Safe Watchdog Interface
Safety Manual

Author:	TTTech Automotive GmbH
Security:	Company Confidential
Document number:	D-SAFEX-S-70-005
Version:	1.8.9
Date:	22.05.2014
Status:	ALM_Published
MKS ID:	232906

TTTech Automotive GmbH
Schoenbrunner Str. 7, A-1040 Vienna, Austria, Tel. + 43 1 585 34 34-0, Fax +43 1 585 34 34-90, office@tttech-automotive.com

Revision History

30.05.2012 V1.0.0 Creation (based on MKS 185841)
27.06.2012 V1.1.0 Reviewed. Some information still open.
03.07.2012 V1.2.0 Added config generation and verification process
05.07.2012 V1.3.0 Added requirements from ETA and Check against System Specification
06.07.2012 V1.3.1 Ready for Release 1.8.2
13.08.2012 V1.3.2 Feedback from Hella-Audit, some texts more precise
10.09.2012 V1.3.3 Added chapter "S-WdgIf Generator - Verification".
13.09.2012 V1.3.4 Dissolved ETA section. Corrected review findings.
15.09.2012 V1.3.5 Safe Watchdog Interface ASIL Release
17.09.2012 V1.8.1 issue48784 (new version)
06.11.2012 V1.8.2 updated according to WdgIf_GetTickCounter() (issue49948)
07.11.2012 V1.8.3 updated after review (issue49948)
03.04.2014 V1.8.4 Update after customer review, changes summarised in the issue52277
24.04.2014 V1.8.5 Updated parts related to AS driver compatibility (issue62032:msg467581, issue59785)
Updated 240758: parameter WdgIfUseAutosarDrvApi
Updated 260205: added vendor ID (WD driver function names)
Added 555654: parameter WDGIF_USE_AUTOSAR_DRV_API
Updated 289398: API differences (WDGIF_USE_AUTOSAR_DRV_API)
Updated 234584, 235159, 283153: API compatibility (WDGIF_USE_AUTOSAR_DRV_API)
Added 556326, changed 289394, 289398, 289412, 289455: Description of the <drv> shortcut
Changed 233039, 234584, 235159, 283153: added *vendor-id* string
08.05.2014 V1.8.6 Updated according to the review remarks (issue62032:msg469458, issue62032:msg469460)
12.05.2014 V1.8.7 Updated according to the review remarks (issue62032:msg472152)
14.05.2014 V1.8.8 Updated according to the review remarks (issue62032:msg473209)
22.05.2014 V1.8.9 Language Review (issue63157)

Table of Contents

Category:	Comment	Keywords:		ID:	552153

We Listen to Your Comments

If there is any information in this document that is wrong, unclear or missing?
Your feedback will help us to continuously improve the quality of this document. Please contact TTTech Automotive GmbH support if you have questions, change requests or suggestions for improvement related to the Safety Module or documentation. The TTTech Automotive GmbH support can be reached via the following e-mail address: support@tttech.com.

1 Introduction

1.1 Purpose of this Document

Category:	Comment	Keywords:		ID:	233001

This document is the Software Safety Manual for the software component Safe Watchdog Interface (S-WdgIf). The S-WdgIf was developed by TTTech as an SEooC according to ISO 26262 (2011) for use in safety related items up to ASIL D (see [ISO26262]). This document contains the requirements that have to be satisfied to integrate and apply the S-WdgIf into a safety-related item.

Category:	Comment	Keywords:		ID:	233003

The S-WdgIf is a part of the S-WdgM Stack. It contains also a S-WdgIf Configuration Generator to generate configuration dependent S-WdgIf code.

Category:	Comment	Keywords:		ID:	233005

This document contains the requirements that have to be met to:

- install the S-WdgIf Generator,
- generate the S-WdgIf code with the S-WdgIf Configuration Generator,
- integrate the S-WdgIf code into an AUTOSAR system, and
- to apply the S-WdgIf within an AUTOSAR system.

Category:	Comment	Keywords:		ID:	233019

Note: This document just describes requirements for the S-WdgIf. This document does not provide a full description of how to create a safe system. For example, this document is not concerned with hardware architectural metrics that may have an influence on software running on this hardware. These considerations are not specific to the S-WdgIf and are thus beyond the scope of this manual.

Category:	Comment	Keywords:		ID:	559910

The S-WdgIf was developed according to AUTOSAR version 3.1.4 [AS_WDGIF_SWS_3_1] and AUTOSAR version 4.0.1 [AS_WDGIF_SWS]. The S-WdgIf is compatible with both AUTOSAR versions but not fully compliant. For the deviations see [TT_WDGIF_UM].

1.1.1 Target Audience and Responsibilities

Category:	Comment	Keywords:		ID:	233007

The requirements are intended for the (system) integrator, who is responsible for the generation of the S-WdgIf configuration, the integration of the S-WdgIf in(to) a safety-related item and its application.

Category:	Requirement	Keywords:		ID:	233009
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall be an expert in the area of functional safety with deep knowledge of ISO 26262 (see [ISO26262]). Moreover, the integrator needs to know:

- the AUTOSAR architecture,
- the ANSI C programing language, and
- the S-WdgIf User Manual [TT_WDGIF_UM]).

Category:	Comment	Keywords:		ID:	233011

The integrator shall ensure that all requirements defined in this Safety Manual are fulfilled in the integrated item.

Category:	Requirement	Keywords:		ID:	233013
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall also follow the instructions in:

- the Safety Manual for the S-WdgM (see [TT_WDGM_SM]) and
- the Safety Manual for the used S-Wdg drivers (see the driver specific Safety Manual. Examples can be found in section "References" at the end of this document) which describe the other parts of the S-WdgM Stack.

1.1.2 Structure of this Document

Category:	Comment	Keywords:		ID:	233017

Requirements are explicitly marked as "Requirement" in this document. All requirements described in this document shall be considered by the integrator. Explanatory text that does not represent an explicit requirement is marked as "Comment".

Category:	Comment	Keywords:		ID:	554241

Note: Document items of the type "Comment" do not represent explicit action items for the integrator, however, the integrator is advised to ensure that there are no contradictions between the comment and the intended S-WdgIf usage.

Category:	Comment	Keywords:		ID:	554243

Comments related to a requirement are placed below the related requirement.

Category:	Comment	Keywords:		ID:	554242

Note: Requirements in this document shall be treated either as safety related or need not be treated as safety related, depending on the S-WdgIf use case:

- If the S-WdgIf is used to monitor a safety related application then for each used S-WdgIf functionality all corresponding requirements shall be treated as safety related.
- If the S-WdgIf is used to monitor a QM application then the SM requirements need not be treated as safety related.

As a consequence, the field "Safety relevant" for each requirement is always empty.

