Safe Watchdog Manager Stack

Safety Case

Author:	TTTech
Reviewer(s):	VLE
Reference:	D-SAFEX-IN-70-001
Security:	Confidential
Version:	1.1.0
Date:	14.08.2014
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 split to three module dependent documents: S-WdgM, S-WdgIf, S-Wdg 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	Version of the documents updated.
1.0.4	2012-11-19	PPU	Version of the documents updated.
1.0.5	2012-11-19	PPU	Version of the documents updated.
1.0.80	2014-03-03	PPU	Based on ver. 1.0.4, the Verifier versions updated only.
1.1.0	2014-08-14	PPU	Versions of artefacts updated for release 1.26.1

Contents

1 Purpose of this Document

This document represents the safety case for the **Safe Watchdog Manager Stack**. In detail it covers following areas:

- **Safe Watchdog Manager Stack** (the common parts)
- **Safe Watchdog Manager**

The other units of the **Safe Watchdog Manager Stack** – the **Safe Watchdog Interface** and the **Safe Watchdog Driver** have separate safety case documents.

The safety case references all relevant documents to provide evidence that the software units have been developed according to requirements of ISO26262:2011 (see [ISO]) for an ASIL D SEooC software component.

The creation of the proof of due diligence document for the whole watchdog safety concept is the responsibility of the integrator of the **Safe Watchdog Manager Stack (S-WdgM Stack)** and is not part of this safety case document.

2 Assumptions on S-WdgM Stack as SEooC

2.1 Assumptions on scope

According to ISO 26262:2011-10, clause 9.2.4.2, Step 1a, the following assumptions on scope of the software component as an SEooC were made:

- **S-WdgM Stack** is integrated into an AUTOSAR 4 or compatible software architecture
- **S-WdgM Stack** must not unintentionally interfere with other software components
- **S-WdgM Stack** expects that the executing hardware is working correctly

3 Software Safety Lifecycles

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

*) As far as related to the **S-WdgM Stack** 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.

4 Software Safety Lifecycle Documentation

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

- Safety manuals as .pdf files with references to the MKS repository,
- 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 the document version number and the document label.
- 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 ISO26262:2011 has been executed as described in the Software Project Plan (SPP).

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 26262:2011 has been assessed in a process audit [AUDIT_S-WdgM].

4.1 Safe Watchdog Manager Stack

This chapter contains common documents related to all three units

- Safe Watchdog Manager
- Safe Watchdog Interface
- Safe Watchdog Driver

4.1.1 Software Project Plan (SPP)

The SPP contains all planning activities for all software units. It also represents the “Safety Plan” as required by ISO26262. Chapter VI of the SPP also contains the software tool qualification plan and software tool qualification report as required by ISO26262 - 8 clause 11.

Document Title	Safe Watchdog Manager Stack Software Project Plan
Document Version	0.7.0
Document Number	D-SAFEX-P-70-001
Location	http://tttechsvn.vie.at.tttech.ttt/trunk/projects/customers/SafeExe-ASIL/03_planning&risk-management/S-WdgM_SPP_V_0_7_0.doc

4.1.2 Functional Safety Concept (FSC)

This document reflects the functional safety concept according to ISO26262 3-8 Functional Safety Concept.
It is the top-level document for the Safe Watchdog Manager Stack and therefore also includes assumptions on the ISO 26262:2011 work product 3-7 Hazard analysis and risk assessment in the scope of this SEooC.

Document Title	Safe Watchdog Manager Stack Functional Safety Concept
Document Version	0.2.0
Document Number	D-SAFEX-S-70-006
Location	MKS ID 262558
Label	Release_1_26_1

4.1.3 Technical Safety Requirements (TSR)

This document describes the technical safety requirements that are assumed for a system using the Safe Watchdog Manager Stack. The technical safety requirements are relevant for the system integrator.

