Elektrobit

Release Notes

EB tresos Safety Time and Execution Protection

Date: 2022-05-20, ID: ASCTIMESE-26, Document version 1.1.8, Status: RELEASED

Elektrobit Automotive GmbH
Am Wolfsmantel 46
91058 Erlangen, Germany
Phone: +49 9131 7701 0
Fax: +49 9131 7701 6333
Email: info.automotive@elektrobit.com

Technical support

https://www.elektrobit.com/support

Legal disclaimer

Confidential information.

Table of Contents

Document History

Version	Date	Author	State	Description
1.0.0	2013-03-15	role1472	DRAFT	Initial version
1.0.1	2013-05-03	geho2654	RELEASED	Release: TimESE-0.98
1.0.2	2013-06-14	role1472	RELEASED	Release: TimESE-1.0
1.0.3	2013-07-04	role1472	RELEASED	Release: TimESE-1.1 (QM)
1.0.4	2013-12-11	maho2907	RELEASED	Release: TimESE-1.2 (safety)
1.0.5	2015-10-23	geho2654	RELEASED	Release: TimESE-1.3 (safety), Maintenance Release
1.0.6	2019-02-13	vika1018	PROPOSED	Changed to the centralised doc engine
1.0.6	2019-02-14	vika1018	RELEASED	Set to released: ASCTIMESE-243
1.0.7	2018-10-26	vika1018	PROPOSED	Release: TimESE-1.4 (safety), Maintenance Release
1.0.8	2019-08-28	vika1018	PROPOSED	Release: TimESE-1.4 (safety), Maintenance Release updated to proper WdgM and WdgIf used module versions
1.0.9	2019-12-17	vika1018	RELEASED	Release: TimESE-2.0 (RFD)
1.1.0	2020-04-27	vika1018	PROPOSED	Release: TimESE-2.1 (RFM) Maintenance Release
1.1.1	2020-06-15	vika1018	PROPOSED	Release: TimESE-2.2 (RFM) Maintenance Release updated the resource consumption chapter with the new information
1.1.2	2020-06-30	vika1018	RELEASED	Release: TimESE-2.2 (RFM) ASCTIMESE-308 set to released
1.1.3	2020-08-27	vika1018	PROPOSED	Updated for TimESE-2.3
1.1.3	2020-09-04	daia1015	PROPOSED	Updated Resource consumption
1.1.3	2020-09-11	daia1015	RELEASED	Release: TimESE-2.3 (safety) ASCTIMESE-322 set to released
1.1.4	2021-04-21	vika1018	PROPOSED	Updated Resource consumption
1.1.5	2021-04-29	vika1018	RELEASED	Release: TimESE-2.4 (safety) ASCTIMESE-358 set to released
1.1.6	2021-12-17	vika1018	RELEASED	Release: TimESE-2.5 (RFM) ASCTIMESE-400 set to released
1.1.7	2022-05-18	vika1018	PROPOSED	Updated Resource consumption

Version	Date	Author	State	Description
1.1.8	2022-05-20	vika1018	RELEASED	Release: TimESE-2.6 (safety) ASCTIMESE-437 set to released

Table 1. Document history

1. Content of the release

1.1. BSW modules

The following table lists all hardware-independent modules which are part of this release.

Module name	Description	Module version
WdgM	Watchdog Manager Module	6.2.4
WdgIf	Watchdog Interface Module	6.2.4

Table 1.1. List of Hardware-Independent Modules

1.2. Documents

Document name	Document version
Safety Manual	0.3.21
Release Notes	1.1.8

Table 1.2. List of documents

2. General Release Notes

2.1. New and Noteworthy

- This release contains bugfixes and improvements (for details see the change log section of the modules).

2.2. AUTOSAR Compatibility

TimE including the AUTOSAR modules WdgM and WdgIf is developed according to AUTOSAR version R4.0 Rev 3 with enhancements compatibility to different AUTOSAR versions is achieved according to the following list:

- R3.1 and R3.2: compatible* with the following configuration constraints:

  TimE does not provide the APIs ActivateAliveSupervision and DeActivateAliveSupervision, but provides integration support for re-direction of these APIs to e.g. the Supervisor.

compatible*: compatible considering the limitations and deviations stated in module-specific release notes section.

2.3. Change log

This chapter lists the changes between different versions.

