
Rationale:	Advanced fault analysis
Use Case:	Improved fault and event tracking and analysis
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.2.9 [BSW04068] Standardized Event forget/unlearn counting

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	Standardization of a event unlearn/forget behavior
Type:	New
Importance:	High
Description:	The property of unlearning capability for diagnostic events shall be configurable/calibratable. The number of cycles for event unlearning shall be configurable/calibratable. The cycle definition itself is event specific property. For emission related events based on the OBD/ISO defined cycles.
Rationale:	Advanced fault analysis
Use Case:	Improved fault and event tracking and analysis
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.2.10 [BSW04069] DEM System status indication

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	DEM shall provide information on indicator upon request of SW-C or other SW Basic modules.
Type:	New
Importance:	High
Description:	DEM shall provide information on indicator (Lamps, text message, beep, ...) upon request of SW-C or other SW Basic modules, which are configured (registered) to this event.
Rationale:	Information distribution to the SW components
Use Case:	Indications of the Malfunction Indicator Lamp (MIL)
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.11 [BSW04070] Event ´occurrence order´ definition

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	DEM shall process the order of the event occurrences in an appropriate and obvious manner.
Type:	New
Importance:	High
Description:	- The occurrence order shall be recognizable by e.g. time stamps or age. (storage of events shall be connected to age or timestamp) - Reoccurrence of events takes over the old position of the event - Reoccurrence of healed events are handled as new events.
Rationale:	Advanced fault analysis
Use Case:	Improved clustering and judging of events
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.2.12 [BSW04071] Event importance definition

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall process events according to their defined importance like priority and/or severity.
Type:	New
Importance:	High
Description:	The events shall be sorted or assigned to a specific priority (e.g. Severity Mask – ISO14229-1,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
Use Case:	Improved clustering and judging of events
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.2.13 [BSW04072] Extended event information

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall provide additional event information to report the occurrence of an event by km-stamp, driving cycles or time.
Type:	New
Importance:	High
Description:	Fault duration e.g. by km-stamp, driving cycles or time - Between failed and passed - Since failed - Since last clear
Rationale:	Advanced fault analysis
Use Case:	Improved clustering and judging of events/faults
Dependencies:	--

Conflicts:	--
Supporting Material:	ISO14229-1

4.1.2.14 [BSW04073] Event combination and compression

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	DEM shall process combined events which may consist of several different events.
Type:	New
Importance:	High
Description:	The DEM shall allow for combining several individual events to a different representing (combined) event that has its own event ID. The configuration of the DEM shall allow for enabling and disabling the support for “combined diagnostic events”. If “combined diagnostic events” are supported the configuration of the DEM shall allow for assigning each “diagnostic event” the attribute “combined diagnostic event ID”.
Rationale:	Advanced fault analysis
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.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.15 [BSW04074] Event related ´environmental data´

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall process event related environmental data.
Type:	New
Importance:	High
Description:	It shall be possible to store different environmental data/freeze frame sets per event.
Rationale:	Advanced fault analysis
Use Case:	Improved clustering and judging of events/faults
Dependencies:	Configuration/calibration: The number of freeze frame sets shall be configurable due to the different domain requirements and ECU complexities.
Conflicts:	--
Supporting Material:	--

4.1.2.16 [BSW04075] Event and DTC assignment

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall assign the SW component specific event to a customer

	specific DTC.
Type:	New
Importance:	High
Description:	Assignment of events to customer specific / standardized DTC's which shall be configurable related to number of DTCs.
Rationale:	Unique Event IDs in DEM
Use Case:	Improved clustering and judging of events/faults
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.17 [BSW04076] System Cycle definition

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	DEM shall provide a set of system cycles that may qualify the event in an additional manner (e.g. OBD)
Type:	New
Importance:	High
Description:	The cycles are used for event qualification or healing. Typical cycles are - driving cycle - engine warm up cycle - ignition on off cycle - power up power down cycle - operation active passive cycle - in or out of voltage range cycle
Rationale:	Event status management, ISO14229
Use Case:	Improved clustering and judging of events/faults
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.18 Interface and API

4.1.2.18.1 [BSW04077] Interface between DEM and NVRAM function

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The DEM uses standard mechanisms provided by NVRAM-Manager.
Type:	New
Importance:	High
Description:	--
Rationale:	Non volatile data storage
Use Case:	The DEM triggers data storage during normal ECU operation to avoid loss of volatile data / event information.
Dependencies:	NVRAM Manager
Conflicts:	--
Supporting Material:	--

