Functional Safety
(according to ISO 26262:2018)

Safety Plan

Title:	Safety Plan - FuSa-02_0070
Project:	i-Q GmbH – complete - GB
Sample:	<<sample>>
Date:	05.04.2021
Status:	Draft
Version:	BF
ASIL:	Maximum ASIL is ASIL C

	Name:	**Date:**	**Signature:**
Prepared:	Jörg Schacht (FSM)		
Checked:			
Approved:			

Inhaltsverzeichnis

Table of Contents

1. Description

This Safety Plan is deliberately sorted according to the Work Products to be created and not according to the activities required by the standard. The reason for this is that corresponding excerpts from this Safety Plan are to be made available to the persons responsible for the corresponding Work Products. In this way, the persons responsible have all the information specified in the standard for their work product in a clear, condensed form in one place.

In addition, most Work Products contain information on which activities are expected for implementation. This is also intended to promote and improve independent work on the work products.

Excerpts from the ISO 26262:2018 standard are identified by the fact that they are reproduced in the original English text and are placed in a frame.

Crossed-out headings indicate that these Work Products should normally be generated, but do not have to be created in the <<PROJECT>> project due to agreements with <<CUSTOMER>> or for other reasons at the << COMPANY>>. A corresponding justification can also be found in this Safety Plan.

The <<PROJECT>> project is a new development, so there are no direct specifications from previous projects. Thus, the chain of reasoning with "proven in use" cannot be applied to this project either.

1.1. *Reference to the Copy Right in the Standard*

The standard contains the following note on page ii in each individual part: "All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester."

In this Safety Plan we explicitly refer to the half sentence: "Unless [...], or required in the context of its implementation, [...]".

In order to be able to implement ISO 26262 sensibly and efficiently in the company, the individual employees must be informed precisely about the exact scope of their activities. They receive this information via the Safety Plan, so that an exact citation of the standard is unavoidable. This document is only used within the company and is not passed on.

This is to make it clear that we are well aware of the copy right, but at the same time we absolutely need the exact wording of the standard for correct implementation. Unfortunately, experience has shown that pure referencing is absolutely counterproductive. This is because the individual employees are confronted with a set of standards of over 800 pages and will therefore not, as a rule, look into the relevant texts of the standard.

Our approach therefore helps to ensure that each employee only has to read the specific parts of the standard that are necessary for the implementation of his or her specific work product.

1.1.1. *References within this document*

References to ISO 26262:2018 within this document are presented as follows:

- (4-7.4.2)
- Reference to ISO 26262:2018 – chapter 4 – subitem 7.4.2

Framed paragraphs are direct wordings from the standard. E.g., definition of "Safety Plan" (according to ISO 26262-1:2018, 3.143).

1-3.143

safety plan

plan to manage and guide the execution of the *safety activities* (3.133) of a project including dates, milestones, tasks, deliverables, responsibilities and resources

1.2. *Definitions of terms related to the standard*

1.2.1. *How to write Standards?*

Source: www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/how-to-write-standards.pdf (20.08.2020)

1.2.1.1. Verbal forms (from ISO)

In all clauses, be clear about what is a requirement and what is a recommendation or other type of statement. In order to make clear what the user must do, the following verbal forms are used in ISO documents:

- Requirements – shall, shall not
- Recommendations – should, should not
- Permission – may, need not
- Possibility and capability – can, cannot

1.2.2. *Must (company specific)*

The word “MUST” in the text is used for legislative or regulatory requirements (e.g. Health and Safety) and must be implemented, and its implementation verified.

The word "Must" in the text is used for legal and regulatory requirements (for example, health and safety related areas) and these MUST be implemented. This implementation must be verified. (The attracted requirement itself cannot be changed. However, a requirement can be replaced by another requirement - engine compartment / interior).

Note: With the negation of this word (must not) you have to be very careful in German, because the translation is: "darf nicht" and not "muss nicht". It is therefore a very clear prohibition!

1.2.3. *Shall (company specific)*

The word “SHALL” is used to indicate a requirement that is contractually binding, meaning it must be implemented, and its implementation verified. These requirements must be followed, without exception.

The word "Shall" is used to indicate a requirement that is contractually binding. It means that it MUST be implemented and verified. These requirements must be followed without exception. (Changes must go through the change management process!).

Note: With the negation of this word (shall not) you have to be very careful in German, because the translation is: "darf nicht" and not "muss nicht". It is therefore a very clear prohibition!

1.2.4. *Should (company specific)*

The word “SHOULD” is used to indicate a goal which must be addressed by the design but is not formally verified. Such recommendations or advice are expected to be followed unless good reasons are stated for not doing so.

The word "Should" identifies goals that must be followed during development, but do not need to be formally verified. It is expected to adopt these recommendations or advice unless there are good reasons not to do so. (Non-compliance with these objectives does not necessarily require a change management process).

1.2.5. *Will (company specific)*

The word “WILL” in the text denotes a provision or an intention in connection with a requirement. This term is also used for indicating information to the supplier about LRU reintegration or any additional data which the supplier should take into account.