Release TimESE-2.6(safety)

2022-05-27

- WdgM module updated from version 6.2.3 to 6.2.4
- WdgIf module updated from version 6.2.3 to 6.2.4

Release TimESE-2.5 (safety)

2021-12-28

- WdgM module updated from version 6.2.2 to 6.2.3
- WdgIf module updated from version 6.2.2 to 6.2.3

Release TimESE-2.4 (safety)

2021-04-29

- WdgM module updated from version 6.2.1 to 6.2.2
- WdgIf module updated from version 6.2.1 to 6.2.2

Release TimESE-2.3 (safety)

2020-09-11

- WdgM module updated from version 6.2.0 to 6.2.1
- WdgIf module updated from version 6.2.0 to 6.2.1

Release TimESE-2.2 (RFM)

2020-06-30

- WdgM module updated from version 6.1.34 to 6.2.0
- WdgIf module updated from version 6.1.21 to 6.2.0

Release TimESE-2.1 (RFM)

2020-04-27

- WdgM module updated from version 6.1.31 to 6.1.34
- WdgIf module updated from version 6.1.19 to 6.1.21

Release TimESE-2.0 (RFD)

2019-12-17

- WdgM module updated from version 6.1.21 to 6.1.31
- WdgIf module updated from version 6.1.10 to 6.1.19

Release TimESE-1.4 (safety)

2019-08-28

- WdgM module updated from version 6.0.21 to 6.1.21
- WdgIf module updated from version 6.0.10 to 6.1.10

Release TimESE-1.3 (safety)

2015-10-23

- WdgM module updated from version 6.0.17 to 6.0.21
- WdgIf module updated from version 6.0.8 to 6.0.10

Release TimESE-1.2 (safety)

2013-12-16

- WdgM module updated from version 6.0.12 to 6.0.17
- WdgIf module not updated (version 6.0.8)

Release TimESE-1.1 (QM)

2013-07-04

- WdgM module updated from version 6.0.10 to 6.0.12
- WdgIf module updated from version 6.0.6 to 6.0.8

Release TimESE-1.0

2013-06-14

- WdgM module updated from version 6.0.9 to 6.0.10
- WdgIf module updated from version 6.0.5 to 6.0.6

Release TIME-0.98

2013-05-03

- WdgM module updated from version 6.0.8 to 6.0.9
- WdgIf module updated from version 6.0.4 to 6.0.5

Release TIME-0.9

2013-03-15

- WdgM module version 6.0.8
- WdgIf module version 6.0.4

3. Resource Consumption

For the performance tests the Autocore lead reference platform: TC29XT from AURIX shall be used.

The following compiler options summarize under which conditions the resource usage tests is performed:

Compiler	Options
TC29XT tasking50r2	--core=tc1.6.x -t --iso=99 --eabi-compliant --integer-enumeration --language=-comments,-gcc,+volatile,-strings --switch=auto --align=0 --default-near-size=0 --default-a0-size=0 --default-a1-size=0 -O2ROP --tradeoff=4 -g --source --fp-model=cflnrStz -DOS_TRICOREARCH=OS_TRICOREARCH_16EP -DOS_CPU=OS_TC29XT -DDEM_DONT_PROVIDE_LEGACY_SYMBOLIC_NAMES -DCOMPILERCFG_EXTENSION_MCAL_FILE

Table 3.1.

The following reference configuration is used for the performance tests:

- 15 Supervised Entities are configured.
- The Supervised Entities use different number of Checkpoints, ranging from 1 to 20 Checkpoints for one Supervised Entity.
- A combination of Alive Supervision, Logical Supervision, and Deadline Supervision is used.

The following resource consumption has been measured:

- Static RAM consumption: 1080 Byte
- Static ROM consumption: 18951 Byte

4. Module Release Notes

4.1. WdgM module release notes

- AUTOSAR R4.0 Rev 3
- AUTOSAR SWS document version: 2.2.0
- Module version: 6.2.4.B632837
- Supplier: Elektrobit Automotive GmbH

4.1.1. Change log

This chapter lists the changes between different versions.

Module version 6.2.4

2022-05-27

- TimE Protection license only: Removed TimE license for Logical Supervision and Deadline Supervision.
- ASCWDGM-979 Fixed known issue: Wrong supervised entity IDs are stored when the WdgMGetAllExpiredSEIDs feature is enabled.
- Add support for multicore mixed criticality.
- Time 2.6 RFM Release (Safety Approved).

Module version 6.2.3

2021-12-28

- ASCWDGM-911 Fixed known issue: Missing memory sections for multi-core main functions declaration.
- ASCWDGM-930 Added support for slave instance triggering of the watchdog drivers.
- ASCWDGM-914 Added support for partition reset.
- ASCWDGM-923 Added new callout to signal a MainFunction violation.
- ASCWDGM-905 Implemented new API to retrieve all expired Supervised Entities.
- Improved the generation of sattelite MainFunction BSWMD information.
- ASCWDGM-949 Fixed known issue: WdgM does not compile when SEs are not mapped to all WdgM core instances via an OsApp ref.

- Internal module improvement. This module version update does not affect module functionality.
- Time 2.5 RFM Release (Safety Approved).

