Safe Watchdog Interface
Safety Case

Author:	TTTech
Reviewer(s):	PPU
Reference:	D-SAFEX-IN-70-002
Security:	Confidential
Version:	1.2.0
Date:	2014-11-20
Status:	Released

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 Chart

A revision is a new edition of the document and affects all sections of this document.

Version	Date	Responsible Person	Modification
0.1.0	2012-07-02	PPU	Creation
0.2.0	2012-07-19	PPU	Corrected ISO/DIS -> ISO
0.3.0	2012-09-27	PPU	Added S-WdgM Stack chapter
0.4.0	2012-10-01	PPU	Versions of artefacts updated
1.0.0	2012-10-01	PPU	Version of this document updated
1.0.1	2012-10-03	PPU	Document derived from common Safety Case document ver. 1.0.0. It contains now the S-WdgIf unit only. Content against 1.0.0 not changed.
1.0.2	2012-10-04	PPU	In the chapter 2 the RAD reference removed and the provided ISO lifecycles added.
1.0.3	2012-11-16	PPU	Update of the collected document versions.
1.0.4	2012-11-19	PPU	Update after issue50199.
1.0.5	2013-01-11	PPU	Update after second TÜV assessment
1.1.0	2014-07-28	VLE	Update of the collected document versions (issue65369)
1.1.1	2014-08-13	VLE	Update after PPU review.
1.2.0	2014-11-20	VLE	Update of the collected document versions (issue69469)

Contents

1 Purpose of this Document

This document represents the safety case for the Safe Watchdog Interface unit. The Safe Watchdog Interface is a part of the Safe Watchdog Manager Stack.

It references all relevant documents to provide evidence that the software units have been developed according to ISO26262 requirements for an ASIL D software unit [ISO].

2 Software Safety Lifecycle Documentation

The software units represent SEooC units according to ISO26262. The following software safety lifecycles were executed as part of the development process of the software units:

Concept phases:
- 3-7 Hazard analysis and risk assessment *)
- 3-8 Functional Safety Concept *)

Product development at the system level:
- 4-6 Technical Safety Concept *)
- 4-7 System Design *)

Product development at the software level:
- 6-5: Initiation of product development at the software level *)
- 6-8: Software unit design and implementation *)
- 6-9: Software unit testing *)

Supporting processes:
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Confidence in the use of software tools

*) As far as related to the S-WdgIf as SEooC

Part 6-6 deals with safety requirements, which are always defined on system level. For the development of the SEooC, we have made assumptions on the safety requirements, which are described in the corresponding SEooC safety manuals. The system integrator must verify that the SEooC fits to the actual system safety requirements.

The other software safety lifecycle phases described by ISO26262 have to be executed by the system integrator.

The following subsections list the software safety lifecycle artifacts of the software units:

- Safety manuals as .pdf files,
- Source code delivered to customer as pointer to the code location,
- Requirement, design documentation, and test specification as references to the respective documents in the MKS repository. They are identified by MKS document id and the document version number,
- Test results as .doc or .pdf files

The customer delivery contains user manuals, safety manuals and source code. All other artifacts can be audited by the customer on request either on-site in TTTech Vienna development location, or via teleconference (e.g. Webex).

The verification and confirmation measures as required by ISO26262 has been executed as described in the Software Project Plan.

The evidence for the execution of all verification and confirmation measures as required by ISO26262 are version-controlled in the following directory:
http://tttechsvn.vie.at.tttech.ttt/trunk/projects/certification/sqa/s-wdgm/evidence

The conformity of the development processes of the S-WdgM Stack with ISO 26262 has been assessed in a process audit [AUDIT_S-WdgM].

2.1 Safe Watchdog Interface

2.1.1 Software Requirements Document (SRD)

This document describes the software requirements for Safe Watchdog Interface. The SRD represents the software unit high-level requirements as required by ISO 26262 6, clause 6.

Document Title	Safe Watchdog Interface - Software Requirements Document
Document Version	1.0.8
Document Number	D-SAFEX-S-70-002
Location	MKS 125936
Label	Release_1_26_3

2.1.2 Unit Design Document (UDD)

The UDD represents the software unit design specification as required by ISO 26262 6, clause 8.

Document Title	Safe Watchdog Interface - Unit Design Document
Document Version	1.0.9
Document Number	D-SAFEX-D-70-001
Location	MKS ID 125939
Label	Release_1_26_3

2.1.3 Source Code

The source code of the software unit is written in the C programming language.

Title	Safe Watchdog Interface - Source Code
Version	3.3.6
Location	http://tttechsvn.vie.at.tttech.ttt/branches/For_SAFEEXE_SERIES_Release_1_26_3/SW/msp-watchdog-if

The exact contents of the Source Code and configuration management tags are described in [RAD].