Category:	Comment	Keywords:		ID:	554244

The list shows some keywords used in requirements and their explanation:

Key Word	Description
must, shall, required, is responsible for, is the responsibility of	Requirement is mandatory.
shall not	Requirement is a prohibition.

table 1

2 Terms

Category:	Comment	Keywords:		ID:	260274

Configuration Tool	A tool (like DaVinci Configurator Pro) that creates a Safe Watchdog Interface configuration.
Error Escalation	The escalation of a detected fault to the Watchdog by a Watchdog reset or omittance of the Watchdog trigger.
Safe Watchdog Driver	The lower and hardware dependent software layer of the S-WdgM Stack. It controls the Watchdog device.
Safe Watchdog Interface	The middle and hardware independent software layer of the S-WdgM Stack.
Safe Watchdog Interface Configuration	The part of the S-WdgIf code that is generated by the S-WdgIf Generator from an ECU description file.
Safe Watchdog Interface Configuration Generator	A tool from TTTech that generates the S-WdgIf Configuration out of an ECU description file. In this document the name is abbreviated to "S-WdgIf Generator". The tool is part of the S-WdgIf package.
Safe Watchdog Manager	The upper and hardware independent software layer of the S-WdgM Stack. It communicates with the application through RTE.
Safe Watchdog Manager Stack	The stack comprises the S-WdgM, the Safe Watchdog Interface and the Safe Watchdog driver(s).
System	A set of elements that relates at least a sensor, a controller and an actuator with one another (see [ISO26262], part1). In this document, the MCU is part of the system.
Watchdog (device)	A Watchdog device is the hardware that provides the watchdog function. It can be an internal watchdog (on the MCU) or an external device.
WD Mode	The "WD Mode" defines the period timeout. It is set with WdgIf_SetMode () and can be "slow", "fast" or "off" (WD disabled). Do not confuse with "WD Trigger Mode".
WD Trigger Mode	The "WD Trigger Mode" defines the WD trigger window (start and length) together with the "WD Mode". It is set with WdgM_SetMode ().

table 2

3 Notations

Category:	Comment	Keywords:		ID:	233039

Notation	Description
text	Italic text is a placeholder for a name or text pattern. E.g.: In Wdg_*infix*_Init (), the text *infix* is a placeholder for the actual name of the used WD driver.
infix	A placeholder with this name is interpreted as follows: • In case of an AUTOSAR 3.1 environment, the placeholder *infix* stands for the name of the configured WD device. • In case of an AUTOSAR 4.0 environment, the placeholder *infix* stands for the pattern *vendor-id_device-name*, where *vendor-id* is the ID of the vendor of the WD driver and *device-name* is the name of the configured WD device.

table 3

4 Abbreviations

Category:	Comment	Keywords:		ID:	233047

API	Application Programming Interface
ASIL	Automotive Safety Integrity Level
AUTOSAR	Automotive Open System Architecture
BSW	Basic Software (AUTOSAR term)
DEM	Diagnostic Event Manager
DET	Development Error Tracer
ECU	Engine Control Unit
ISO	International Organization for Standardization
MCU	Microcontroller Unit
MPU	Memory Protection Unit. Usually this is part of the Microcontroller.
MemMap	Memory Mapping (for Memory Management)
QM	Quality Managed (Software)
SM	Safety Manual
SPI	Serial Peripheral Interface (Module)
S-Wdg	Safe Watchdog Driver (from TTTech)
S-WdgM	Safe Watchdog Manager (from TTTech)
S-WdgIf	Safe Watchdog Interface (from TTTech)
S-WdgM Stack	The "S-WdgM Stack" comprises the S-WdgM, the S-WdgIf and the used Safe Watchdog driver(s).
WD	Watchdog
WdgM	Watchdog Manager according to the AUTOSAR 4.0 specification
WdgIf	Watchdog Interface according to the AUTOSAR 4.0 specification

table 4

5 Safe Watchdog Interface Overview

Category:	Comment	Keywords:		ID:	233043

For an overview of and more details about

- the S-WdgIf,
- the other S-WdgM Stack components, and
- the S-WdgIf Generator

see the according user manuals and Safety Manuals:

- for the S-WdgM: [TT_WDGM_UM], [TT_WDGM_SM],
- for the S-WdgIf: [TT_WDGIF_UM] and this document, or
- for the S-Wdg drivers: the according Safety Manual.

See section "References" at the end of this document.

6 System Assumptions

Category:	Comment	Keywords:		ID:	270643

The system assumptions are a subset of the S-WdgM system assumptions (see [TT_WDGM_SM]).

Category:	Comment	Keywords:		ID:	559912

The S-WdgIf is designed for integration into an AUTOSAR 3.1.4 and 4.0.1 system. However, it is not restricted to these AUTOSAR versions. The software module can also be integrated into other versions of AUTOSAR and other system SW architectures, provided that the integration related requirements listed in the Safety Manual are met.

6.1 Assumptions in this Document

Category:	Comment	Keywords:		ID:	282959

The following requirements and comments are placed in the according context in this document. They may be interpreted as system assumptions or not - depending on the circumstances the system is developed and applied:

Requirement	Description
260213, 234568, 235165, 237306	Quality level degradation by external interfaces to 3rd party modules. *1).
260213	Quality level degradation by external interfaces to S-WdgM Stack modules *2).
236022	S-WdgIf functionality affected by other SW.
260197, 260217, 236258, 236382	WD driver and WD device.
236356	Memory sections, access rights.
236044, 237369, 236430, 236434	Memory corruption.
260205	External Interfaces.

table 5

*1) The 3rd party modules are not part of the S-WdgM Stack.
*2) The external interfaces between S-WdgM, S-WdgIf and S-Wdg do not have to be verified if:

- the modules are part of the same S-WdgM Stack release,
- the modules are not altered by the integrator, and
- the modules are integration tested by TTTech.

7 S-WdgIf Function Requirements

Category:	Comment	Keywords:		ID:	270650
For the system requirements that the S-WdgM Stack fulfills, see[TT_WDGM_SM].					

8 S-WdgIf Configuration

Category:	Comment	Keywords:		ID:	233053

The S-WdgIf Configuration is the part of the S-WdgIf code that is generated with the S-WdgIf Generator out of a given ECU description file.
This section lists the safety requirements for the creation of a S-WdgIf Configuration.

Category:	Comment	Keywords:		ID:	233055

For a description of

- the configuration fields in the ECU description file and
- how to create S-WdgIf code out of the ECU description file

see [TT_WDGIF_UM].

8.1 Configuration Check-List

Category:	Comment	Keywords:		ID:	233059

The S-WdgIf Generator performs basic checks on the ECU description file when it generates the S-WdgIf Configuration.
The following list provides instructions for manual checks of safety relevant configuration values that cannot be performed by the S-WdgIf Generator.

8.1.1 General Requirements

Category:	Requirement	Keywords:		ID:	234105
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall set the configuration parameters according to the project specification.

Category:	Requirement	Keywords:		ID:	552162
Label:		Safety relevant:			
Related To:		Related To':			

The ECU description file that serves as input for the generation of the S-WdgIf Configuration files shall comply to the AUTOSAR schema defined in comment 559910 above.

Category:	Comment	Keywords:		ID:	554249

Note: These are the AUTOSAR versions for which the S-WdgIf was developed and tested.

Category:	Comment	Keywords:		ID:	554878

The AUTOSAR version used for S-WdgIf integration tests is defined in [TT_WDGS_ITR].

8.1.2 Compiler Settings

Category:	Requirement	Keywords:		ID:	240758
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__264807,__MKSID__264811,__MKSID__552843		

The following fields in the ECU description file shall be "true" if the according feature shall be enabled, otherwise "false":

Field	Feature
WdgIfVersionInfoApi	Enable Version API.
WdgIfDevErrorDetect	Enable Development error detection.
WdgIfUseAutosarDrvApi	Enable AUTOSAR compatible WD driver API.

table 6

Category:	Requirement	Keywords:		ID:	240769
Label:		Safety relevant:			
Related To:		Related To':			

If an internal HW tick counter is used, then the field WdgIfInternalTickCounterRef shall be defined such that is refers to a WD driver, otherwise the field WdgIfInternalTickCounterRef is omitted.