Module version 6.2.2

2021-04-29

- ASCWDGM-826: Added ASR 4.3 service component compatibility for WdgM.
- ASCWDGM-865 Fixed known issue: Code generator mixes Index and WdgMSupervisedEntityId for symbol names.
- Internal module improvement. This module version update does not affect module functionality.
- Added generation of MainFunction Timing Event for TimE.
- Behavior improvement: Decrease execution time for configurations which have many Supervised Entities configured.
- Time 2.4 RFM Release (Safety Approved).

Module version 6.2.1

2020-09-11

- Change all NO_INIT memory sections to CLEARED and restriction on Deadline Supervision in the Limitations.xml file due to multicore use.
- Internal module improvement.
- Time 2.3 RFM Release (Safety Approved).

Module version 6.2.0

2020-06-30

- Time 2.2 RFM Release (Safety Approved).

Module version 6.1.34

2020-05-04

- Time 2.1 RFM Release.

Module version 6.1.33

2020-04-03

- ASCWDGM-812 Fixed known issue: WdgM_Mainfunction not generated for slaves

Module version 6.1.32

2020-02-21

- ASCWDGM-803 Fixed known issue: Different memory mapping area for definition and declaration of WdgM_EB_GlobalStatus
- ASCWDGM-795 Fixed known issue: WdgM service component does not work with multi-core distribution
- ASCWDGM-813 Fixed known issue: "Space" character present in the last line of the file WdgM_Lcfg.h leads to compiler error

Module version 6.1.31

2019-12-17

- TimE 2.0 RFD Release.

Module version 6.0.31

2019-10-11

- ASCWDGM-758 Fixed known issue: BSWMD does not generate the BSW implementations of all cores.

Module version 6.0.30

2019-06-14

- Implemented multicore support.

Module version 6.0.29

2018-10-25

- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.28

2018-06-22

- ASCWDGM-654 Fixed known issue: Variables are not assigned to a memory section.
- Internal module improvement. This module version update does not affect module functionality
- Removed AUTOSAR 3.1 support from the module.

Module version 6.0.27

2018-03-02

- Internal module improvement. This module version update does not affect module functionality
- Invert logic for AUTOSAR 4.0.2 and remove AUTOSAR 3.x legacy support for symbolic names
- ASCWDGM-629 Fixed known issue: Behaviour changed when the same alive supervision is used after switching the mode.
- Added immediate mode switch when calling WdgM_SetMode().

Module version 6.0.26

2017-09-22

- ASCWDGM-594 Fixed known issue: Dem event in WdgM_Cfg.h causes compilation error
- Comply to MISRA-C:2012

Module version 6.0.25

2017-03-31

- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.24

2017-03-10

- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.23

2016-11-07

- Extended license checks for logical supervision or deadline supervision to cover new license strings EB_-TIME_CFM and EB_TIME_DM as well.

Module version 6.0.22

2015-11-06

- Added non-functional code improvements to fix compiler warnings.

Module version 6.0.21

2015-10-23

- Added non-functional code improvements to fix compiler warnings.

Module version 6.0.20

2015-06-19

- ASCWDGM-515 Fixed known issue: Support for automatic configuration of DEM events

Module version 6.0.19

2015-01-07

- Added non-functional code improvements to fix MISRA violations.

Module version 6.0.18

2014-04-25

- Added non-functional code improvements to improve text of some container descriptions

Module version 6.0.17

2013-12-13

- Added support for the integration into an AUTOSAR 3.1 environment
- ASCWDGM-467 Fixed known issue: Compilation fails on case-sensitive file systems
- ASCWDGM-493 Fixed known issue: Configuration for reporting of DEM events `WDGM_E_MONITORING` and `WDGM_E_SET_MODE` is not possible if DEM event `WDGM_E_IMPROPER_CALLER` is not used

Module version 6.0.16

2013-10-11

- Added non-functional code improvements to update source code documentation for production error reporting
- ASCWDGM-474 Fixed known issue: The WdgM may not compile if reporting a production error to the Diagnostic Event Manager is configured
- Added non-functional code improvements to ease the integration of the WdgM into an ASR31 environment
- TimE Protection license only: Removed obsolete feature for the configuration of DEM callouts

Module version 6.0.15

2013-08-07

- Added non-functional code improvements to fix incorrect generation of macro values `0.0U` to `0U`

Module version 6.0.14

2013-07-24

- Added non-functional code improvements to deal with tasking compiler bug on XC2361E (V2.5 r1)

Module version 6.0.13

2013-07-23

- ASCWDGM-447 Fixed known issue: The WdgM uses incorrect compiler abstraction

Module version 6.0.12

2013-07-11

- Fixed minor code issues (non-function changes) for future debugging support

Module version 6.0.11

2013-06-25

- Fixed compiler warning on XC2k derivate reported from a tasking compiler
- Added non-functional code improvements
- ASCWDGM-412 Fixed known issue: TimE Protection license only: A data corruption in the internal WdgM data may not result in Global Supervision Status `EXPIRED`