The HIS metrics and the MISRA rule check are performed with the tool QA-C.
The HIS metrics report can be found in the folders
http://tttechsvn.vie.at.tttech.ttt/trunk/projects/customers/SafeExe-ASIL/04_technical-documents/HIS_MISRA_checks/Release_1_26_3/S-WdgIf/
All HIS metrics violations are justified in the respective source files.

The results of the MISRA-check can be found in the folders
http://tttechsvn.vie.at.tttech.ttt/trunk/projects/customers/SafeExe-ASIL/04_technical-documents/HIS_MISRA_checks/Release_1_26_3/S-WdgIf/
All violations are justified. The justifications are provided as comments in the respective source files.

2.1.4 Unit Test Specification (UTS)

The UTS contains a detailed test specification of the software unit according to the requirements of ISO 26262 6, clause 9 . The UTS demonstrates 100% requirements coverage.

Document Title	Safe Watchdog Interface - Unit Test Specification
Document Version	1.0.11
Document Number	D-SAFEX-V-70-002
Location	MKS ID 125942
Label	Release_1_26_3

2.1.5 Unit Test Report (UTR)

The UTR contains a detailed unit test report according to the requirements of ISO 26262 6, clauses 8 and 9. The UTR shows that all tests and review procedures specified in the UTS passed and that 100% MC/DC coverage is achieved.

Document Title	Safe Watchdog Interface - Unit Test Report
Document Version	1.0.5
Document Number	D-SAFEX-V-70-006
Location	\\fileserver.vie.at.tttech.ttt\projects\certification\tttech-automotive\release\S-WdgM\S-WdgIf\UTR\UTR_WdgIf_D-SAFEX-V-70-006_V_1_0_5\UTR_WdgIf_D-SAFEX-V-70-006_V_1_0_5.pdf

2.1.6 Safety Manual (SM)

The Safety Manual (SM) contains the requirements for the integrator of the software unit. All requirements described in this document must be followed. In specific, the SM describes for which configuration (configuration parameters, used hardware, compiler and linker settings) the software unit has been tested according to ISO 26262 requirements. Moreover, the SM describes which SW safety lifecycle requirements and recommendations of ISO 26262 were not executed during the development of the software unit. These requirements and recommendations have to be considered by the integrator of the software unit.

Document Title	Safe Watchdog Interface - Safety Manual
Document Version	1.8.9
Document Number	D-SAFEX-S-70-005
Locations	MKS 232906
Label	Release_1_26_3

2.1.7 Event Tree Analysis (ETA)

The ETA is the event tree analysis that was performed as part of the Safe Watchdog Manager (S-WdgIf) software development according to the requirements and recommendations of ISO 26262

Document Title	Safe Watchdog Interface - Event Tree Analysis
Document Version	1.0.0
Document Number	D-SAFEX-S-70-012
Locations	MKS ID 263814
Label	Release_1_26_3

3 Summary

The evidence in sections

- T b !Tb !M !E b

and the assessment reports [AUDIT_S-WdgM] shows that the S-WdgIf unit has been developed as a SEooC component according to ISO26262:2011 and can be used for up to ASIL D.

It is safe to integrate the SW unit into safety-related systems developed according to ISO 26262:2011, if the requirements that are described in the Safety Manual (SM) are fulfilled by the system integrator.

4 Abbreviations and Glossary

Acronym / Term	Meaning
API	Application Programmer Interface

Acronym / Term	Meaning
ASIL	Automotive Safety Integrity Level
HIS	Herstellerinitiative Software
ISO	International Standard
MC/DC	Modified Condition/Decision Coverage
MISRA	Motor Industry Software Reliability Association
MKS	MKS Integrity software tool made by MKS Software Inc.
SEooC	Safety Element out of Context according to ISO 26262-10
SW	Software Specification

5 References

5.1 Documents Available on Request

The following documents are not part of the customer delivery. The documents can be made available in video conferences (e.g., WebEx) or in on-site audits at the development center of TTTech in Vienna. If necessary, please contact the TTTech Automotive Support at support@tttech-automotive.com.

[AUDIT_S-WdgM]	TÜV NORD Institut für Fahrzeugtechnik & Mobilität, **A/** **Report on the Functional Safety Audit for TTTech's Safe Watchdog Manager Stack (ISO 26262 / ASIL D)** 1. Report-No: 8109170322-B01, Version 1.0, 2012-07-18 2. Report-No: 8109170322-B02, Version 1.0 2012-12-20 **B/** **Functional Safety Assessment Report of "Safe Watchdog Manager Stack" conformity against ISO26262, ASIL D.** 3. Report-No: 8109170322-B04, Version 1.0 2013-02-25
[COMPL]	TTTech Computertechnik AG, ISO_DIS_26262_Compliance.xls, D-INT-CL-70-001
[TT_ASDM_322]	TTTech Automotive GmbH, Automotive Software Development Manual, V3.2.2, D-100-T-70-001

5.2 Other Documents

[ISO]	International Organization for Standardization, International Standard ISO26262 Road vehicles Functional safety (all parts), 2011