The word "Will" in the text describes a specification or declaration of intent in connection with a requirement. This term is also used to provide information to the supplier about LRU (line replaceable unit) installation or additional data material that the supplier should consider. (This is NEVER a requirement. [Comment] - Facts communicated by the customer. - Example: To be installed in the engine compartment)

1.2.6. *May (company specific)*

The word “MAY” in the text denotes a permissible practice or action. It does not express a requirement.

The word "May" in the text describes a permission. It is not a requirement. (Example: In case of EMC problems, it is allowed to make a ground connection between housing and vehicle ground).

1.2.7. *Assessment (company specific)*

The aim of an assessment is always to check processes with a constructive character. Constructive character means that an assessment report can contain something positive and not only look for "mistakes". It is about so-called findings, strengths and weaknesses. What has the organization under review done well in terms of its process area, and what can be done better? People from the company under review can also sit in on an assessment. Often as observers or co-assessors.

In an assessment, the guideline for a later audit is defined.

1.2.8. *Audit (project specific)*

In an audit, the focus is more on non-compliance with certain processes and procedures; moreover, an audit is usually destructive and organized externally. The information collected is limited to missing or "wrong" implementations. An audit is generally very much about compliance with rules.

In an audit, compliance with the guidelines defined in an assessment, for example, is checked and evaluated.

1.3. *Excerpt from ISO 26262-1:2018 - Definition of terms*

1-3.143 Safety plan

plan to manage and guide the execution of the *safety activities* (3.133) of a project including dates, milestones, tasks, deliverables, responsibilities and resources

1.4. *Extract from ISO 26262-2:2018 - Tailoring*

2-6.4.5 Tailoring of the safety activities

6.4.5.1 A safety activity with regard to a specific item development may be tailored i.e. omitted or performed in a different manner than prescribed in the reference ISO 26262 lifecycle. If such a safety activity is tailored, then

a) the tailoring shall be defined in the safety plan (see 6.4.6.5, b); and

b) a rationale as to why the tailoring is appropriate and sufficient to achieve functional safety shall be available.

NOTE 1 The rationale considers the ASILs of the corresponding requirements.

NOTE 2 The rationale for the tailoring is included in the safety plan and reviewed during the confirmation review of the safety plan (see 6.4.9) or during the functional safety assessment (see 6.4.12).

NOTE 3 This requirement applies to tailoring for application on a specific item. With regard to tailoring of the safety lifecycle for application across item developments within an organization, only 5.4.6 applies.

6.4.5.2 If a safety activity is tailored in accordance with 6.4.5.1 as a result of an impact analysis in accordance with 6.4.3 or 6.4.4, then the tailoring shall comply with 6.4.6.7.

6.4.5.3 If a safety activity is tailored in accordance with 6.4.5.1 as a result of a proven in use argument, then the tailoring shall comply with ISO 26262-8:2018, Clause 14.

6.4.5.4 If a safety activity is tailored in accordance with 6.4.5.1 because of an evaluation of hardware elements, the tailoring shall comply with ISO 26262-8:2018, Clause 13.

6.4.5.5 If a safety activity is tailored in accordance with 6.4.5.1 because of a qualification of software components, the tailoring shall comply with ISO 26262-8:2018, Clause 12.

6.4.5.6 If a safety activity is tailored in accordance with 6.4.5.1 based on a rationale that considers the confidence in the usage of software tools, then the tailoring shall comply with ISO 26262-8:2018, Clause 11.

6.4.5.7 If the safety activities are tailored in accordance with 6.4.5.1 because an element is developed as a Safety Element out of Context (“SEooC”), then

a) the development of the safety element out of context shall be based on a requirement specification that is derived from assumptions on an intended use and context, including its external interfaces; and

b) the assumptions on the intended use and context of the safety element out of context shall be validated when the element is integrated in its target application.

NOTE The ISO 26262 series of standards as a whole cannot be applied to an element developed as a safety element out of context because functional safety is not an element property (however, an element of an item can be identified as safety related). Functional safety is an item property that can be evaluated by means of a functional safety assessment.

EXAMPLE A microcontroller developed as a safety element out of context

NOTE 2 See ISO 26262-10 for further details of a Safety Element out of Context development.

6.4.5.8 This requirement applies to item developments for T&B: if an application that is out of scope of the ISO 26262 series of standards is being interfaced with a base vehicle or item that has been developed in accordance with those standards, then tailoring of corresponding safety activities shall be performed in accordance with ISO 26262-8:2018, Clause 15.

6.4.5.9 This requirement applies to item developments for T&B: if safety activities are performed to achieve confidence that a system or component not developed according to the ISO 26262 series of standards satisfies the required level of functional safety needed for the integration into an item developed in accordance with those standards, then tailoring of these safety activities shall be performed in accordance with ISO 26262-8:2018, Clause 16.

6.4.6.4 The safety plan shall either be:

a) referenced in the project plan, or

b) included in the project plan, such that the safety activities are distinguishable.