Module version 6.0.10

2013-06-14

- ASCWDGM-379 Fixed known issue: Inconsistent starting point of the Supervision Reference Cycle for the first evaluation of Alive Supervision
- ASCWDGM-378 Fixed known issue: TimE Protection license only: The WdgM never recovers from `FAILED` state in case the Error Recovery feature is enabled and only Deadline Supervision or/and Logical Supervision are configured for the current WdgM mode

- ASCWDGM-383 Fixed known issue: Wrong individual mode switch notification behavior during initialization and de-initialization phases
- ASCWDGM-384 Fixed known issue: TimE Protection license only: Missing checks allow an inconsistent configuration leading to undefined behavior if Deadline or Logical Supervision is used
- ASCWDGM-385 Fixed known issue: TimE Protection license only: Deadline Supervision may not be evaluated according to the specification with respect to parameters `WdgMMainFunctionPeriodTolerance`, `WdgMSupervisionCycle`, `WdgMDeadlineMax`, and `WdgMDeadlineMin`
- Added non-functional code improvements
- Added simple Dbg instrumentation for tracing of function enter/exit points
- ASCWDGM-385 Fixed known issue: Unspecified behavior if `WdgIf_SetMode` fails during initialization of the WdgM.
- ASCWDGM-393 Fixed known issue: TimE Protection license only: Unspecified behavior of Alive Supervision if configured together with Logical or Deadline Supervision and an enabled Error Recovery
- ASCWDGM-397 Fixed known issue: TimE Protection license only: The WdgM does not compile for some specific Deadline Supervision configurations
- ASCWDGM-404 Fixed known issue: The WdgM does not compile if more than one CallerId ID is configured for a mode switch request
- ASCWDGM-406 Fixed known issue: TimE Protection license only: Unspecified behavior if the WdgM switches back to an old mode while some Supervisions are still active

Module version 6.0.9

2013-04-30

- Added non-functional code improvements
- ASCWDGM-359 Fixed known issue: TimE Protection license only: WdgM does not compile if callout API is configured for `GetExpectedWdgMMode`
- ASCWDGM-361 Fixed known issue: TimE Protection license only: Deadline Supervision is not performed for Checkpoints which are configured to be both Start Checkpoint and End Checkpoint
- Implemented tracking of a failed Logical Supervision Status for the successor Checkpoints of a Logical Supervision Graph
- ASCWDGM-363 Fixed known issue: TimE Protection license only: A failed Deadline Supervision may not lead to global state `EXPIRED` if Error Recovery is enabled
- ASCWDGM-369 Fixed known issue: TimE Protection license only: The individual mode switch callout API contains an incorrect old mode if the Supervised Entity is deactivated
- ASCWDGM-371 Fixed known issue: The WdgM does not overwrite an active initialization request when required to by a call to `WdgM_DeInit()`

Module version 6.0.8

2013-03-15

- Added support for Alive Supervision of multiple Checkpoints of a Supervised Entity
- TimE Protection license only: Added support for Logical Supervision
- TimE Protection license only: Added support for Deadline Monitoring
- TimE Protection license only: Implemented detection of deadline violation of Supervised Entities in the granularity of the main function cycle
- Implemented smooth error reaction without a reset for individual Supervised Entities
- TimE Protection license only: Implemented detection of timing violation of schedule main function
- Added non-functional code improvements

Module version 6.0.7

2013-02-08

- Added specification of Memory Mappings to Basic Software Module Description

Module version 6.0.6

2012-12-21

- Added non-functional code improvements
- Implemented usage of AUTOSAR conform type naming for `ModeDeclarationGroups`
- TimE Protection license only: Added support for integration in safety projects up to ASIL level D

Module version 6.0.5

2012-10-12

- Added AUTOSAR 3.2 support of Rte Interface and SWCD
- Added non-functional code improvements
- Added support for optional generation of Service APIs according to AUTOSAR 3.2

Module version 6.0.4

2012-08-17

- Added definition of Exclusive Area Activation in Basic Software Module Description

- Fixed minor issues in generated WdgM Service Component Description
- Added support of symbolic name generation for Checkpoint IDs via Rte

Module version 6.0.3

2012-07-13

- Added internal mode switch to a final mode within `WdgM_DeInit` is now optional

Module version 6.0.2

2012-06-15

- Updated WdgM to derive value for `WdgMWatchdogName` from container name
- Fixed compiler warning in case no Wdgs are configured
- ASCWDGM-248 Fixed known issue: The Watchdog trigger conditions are incorrectly updated in the `MainFunction()` after an enforced reset via `WdgM_PerformReset()`
- Added switches for optional containers on same tabs as lists
- ASCWDGM-256 Fixed known issue: Inconsistent storage class specification for `WdgM_EB_UpdateTriggerConditions()` and `WdgM_EB_SetMode()` cause an error or warning

Module version 6.0.1

2012-03-16

- Added non-functional code improvements
- Added generation of BSWMD

Module version 6.0.0

2012-02-17

- Initial AUTOSAR 4.0 version

4.1.2. New features

- Support for mixed core ASIL levels.

