**Functional Safety Concept**

Template

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Project:** | ISO 26262: Recommended Practice – SMARTcode | | | | | | | | | **Company:** | n.a. | | | | | | | | | **Document Status:** | Verified | | | | | | | | | **Maturity Level:** | <50% compliant | | | | | | | | |  | | |  | |  | |  | | | **Author:** | | **Company:** | | **Role:** | | **Email:** | | | [author] | | [company name] | | [role] | | [@address] | | |  | |  | |  | |  | | | **Stakeholder:** | | **Company:** | | **Role:** | | **Email:** | | | [stakeholder\_ 1] | | [company name] | | [role] | | [@address] | | | [stakeholder\_ 2] | | [company name] | | [role] | | [@address] | | | [stakeholder\_ 3] | | [company name] | | [role] | | [@address] | | | [stakeholder\_ 4] | | [company name] | | [role] | | [@address] | | | [stakeholder\_ x] | | [company name] | | [role] | | [@address] | | |  | | |
|  |  | | |
|  |  |  |  |

**Change History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Revision** | **Date** | **Author** | **Chapter(s)** | **Reason** | **Change** |
| *1* | *01-01-2016* | *J. Johnsson* | *1* | *Content out of date* | *Removed completed tasks* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Table of Contents

[Table of Contents 2](#_Toc459971529)

[1 To do list 3](#_Toc459971530)

[2 RASI(C) chart 3](#_Toc459971531)

[3 Conventions 4](#_Toc459971532)

[3.1 Document status 4](#_Toc459971533)

[3.2 Maturity level assignment 5](#_Toc459971534)

[4 Abbreviated terms 6](#_Toc459971535)

[5 Purpose and scope 6](#_Toc459971536)

[6 Related documents 7](#_Toc459971537)

[6.1 Input documents 7](#_Toc459971538)

[6.2 Work products 7](#_Toc459971539)

[6.3 Other related documents 7](#_Toc459971540)

[7 ISO26262 compliance 8](#_Toc459971541)

[7.1 Maturity level indication rationale 8](#_Toc459971542)

[7.2 Elements and aspects of this document which are not compliant to ISO26262 8](#_Toc459971543)

[8 System – subsystem decomposition 8](#_Toc459971544)

[9 Safety Goal attributes 9](#_Toc459971545)

[10 Functional Safety Requirements and Allocation 10](#_Toc459971546)

[Appendix A – Review form for TSC template (Template only!!!) 12](#_Toc459971547)

# To do list

This chapter shall provide a complete list of known missing elements or actions to reach the desired maturity level of this document.

# RASI(C) chart

Fill in the responsibilities with regards to this document in the RASI(C) chart below.

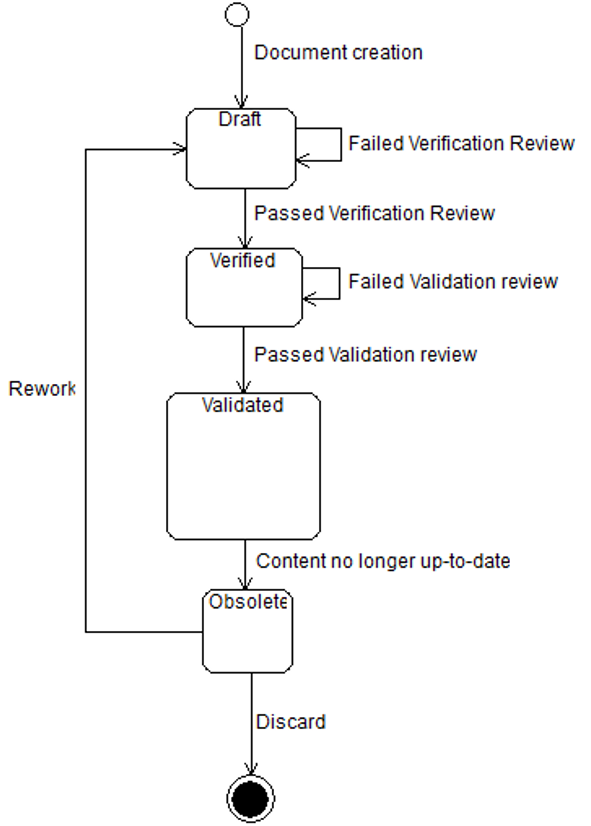
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Name | Tasks/Activities | Company | Email address |
| Responsible | *James Smith* |  | *CompanyX* | *jsmith@companyx.com* |
| Accountable |  |  |  |  |
| Supportive |  |  |  |  |
| Informed |  |  |  |  |
| Consulted (optional) |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| Name | Role | Role description |
| *James Smith* | *FSM* | *Functional Safety Manager, responsible for the conformance of [company / department] to ISO26262.* |
| [name] | [role] | [description] |
|  |  |  |
|  |  |  |