NOTE The safety plan can incorporate cross-references to other information under configuration management (see ISO 26262-8:2018, Clause 7). Cross-references are generally preferable to the parallel

description of activities in different work products, or in other documents that are under configuration management.

6.4.6.5 The safety plan shall define the planning of the activities and procedures for achieving functional safety, including:

a) the implementation of project-independent safety activities in accordance with Clause 5 into project-specific safety management;

b) the definition of the tailored safety activities, in accordance with 6.4.5, if applicable;

NOTE For example, tailoring as a result of an impact analysis at item level (see 6.4.3) or at element level (see 6.4.4). Refer also to 6.4.6.7.

c) the planning of the safety activities to comply with the requirements of ISO 26262-3, ISO 26262-4, ISO 26262-5 and ISO 26262-6;

d) the planning of the supporting processes, in accordance with ISO 26262-8, including if applicable, the reference to the Development Interface Agreements ("DIA"s) that define the interfaces with the safety plans of the other parties in a distributed development, in accordance with ISO 26262-8:2018, Clause 5;

e) the planning of the integration and verification activities to comply with the requirements of ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6 and ISO 26262-8:2018, Clause 9; and the planning of the safety validation activities in accordance with ISO 26262-4:2018, Clause 8;

NOTE 1 The work product "safety plan" includes detailed integration, verification, and safety validation planning, however such planning can be in other documents (see ISO 26262-8:2018, Clause 10).

f) the scheduling of the confirmation reviews, the functional safety audit and the functional safety assessment in accordance with 6.4.9 to 6.4.12;

NOTE 2 The level of independence given in 6.4.9 of a person that carries out a confirmation measure is specified in the safety plan.

NOTE 3 The safety manager is responsible for scheduling the confirmation measures. The details of a confirmation measure are planned by the person responsible for that confirmation measure.

g) the planning of the analysis of dependent failures, if applicable, and the safety analyses to comply with the requirements of ISO 26262-3, ISO 26262-4, ISO 26262-5, ISO 26262-6, ISO 26262-9:2018, Clause 7 and ISO 26262-9:2018, Clause 8;

NOTE 4 The objectives and scope of the safety analyses are defined during their planning and depend on the corresponding sub-phase and context.

h) the provision of the proven in use arguments of the candidates in accordance with ISO 26262-8:2018, Clause 14, if applicable; and

i) the provision of the confidence in the usage of software tools in accordance with ISO 26262-8:2018, Clause 11, if applicable.

6.4.6.7 In the case of a modification of the item, a modification of the environment of an existing item, in accordance with 6.4.3, or in the case an element reused in accordance with 6.4.4:

a) the reference safety life cycle of the ISO 26262 series of standards shall be tailored based on the results of the corresponding impact analysis;

NOTE 1 The tailored safety activities are defined in the safety plan considering the applicable lifecycle phases and sub-phases (see 6.4.5).

b) the affected work products that need to be created or updated shall be identified, described and reworked accordingly; and

NOTE 2 The affected work products include the safety validation specification (see ISO 26262-4:2018, Clause 8).

c) in the case of safety documentation that does not comply with the ISO 26262 series of standards, the necessary activities to comply with the corresponding requirements of these standards shall be determined.

EXAMPLE 1 An element developed according to a safety standard different from the ISO 26262 series of standards, with the corresponding safety documentation being incomplete to comply with ISO 26262

EXAMPLE 2 A legacy element with missing safety documentation, or safety documentation insufficient to comply with ISO 26262

6.4.6.8 The safety plan shall be updated incrementally, as a minimum at the beginning of each phase.

NOTE At least at the beginning of each phase, the safety plan is updated so as to detail the planning of the safety activities of that phase. The safety plan can be further detailed in a sub-phase.

6.4.6.9 The work products required by the safety plan shall be kept up-to-date during the development phases so as to maintain an adequate representation of the item, or element, until and at the release for production.

6.4.6.10 In the case of a distributed development, both the customer and the supplier shall define a safety plan regarding the respective safety activities.