4.1.3. Elektrobit-specific enhancements

This chapter lists the enhancements provided by the module.

- Optimized usage of WdgM in case no RTE is used

  Description:

  The parameter `WdgMRteUsage` (see `WDGM.EB.WdgMRteUsage_Conf`) can be used to disable the RTE interface of the Watchdog Manager. This means that the Watchdog Manager module can be used without an RTE if needed.

  Rationale:

  Disabling the usage of the Rte makes the integration of the WdgM at the beginning easier.

- Enhanced production error reporting

  Description:

  An enhanced production error reporting mechanism has been introduced. This allows to configure the following options independently for each Dem event:

  - Report production errors to the Diagnostics Event Manager (Dem).
  - Report production errors to the Development Error Tracer (Det) as development errors.
  - Do not report production errors at all.

  If a production error is redirected towards the Det, you may configure the reported Det error-ID.

  Rationale:

  This enhancement implements the HIS requirements concerning fault operation and error detection: HisGen0007, HisGen0008, and HisGen0009.

- Watchdog Manager mode switch to a sleep mode

  Description:

  The configuration parameter `WdgMSleepMode` in the general tab of a `WdgMConfigSet` entry (see `WDGM.EB.WdgM_DeInit.2`) allows the integrator to specify a sleep mode. The `WdgM_DeInit` function then updates the trigger conditions via a Watchdog Manager mode switch to this sleep mode.

  Rationale:

  The integrator of the WdgM can specify the WdGM sleep mode. The EcuM does not need to explicitly switch the WdgM mode before it calls the `DeInit` function.

- Provision of Checkpoint IDs via WdgM Service Component Description

  Description:

The WdgM Service Component Description specifies the name of the configured Checkpoint IDs of each Supervision Entity as a constant within the interface description as follows: `WdgMConf_WdgMCheckpoint_<CheckpointName>`.

Rationale:

A SWC usually includes only the corresponding Rte header file and not the BSW header file of the Watchdog Manager. Therefore, the Rte must have knowledge about the configured Checkpoint IDs in order to generate the symbolic name values for the Checkpoint IDs used in the SWC.

- Support for optional generation of AUTOSAR 3.2 Service Component Description

  Description:

  Support for the generation of AUTOSAR 3.2, or AUTOSAR 4.0 service APIs and Software Component Description as well as default service APIs and Software Component Description which can be configured to adhere either to AUTOSAR 3.2 or 4.0 schema version.

  Rationale:

  AUTOSAR 3.2/3.1 application SWCs of Tier-1 shall be deployed in an AUTOSAR 4.0 environment or AUTOSAR 3.2/3.1 environment.

- Support for the configuration of callout functions for the integration into projects with ASIL level up to ASIL D

  Description:

  The Watchdog Manager provides the configuration of callout functions for the following:

  - Error indication (instead of DET and DEM reporting).
  - Periodically polling the information regarding the Watchdog Manager state (e.g. Initialization, Watchdog Manager Mode, etc.) from an external entity (e.g. Safety Manager) instead of providing the APIs `WdgM_Init`, `WdgM_DeInit`, or `WdgM_SetMode`.

  Rationale:

  Support for the integration of Time and Execution Protection for automotive projects with ASIL level up to ASIL D.

- Detection of deadline violations in the granularity of the main function cycle

  Description:

  In addition to deadline supervision of AUTOSAR, the Watchdog Manager detects a deadline violation in the granularity of the main function period in case the Stop Checkpoint of an active deadline monitoring is never called.

  Rationale:

Required for projects having ASIL level up to ASIL D.

- Detection of timing violation of scheduled main function

  Description:

  The Watchdog Manager monitors its own main function period and reports an error in case a timing violation is detected.

  Rationale:

  Required for projects having ASIL level up to ASIL D.

- Smooth error reaction without a reset for individual Supervised Entities.

  Description:

  The Watchdog Manager provides the configuration of a smooth error reaction with error recovery for individual Supervised Entities. In this case, the Watchdog Manager reports the status of a failed Supervision without entering the `Expired` state such that a Watchdog reset will not be performed.

  Rationale:

  Projects may require a different error strategy than provided by the Watchdog Manager (Watchdog reset) in case a Supervised Entity fails.

- Tracking of a failed Logical Supervision Status for the successor Checkpoints of a Logical Supervision Graph

  Description:

  If the Watchdog Manager detects a failed Logical Supervision for a called Checkpoint participating in an active Supervision Graph, then a call to the API `WdgM_CheckpointReached()` shall return `E_NOT_OK` for all successor Checkpoints of this Supervision Graph.