Category:	Comment	Keywords:		ID:	240773

If WdgIfInternalTickCounterRef is a S-WdgIf information and refers to a WD driver, the driver must

- support an internal tick counter and
- its parameter WdgInternalTickCounter must be "true".

This is checked automatically by the S-WdgIf Configuration Generator.

8.1.3 Post Build Configuration and Application Settings

Category:	Comment	Keywords:		ID:	240764

This section provides a check list for the various aspects and configuration fields that must be considered for post build configuration of the S-WdgIf.

Category:	Comment	Keywords:		ID:	240766

For further information on configuration fields see [TT_WDGIF_UM].

Category:	Requirement	Keywords:		ID:	260197
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall make sure that the configuration has

- only one WD driver and
- only one WD device for the driver

defined.

Category:	Comment	Keywords:		ID:	242221
The current implementation of the S-WdgM Stack supports only one WD device per WD driver. If configured so, the S-WdgIf Generator yields an error message.					

Category:	Comment	Keywords:		ID:	260225
As a consequence, the device index that is passed to the WD driver functions is always 0.					

Category:	Requirement	Keywords:		ID:	260199
Label:		Safety relevant:			
Related To:		Related To':			
The integrator shall ensure that the names of the WD driver functions in the generated S-WdgIf configuration match the actual names of the functions in the WD driver.					

Category:	Requirement	Keywords:		ID:	260205
Label:		Safety relevant:			
Related To:		Related To':			

In case a Watchdog Driver is used that is not implemented by TTTech, the integrator shall make sure that the WD driver supports the following functions:

- Wdg_*infix*_SetMode () and
- Wdg_*infix*_SetTriggerWindow () or Wdg_*infix*_SetTriggerCondition ().

Category:	Comment	Keywords:		ID:	260201
The S-WdgIf Generator fills the placeholder (*infix*) automatically.					

Category:	Requirement	Keywords:		ID:	260217
Label:		Safety relevant:			
Related To:		Related To':			

If an internal HW tick counter is configured (i.e. WdgIfInternalTickCounterRef is defined),
then the integrator shall make sure that the WD driver supports the function Wdg_*infix*_GetTickCounter ().

Category:	Requirement	Keywords:		ID:	260213
Label:		Safety relevant:			
Related To:		Related To':			

In case a Watchdog Driver is used that is not implemented by TTTech, the integrator shall verify that the functions that are offered by the WD driver (listed in section "Expected Interface", Comment 234584) and called from the S-WdgIf do not degrade the quality level of the S-WdgIf below the required quality level.

9 S-WdgIf Configuration Generator

Category:	Comment	Keywords:		ID:	234331
This section lists the safety requirements for the installation and application of the S-WdgIf Generator.					

Category:	Comment	Keywords:		ID:	234333
For information on how to use the S-WdgIf Generator, see [TT_WDGIF_UM].					

Category:	Comment	Keywords:		ID:	234335
Note: the S-WdgIf Generator is **not** ASIL-D and ilts output cannot be trusted. The generated files must be verified manually as described in "S-WdgIf Generator - Verification".					

9.1 S-WdgIf Generator - Installation

Category:	Requirement	Keywords:		ID:	234339
Label:		Safety relevant:			
Related To:		Related To':			
If the S-WdgIf Generator is installed and used on a different OS than Windows 7 with Service Pack 1, the integrator is responsible for ensuring that the change of the underlying OS does not affect the behavior and output of the S-WdgIf Generator.					

Category:	Comment	Keywords:		ID:	234341
The S-WdgIf Generator has been tested on Windows 7 with Service Pack 1.					

9.2 S-WdgIf Generator - Application

Category:	Requirement	Keywords:		ID:	234345
Label:		Safety relevant:			
Related To:		Related To':			
The selected output path for the generated S-WdgIf code (runtime argument "OUTPUT-DIRECTORY") shall be empty before the S-WdgIf Generator is started.					

Category:	Comment	Keywords:		ID:	234347
If the output path is not empty, code from previous generation runs may be accidentally integrated into the AUTOSAR system.					

Category:	Comment	Keywords:		ID:	263318
The names of the generated files are listed on standard error (stdout).					

Category:	Requirement	Keywords:		ID:	234349
Label:		Safety relevant:			
Related To:		Related To':			
If the S-WdgIf Generator aborts the generation process with an error, the (partially) generated output files shall not be used in an AUTOSAR system.					

Category:	Comment	Keywords:		ID:	234351
Error messages start with "Error" and they are displayed on standard error (stderr). If successful, the S-WdgIf Generator returns error level 0, otherwise an error level higher than 0 is returned.					

Category:	Requirement	Keywords:		ID:	234353
Label:		Safety relevant:			
Related To:		Related To':			
If the S-WdgIf Generator displays a warning message, the integrator shall ensure that the cause of the warning does not invalidate the generated S-WdgIf Configuration.					

Category:	Comment	Keywords:		ID:	234355
Warning messages start with "Warning" and are displayed on standard error (stderr). If successful (although with a warning), the S-WdgIf Generator returns error level 0, otherwise an error level higher than 0 is returned.					

Category:	Comment	Keywords:		ID:	234359
TTTech provides a sample demonstration configuration with four supervised entities. The files may be used by the integrator, but they are intended for demonstration only.					

Category:	Comment	Keywords:		ID:	234361
The S-WdgIf Generator is not configurable. The S-WdgIf Generator process is controlled by the input arguments only.					

9.3 S-WdgIf Generator - Verification

Category:	Comment	Keywords:		ID:	289334
This section describes how to verify the generated files manually.					

Category:	Requirement	Keywords:		ID:	289342
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__297368		
Check that the set of generated files is complete. It consists of: • WdgIf_Cfg_Features.h, • WdgIf_Lcfg.h, and • WdgIf_Lcfg.c.					

9.3.1 Check of WdgIf_Cfg_Features.h

Category:	Requirement	Keywords:		ID:	289346
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__264811		
If - and only if - WdgIfVersionInfoApi in the ECU Description file is "true", then WDGIF_VERSION_INFO_API shall be set STD_ON, otherwise STD_OFF.					

Category:	Requirement	Keywords:		ID:	555654
Label:		Safety relevant:			
Related To:	__MKSID__552843	Related To':			

If - and only if - WdgIfUseAutosarDrvApi in the ECU Description file is "true",
then WDGIF_USE_AUTOSAR_DRV_API shall be set STD_ON, otherwise STD_OFF.

Category:	Requirement	Keywords:		ID:	289352

Category:	Requirement	Keywords:		ID:	289394
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__58842		

The following structures shall be defined:
- "WdgIf_InterfaceFunctionsType *infix*_functions",
- "WdgIf_InterfaceFunctionsPerWdgDeviceType WdgIf_FunctionsPerWdg [WDGIF_NUMBER_OF_WATCHDOGS]" (an array of structures), and
- "WdgIf_InterfaceType WdgIf_Interface".

Category:	Requirement	Keywords:		ID:	289406
Label:		Safety relevant:			
Related To:		Related To':			

The structures listed in 289394 above shall be memory mapped to WDGIF_START_SEC_CONST_UNSPECIFIED.

Category:	Requirement	Keywords:		ID:	289398
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__55578,__MKSID__55580		

The structure "*infix*_functions" shall contain the following field values (and in this order):
- "Wdg_*infix*_SetMode" and
- "Wdg_*infix*_SetTriggerWindow" if WDGIF_USE_AUTOSAR_DRV_API is set to STD_OFF and "Wdg_*infix*_SetTriggerCondition" if WDGIF_USE_AUTOSAR_DRV_API is set to STD_ON.