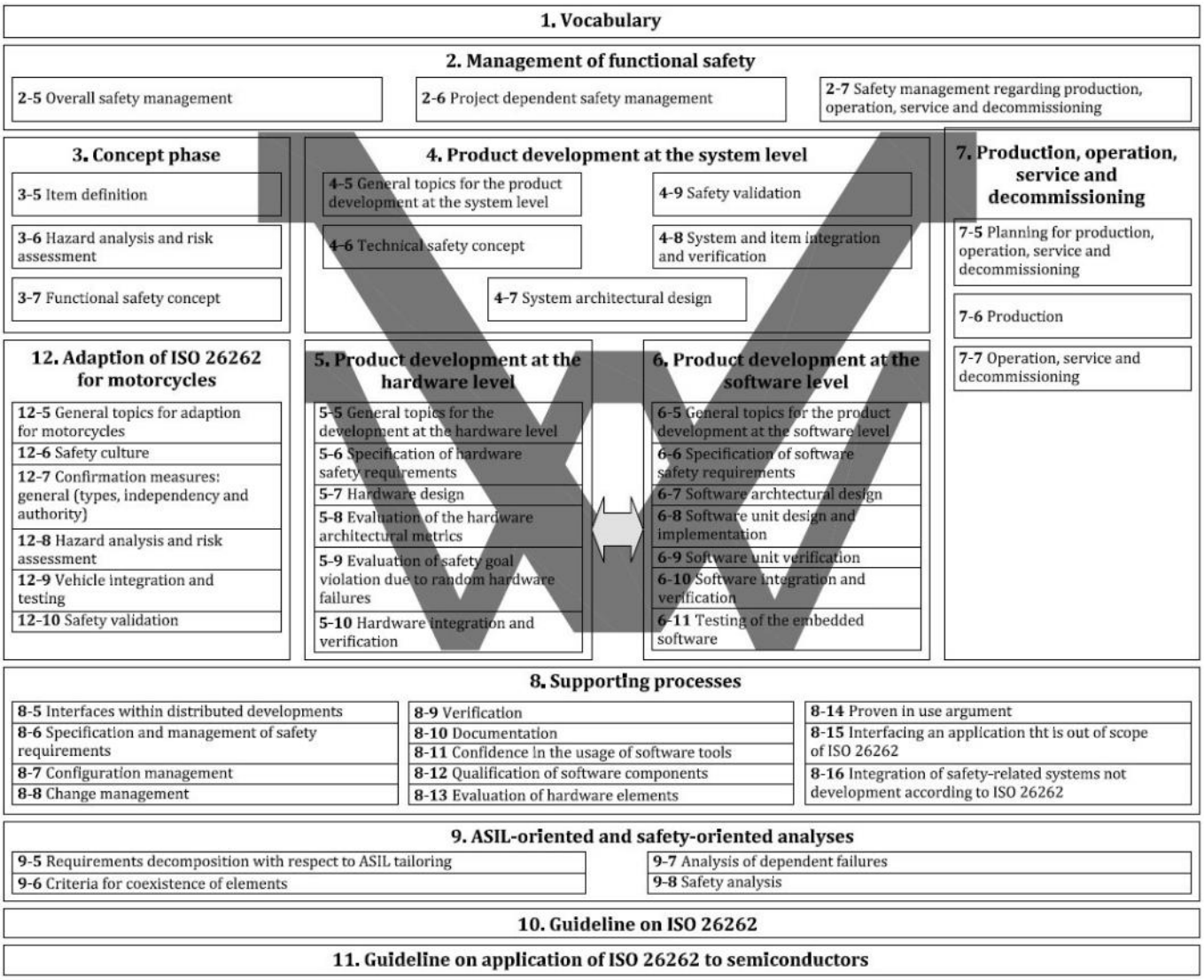
NOTE The corresponding Development Interface Agreement is defined in accordance with ISO 26262-8:2018, Clause 5.

6.4.7 Progression of the safety lifecycle

6.4.7.1 In the case of a lack of information from the pertinent preceding sub-phases, a subsequent sub-phase shall only start if the lack of information does not cause an unreasonable risk regarding functional safety.

NOTE For cases where the lack of information can jeopardize the project, the issue is escalated.

6.4.7.2 The work products required by the safety plan shall be subject to configuration management, change management and documentation, in accordance with ISO 26262-8:2018, Clause 7, ISO 26262-8:2018, Clause 8 and ISO 26262-8:2018, Clause 10, respectively, no later than the time of entering the phase “product development at the system level” (see ISO 26262-4).



Picture 1: V-model of ISO 26262:2018

1.5. *Overview of all Work Products*

In this Safety Plan, only the Work Products that are to be created for the current project are shown according to the tailoring performed. The complete overview of all Work Products can be found in the file: „FuSa-00_0000_ListeAllerWorkProducts_ISO26262-2018.xlsx“.

In this file, in addition to the reasons why a Work Product does not have to be created (has been tailored), you will also find the times in the form of milestones at which the respective Work Product should be started and when it must be completed accordingly.

1.6. *Explanation of the table for each Work Product*

The following information is stored in the tables at the beginning of each description of the respective Work Products:

- ID according to standard:
- PDF created on:
- Name of the Work Product:

- File path:
- Responsible author:
- Work Product Predecessor:
- B-phase
  - Prepared:
  - In progress:
  - Complete:
  - Reviewed:
  - Released:
  - Audited:
- C-phase
  - Prepared:
  - In progress:
  - Complete:
  - Reviewed:
  - Released:
  - Audited:

2. Applicable Documents

Reference	Name of Document
H:\Normen\ISO\ISO 26262	ISO-26262:2018, part 1 - Vocabulary ISO-26262:2018, part 2 - Management of Functional Safety ISO-26262:2018, part 3 - Concept Phase ISO-26262:2018, part 4 - System Level ISO-26262:2018, part 5 - Hardware Level ISO-26262:2018, part 6 - Software Level ISO-26262:2018, part 7 - Production and Operation ISO-26262:2018, part 8 - Supporting Processes ISO-26262:2018, part 9 - ASIL ISO-26262:2018, part 10 - Guideline ISO 26262:2018, part 11 - Guidelines on application of ISO 26262 to semiconductors ISO 26262:2018, part 12 - Adaptation of ISO 26262 for motorcycles