  Rationale:

  A Software Component participating in a control loop (e.g. responsible for controlling an actuator) may trust on the return value of the API `WdgM_CheckpointReached()` to decide whether or not the input values are produced in the correct sequence. Thus the input values can be used independent of the schedule period of Watchdog Manager `MainFunction`.

4.1.4. Deviations

This chapter lists the deviations of the module from the AUTOSAR standard.

- BswM_WdgM_RequestPartitionReset API is not supported

Description:

In contrast to WDGM225 which states that the WdgM shall restart/shutdown the partition of an OS Application which is configured for a Supervised Entity by calling `BswM_WdgM_RequestPartitionReset` of the Basic Software Mode Manager module, the WdgM will call `WdgMRequestPartitionResetCallout` (see WDGM.EB.TIMEPM.WDGM020121_Conf) of container `WdgMSupervisorCallouts` instead.

Requirements:

WDGM225, WDGM162

- Post-build time configuration

Description:

Only pre-compile time configuration is supported (reference to product description: ASCPD-77)

Requirements:

WDGM127, WDGM004, WDGM042, WDGM010, WDGM029, WDGM266, WDGM255

- The WdgM does not check if a Supervised Entity ID equals some AUTOSAR module ID

Description:

In contrast to AUTOSAR which does not allow the configuration of SWC Supervised Entities with a Supervised Entity ID value that is equal to the module ID of any AUTOSAR BSW module, there is no such constraint on the Supervised Entity ID values. Users/integrators are responsible for the correct configuration of Supervised Entity ID values and the possible consequences.

Rationale:

There may exist use-cases in legacy projects where some Supervised Entities are not associated to SWCs. Therefore these Supervised Entities may require the configuration of the ID of some AUTOSAR BSW module.

Requirements:

WDGM307

- Optional detection of production code errors

Description:

In contrast to AUTOSAR which does not allow to switch off the detection of production code errors for each individual production code error, the following is possible:

- To keep the production code error as specified.
- To report the production code error to the Development Error Tracer (DET) instead.

- To completely switch off the detection of the production code error.

Rationale:

User-specific configuration of production code errors.

Requirements:

WDGM015

- De-initialization of the Watchdog Manager independent of global Supervision Status

Description:

In contrast to AUTOSAR which allows the de-initialization only from global Supervision Status `WDGM_GLOBAL_STATUS_OK`, the Watchdog Manager can be de-initialized independent of the actual global Supervision Status.

Rationale:

The caller of `WdgM_DeInit` must be aware of the actual global Supervision Status.

Requirements:

WDGM286

- Consistent interpretation of parameter `WdgMFailedAliveSupervisionRefCycleTol`

Description:

AUTOSAR generally defines the parameter `WdgMFailedAliveSupervisionRefCycleTol` as the number of allowed failed reference cycles until a Supervised Entity goes into state `WDGM_LOCAL_STATUS_EXPIRED`. However, AUTOSAR specifies a state machine where one additional failed reference cycle is allowed. In contrast to the state machine specified in AUTOSAR, the implementation allows at most `WdgMFailedAliveSupervisionRefCycleTol` failed reference cycles until a Supervised Entity goes into state `WDGM_LOCAL_STATUS_EXPIRED`.

See Bugzilla entry http://www.autosar.org/bugzilla/show_bug.cgi?id=58303

Requirements:

WDGM206, WDGM204

- Consistent interpretation of parameter `WdgMExpiredSupervisionCycleTol`

Description:

AUTOSAR generally defines the parameter `WdgMExpiredSupervisionCycleTol` as the number of allowed main function cycles in global state `WDGM_GLOBAL_STATUS_EXPIRED` until the WdgM enters the global state `WDGM_GLOBAL_STATUS_STOPPED`. However, AUTOSAR specifies a state machine where

two additional main function cycles in global state `WDGM_GLOBAL_STATUS_EXPIRED` are allowed. In contrast to the state machine specified in AUTOSAR, the implementation allows at most `WdgMExpiredSupervisionCycleTol` main function cycles in global state `WDGM_GLOBAL_STATUS_EXPIRED` until the WdgM enters the global state `WDGM_GLOBAL_STATUS_STOPPED`.

See Bugzilla entry http://www.autosar.org/bugzilla/show_bug.cgi?id=58303

Requirements:

WDGM077, WDGM219, WDGM220

- Symbolic port names instead of numeric port name numbering

Description:

In contrast to requirements WDGM.ASR40.WDGM147 and WDGM.ASR40.WDGM149, the RTE ports are named by their symbolic short name taken from the configuration.

Rationale:

Symbolic port names do not change when ports are deleted or inserted as it is the case for numeric names because they get renumbered and need to be reconnected. Also the symbolic name can be chosen to reflect the purpose of a port which makes the port connection process easier and less error prone.