4.1.2.18.2 [BSW04030] Interface between DEM and Monitoring SW Component

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The DEM shall provide an interface via the RTE to monitoring SW components for reporting and processing diagnostic test results.
Type:	New
Importance:	High
Description:	The DEM shall provide via the RTE an Interface to Monitoring SW Components for reporting and processing diagnostic results. Monitoring SW-components report diagnostic results as soon as new results are available.
Rationale:	Interface to event generating monitoring SW-Components
Use Case:	Ensure the basic diagnostic functionality
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.2.18.3 [BSW04031] Interface between DEM and Function Inhibition Manager

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The DEM shall notify the Function Inhibition Manager (FIM) upon changes of the event status in order to process them according to the SW components dependencies.
Type:	New
Importance:	High
Description:	Control (enable/disable) of functionalities of SW components based on the following inhibit condition: - faults
Rationale:	DEM information for Inhibition of functions.
Use Case:	Usage of DEM information for Inhibition of functions.
Dependencies:	FIM is not specified yet.
Conflicts:	--
Supporting Material:	--

4.1.3 Diagnostic communication management (DCM)

4.1.3.1 [BSW04007] Provide Diagnostic service handling

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The DCM shall provide the Diagnostic service handling for the SW-Components which are using the DCM.
Type:	New
Importance:	High
Description:	The DCM shall provide the diagnostic service handling, according to ISO14229-1, ISO 15031-5 and ISO 15765-4 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.
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1, ISO 15031-5, ISO 15765-4

4.1.3.2 [BSW04021] Switch diagnostic communication access

Initiator:	WP4.2.2.1.4
Date:	11.08.2004
Short Description:	The DCM shall support the handling of different diagnostic sessions in parallel.
Type:	New
Importance:	High
Description:	DCM needs to 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:	A internal vehicle diagnostic tester communication is interrupted by OBD diagnostic access request.
Dependencies:	[BSW04032] Support of different diagnostic addresses [BSW04061] Multiple or parallel usage from different applications of the DEM functionality
Conflicts:	--
Supporting Material:	--

4.1.3.3 [BSW04032] Support of different diagnostic addresses

Initiator:	WP4.2.2.1.4
Date:	18.08.2004
Short Description:	Different diagnostic addresses shall be supported by multiple (physical) channels.
Type:	New
Importance:	High
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 request are allowed in parallel.
Rationale:	High flexibility and granularity for addressing of SW-Components
Use Case:	At the service (garage) a fault symptom is based on functionality. The service only wants to address this functionality.
Dependencies:	[BSW04021] Switch diagnostic communication access [BSW04080] Support multi-channel capability for diagnostic communication
Conflicts:	--
Supporting Material:	--

4.1.3.4 [BSW04080] Support multi-channel capability for diagnostic communication

Initiator:	WP4.2.2.1.4
Date:	10.11.2004
Short Description:	The DCM shall support a multi-channel functionality for a parallel diagnostic communication.
Type:	New
Importance:	High
Description:	Advanced ECUs contain more than one functionality (e.g. board computer, instrument cluster). The DCM shall ensure that external/internal diagnostic tools could communicate to these functionalities in parallel. The DCM shall provide a multi-channel capability to handle the communication in parallel.
Rationale:	External and internal diagnostic tools could access different functionalities within the ECU in parallel.
Use Case:	Production: Parallel test sequence processing of different functions with an external diagnostic tool. Service (Garage): Reading the DTC's of all functions within an ECU in parallel.
Dependencies:	[BSW04021] Switch diagnostic communication access [BSW04032] Support of different diagnostic addresses
Conflicts:	--
Supporting Material:	--

4.1.3.5 Supported diagnostic Services

4.1.3.5.1 [BSW04000] Support Diagnostic Standard UDS (ISO14229-1)

Initiator:	WP4.2.2.1.4
Date:	20.7.2004
Short Description:	The DEM and DCM shall support Diagnostic Standard UDS (ISO14229-1).
Type:	New
Importance:	High
Description:	The DEM and DCM shall support all services of UDS Standard (ISO14229-1).
Rationale:	It will be the newest and harmonized Standard
Use Case:	Diagnostic with a UDS Tester
Dependencies:	[BSW04004] Configuration of Services by ISO Standards
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.3.5.2 [BSW04001] Support Diagnostic Standard OBD (ISO15031-5)