Table 1: Applicable Documents

3. Referenced Documents

Reference	Name of Document
[BM20]	VDA Band: Prozessbeschreibung Besondere Merkmale BM, 2. Ausgabe vom April 2020
[DOK18]	VDA Band 1, Dokumentation und Archivierung, 4. Ausgabe vom Mai 2018
[GEBH13]	Vera Gebhardt, Gerhard M. Rieger, Jürgen Mottok, Christian Gießelbach; Funktionale Sicherheit nach ISO 26262 – Ein Praxisleitfaden zur Umsetzung; dpunkt.verlag 2013 (e-Book)
[HELM13]	Ekkehard Helmig, ISO 26262 – Funktionale Sicherheit in Personenfahrzeugen; InTeR – Zeitschrift zum Innovations- und Technikrecht, Frankfurt am Main: Deutscher Fachverlag GmbH 2013 (S. 28-33)
[HILL12]	Martin Hillenbrand, Funktionale Sicherheit nach ISO 26262 in der Konzeptphase der Entwicklung von Elektrik/Elektronik Architekturen von Fahrzeugen (Dissertation), Scientific Publishing 2012 (http://dx.doi.org/10.5445/KSP/1000025616)
[MSA10]	Measurement System Analysis, AIAG, 4. Ausgabe vom Juni 2010
[PPF12]	VDA Band 2, Sicherung der Qualität von Lieferungen – Produktionsprozess- und Produktfreigabe, 5. Überarbeitete Auflage, November 2012
[ROSS14]	Hans-Leo Ross; Funktionale Sicherheit im Automobil – ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen; Hanser Verlag 2014 (e-Book).
[SPC05]	Statistical Process Control, AIAG, 2. Ausgabe vom Juli 2005
[VDA12]	Verband der Automobilindustrie; Auto & Normung, NA-Automobil Jahresbericht 2012 https://www.vda.de/dam/vda/publications/Jahresbericht%202012/1341308052_de_437643196.pdf
[FMEA19]	VDA Band: AIAG & VDA FMEA-Handbuch, 1. Ausgabe vom Juni 2019
	The following punctuation marks are used: Name, first name: Title. Subtitle. Volume. Place of publication: Publisher Year of publication (series and volume number), p..

Table 2: Referenced Documents

4. Amendment Record

Issue	Date	Changes
001	17.05.2020	Adaptation of the structure to the 2018 version - Only the names / headings of the work products have been changed.
002	24.05.2020	Tables (with WP details) revised, WPs for part 12 added, capitalisation of WP titles, all directories updated.
003	01.06.2020	WP line to 0930 added. Tables completed.
004	07.06.2020	Last changes for the review by Astrid Hildebrandt and Timo Lang, tables with milestones added
005	08.06.2020	All numbering and indexes updated; formal trifles standardised
006	27.07.2020	Comments and suggested changes incorporated
AG	06.08.2020	Numbering brought up to date based on the review together with Astrid Hildebrandt. Additional reviews (deemed necessary) added to the work products.
AH	10.08.2020	Cross-check with list of Work Products and DIAs
AI	02.09.2020	Last changes for the first official release by BF
AJ	07.09.2020	Amendments by Astrid Hildebrandt incorporated
AK	10.09.2020	File path deleted from footer; German explanation added to Work Products.
AL	14.09.2020	German declarations at Work Products completed, numbers and names of PEP gates updated - version for release by BF
BA	27.11.2020	Comments from the review incorporated
BB	30.12.2020	Changes from the PEP incorporated
BC	01.02.2021	Changes from the PEP incorporated
BD	15.02.2021	Final alignment with PEP, list of work products Basis for splitting into mixed-language version (so far) and English-only version
BE	04.03.2021	Review by AH (translation)
BF	04.03.2021	Changes done by Jörg Schacht

Table 3: Amendment Record

5. Planning and Project Management

5.1. *Planning of the individual Work Products*

The planning of the individual work products can be found in the file "FuSa-00_0000_ListeDerWorkproducts.xlsx". In this file, each work product is assigned to two gates from the product creation process. One is the start gate and the other is the gate at which the work product should be finished.

The gates have the following numbers and descriptions:

Q-Gate	M-Gate	Task completed:	Task started:
	MG00	Research phase completed	Offer and acquisition launched
Q1	MG01	Offer and acquisition	Start A pattern
	MG02	Finish A-pattern design	
Q2	MG03	Completion A Sample / Completion PT Testing	Start B pattern
	MG04	Finish B-phase design	
Q3	MG05	B-model degree / DV degree	Start C pattern
	MG06	C-phase design finish	
Q4	MG07	Completion C pattern / Completion PV	Start D pattern
Q5	MG08	Completion D-pattern / Completion Ap-proval Test	Start of series production (SOP)
	MG09	End of series production (EOP)	Start of separate spare parts disposal

Table 4: Numbering of the Maturity Gates (OLD)

The maintenance of the dates for the individual gates is documented in the project plan.