|  |  |
| --- | --- |
| Responsibility | Description |
| Responsible | *The person who is ultimately responsible for the delivery of the work product. This person has to ensure the correctness, completeness, retention and availability of this document.* |
| Accountable | *The person who has ultimate accountability and approval authority. This person is legally responsible for the correct implementation according to ISO26262.* |
| Supportive | *The team or person(s) supporting carrying out the “real” work. They are committed to the completion of the work product.* |
| Informed | *Person(s) who must stay informed regarding results or actions taken but are not involved in final decision-making.* |
| Consulted | *(Optional) Those who can provide valuable input into the development of work products and are capable of determining the quality and correctness of the work product.* |

# Conventions

## Document status



Document life cycle

|  |  |
| --- | --- |
| Draft | When a new document is created the status “Draft” will be assigned. Only after a positive verification review the document can be promoted to “Verified” by performing a verification review. Also Obsolete documents can be assigned the status “Draft” after changes have been made to update.  *Please refer to ISO26262-2 Table D.1 – Overview of verification reviews.* |
| Verified | Status after a successful verification review according to ISO26262-2 has been performed on a document with status “Draft”. |
| Validated | Status after a successful validation review according to ISO26262-2 has been performed on a document with status “Verified”. |
| Obsolete | The status of the document should be changed to “Obsolete” when its contents no longer match the current state of the Item, System or organization it concerns, **regardless of the former document state.** |

## Maturity level assignment

At every validation review an estimate is made regarding the maturity level of this document. The estimate is based on the amount of ISO26262 requirements this document satisfies in relation to how many still have to be satisfied.

Only the person(s) responsible for the validation review may determine the maturity level of the Safety Case documents.

The maturity level will be assigned based on a scale of 0 – 4:

1. Not compliant
2. <50% compliant, roughly half of the aspects mentioned in ISO26262 are covered
3. <75% compliant, roughly ¾ of the aspects mentioned in ISO26262 are covered
4. <90% compliant, most of the aspects mentioned in ISO26262 are covered
5. >90% compliant, so far to judge every aspect of the ISO26262 is covered

# Abbreviated terms

List all abbreviations here which are used in this document and are not covered by ISO26262-1 Clause 2

# Purpose and scope

The Functional Safety Concept encompasses functional, implementation independent requirements on the safety of the Item. It refines the Safety Goals by defining the Safety Goals attributes and it establishes a link between the functional safety requirements and the preliminary architecture. The preliminary architecture is subject to refinement in order to ultimately evolve into the safety-compliant system.

The functional safety requirements are allocated either to the preliminary architectural elements of the item, or to external measures.

To do: add scope of item here

# Related documents

The initiation of the validation plan is described in ISO26262-4, clause 5. The refinements of the validation plan are described in ISO26262-4, clause 6.4.6 and clause 9.4.2.

## Input documents

For creating the validation plan:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document title | Internal ID | Revision nr | Status | Resource location |
| Project plan |  |  |  |  |
| Safety plan |  |  |  |  |
| Functional safety assessment plan |  |  |  |  |
| Functional safety concept |  |  |  |  |

For refining the validation plan:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document title | Internal ID | Revision nr | Status | Resource location |
| Technical safety requirements specification |  |  |  |  |
| HARA |  |  |  |  |
| Safety Goals |  |  |  |  |
| Functional Safety Concept |  |  |  |  |

## Work products

The following work products result from a validation activity:

* **Validation plan (refined)**
* **Validation report (as a result of the evaluation of the validation plan)**

## Other related documents

If any other documents are used to create the Validation Plan, please note them here.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document title | Internal ID | Revision nr | Status | Resource location |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# ISO26262 compliance

## Maturity level indication rationale

## Elements and aspects of this document which are not compliant to ISO26262

# System – subsystem decomposition

The Item can be decomposed into systems and sub system in order to form the input to the chapter “Functional Safety Requirements and Allocation”. The Functional Safety Requirements are derived from the Safety Goals, after which the preliminary architectural elements are added to fulfil the Functional Safety Requirements.