Category:	Comment	Keywords:		ID:	289410

The fields refer to the functions of the used WD driver to set the WD trigger.

Category:	Requirement	Keywords:		ID:	289412
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__297362,__MKSID__297324		

The array WdgIf_FunctionsPerWdg shall contain a single array item with the following field values (in this order):
- "&*infix*_functions" and
- "0".

Category:	Comment	Keywords:		ID:	289414

The value 0 refers to the position of each WD (starting with 0) assigned to the WD driver referred to by *infix*. There is only one WD configurable for a driver.

Category:	Requirement	Keywords:		ID:	289455
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__55582,__MKSID__297312,__MKSID__239282		

The structure WdgIf_Interface shall contain the following field values:
- "WDGIF_NUMBER_OF_WATCHDOGS",

- "WdgIf_FunctionsPerWdg", and
- "Wdg_*infix*_GetTickCounter" if - and only if - WDGIF_INTERNAL_TICK_COUNTER is set to STD_ON.

10 Safe Watchdog Interface

Category:	Comment	Keywords:		ID:	234556
This section lists the safety requirements for the integration and application of the S-WdgIf code in/into an AUTOSAR system.					

10.1 API Specification

Category:	Comment	Keywords:		ID:	234560
This section describes the imported types and definitions and the expected interface. It also describes safety related aspects of types, definitions and functions implemented in the S-WdgIf. Some types, definitions and interfaces depend on the used S-WdgIf Configuration.					

Category:	Comment	Keywords:		ID:	234562
For more information see [TT_WDGIF_UM]. For more information about types, definitions and functions implemented in the S-Wdg drivers, see the Safety Manuals of the drivers. Safety Manuals and User Manuals of the drivers tested by TTTech can be found in section "References" at the end of this document.					

Category:	Comment	Keywords:		ID:	234564
For further requirements related to imported types, definitions and interfaces, see section "S-WdgIf Integration" below.					

Category:	Comment	Keywords:		ID:	234566
The integrator is responsible for the correct import of the types and definitions that are listed in section "Imported Types and Definitions" below.					

Category:	Requirement	Keywords:		ID:	234570
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for the correct application of the interface functions.					

Category:	Requirement	Keywords:		ID:	234572
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for ensuring that all external functions that are called from within the S-WdgIf code are imported from the correct versions of AUTOSAR.					

Category:	Comment	Keywords:		ID:	559643
For the supported AUTOSAR versions, see comment 559910 above.					

Category:	Comment	Keywords:		ID:	546265
The external functions are defined in section "Expected Interface" below.					

Category:	Requirement	Keywords:		ID:	234574
Label:		Safety relevant:			
Related To:		Related To':			

The inclusion of AUTOSAR files or any other files different from S-WdgIf files shall not redefine any identifier that is defined in the S-WdgIf code. E.g., redefinitions with #define macros.

Category:	Requirement	Keywords:		ID:	234568
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall verify that no external interface of the S-WdgIf listed in this section degrades the quality level of the S-WdgIf below the required quality level.

Category:	Comment	Keywords:		ID:	559038

The external interfaces are defined in section "Expected Interface" below.

Category:	Comment	Keywords:		ID:	234576

For example, if an external function of quality level ASIL C is called by the S-WdgIf, it degrades the quality level of the S-WdgIf to ASIL C (if no precautions were taken), although the required quality level is ASIL D.

10.1.1 Expected Interface

Category:	Comment	Keywords:		ID:	234580

This section lists the external functions that are called by the S-WdgIf.

Category:	Comment	Keywords:		ID:	234582

For an overview of functions that are called by the S-WdgIf see [TT_WDGIF_UM].

Category:	Comment	Keywords:		ID:	234584

The following functions of the WD driver in the lower layer are called:

Function	Module
Wdg_*infix*_SetMode () *)	WD Driver
Wdg_*infix*_SetTriggerWindow () or Wdg_*infix*_SetTriggerCondition() **) ***)	WD Driver

table 7

*) If the function WdgIf_SetMode () is called with parameter DeviceIndex=*i*, then it calls the function that is configured for the *i*-th WD - referred to by *infix* - in the S-WdgIf configuration for the configuration field Wdg_*infix*_SetMode.

**) If the function WdgIf_SetTriggerWindow () or WdgIf_SetTriggerCondition () is called with parameter DeviceIndex=*i*, then it calls the function that is configured for the *i*-th WD - referred to by *infix* - in the S-WdgIf configuration for the configuration field Wdg_*infix*_SetTriggerWindow.

***) If the configuration parameter WdgIfUseAutosarApi is set to "true", then the S-WdgIf expects the WD driver to provide the function Wdg_*infix*_SetTriggerWindow () (which is the AUTOSAR API compatibility mode). Otherwise, the S-WdgIf expects the WD driver to provide the function

Wdg_*infix*_SetTriggerCondition () (which is the TTTech API compatibility mode).

Category:	Comment	Keywords:		ID:	235159

Some functions are called by the S-WdgIf depending on the compiler switches as listed here:

Compiler Switch	Function	Module
WDGIF_DEV_ERROR_DETECT is set to STD_ON	Appl_Det_ReportError () *)	DET
WDGIF_INTERNAL_TICK_COUNTER is set to STD_ON	Wdg_*infix*_GetTickCounter () **)	WD Driver
WDGIF_USE_AUTOSAR_DRV_API	If set to STD_ON, then Wdg_*infix*_SetTriggerWindow () is called, otherwise Wdg_*infix*_SetTriggerCondition () is called ***)	WD Driver

table 8

*) This is a wrapper function. See section "Implementation of Wrapper Function Appl_Det_ReportError ()" below for information.

**) If the function WdgIf_GetTickCounter () is called with WDGIF_INTERNAL_TICK_COUNTER set to STD_ON, then it calls the function that is configured in the S-WdgIf configuration for the configuration field Wdg_*infix*_GetTickCounter.

***) WDGIF_USE_AUTOSAR_DRV_API is set to STD_ON for the AUTOSAR compatibility mode and set to STD_OFF for the TTTech compatibility mode.

10.1.1.1 Implementation of Wrapper Function Appl_Det_ReportError ()

Category:	Comment	Keywords:		ID:	238269

The function Det_ReportError () may not meet the required quality level and need to be wrapped so that freedom from interference with the S-WdgIf is guaranted. The according wrapper function is called Appl_Dem_ReportError (). The S-WdgIf calls the function Appl_Dem_ReportError () instead of Dem_ReportError ().

Category:	Comment	Keywords:		ID:	260666

Note: Det_ReportError () is only called if WDGIF_DEV_ERROR_DETECT is set to STD_ON.

Category:	Requirement	Keywords:		ID:	260664
Label:		Safety relevant:			
Related To:		Related To':			

The wrapper function Appl_Det_ReportError () shall be declared in a separate header-file named Appl_Det.h. This header file shall include Det.h for the wrapped AUTOSAR function.

Category:	Requirement	Keywords:		ID:	235165
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall verify that a call of this function does not degrade the S-WdgIf below the required quality level.

Category:	Comment	Keywords:		ID:	235862

For this reason, the integrator is advised to revise the necessity of the expected interfaces.

10.1.2 Imported Types and Definitions

Category:	Comment	Keywords:		ID:	235866

This section lists the types and definitions that are imported by the S-WdgIf.