Requirements:

WDGM147, WDGM149

- `WdgM_GetVersionInfo` as a function

Description:

In contrast to WDGM262 which suggests to implement the API as a macro in case caller and callee of `WdgM_GetVersionInfo` are available at compile time, the WdgM always implements the API as a function.

Requirements:

WDGM262

- No AUTOSAR Debugging support

Description:

WdgM is not instrumented for the usage with AUTOSAR Debugging.

Requirements:

WDGM238, WDGM239, WDGM240, WDGM241, WDGM242, WDGM234, WDGM235, WDGM236, WDGM237

- WdgM does not check the versions of other modules

  Description:

  In contrast to WDGM013, the WdgM does not check the version numbers of included header files from other modules.

  Rationale:

  In general, the modules are delivered within a whole AutoCore delivery, in which the versions are consistent and therefore do not have to be checked.

  Furthermore, this allows the combination of the module with other AUTOSAR compatible but not fully compliant modules. This might e.g., permit to combine the module with (adapted) modules from different AUTOSAR releases or with non-AUTOSAR modules that simulate the necessary behavior.

  Requirements:

  WDGM013

- Mode switch is done synchronously or asynchronously (synchronously to `MainFunction`) if the WdgMSetModeSynchron is set respectively not set.

  Description:

  In contrast to AUTOSAR which specifies that a call to `WdgM_SetMode` immediately switches the WdgM mode (WDGM186), the `WdgM_SetMode` request is applied either at the end of the next `MainFunction` call, either like AUTOSAR specifies, depending on how the WdgMSetModeSynchron parameter is configured.

  See Bugzilla entry http://www.autosar.org/bugzilla/show_bug.cgi?id=57805.

  Requirements:

  WDGM154

- (De-)Initialization is done synchronously to `MainFunction`

  Description:

  In contrast to AUTOSAR which specifies that a call to `WdgM_Init` or `WdgM_DeInit` immediately initializes or de-initializes the Watchdog Manager, the Watchdog Manager is (de-)initialized at the next `MainFunctionCycle`.

  Requirements:

  WDGM268, WDGM269, WDGM285, WDGM298, WDGM296, WDGM151, WDGM018, WDGM135, WDGM350, WDGM286, WDGM261

- Non-compliant deviations in vendor-specific module definition file

Description:

The vendor-specific module definition file (VSMD) has non-compliant deviations to the AUTOSAR specification:

Violations against Rule EcucSws_1014: Additional vendor specific parameter definitions (using ParameterTypes), container definitions and references shall be added to the VSMD according to the alphabetical order.

This affects variables and containers in following StMD-Nodes:

- `/AUTOSAR/WdgM`
- `/AUTOSAR/WdgM/WdgMGeneral`

Rationale:

A merge of AUTOSAR and vendor specific variables in these containers intentionally results in a different order for a clear arrangement of vendor specific parameters in EB tresos Studio.

4.1.5. Limitations

This chapter lists the limitations of the module. Refer to the module references chapter *Integration notes*, subsection *Integration requirements* for requirements on integrating this module.

- Restriction of numbering of Checkpoint IDs

  Description:

  WDGM306_Conf does not specify any constraints for the parameter `WdgMCheckpointId` except that the ID must be unique within the Supervised Entity. In contrast to WDGM306_Conf, all Checkpoint IDs within a Supervised Entity must be zero-based and dense.

  Rationale:

  This reduces the consumption of RAM and ROM.

  Requirements:

  WDGM306_Conf

- Restriction of number of configurable Checkpoints per Supervision Entity

  Description:

The AUTOSAR Specification of the Watchdog Manager specifies that the container `WdgMCheckpoint` as part of `WdgMSupervisedEntity` has a maximum multiplicity of 65535. In contrast to this, at most 256 checkpoints can be configured for a Supervision Entity.

Rationale:

This reduces the consumption of RAM and ROM.

Requirements:

WDGM305_Conf

- Restriction of number of configurable Supervision Entities

Description:

The AUTOSAR Specification of the Watchdog Manager specifies that the container `WdgMSupervisedEntity` as part of `WdgMGeneral` has a maximum multiplicity of 65535. In contrast to this, at most 256 Supervised Entities can be configured.

Rationale:

This reduces the consumption of RAM and ROM.

Requirements:

WDGM303_Conf

- Restriction on ID range of Checkpoints and Supervised Entities

Description:

AUTOSAR states that the range of valid IDs depends on the number of configured Supervised Entities and on the chosen platform type. In contrast to this, the WdgM always uses the maximum possible range of `uint16` instead of `uint8`.

Requirements:

WDGM038

- Restriction on dynamic change of the main function period

Description:

In contrast to AUTOSAR which specifies a mode-dependent `WdgM_MainFunction` period, the `MainFunction` period is always defined via the `WdgMSupervisionCycle` parameter of the first configured mode.

- Restriction on architectural assumption regarding data access

Description:

The CPU of the ECU where WdgM is integrated provides 32-bit data types which can be read and written in an atomic way.