Complete preliminary system – subsystem decomposition documents to be added.

# Safety Goal attributes

The Safety Goals are defined in the HARA and provided with an ID. During the definition of the Functional Safety Concept the safety goal attributes are assigned to each Safety Goal.

Status:

* Fault detection &
* …failure mitigation
* Transition to the safe state
* Fault tolerance time which maintain the item in a safe state
* Driver warning in order to reduce the risk exposure time to an acceptable level
* Arbitration logic to select the most appropriate control request from multiple requests generated simultaneously by different functions (iso26262-3, clause 8)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ID +**  **Safety Goal** | **Attributes of Safety Goal** | | | | | |
| **Related hazard (from HARA)** | **Integrity + target lvl compliance** | **Safe State** | **FTT (ms)** | **Warning Concept** | **Degradation concept/ Emergency operation** |
| Safety goal from HARA |  | Automotive Safety Integrity Level (ASIL A-D) | Safe State | Fault Tolerance Time (FTT) Time span in which a system will not transition into a dangerous state despite a fault | The warning concept must be stated here. Example: *Fault detection and warning of the driver in order to keep the vehicle in a safe state* | The degradation concept must be stated here. Example: *Detection and neutralization of the fault through transition into a safe state* |
| SG1 Unintended locking while vehicle is in motion must be prevented |  | ASIL D, 50% | Electric steering column lock is disengaged | 100 ms | 1) Faults which in combination with another fault lead to a violation of the safety goal are communicated to the driver as a warning (yellow lamp). Degradation 1) is to be initiated.  2) Faults which without a detection and control measure would lead to a violation of the safety goal are communicated to the driver as an alarm (red lamp) telling them to immediately go to a garage. Degradation 2) is to be initiated. | 1) After a number of vehicle starts, which have to be defined, the ESCL function is deactivated.  2) Functionality will be deactivated within the fault tolerance time (FTT) |
| SG2 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Functional Safety Requirements and Allocation

The functional safety requirements need to be allocated to either the preliminary architectural elements of the item or an external measure. The functional safety requirements need to be traceable to their corresponding preliminary architectural implementation or external measure.

Please refer to the Item Definition for the top level architecture of which the preliminary architectural elements are derived.

SG1: Unintended locking while vehicle is in motion must be prevented

Safe State: Electric steering column lock is disengaged

|  |  |  |
| --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Integrity** |
| FSR1.1 | Vehicle speed v shall be detected | D |
| FSR1.2 |  |  |
| FSR1.3 |  |  |
| FSR1.x |  |  |

Evaluation of the request “Locking”

ASIL D

**Vehicle Speed (from other item)**

**ASIL D**

Steering column

ESCL-actuator

ASIL D

Detection Ignition key

QM

*Note: new function blocks are marked “****bold****”*

SG2: …

Safe State: …

|  |  |  |
| --- | --- | --- |
| **ID** | **Functional Safety Requirement** | **Integrity** |
| FSR2.1 | … | D |
| FSR2.2 |  |  |
| FSR2.3 |  |  |
| FSR2.x |  |  |

Function

ASIL x

**Function**

**ASIL x**

Function

Function

ASIL x

Function

QM

*Note: This is an example, new function blocks are marked “****bold****”*

# Appendix A – Review form for TSC template (Template only!!!)

**Change History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Revision** | **Date** | **Author** | **Chapter(s)** | **Reason** | **Description** |
| 0.01 | 04-07-2016 | R. vd Boom | All | Increase usability of these documents | Processing general feedback to all template documents |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Review Log**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Revision** | **Date** | **Reviewer** | **Chapter(s)** | **Result** | **Comments** |
| 1 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Notes to editor**