Initiator:	WP4.2.2.1.4
Date:	20.7.2004
Short Description:	The DEM and DCM shall support Diagnostic Standard OBD (ISO15031-5).
Type:	New
Importance:	High
Description:	The DEM and DCM shall support all services of OBD Standard (ISO15031-5).
Rationale:	This standard is required for emission related control units by law
Use Case:	Diagnostic with a OBD Tester (e.g. Scan Tool)
Dependencies:	[BSW04004] Configuration of Services by ISO Standards
Conflicts:	--
Supporting Material:	ISO15031-5

4.1.3.5.3 [BSW04005] SecurityAccess level handling is managed by DCM

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The DCM shall manage Security Access level handling.
Type:	New
Importance:	High
Description:	The DCM shall manage the handling of the UDS-service SecurityAccess (0x27) and also the Security level handling. The accessibility of the services (service identifier) in the actual security level shall be checked by the DCM
Rationale:	Some diagnostic services are in dependence to a security access level. Therefore it is necessary that the DCM has knowledge 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.
Dependencies:	[BSW04000] Support Diagnostic Standard UDS
Conflicts:	--
Supporting Material:	--

4.1.3.5.4 [BSW04006] Session handling is managed by DCM

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	Session handling of different diagnostic sessions is managed by DCM.
Type:	New
Importance:	High
Description:	The DCM 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 that the DCM has knowledge 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.
Dependencies:	[BSW04000] Support Diagnostic Standard UDS [BSW04005] SecurityAccess level handling is managed by DCM
Conflicts:	--
Supporting Material:	--

4.1.3.5.5 [BSW04016] Provision of Busy Handling

Initiator:	WP4.2.2.1.4
Date:	11.08.2004
Short Description:	The DCM shall support a “Busy handling” by sending a negative response 0x78.
Type:	New
Importance:	High
Description:	DCM 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.
Dependencies:	[BSW04000] Support Diagnostic Standard UDS
Conflicts:	--
Supporting Material:	ISO15765-3, ISO14229-1

4.1.3.5.6 [BSW04019] Application callback after transmit confirmation

Initiator:	WP4.2.2.1.4
Date:	11.08.2004
Short Description:	The DCM shall confirm transmitting if complete to continue processing.
Type:	New
Importance:	High
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.

Use Case:	E.g. call of the reset function. This call needs to be done after transmission of the positive response is over.
Dependencies:	--
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.3.5.7 [BSW04020] Suppression of Responses

Initiator:	WP4.2.2.1.4
Date:	11.08.2004
Short Description:	DCM shall suppress responses to diagnostic tool requests.
Type:	New
Importance:	High
Description:	DCM shall suppress responses in following cases: - Suppress positive response (SuppressPosRequest Bit set) - Suppress negative responses (NRC 11, 12 and 31 at functional addressing)
Rationale:	This behavior is specified by ISO 14229-1. Prevent bus burst as result of a functional request.
Use Case:	--
Dependencies:	[BSW04000] Support Diagnostic Standard UDS
Conflicts:	--
Supporting Material:	ISO14229-1 chapter 6.5.2.2 “Functionally addressed client request message ISO15031-5 chapter 4.1.4 “Data not available”

4.1.3.5.8 [BSW04033] Upload/Download services for data handling

Initiator:	WP4.2.2.1.4
Date:	18.08.2004
Short Description:	The DCM shall support the upload/download services for reading/writing data in an ECU in a extended and manufacturer specific diagnostic session.
Type:	New
Importance:	High
Description:	The UDS services RequestDownload, RequestUpload, TransferData, RequestTransferExit (0x34-0x37) are used for data handling, e.g. accessing NVRAM. This does not interfere the reprogramming, because this is handled by the bootloader.
Rationale:	Enable a possibility to modify set of parameters.
Use Case:	End of line configuration in the manufacturing.
Dependencies:	[BSW04000] Support Diagnostic Standard UDS
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.3.5.9 [BSW04036] Format checking of diagnostic services

Initiator:	WP4.2.2.1.4
Date:	18.08.2004
Short Description:	The DCM shall check the format of diagnostic service. An incorrect service shall be rejected by a negative response.
Type:	New
Importance:	Low