The actual implementation of each Work Product is documented in this Safety Plan in the table at the beginning of each Work Product.

B-phase	**Prepared:**	**In progress:**	**Complete:**	**Verified:**	**Released:**	**Audited:**
C-phase	**Prepared:**	**In progress:**	**Complete:**	**Verified:**	**Released:**	**Audited:**

Table 5: Status of the respective work product in the B pattern and C pattern

New designations:

Q-Gate	M-Gate	Task completed:	Task started:	Disci.Milestones
	MG00	Research phase completed	Offer and acquisition launched	
QG1	MG01	Offer and acquisition	Start A pattern	

Q-Gate	M-Gate	Task completed:	Task started:	Disci.Milestones
	MG02	Completion A-pattern Requirements		XX-A1
	MG03	Finish A-pattern design (Freeze)		XX-A2
	MG04	Completion A-model engineering release	Start Prototype Testing	XX-A3
QG2	MG05	Completion A Sample / Completion PT Testing	Start B pattern	
	MG06	Completion B-phase Requirements		XX-B1
	MG07	Finish B-phase design (Freeze)		XX-B2
	MG08	Completion B-phase engineering release	Start Design Verification	XX-B3
QG3	MG09	B-model degree / DV degree	Start C pattern	
	MG10	Completion C-phase Requirements		XX-C1
	MG11	Finish C-phase design (Freeze)		XX-C2
	MG12	Completion C-Sample Engineering Release	Start Product&Process Validation	XX-C3
QG4	MG13	Completion C pattern / Completion PV	Start D pattern	
QG5	MG14	Completion D-Muster / Completion Approval Test	Start of series production (SOP)	
	MG15	End of series production (EOP)	Start of the separate spare parts supply	

Table 6: Numbering of the Maturity Gates (NEW)

5.2. *Report on possible deviations in safety activities*

Within the framework of weekly internal meetings (telephone conferences), the deviations that have occurred are discussed and, if necessary, recorded in a LOP and followed up until completion.

The communication of possible deviations to the client also takes place in weekly meetings between the project manager and the responsible persons on the client side.

6. ISO 26262:2018, part 1 – Vocabulary

Part 1 of the standard only contains definitions and no work products to be created.

Therefore, there are no further descriptions in this part of the document.

7. ISO 26262:2018, part 2 - Management of Functional Safety

7.1. *FuSa-00_0000 List of all Work Products*

ID according to standard:	(not mentioned with ID in the standard)					
PDF created on:						
Name of the work product:						
File path:						
Responsible author:	Jörg Schacht (Functional Safety Manager, AFSE)					
Work Product Predecessor:	n/a					
B-phase	**Prepared:**	**In progress:**	**Complete:**	**Verified:**	**Released:**	**Audited:**
C-phase	**Prepared:**	**In progress:**	**Complete:**	**Verified:**	**Released:**	**Audited:**

The list of all work products is the basis for all further considerations and serves as the starting point for this Safety Plan. The entries in the ISO 26262:2018 standard serve as the basis for these lists.

The list of work products is compiled once for passenger cars and once for motorbikes.

In addition to the Work Products, which have their own ID in the standard, we have identified further Work Products in the <<FIRMA>>, which are only mentioned implicitly.

In total, we have presented 11 confirmation measures as separate work products (see 7.15).

By splitting some Work Products into individual components, the following additional Work Products are created: 111, 112 / 221, 222, 223, 224 / 232, 233 / 311, 312, 313, 314, 315, 316 (14 for cars) and 1421, 1422, 1423, 1424 (4 for motorbikes).

WP#	WP name according to ISO26262:2018	Add. WP#	Additionally WP names
110	Evidence of safety management regarding production (a), operation, service and decommissioning (b)	111	Evidence of safety management regarding production (a)
		112	Evidence of safety management regarding operation, service and decommissioning (b)
220	Verification report for system architectural design (a), the hardware-software interface (HSI - b) specification, the specification of requirements for production, operation, service and decommissioning (c), and the technical safety concept (d)	221	Verification report for system architectural design (a)

WP#	WP name according to ISO26262:2018	Add. WP#	Additionally WP names
		222	Verification report for the hardware-software interface (HSI) specification (b),
		223	Verification report for the specification of requirements for production, operation, service and decommissioning (c)
		224	Verification report for the technical safety concept (d)
310	Hardware Safety Analysis Report (FMEA, FMEDA, FTA)	311	Hardware-FMEA
		312	Safety analyses verification report (Hardware-FMEA)
		313	Hardware-FMEDA
		314	Safety analyses verification report (Hardware-FMEDA)
		315	Hardware-FTA
		316	Safety analyses verification report (Hardware-FTA)
1420	Verification report for system architectural design, the hardware-software interface (HSI) specification, the specification of requirements for production, operation, service and decommissioning, and the technical safety concept	1421	Verification report for system architectural design
		1422	Verification report for the hardware-software interface (HSI) specification
		1423	Verification report for the specification of requirements for production, operation, service and decommissioning
		1424	Verification report for the technical safety concept

Table 7: Division of the Work Products

This results in a total list of 144 Work Products without consideration of Part 12 for motorbikes or 176 Work Products with consideration of Part 12 for motorbikes.