Category:	Comment	Keywords:		ID:	235886

The following types and definitions are imported from Platform_Types.h and used:
Types:
uint8
uint16
uint32

Category:	Comment	Keywords:		ID:	235888

The following types and definitions are imported from Std_Types.h and used:
Types:
Std_VersionInfoType (only if WDGIF_VERSION_INFO_API is set to STD_ON)
Std_ReturnType
Definitions:
STD_ON
STD_OFF

Category:	Comment	Keywords:		ID:	235890

The following definitions are imported from "Compiler.h" and used:
Definitions:
AUTOMATIC
FUNC
NULL_PTR
P2CONST
P2FUNC
P2VAR
VAR

Category:	Comment	Keywords:		ID:	235892

The following definitions are imported from "Compiler_Cfg.h" and used:
WDGIF_APPL_DATA
WDGIF_CODE
WDGIF_CONST
WDGIF_APPL_CONST
WDGIF_VAR

Category:	Comment	Keywords:		ID:	235894

The following definitions are imported from "MemMap.h" and used:
In WdgIf.c:
WDGIF_START_SEC_CODE

WDGIF_STOP_SEC_CODE
In WdgIf_Lcfg.c:
WDGIF_START_SEC_CONST_UNSPECIFIED
WDGIF_STOP_SEC_CONST_UNSPECIFIED

10.1.3 Error Handling

Category:	Comment	Keywords:		ID:	235916

This section describes the error codes that are set by the S-WdgIf (using the DET mechanism) and the return values from S-WdgIf API functions..

10.1.3.1 DET Errors

Category:	Comment	Keywords:		ID:	235920

DET Errors are intended to support the development of an application. During software development, the compiler directive WDGIF_DEV_ERROR_DETECT is usually set to STD_ON. Once the software is safe enough so that no further DET error can occur, the option is deactivated. For safety reasons the DET errors that are returned by the S-WdgIf are listed here.

Category:	Comment	Keywords:		ID:	235896

If the compiler switch WDGIF_DEV_ERROR_DETECT is set to STD_ON, then the S-WdgIf reports the following development errors using the function Appl_Det_ReportError ():

DET Error	Code	Description
WDGIF_E_PARAM_DEVICE	0x01	A WD device is referenced that is not defined in the S-WdgIf configuration. *)
WDGIF_E_PARAM_PTR	0x02	WdgIf_GetVersionInfo () is called with NULL-pointer as parameter.

table 9

*) Possible reasons are:
- the pointer to the WdgIf configuration is NULL,
- the device index is higher than the number of WDs in the WdgIf configuration, and
- the pointer to the referenced WD function is NULL.

The DET errors are defined in WdgIf.h.

Category:	Comment	Keywords:		ID:	235868

The definition WDGIF_E_PARAM_DEVICE is an AUTOSAR definition (see [AS_WDGIF_SWS]).
The definition WDGIF_E_PARAM_PTR is TTTech specific.

Category:	Requirement	Keywords:		ID:	235932
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for making sure that - once the compiler switch WDGIF_DEV_ERROR_DETECT is set to STD_OFF - no error relevant to DET can occur.

10.1.3.2 Return Values

Category:	Comment	Keywords:		ID:	235936

The following functions return E_NOT_OK in case an error occured:

Function	Comment
WdgIf_SetMode ()	DET error WDGIF_E_PARAM_DEVICE was reported or the called function Wdg_*infix*_SetMode () of the WD driver returned E_NOT_OK.
WdgIf_SetTriggerCondition ()	DET error WDGIF_E_PARAM_DEVICE was reported or the called function Wdg_*infix*_SetTriggerWindow () of the WD driver returned E_NOT_OK.
WdgIf_SetTriggerWindow ()	DET error WDGIF_E_PARAM_DEVICE was reported or the called function Wdg_*infix*_SetTriggerWindow () of the WD driver returned E_NOT_OK.

table 10

Category:	Comment	Keywords:		ID:	235938

The return codes are handled by the S-WdgIf function that calls one of the functions above.

10.2 Functional Specification

Category:	Comment	Keywords:		ID:	283401

A detailed functional specification of the S-WdgIf module is provided in [TT_WDGIF_UDD].

Category:	Requirement	Keywords:		ID:	236022
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for ensuring that the S-WdgIf functionality is not unintentionally affected by other software (especially the AUTOSAR SW). This is, e.g., manipulation of local variables of S-WdgIf functions.

Category:	Comment	Keywords:		ID:	287742

This includes:

- memory corruption (see section "S-WdgIf Application" below),
- source code modifications, and
- API function calls with wrong parameters.

10.3 S-WdgIf Configuration

Category:	Comment	Keywords:		ID:	236026

The S-WdgIf has two kinds of configuration:

- pre-processor options and
- link-time configuration data.

Category:	Comment	Keywords:		ID:	236032

The pre-processor options are generated out of an ECU configuration using the S-WdgIf Generator (coded in the generated file WdgIf_Cfg_Features.h).
They activate or deactivate certain S-WdgIf features and cannot be altered during runtime.
See section "S-WdgIf Configuration Generator" in this document for details on the S-WdgIf Generator and its application.
See [TT_WDGIF_UM] for details on the pre-processor options.

Category:	Comment	Keywords:		ID:	236034

The link-time configuration data is also generated out of the ECU configuration using the S-WdgIf Generator (coded in the generated files WdgIf_Lcfg.h and WdgIf_Lcfg.c).
The link-time configuration defines the used WD devices with links to the device specific functions and cannot be altered during runtime.
See section "S-WdgIf Configuration Generator" above for details on the S-WdgIf Generator and its application.
See [TT_WDGIF_UM] for more information about on the link-time configuration data.

Category:	Comment	Keywords:		ID:	236042

The integrator is responsible for generation and verification of configuration data as depicted in section "S-WdgIf Configuration Generator" above.

Category:	Requirement	Keywords:		ID:	236044
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall guarantee that the configuration data is not altered, e.g. through erroneous HW.

Category:	Comment	Keywords:		ID:	236046

This can be realized - for example - with ECC ROM/FLASH checks, cyclical ROM/FLASH checks, and start up ROM/FLASH checks.

10.4 File Structure

Category:	Comment	Keywords:		ID:	236055

For information about the S-WdgIf file structure see [TT_WDGIF_UM].

Category:	Comment	Keywords:		ID:	236057

The following table shows the files that are only included when the according compiler directive is set to STD_ON:

Include File	Compiler Directive
Det.h	WDGIF_DEV_ERROR_DETECT

table 11

Category:	Comment	Keywords:		ID:	236061
See also the requirement 234574 for File inclusion.					

10.5 S-WdgIf Integration

Category:	Comment	Keywords:		ID:	236065
This section describes how to integrate the S-WdgIf into a safety-relevant system.					

Category:	Requirement	Keywords:		ID:	236240
Label:		Safety relevant:			
Related To:		Related To':			
It is the responsibility of the integrator to demonstrate that the generated S-WdgIf configuration is sufficient for the considered system.					

Category:	Requirement	Keywords:		ID:	236256
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for a correct integration of the S-WdgIf code on the system level as described in this section.					

Category:	Requirement	Keywords:		ID:	236258
Label:		Safety relevant:			
Related To:		Related To':			
The integrator shall verify that the chosen WD device(s), which is internal or external, meets the system's safety requirements.					

Category:	Comment	Keywords:		ID:	236260
For single oscillator MCU's (where the watchdog clock is derived from the CPU main clock) it is recommended to use an external watchdog device with its own oscillator as well.					