Description:	The format checking shall include the service identifier (SID). Existing sub-service identifier shall be checked. The checks shall include: - diagnostic mode - access-level - message length Note: Further checking is done by the application.
Rationale:	The application won't get a request with incorrect format.
Use Case:	Failure Handling in communication.
Dependencies:	[BSW04000] Support Diagnostic Standard UDS
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.3.5.10 [BSW04083] Configurable behavior for NRC $78 handling in DCM for transition to bootloader

Initiator:	WP-2.1.4
Date:	07.03.2012
Short Description:	The DCM shall provide a configuration parameter to switch the NRC $78 handling for the session transition to bootloader on and off.
Type:	New
Importance:	Low
Description:	The DCM shall trigger the transmission of NRC 0x78 (Response pending), if and only if the configuration parameter DcmRespPendingOnTransitionToBootloader is set to TRUE. Otherwise (configuration parameter DcmRespPendingOnTransitionToBootloader is set to FALSE) the transition to bootloader shall be triggered immediately.
Rationale:	-
Use Case:	-
Dependencies:	[BSW04000] Support Diagnostic Standard UDS
Conflicts:	--
Supporting Material:	ISO14229-1

4.1.3.6 Timing Requirements

4.1.3.6.1 [BSW04015] Provision of timing handling according to ISO15765-3

Initiator:	WP4.2.2.1.4
Date:	11.08.2004
Short Description:	The DCM shall support timing handling according to ISO15765-3.
Type:	New
Importance:	High
Description:	In ISO15765-3 timing handling for physical and functional communication is described. Also how to react on errors. DCM 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.
Dependencies:	[BSW04059] Configuration of timing parameter
Conflicts:	--
Supporting Material:	ISO15765-3

4.1.3.7 Resource Usage

4.1.3.7.1 [BSW04017] Provide optimized buffer handling

Initiator:	WP4.2.2.1.4
Date:	11.08.2004
Short Description:	The DCM shall provide an optimized buffer handling, which could be used by the SW Component.
Type:	New
Importance:	High
Description:	If an SW Component gets a diagnostic request, it could be possible that the corresponding response required a huge amount of data to be transferred. In the case that the SW Component is not able to handle the Data of the response at one time, the DCM shall provide an optimized buffer handling to realize the response.
Rationale:	If there is no mechanism, as e.g. a ring buffer or buffer swapping, each ECU is forced to provide a Buffer, which could be as big as the maximum amount of Data that could be transferred over the used physical connection at one time.
Use Case:	Handling Diagnostic services, with the requirement to read a huge amount of data out of the ECU. Typically, these are services, which are used to read all DTC´s, transfer data, read or write data.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.3.8 Interface and API

4.1.3.8.1 [BSW04078] Interface to fault memory, fault status

Initiator:	WP4.2.2.1.4
Date:	29.02.2004
Short Description:	The DCM shall use a common API of the diagnostic event manager to access the fault memory.
Type:	New
Importance:	High
Description:	An external or internal diagnostic tool needs access to the fault memory to get or change information about the fault status. An interface between diagnostic communication management and diagnostic event management is required.
Rationale:	The DCM and the DEM are separated modules with the necessity to interact. Therefore an interface is necessary.
Use Case:	A diagnostic test tool needs to read or clear the fault memory with the corresponding diagnostic services, e.g. “ReadDTCInformation”, “ClearDiagnosticInformation”
Dependencies:	[BSW04002] Diagnostic event (error) management
Conflicts:	--
Supporting Material:	--

4.1.3.8.2 [BSW04011] Provide diagnostic state information

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The DCM shall provide diagnostic state information (e.g. session state, security access information) for AUTOSAR Software Component via RTE.
Type:	New
Importance:	High
Description:	The Software modules above the RTE 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.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.3.8.3 [BSW04003] Interface to PDU Router shall be network independent

Initiator:	WP4.2.2.1.4
Date:	21.7.2004
Short Description:	The interface of the DCM to PDU Router (CAN/LIN; FlexRay; MOST) shall be network independent.
Type:	New
Importance:	High
Description:	All network (CAN, LIN, FlexRay, MOST) dependent parts shall be done outside the DCM module. That means the module PDU Router shall provide a network independent interface.
Rationale:	The DCM 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:	DCM has to be network independent. So, the interface to the Transport Protocol shall be network independent.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.3.8.4 [BSW04079] The size of a FreezeFrame shall be reported to the DCM by the DEM