- Restriction on Deadline Supervision

Description:

Checkpoints used in Deadline Supervision must be called from the same core.

4.1.6. Open-source software

WdgM does not use open-source software.

4.2. Wdglf module release notes

- AUTOSAR R4.0 Rev 3
- AUTOSAR SWS document version: 2.5.0
- Module version: 6.2.4.B632837
- Supplier: Elektrobit Automotive GmbH

4.2.1. Change log

This chapter lists the changes between different versions.

Module version 6.2.4

2022-05-27

- Time 2.6 RFM Release (Safety Approved).

Module version 6.2.3

2021-12-28

- Internal module improvement. This module version update does not affect module functionality.

- Time 2.5 RFM Release (Safety Approved).

Module version 6.2.2

2021-04-29

- Internal module improvement. This module version update does not affect module functionality.
- Time 2.4 RFM Release (Safety Approved).

Module version 6.2.1

2020-09-11

- Change all NO_INIT memory sections to CLEARED.
- Internal module improvement.
- Time 2.3 RFM Release (Safety Approved).

Module version 6.2.0

2020-06-30

- Time 2.2 RFM Release (Safety Approved).

Module version 6.1.21

2020-05-04

- Time 2.1 RFM Release.

Module version 6.1.20

2020-02-21

- ASCWDGIF-321 Fixed known issue: Wrong checks in the configuration for VendorApiInfix will lead to generation fails.

Module version 6.1.19

2019-12-17

- Time 2.0 RFD Release.

Module version 6.0.19

2019-10-11

- Implemented ASIL tags.

Module version 6.0.18

2019-06-14

- Implemented multicore support.
- Support for BSWMD VendorApiInfix.

Module version 6.0.17

2019-04-18

- Update generator to disable vendor infix for a single referenced driver.

Module version 6.0.16

2018-10-25

- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.15

2018-05-25

- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.14

2018-03-02

- Implemented macro-redefinition guards.
- Implemented compliance to MISRA-C:2012.
- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.13

2017-09-22

Module version 6.0.12

2017-04-03

- Internal module improvement. This module version update does not affect module functionality.

Module version 6.0.11

2016-11-07

- Changed WdgIf_ModeType form enumaration to macro definition.

Module version 6.0.10

2014-07-11

- Improved ECUC parameter checks

Module version 6.0.9

2013-12-13

- Added non-functional code improvements
- Updated the Basic Software Module Description to specify all external and internal APIs (Basic Software Module Entities)

Module version 6.0.8

2013-07-04

- Added non-functional code improvements

Module version 6.0.7

2013-06-25

- Added non-functional code improvements

Module version 6.0.6

2013-06-14

- Added non-functional code improvements

Module version 6.0.5

2013-05-10

- ASCWDGIF-207 Fixed known issue: WdgIf uses wrong API calls to the Wdg driver if multiple Wdgs are configured

Module version 6.0.4

2013-03-15

- Added non-functional code improvements

Module version 6.0.3

2013-02-08

- Added specification of memory mappings to Basic Software Module Description

Module version 6.0.2

2012-10-12

- Changed the top-level structure of the software-component description in the ARXML files from `/AUTOSAR/WdgIf` to `/AUTOSAR_WdgIf`
- Added non-functional code improvements

Module version 6.0.1

2012-03-16

- Added macro definition for single Wdg driver independent of Det
- Removed compiler warnings for redefined `WdgIf_SetMode` and `WdgIf_SetTriggerCondition`
- Added symbolic name values for `WdgIfDeviceIndex`
- Added generation of BSWMD

Module version 6.0.0

2012-02-17

- Initial AUTOSAR 4.0 version

4.2.2. New features

- No new features have been added since the last release.

4.2.3. Elektrobit-specific enhancements

This chapter lists the enhancements provided by the module.

- This module provides no Elektrobit-specific enhancements.

4.2.4. Deviations

This chapter lists the deviations of the module from the AUTOSAR standard.

- No consistency check between code files and header files

  Description:

  The inter-module version checks as specified by the WdgIf SWS are not implemented.

  Rationale:

  - The required compile-time version checks would result in an inflexible, hardly integratable basic software stack.
  - EB tresos AutoCore is an already integrated product.
  - The project handling of EB tresos Studio provides means to enforce that only modules with the same EB tresos AutoCore release version can be added to the project.

  Requirements:

  WDGIF005

- No AUTOSAR Debugging support

  Description:

WdgIf is not instrumented for the usage with AUTOSAR Debugging.

WDGIF052, WDGIF053, WDGIF054, WDGIF055

4.2.5. Limitations

This chapter lists the limitations of the module. Refer to the module references chapter *Integration notes*, subsection *Integration requirements* for requirements on integrating this module.

- For this module no limitations are known.

4.2.6. Open-source software

WdgIf does not use open-source software.