Document Title	Safe Watchdog Manager Stack - Technical Safety Requirements
Document Version	0.2.0
Document Number	D-SAFEX-S-70-021
Location	MKS ID 262750

Label	Release_1_26_1

4.1.4 System Design (SD)

This document reflects the system design document according to ISO 26262:2011 [ISO] 4-7 System Design for the system using the Safe Watchdog Manager Stack. It is based on the technical safety requirements document [TSR] of the ISO 26262:2011 [ISO] work product 4-6 Technical Safety Requirements in the scope of this SEooC.

Document Title	Safe Watchdog Manager Stack - System Design Specification
Document Version	0.2.0
Document Number	D-SAFEX-D-70-007
Location	MKS ID 263048
Label	Release_1_26_1

4.1.5 Software Requirements Document (SRD)

This document describes the software requirements for Safe Watchdog Manager Stack. The SRD represents the software unit high-level requirements as required by ISO 26262:2011 – 6, clause 6.

Document Title	Safe Watchdog Manager Stack - Software Requirements Document
Document Version	1.0.5
Document Number	D-SAFEX-D-70-024
Location	MKS ID 264112
Label	Release_1_26_1

4.1.6 Software Architecture Document (SAD)

This document describes the software architecture of the Safe Watchdog Manager Stack.

Document Title	Safe Watchdog Manager Stack - Software Architecture Document
Document Version	1.0.2
Document Number	D-SAFEX-S-70-016
Location	MKS ID 266056
Label	Release_1_26_1

4.1.7 Integration Test Specification (ITS)

This document describes the Integration Test, that verifies the Watchdog Manager, Watchdog Interface and Watchdog Driver which are compatible with other AUTOSAR components and shows the expected behaviour at runtime.

Document Title	Safe Watchdog Manager Stack - Integration Test Specification
Document Version	2.1.2
Document Number	D-SAFEX-V-01-001
Location	MKS ID 61036
Label	Release_1_26_1 *1)

4.1.8 Integration Test Report (ITR)

This document contains a detailed integration test report of the Safe Watchdog Manager Stack according to the requirements of ISO 26262:2011

Document Title	Safe Watchdog Manager Stack - Integration Test Report
Document Version	2.0.21
Document Number	D-SAFEX-V-01-002
Location	MKS ID 280966
Label	Release_1_26_1 *1)
Location PDF	\\fileserver.vie.at.tttech.ttt\sw-development\software-releases\external\TTX\2014\safe_execution_V1_26_0_2014_05_27_internal_documents\integration_test\safe_execution_integration_test_report_v1_26_0.pdf

*1) The S-WdgM and S-WdgIf Integration test was executed on the V850PJ4 platform (evaluation board) in the 1.26.0 TTTech Release. The S-Wdg driver integration test was executed on the R7F701353 customer platform with the TLE4473 watchdog at the 1.25.0 TTTech Release.

4.2 Safe Watchdog Manager

This chapter contains documents related to Safe Watchdog Manager module.

4.2.1 Software Requirements Document (SRD)

This document describes the software requirements for Safe Watchdog Manager. The SRD represents the software unit high-level requirements as required by ISO 26262:2011 – 6, clause 6.

Document Title	Safe Watchdog Manager Software Requirements Document
Document Version	1.0.10
Document Number	D-SAFEX-S-70-004
Location	MKS ID 53448
Label	Release_1_26_1

4.2.2 Unit Design Document (UDD)

The UDD represents the software unit design specification as required by ISO 26262:2011 – 6, clause 8.

Document Title	Safe Watchdog Manager Unit Design Document
Document Version	1.0.6
Document Number	D-SAFEX-D-70-002
Location	MKS ID 53535
Label	Release_1_26_1

4.2.3 Source Code

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

Title	Safe Watchdog Manager Source Code
Version	3.3.2
Location	http://tttechsvn.vie.at.tttech.ttt/trunk/SW/msp-watchdog-mgr

The HIS metrics and the MISRA rule check are performed with the tool QA-C.
The HIS metrics report can be found in the files
http://tttechsvn.vie.at.tttech.ttt/trunk/projects/customers/SafeExe-ASIL/04_technical-documents/HIS_MISRA_checks/Release_1_26_0.
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_0
All violations are justified. The justifications are provided as comments in the respective source files.