10.5.1 Import from AUTOSAR Definitions into S-WdgIf

Category:	Requirement	Keywords:		ID:	236264
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for the correct implementation of all types and definitions that are imported from AUTOSAR header files and used by the S-WdgIf code according to AUTOSAR specifications.					

Category:	Comment	Keywords:		ID:	554231
See also section "Imported Types and Definitions" above.					

Category:	Requirement	Keywords:		ID:	236266
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for providing the AUTOSAR header files for the import of the AUTOSAR types and definitions.					

Category:	Comment	Keywords:		ID:	236268
For a list of imported AUTOSAR types and definitions and the related header files, see section "Imported Types and Definitions" above.					

Category:	Requirement	Keywords:		ID:	236270
Label:		Safety relevant:			
Related To:		Related To':			
The inclusion of AUTOSAR header files into the S-WdgIf code shall not redefine any identifier that is defined within the S-WdgIf code. This prohibits, for example, redefinitions with #define macros.					

Category:	Requirement	Keywords:		ID:	236272
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for providing the correct code of used AUTOSAR functions. That is, correct in version and functionality.					

Category:	Comment	Keywords:		ID:	236274
For a list of used AUTOSAR functions, see section "Expected Interface" above.					

Category:	Requirement	Keywords:		ID:	236276
Label:		Safety relevant:			
Related To:		Related To':			
It is the responsibility of the integrator to provide a file Std_Types.h according to the comments in section "Imported Types and Definitions" above.					

Category:	Requirement	Keywords:		ID:	236278
Label:		Safety relevant:			
Related To:		Related To':			
It is the responsibility of the integrator to provide a file Platform_Types.h according to the comments in section "Imported Types and Definitions" above.					

Category:	Requirement	Keywords:		ID:	236280
Label:		Safety relevant:			
Related To:		Related To':			
It is the responsibility of the integrator to provide a file Compiler.h and a file Compiler_Cfg.h according to the comments in section "Imported Types and Definitions" above.					

Category:	Comment	Keywords:		ID:	236282
Note: Some other integrated products provide their own contents for Compiler_Cfg.h. They need to be merged into the file Compiler_Cfg.h of the system.					

Category:	Requirement	Keywords:		ID:	236284
Label:		Safety relevant:			
Related To:		Related To':			
It is the responsibility of the integrator to provide a file MemMap.h according to the AUTOSAR specifications.					

Category:	Comment	Keywords:		ID:	236600
In contrast to the S-WdgM, there is no configuration dependent memory management. All memory management definitions for the S-WdgIf are located in MemMap.h.					

Category:	Comment	Keywords:		ID:	236286
Note: Some other integrated products provide their own contents for MemMap.h. They need to be merged into the file Memmap.h file for the system.					

Category:	Comment	Keywords:		ID:	236290
TTTech provides example files for • MemMap.h (which includes the files WdgM_MemMap.h or WdgM_OSMemMap.h, and Wdg_MemMap.h) and • demo_MemMap.h (with the memory mapping definitions of the complete S-WdgM Stack).					

Category:	Comment	Keywords:		ID:	561554
The file WdgM_MemMap.h is used in AUTOSAR 3.1 enviroments. The file WdgM_OSMemMap.h is used in AUTOSAR 4.0 enviroments.					

10.5.2 Memory Mapping

Category:	Comment	Keywords:		ID:	236350
This section lists the requirements for the memory mapping of the S-WdgIf data and code (including the generated S-WdgIf code).					

Category:	Requirement	Keywords:		ID:	236762
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for the inclusion of the correct MemMap.h file into the S-WdgIf code.					

Category:	Requirement	Keywords:		ID:	236356
Label:		Safety relevant:			
Related To:		Related To':			
The integrator is responsible for the correct assignment of S-WdgIf data and code (including the generated S-WdgIf code) to the various memory sections according to the memory mapping keywords provided by the S-WdgIf.					

Category:	Comment	Keywords:		ID:	236612
For the memory sections that are supported by the S-WdgIf see comment 235894 in section "Imported Types and Definitions" above.					

10.5.3 S-WdgIf Files

Category:	Requirement	Keywords:		ID:	236360
Label:		Safety relevant:			
Related To:		Related To':	__MKSID__297368		

The integrator shall ensure that only
- files of a single delivered package and
- files generated with tools of this package

are installed.

These are the files:
- WdgIf_Cfg_Features.h (generated),
- WdgIf_Lcfg.h (generated),
- WdgIf_Lcfg.c (generated),
- WdgIf_Cfg.h,
- WdgIf_Types.h,
- WdgIf.h, and
- WdgIf.c.

10.5.4 Compilation and Linkage

Category:	Requirement	Keywords:		ID:	236366
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for compilation of the S-WdgIf code with a compiler that is compliant to ANSI ISO/IEC 9899:1990.

Category:	Comment	Keywords:		ID:	236370
The generated code is compliant to ANSI ISO/IEC 9899:1990. It is also known as "ANSI C (C89)" and "ISO C (C90)".					

Category:	Requirement	Keywords:		ID:	236374
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for compilation and linkage of the S-WdgIf into the AUTOSAR system in accordance with the system requirements.

Category:	Requirement	Keywords:		ID:	236378
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall guarantee that the compiled and linked target binary is correctly loaded into the target system.

10.5.5 S-WdgM Stack Requirements

Category:	Comment	Keywords:		ID:	555505

This section lists the requirements for the S-WdgM Stack that must be met for safe functioning of the S-WdgIf.

Category:	Requirement	Keywords:		ID:	236382
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall make sure that the S-WdgIf communicates with
- an internal WD device (MCU inside) or
- an external WD device.

Category:	Comment	Keywords:		ID:	558045

The communication between the S-WdgIf and the WD driver can be tested with negative integration tests.

Category:	Comment	Keywords:		ID:	236384

For ASIL C and D systems, it is recommended to use an external WD device with independent time based clock, reset circuit and power path.

Category:	Comment	Keywords:		ID:	236386

See
- ISO 26262 (see [ISO26262], part 6, section 7.4.14, table 4/1d) and
- Microcontroller manufacturer recommendation(see e.g. [TI_SPNU511_UM] section 5.3.6).

Category:	Requirement	Keywords:		ID:	237306
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall verify that the communication path to the external WD does not degrade the quality level below the required quality level.

Category:	Comment	Keywords:		ID:	554234

The requirement 237306 above is only relevant when an external WD is used.
Note: The communication path to the external WD could be e.g. a SPI driver.

Category:	Requirement	Keywords:		ID:	237369
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall guarantee that the S-WdgIf program code - including configuration code - can not be corrupted.

Category:	Comment	Keywords:		ID:	554832

This can be realized - for example - with ECC ROM/FLASH checks, cyclical ROM/FLASH checks, and start up ROM/FLASH checks.

10.6 S-WdgIf Application

Category:	Comment	Keywords:		ID:	236760

In contrast to the S-WdgM, the S-WdgIf API functions are not called from application level.
Except WdgIf_GetVersionInfo (), all S-WdgIf functions are called by the S-WdgM.
However, there are a few requirements to be considered on system level.

Category:	Comment	Keywords:		ID:	261300

The S-WdgIf does not alter data that is passed through from or to the S-WdgM.
Only the contents of the variable whose address is passed as parameter to WdgIf_GetVersionInfo () is altered.

Category:	Requirement	Keywords:		ID:	236428
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for correct handling and escalation of errors detected by the S-WdgIf code via DET monitoring.