Initiator:	WP4.2.2.1.4
Date:	3.11.2004
Short Description:	The DEM shall be able to report the size of a FreezeFrame to the DCM.
Type:	New
Importance:	High
Description:	If FreezeFrames are supported the DEM shall be able to determine the size of a FreezeFrame and to provide this information via API call. The DCM requires this information due to the allocation of memory space for the storage of the FreezeFrame information.
Rationale:	FreezeFrames information to be provided for event analysis
Use Case:	An external testing tool connected to the vehicle requests currently stored

	error codes and the corresponding environmental data.
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.4 Configuration

4.1.4.1 [BSW04059] Configuration of timing parameter

Initiator:	WP4.2.2.1.4
Date:	30.08.2004
Short Description:	The DCM and DEM shall support the configuration of timing parameters.
Type:	New
Importance:	High
Description:	Every physical layer requires specific timing parameter values therefore it is necessary to include the ability to configure the timing constrains 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)
Dependencies:	[BSW04015] Provision of timing handling according to ISO15765-3
Conflicts:	--
Supporting Material:	--

4.1.4.2 [BSW04024] Configurable size of transferred data

Initiator:	WP4.2.2.1.4
Date:	18.08.2004
Short Description:	The DEM and DCM shall handle a configurable size of data transferred between DEM <-> DCM and DEM<->SW-C.
Type:	New
Importance:	High
Description:	Configurable parameters for setting the maximum size of data to be transferred via API-call.
Rationale:	Optimized usage of resources.
Use Case:	Transfer environmental / FreezeFrame data between DEM and DCM
Dependencies:	--
Conflicts:	--
Supporting Material:	--

4.1.4.3 [BSW04064] Event buffer shall be configurable concerning size

Initiator:	WP4.2.2.1.4
Date:	03.8.2004
Short Description:	The DEM shall support buffers of scalable sizes for the storage of the events, status information and environmental data.
Type:	New
Importance:	High
Description:	a) For the internal administration the DEM 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 DEM b) 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.
Dependencies:	[BSW106] (see SWS DEM document)
Conflicts:	--
Supporting Material:	--

4.2 Non-Functional Requirements (Qualities)

4.3 Output for other Modules

4.3.1 Requirements on Services (Services Layer)

[BSW04031] Interface to Function Inhibition Manager
[BSW04077] Interface between DEM and NVRAM function
[BSW04003] Interface to PDU Router shall be network independent

4.3.2 Requirements on RTE

[BSW04030] Interface between DEM and Monitoring SW Component
[BSW168] Diagnostic Interface of SW components
[BSW04011] Provide diagnostic state information
[BSW04012] Describe Interaction between Diagnostic service handling and Mode management (e.g. ECU Reset)

4.3.3 Requirements on ECU Abstraction Layer

[BSW04077] Event management needs access to NVRAM function
[BSW04014] Diagnostic needs access to RAM, ROM, EEPROM (read Memory by Address)
[BSW04003] Interface to PDU Router shall be network independent

5 References

5.1 Deliverables of AUTOSAR

[1] General Requirements of Basic Software Modules
AUTOSAR_SRS_General.pdf

[2] Specification of the Virtual Functional Bus
AUTOSAR_VirtualFunctionBus.pdf

5.2 Related standards and norms

5.2.1 ITEA-EAST

[3] D1.5-General Architecture; ITEA/EAST-EEA, Version 1.0; chapter 3, page 72 et seq.

[4] D2.1-Embedded Basic Software Structure Requirements; ITEA/EAST-EEA, Version 1.0 or higher

[5] D2.2-Description of existing solutions; ITEA/EAST-EEA, Version 1.0 or higher.

5.2.2 ISO

[6] ISO14229-1 Unified diagnostic services (UDS) - Part 1: Specification and Requirements (ISO DIS 26.05.2004)

[7] ISO15031-5 Communication between vehicle and external equipment for emissions-related diagnostics - Part 5: Emissions-related diagnostic services (2005-01-13)

[8] ISO15765-3 Diagnostics on controller area network (CAN) - Part 3: Implementation of unified diagnostic services (UDS on CAN) (2004-10-06)

[9] ISO 15765-4 Diagnostics on controller area network (CAN) - Part 4: Requirements for emissions-related systems (2005 01-04)