4.2.4 Unit Test Specification (UTS)

The UTS contains a detailed test specification of the software unit according to the requirements of ISO 26262:2011 – 6, clause 9 . The UTS demonstrates 100% requirements coverage.

Document Title	Safe Watchdog Manager Unit Test Specification
Document Version	1.0.22
Document Number	D-SAFEX-V-70-001
Location	MKS ID 61477
Label	Release_1_26_1

4.2.5 Unit Test Report (UTR)

The UTR contains a detailed unit test report according to the requirements of ISO 26262:2011 – 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 Manager Unit Test Report
Document Version	1.0.4
Document Number	D-SAFEX-V-70-005
Location	http://tttechsvn.vie.at.tttech.ttt/trunk/projects/customers/SafeExe-ASIL/04_technical-documents/Reviews/S-WdgM/UTR/S-WdgM-Stack_UTR_WdgM_D-SAFEX-V-70-005_V_1 0 4.pdf

4.2.6 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 26262:2011 requirements. Moreover, the SM describes which SW safety lifecycle requirements and recommendations of ISO 26262:2011 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 Manager Safety Manual
Document Version	2.3.28
Document Number	D-SAFEX-S-70-001
Locations	MKS ID 228403
Label	Release_1_26_1

4.2.7 Safe Watchdog Manager Verifier

4.2.7.1 Software Requirements Document (SRD)

This document lists the requirements to be fulfilled by the Safe Watchdog Manager Configuration Verifier.

Document Title	Safe Watchdog Manager Verifier Software Requirements Document
Document Version	1.0.2
Document Number	D-SAFEX-S-70-007
Location	MKS ID 239129
Label	Release_1_26_1

4.2.7.2 Source Code

The verifier source code is written in the C programming language. It is delivered as a .dll file.

Title	Safe Watchdog Manager Verifier Source Code
Version	1.2.11
Location	http://tttechsvn.vie.at.tttech.ttt/trunk/SW/msp-watchdog-mgr-config/src/C

4.2.7.3 Unit Test Specification (UTS)

The UTS contains a detailed test specification of the software unit according to the requirements of ISO 26262:2011 – 6, clause 9.

Document Title	Safe Watchdog Manager Verifier Unit Test Specification
Document Version	1.0.3
Document Number	D-SAFEX-V-70-009
Location	MKS ID 313571
Label	Release_1_26_1

4.2.7.4 Unit Test Report (UTR)

The UTR contains a detailed unit test report according to the requirements of ISO 26262:2011 – 6, clauses 8 and 9. The UTR shows that all tests and review procedures specified in the UTS passed.

Document Title	Safe Watchdog Manager Verifier Unit Test Report
Document Version	1.0.1
Document Number	D-SAFEX-V-70-010
Location	http://tttechsvn.vie.at.tttech.ttt/trunk/projects/customers/SafeExe-ASIL/04_technical-documents/Unit_Test_Reports/S-WdgM-Stack_UTR_WdgMVerifier_D-SAFEX-V-70-010_V_1.0.1.doc

5 Summary

The evidence in sections

- “Assumptions on S-WdgM Stack as SEooC”,
- “Software Safety Lifecycles”
- “Software Safety Lifecycle Documentation”

and the assessment reports [AUDIT_S-WdgM] shows that the S-WdgM Stack 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.

6 Abbreviations and Glossary

Acronym / Term	Meaning
API	Application Programmer Interface
ASIL	Automotive Safety Integrity Level
HIS	Herstellerinitiative Software
HW	Hardware
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 26262:2011-10
SM	Safety Manual
SW	Software

7 References

7.1 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.** Report-No: 8109170322-B04, Version 1.0 2013-02-25
[COMPL]	TTTech Computertechnik AG, ISO_DIS_26262_Compliance.xls, D-INT-CL-70-001

7.2 Other Documents

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