Category:	Comment	Keywords:		ID:	236756

Returned error codes are handled by the caller of the function that returns a DET error.

Category:	Requirement	Keywords:		ID:	236430
Label:		Safety relevant:			
Related To:		Related To':			

The data that is used by the S-WdgIf, especially the S-WdgIf Configuration data, shall not be modified by any other SW of the system.

Category:	Requirement	Keywords:		ID:	236432
Label:		Safety relevant:			
Related To:		Related To':			

It shall be considered that the S-WdgIf code has no mechanism for detecting and/or correcting the following errors:

- corruption of the S-WdgIf memory for constants,
- corruption of the S-WdgIf code memory, and
- corruption of the S-WdgIf local RAM memory (i.e. the local variables placed on the stack).

Category:	Requirement	Keywords:		ID:	236434
Label:		Safety relevant:			
Related To:		Related To':			

The integrator shall guarantee that the address spaces that are listed in the requirement above and for which the S-WdgIf offers no mechanism for error detection and error correction can not be corrupted.

Category:	Comment	Keywords:		ID:	236438

If a mechanism for detecting/correcting of such manipulations is implemented in the application level or system level, then it should also cover the S-WdgIf code.

10.6.1 S-WdgIf API Functions

Category:	Comment	Keywords:		ID:	262246

There are no function specific requirements for the S-WdgIf API functions, except WdgIf_GetVersionInfo (). However, some requirements concern all functions need to be met.

Category:	Comment	Keywords:		ID:	262301

The considered API functions/macros are:

- WdgIf_Setmode (),
- WdgIf_SetTriggerCondition (),
- WdgIf_SetTriggerWindow (),
- WdgIf_GetTickCounter (), and
- WdgIf_GetVersionInfo () (macro).

Category:	Requirement	Keywords:		ID:	262242
Label:		Safety relevant:			
Related To:		Related To':			

It is the responsibility of the integrator to verify the correctness of parameters passed to the S-WdgIf API functions. Especially, that parameters are not modified when passed from S-WdgM API functions to S-WdgIf API functions .

Category:	Requirement	Keywords:		ID:	262243
Label:		Safety relevant:			
Related To:		Related To':			

Some S-WdgIf API functions have a pointer to data as argument. The integrator is responsible that this data is not modified by code other than the S-WdgM.

Category:	Requirement	Keywords:		ID:	265954
Label:		Safety relevant:			
Related To:	__MKSID__263878	Related To':			

WdgIf_GetVersionInfo () shall be called with a correct pointer (e.g. use a pointer of type Std_VersionInfoType without a type cast).

10.6.2 Memory Access

Category:	Comment	Keywords:		ID:	236784

The S-WdgIf does not access the hardware registers directly. The hardware could be accessed by calls of the S-Wdg driver functions. The access of registers by the S-Wdg driver is platform and implementation dependent and "supervisor" or "privileged" MCU mode may be necessary.

10.6.3 Concurrent Function Calls

Category:	Comment	Keywords:		ID:	283153

The following table shows which functions may run concurrently:

The function below is interrupted by the function on the right side	WdgIf_SetMode ()	WdgIf_SetTriggerCondition ()	WdgIf_SetTriggerWindow ()	WdgIf_GetVersionInfo ()	WdgIf_GetTickCounter ()
WdgIf_SetMode ()	HW	HW	HW	Y	Y (reg)
WdgIf_SetTriggerCondition ()	HW	HW	HW	Y	Y (reg)
WdgIf_SetTriggerWindow ()	HW	HW	HW	Y	Y (reg)
WdgIf_GetVersionInfo ()	Y	Y	Y	Y (ptr)	Y
WdgIf_GetTickCounter ()	Y (reg)	Y (reg)	Y (reg)	Y	Y

figure 1

HW	The interruption is HW dependent and only allowed if interruption of the corresponding WD driver function is allowed. The corresponding function is: • for WdgIf_SetMode (): Wdg_*infix*_SetMode (), • for WdgIf_SetTriggerCondition (): Wdg_*infix*_SetTriggerWindow () or Wdg_*infix*_SetTriggerCondition () (depending on the AUTOSAR version) • for WdgIf_SetTriggerWindow (): Wdg_*infix*_SetTriggerWindow () or Wdg_*infix*_SetTriggerCondition () (depending on the AUTOSAR version) • for WdgIf_GetTickCounter (): Wdg_*infix*_GetTickCounter ()
Y	Interruption is allowed

Y(ptr)	Interruption is allowed only if the pointers, given as an output parameter to the function, are different
Y(reg)	Interruption is allowed only if the function Wdg_*infix*_GetTickCounter () is implemented as a pure HW register read.

table 12

11 Safety Lifecycle Tailoring

Category:	Comment	Keywords:		ID:	234297
This section describes which phases of the S-WdgIf product safety lifecycle according to [ISO26262] were executed by TTTech during the development and which phases have to be executed by the integrator.					

Category:	Comment	Keywords:		ID:	234299
The S-WdgIf is a software unit representing a safety element out of context (SEooC) according to [ISO26262], part 10. The SW requirements of the S-WdgIf are based on [AS_WDGIF_SWS] and [TT_WDGIF_SRD] with deviations listed in [TT_WDGIF_UM]. The architectural design is documented in [TT_WDGIF_UDD].					

Category:	Comment	Keywords:		ID:	234301

software architecture through traceability

Category:	Requirement	Keywords:		ID:	234315
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for the execution of ISO/DIS 26262 phase 6-10 (SW integration and testing) to verify that S-WdgIf code is correctly integrated into the system.

Category:	Requirement	Keywords:		ID:	234319
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for the execution of phase ISO/DIS 26262 6-11 (Verification of SW safety requirements) to verify the safety requirements that are related to the S-WdgIf code.

12 Qualification

Category:	Comment	Keywords:		ID:	234207
The S-WdgIf has been developed according to the requirements in [ISO26262] as specified in section "Safety Lifecycle Tailoring" above. It can be integrated in systems up to ASIL D, provided that all requirements in this document are fulfilled.					

Category:	Comment	Keywords:		ID:	234209
The hardware dependent qualification data for the S-WdgIf for each platform can be found in the S-Wdg drivers' Safety Manuals.					

Category:	Comment	Keywords:		ID:	234211
The S-WdgM Stack Safety Case [TT_WDGS_SC] lists all S-WdgIf qualification documents.					

Category:	Comment	Keywords:		ID:	234213
The S-WdgIf unit tests are specified in [TT_WDGIF_UTS]. The S-WdgIf tests of the unit test framework are specified in [TT_WDGS_UTS]. The integration tests of the S-WdgM Stack are specified in [TT_WDGS_ITS].					

Category:	Comment	Keywords:		ID:	260894
The environments and S-WdgIf Configurations of integration tests that have been conducted by TTTech can be found in the Safety Manual of the various S-Wdg drivers (e.g. [TT_WDGDR_*platform*_SM], where *platform* is the used platform. See also section "References" at the end of the document).					

Category:	Requirement	Keywords:		ID:	234215
Label:		Safety relevant:			
Related To:		Related To':			

The integrator is responsible for the qualification of the S-WdgIf code for the used environment. This means that the S-WdgIf code must be integration tested against this environment.

The environment comprises:

- the target CPU,
- the compiler and linker,
- the compiler and linker settings,
- S-WdgIf pre-compile configurations, and
- the used WDs and WD drivers.