(Part 1: 0 WPs / Part 2: 19 WPs / Part 3: 7 WPs / Part 4: 24 WPs / Part 5: 19 WPs / Part 6: 24 WPs / Part 7: 13 WPs / Part 8: 29 WPs / Part 9: 9 WPs / Part 10: 0 WPs)

Due to the agreements with our customer <<CUSTOMER>>, a part of these Work Products does not fall under the responsibility of the <<FIRM>>. According to the agreements with <<CUSTOMER>>, which have been documented in the DIA, a total of 19 Work Products are omitted, so that in the current project <<PROJECT>> a total of 125 Work Products are to be created at <<FIRMA>>. (Status: 15.02.2021)

7.2. *FuSa-02_0001 Functional Safety Audit (CM)*

ID according to standard:	(not mentioned with ID in the standard) - 2-T1(10)
PDF created on:	
Name of the work product:	
File path:	
Responsible author:	
Work Product Predecessor:	No predecessors defined in the standard. // No predecessors defined at the <<FIRMA>>.

B-phase	**Prepared:**	**In progress:**	**Complete:**	**Verified:**	**Released:**	**Audited:**
C-phase	**Prepared:**	**In progress:**	**Complete:**	**Verified:**	**Released:**	**Audited:**

2-6.4.11 Functional safety audit

6.4.11.1 For items and elements where the highest ASIL of the safety requirements is ASIL (B), C, or D: a functional safety audit shall be carried out in accordance with 6.4.9; and shall be finalized before the release for production.

6.4.11.2 A person responsible to carry out a functional safety audit shall be appointed in accordance with 5.4.4 and 5.4.2.7.

6.4.11.3 A functional safety audit may be based on a judgement of whether the process related objectives of the ISO 26262 series of standards are achieved.

NOTE The achievement of an objective of the ISO 26262 series of standards is considered against the corresponding requirements of these standards.

EXAMPLE The objectives of the requirements of clause 6 are specified in 6.1.

6.4.11.4 The person responsible to carry out a functional safety audit shall provide a report that contains a judgement of the implementation of the processes required for functional safety, based on:

a) an evaluation of the implementation of the processes against the definitions of the activities referenced or specified in the safety plan;

b) an evaluation of the safety plan against the organization-specific rules and processes (refer to 5.5.1);

c) an evaluation of the arguments, if provided, as to why the process related objectives of the ISO 26262 series of standards are achieved;

NOTE 1 Persons responsible for safety activities can provide an argument as to why the corresponding objectives of the ISO 26262 series of standards are achieved in order to facilitate a functional safety audit, considering 6.4.11.3.

NOTE 2 Compliance with all the corresponding ISO 26262 requirements is a sufficient rationale for having achieved an ISO 26262 objective.

d) an evaluation of whether the work products required by the safety plan are available;

e) an evaluation of whether the work products required by the safety plan products comply with ISO 26262-8:2018, 10.4.3 and are consistent between one another; and

f) improvement recommendations in accordance with 5.4.2.6, if applicable, e.g. in the case of noncompliances.

NOTE 3 A functional safety audit can be performed together, or synchronized, with an Automotive Software Process Improvement and Capability determination assessment (see also the ISO/IEC 33000 series of standards). However, an Automotive SPICE® assessment is not sufficient to perform the functional safety assessment in accordance with 6.4.12.

NOTE 4 An organization's process definitions can address multiple standards at the same time, e.g. the ISO 26262 series of standards and Automotive SPICE® configuration management process requirements. This coordination of processes can help to avoid duplication of work or process inconsistencies. For these coordinated processes, organization-specific process cross-references to the requirements of the ISO 26262 series of standards and to Automotive SPICE can be provided.

NOTE 5 A functional safety audit performed in an early phase in a project is beneficial to identify weaknesses in the processes.

2-C.11 Functional safety audit (see 6.4.11)

The goal is to judge whether the implementation of the processes required for functional safety, considering the definitions of the activities referenced or specified in the safety plan, achieve the process related objectives of the ISO 26262 series of standards.

2-6.2 General

[…]

Confirmation measures include confirmation reviews, a functional safety audit and a functional safety assessment:

— confirmation reviews are intended to judge whether the key work products (see Table 1) provide sufficient and convincing evidence of their contribution to the achievement of functional safety;

— if applicable, a functional safety audit evaluates the implementation of the processes required for the safety activities; and

— if applicable, a functional safety assessment judges whether the item achieves functional safety, or judges the contribution to the achievement of functional safety e.g. concerning the development of elements.

Table 1 lists the confirmation measures.

In addition to the confirmation measures, verification activities are performed. These verification activities, which correspond to requirements of other parts of the ISO 26262 series of standards, are intended to verify that the associated work products fulfil the project requirements and the technical requirements, especially with respect to use cases and failure modes.

Finally, the person responsible for the release of the item, or elements of the item, decides whether the item, or element(s), is ready for series-production and operation, based on the evidence that supports confidence in the achieved functional safety.

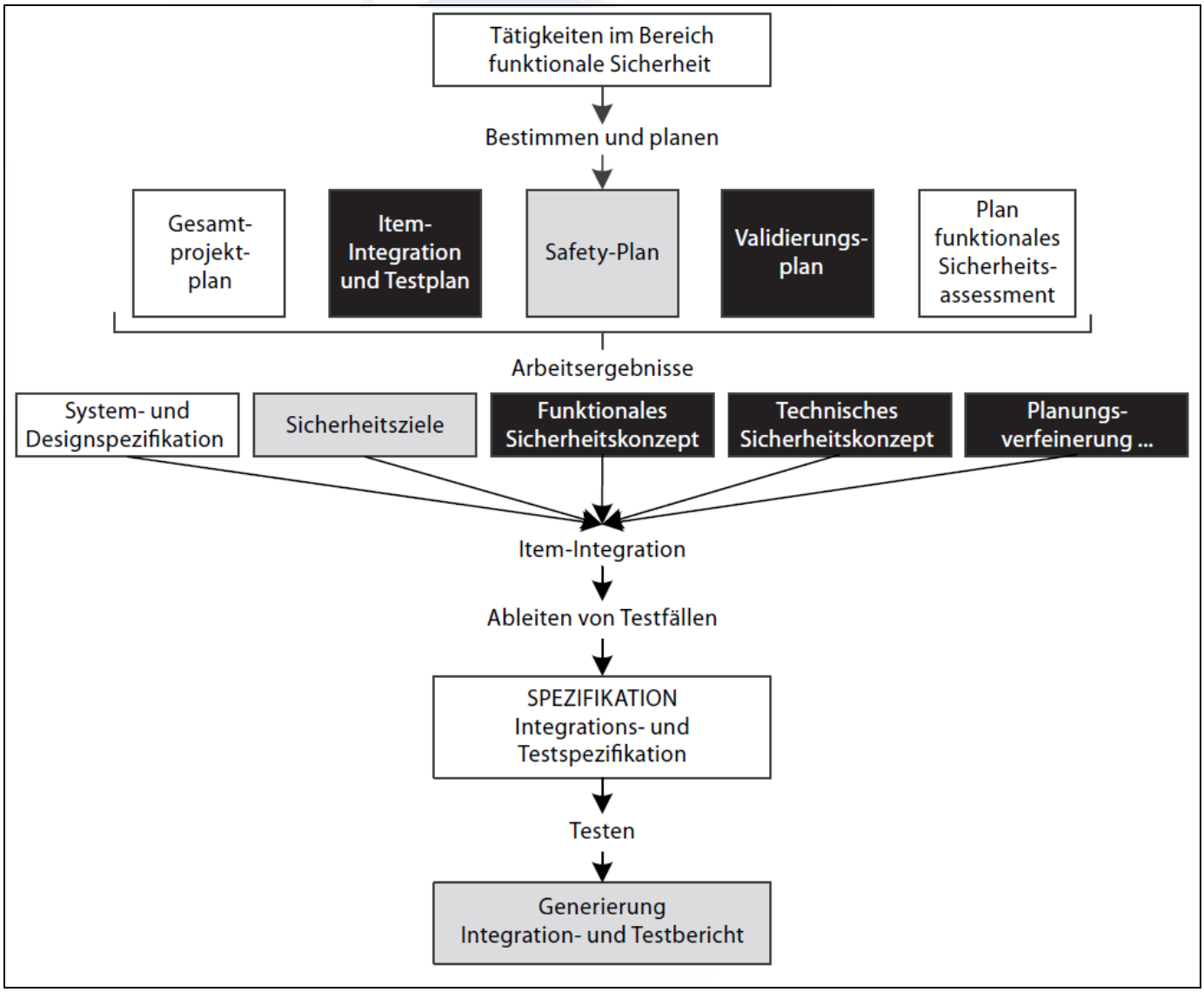
The Functional Safety Audit is an assessment of the functional safety process. It is in no way an assessment of the results of the product or the project!

Within the scope of compliance with the requirements of ISO 26262:2018, such an assessment of results does not take place.

In an audit, compliance with the guideline defined in an assessment, for example, is checked and evaluated. (Assessment: Do the company's specifications comply with the standard? Audit: Does the procedure in the project comply with the company's specifications?)

The aim of the Functional Safety Audit (FSA) is to check the implementation of the functional safety process in accordance with ISO 26262:2018 during the work performed in the process against the activities and specifications planned in the Safety Plan.

Depending on the ASIL level, the audit must be performed by another (ASIL B) or even organisationally independent (ASIL C: another team, ASIL D: other department or organisation) person. The level of independence is defined in ISO26262-2:2018, 6.4.9.1 Table1.



Picture 2: Activities and work results [GEBH13, page 36]

As the <<PROJECT>> project is the first ISO 26262:2018 project at the <<FIRM>>, it was decided internally that the Functional Safety Audit would first be carried out internally by the Quality department. In this way, inconsistencies should be detected and eliminated as early as possible.