Category:	Requirement	Keywords:		ID:	234217
Label:		Safety relevant:			
Related To:		Related To':			

If the S-WdgIf is used in an environment that differs in any way from the environment it has been tested with (according to [TT_WDGS_ITS] and [TT_WDGIF_UTS]), then the integrator shall analyze the consequences of the differences and conduct corresponding tests (see [ISO26262] part 6, clause 9, in particular [ISO26262] clause 9.4.6).

Category:	Comment	Keywords:		ID:	234219
TTTech offers qualification of the S-WdgIf for customer-specific configurations.					

Category:	Requirement	Keywords:		ID:	265956
Label:		Safety relevant:			
Related To:	__MKSID__263827,__MKSID__263846,__MKSID__263860	Related To':			
The integrator shall run integration tests with the generated configurations for S-WdgM and S-WdgIf.					

13 Resource Requirements

Category:	Comment	Keywords:		ID:	234197

The memory consumption and runtime consumption of the S-WdgIf depends on the chosen HW, which itself is chosen by the used S-Wdg driver.
The resource requirements of the complete S-WdgM Stack can be found in the Safety Manual of the according S-Wdg driver.

14 Constraints and known Problems

Category:	Comment	Keywords:		ID:	290609
For known problems see the Release Notes document delivered with this software module.					

15 References

Category:	Comment	Keywords:		ID:	234117
[ISO26262] ISO26262, Internation Standard, Road vehicles- Functional safety, First edition 2011-11-15					

Category:	Comment	Keywords:		ID:	234119
[TT_WDGM_SM] TTTech Automotive GmbH, Safe Watchdog Manager - Safety Manual, D-SAFEX-S-70-001					

Category:	Comment	Keywords:		ID:	234121
[TT_WDGDR_MPC56xx_SM] TTTech Automotive GmbH, Safe Watchdog Driver for MPC56xx - Safety Manual, D-MSP-M-70-022					

Category:	Comment	Keywords:		ID:	554844
[TT_WDGDR_SAFETCORE_SM] TTTech Automotive GmbH, Safe Watchdog Driver for TriCore and SafeTcore - Safety Manual, D-SAFEX-S-70-013					

Category:	Comment	Keywords:		ID:	234125
[TT_WDGDR_TMS570LS3x_SM] TTTech Automotive GmbH, Safe Watchdog Driver for TMS570LS3x - Safety Manual, D-SAFEX-S-70-015					

Category:	Comment	Keywords:		ID:	234123
[TT_WDGDR_V850E2PJ4_SM] TTTech Automotive GmbH, Safe Watchdog Driver for V850E2PJ4 - Safety Manual, D-SAFEX-S-70-029					

Category:	Comment	Keywords:		ID:	554842
[TT_WDGDR_TMS570LS_TPS65381_SM] TTTech Automotive GmbH, Safe Watchdog Driver for TMS570LS_TPS65381 - Safety Manual, D-SAFEX-S-70-038					

Category:	Comment	Keywords:		ID:	554840
[TT_WDGDR_MPC5643L_ATA5021_SM] TTTech Automotive GmbH, Safe Watchdog Driver for MPC5643L_ATA5021 - Safety Manual, D-SAFEX-S-70-049					

Category:	Comment	Keywords:		ID:	234127
[TT_WDGS_SC] TTTech Automotive GmbH, Safe Watchdog Manager Stack - Safety Case, D-SAFEX-IN-70-001					

Category:	Comment	Keywords:		ID:	234129
[TT_WDGM_UM] TTTech Automotive GmbH, Safe Watchdog Manager - User Manual, D-MSP-M-70-001					

Category:	Comment	Keywords:		ID:	234131
[TT_WDGIF_UM] TTTech Automotive GmbH, Safe Watchdog Interface - User Manual, D-MSP-M-70-006					

Category:	Comment	Keywords:		ID:	234133
[TT_WDGDR_MPC56xx_UM] TTTech Automotive Gmbh, Safe Watchdog Driver (MPC56xx) - User Manual, D-MSP-M-70-008					

Category:	Comment	Keywords:		ID:	234135
[TT_WDGDR_SAFETCORE_UM] Safe Watchdog Driver (SafeTcore) - User Manual, D-MSP-M-70-007					

Category:	Comment	Keywords:		ID:	234137
[TT_WDGDR_TMS570LS3x_UM] TTTech Automotive GbmH, Safe Watchdog Driver (TMS570LS3x) - User Manual, D-MSP-M-70-010					

Category:	Comment	Keywords:		ID:	234143
[AS_WDGM_SWS] AUTOSAR, Specification of Watchdog Manager, Version 2.0.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	234145
[AS_WDGIF_SWS] AUTOSAR, Specification of Watchdog Interface, Version 2.3.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	559938
[AS_WDGIF_SWS_3_1] AUTOSAR, Specification of Watchdog Interface, Version 2.2.2, Release 3.1, Revision 1					

Category:	Comment	Keywords:		ID:	234147
[AS_WDGDR_SWS] AUTOSAR, Specification of Watchdog Driver, Version 2.3.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	237766
[AS_RTE_SWS] AUTOSAR, Specification of RTE, Version 3.0.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	234149
[AS_STDTYP_SWS] AUTOSAR, Specification of Standard Types, Version 1.3.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	234151
[AS_COMABS_SWS] AUTOSAR, Specification of Compiler Abstraction, Version 3.0.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	234153
[AS_PLTFM_SWS] AUTOSAR, Specification of Platform Types, Version 2.3.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	234155
[AS_MEM_SWS] AUTOSAR, Specification of Memory Mapping, Version 1.2.0, Release 4.0, Revision 1					

Category:	Comment	Keywords:		ID:	234177
[TI_SPNU511_UM] Texas Instruments, Safety Manual for TMS570LS31x/21x and RM48x Hercules™ ARM® Safety Critical Microcontrollers - User's Guide, Literature Number: SPNU511A, February 2012					

15.1 Internal Documents

Category:	Comment	Keywords:		ID:	283409

The following referenced documents are internal TTTech Automotive GmbH document. For inspection, please contact TTTech Automotive GmbH:

Category:	Comment	Keywords:		ID:	283417

[TT_WDGIF_ETA] TTTech Automotive GmbH, Safe Watchdog Interface - Event Tree Analysis, D-SAFEX-S-70-012

Category:	Comment	Keywords:		ID:	283419

[TT_WDGIF_SRD]] TTTech Automotive GmbH, Safe Watchdog Interface - Software Requirements Document, D-SAFEX-S-70-002

Category:	Comment	Keywords:		ID:	283421

[TT_WDGIF_UDD] TTTech Automotive GmbH, Safe Watchdog Interface - Unit Design Document, D-SAFEX-D-70-001

Category:	Comment	Keywords:		ID:	283423

[TT_WDGIF_UTS] TTTech Automotive Gmbh, Safe Watchdog Interface - Unit Test Specification, D-SAFEX-V-70-002

Category:	Comment	Keywords:		ID:	283427

[TT_WDGS_UTS] TTTech Automotive Gmbh, Safe Watchdog Manager Stack - Unit Test Specification - Test Framework, D-SAFEX-V-70-008

Category:	Comment	Keywords:		ID:	283425

[TT_WDGS_ITS] TTTech Automotive GmbH, Safe Watchdog Manager Stack - Integration Test Specification, D-SAFEX-V-01-001

Category:	Comment	Keywords:		ID:	554880

[TT_WDGS_ITR] TTTech Automotive GmbH, Safe Watchdog Manager Stack - Integration Test Report, D-SAFEX-V-01-002