System Architecture Specification

Customer

Project

**Revision History**

| **Version** | **Date** | **Change Description / Reason** | **Author** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

1. Introduction 4

1.1 Scopes and Focus Levels 4

1.2 Definitions, Glossary 5

1.3 References 5

2. System context 6

2.1 Graphical Representation 6

2.2 Description 7

2.3 External Interfaces Description 7

3. General System Concepts 7

3.1 Common Scope 7

3.2 Environment Scope 8

3.3 Functionality Scope 10

4. Technical system architecture 11

4.1 Graphical representation 11

4.2 Description of single subsystems/modules 12

4.3 Internal Interfaces description 15

5. Technical Safety Concept 15

5.1 System Safety Integrity Measures (SSI) 15

5.2 TSC to achieve individual safety goals 17

5.3 Safety Integrity Summary 21

5.4 Further safety requirements 23

# Introduction

This System Design applies to project **<PROJECT name>** and is binding for all phases of the project. The document describes how the system is embedded on vehicle level, how the system is structured and how the various sub-systems communicate with each other. This document is based on MHE Form 8303 System Architecture Specification.

For each element it must be known which functions are allocated to. It must be ensured, that all requirements are considered consistently in the system architecture.

By use of diagrams the single system elements, physical interfaces and communication mechanisms are defined and described.

The interfaces of system elements to external devices and the interaction between them are listed and described.

An allocation of functional and non-functional requirements to HW or/and SW elements is made.

Additionally the following questions must be answered by system architecture design:

* Is it possible to combine elements into subsystems in a way, that subprojects can be initiated?

Can these subsystems be purchased or must they be developed?

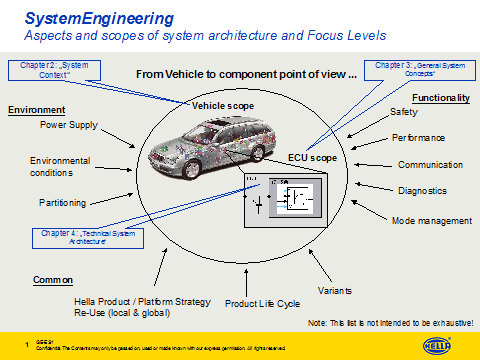
* Is it possible to use (sub) systems from former programs (“Reuse”)?
* Must subsystems be developed within MHE or could they be delegated to subcontractors?

## Scopes and Focus Levels

The structure of this document is based on the following principles:

* **Requirements** on the system architecture have to be described in the System Requirements Specification. This document is considered as a derived document, i.e. concepts and solutions are described. The mapping and allocation of these requirements to the system architecture has to be documented via Doors-Links to the corresponding chapter/objects in this document from traceability point of view.
* Different pre-defined **scopes** as a kind of "checklist" from System Engineering point of view have to be considered and to be answered. Of course further scopes are possible or even required due to the actual project.
* The focus **level** is changing from the highest vehicle level ("Black Box View") to the ECU and its sub-modules ("White Box View") along the document structure, i.e. a kind of "zooming in" is performed in this document.
* In principle these pre-defined scopes have to be considered on each level and therefore they are "repeated" in a similar way on each level.

These issues and their mapping to the document structure are visualized for better understanding in the sketch below.



## Definitions, Glossary

*Definitions of terms see document “Terms and Abbreviations in the Development of Product-related Software“.*

|  |  |
| --- | --- |
| tbd | to be defined |

## References

*Complete list of all documents referenced or concerned, including date (e.g. customer standards, specification of relevant system components etc.)*

**Table: List of referenced documents**

|  |  |  |  |
| --- | --- | --- | --- |
| **MKS version** | **Date** | **Status** | **Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# System context

## Graphical Representation

*Include a block diagram of the entire system which describes the interrelation on vehicle level.*

*The following diagram shows an example of such a block diagram.*



Include an exploded assembly view here. An example can be seen below

*The following list of hotspots (according to the numeration in the diagram) and examples should be used as a guideline for the aspects to be stated/described*

*in the diagram and/or the following textual chapters.*



*From which ECUs are messages received?*

*- Available in all variants?*

*- ECU supervision defined/required?*

*- Gateway included? (Gateway behaviour in case of lost TX-ECUs? Obsolete information indicated/available?)*

*- Own ECU affected in case of changes in other ECUs? (“Communication-Matrix”)*

**

*Which ECUs receive messages?*

*- Required in all variants?*

*- Required information available in all variants?*

*- Principal use of information (e.g. implicit timing/delay requirements, required robustness, plausible ECU requirements for requested vehicle function)?*

**

*External components environment?*

*- Sensors/Actuators only connected to own ECU?*

*- External power supply? (e.g. possible delays after power-up and/or before power-down?)*

*- Example: external sensor needs additional time for data storage after end of communication*

**

*Distributed HW line interfaces?*

*- Internal connection (e.g. switch, open-collector, …) of all (!) participants? (e.g. max./min. load, remaining voltage, different states)*

*- External power supply? (e.g. possible delays after power-up and/or before power-down?)*

**

*Power supply from battery?*

*- Different power supply lines available?*

*- If yes, dedicated purposes (e.g. load, electronic, quiescent current, …)?*

*- Supervision concept? (e.g. only partly line failure)*

*- Different battery connections? (e.g. probable voltage differences)*

**

*Power supply ground concept?*

*- Different ground connection lines available?*

*- If yes, dedicated purposes (e.g. load, electronic, quiescent current, …)?*

*- Different ground connection points? (e.g. probable ground voltage differences/offsets)*

## Description

*The diagram describes the technical interrelations of the whole system on vehicle level. Distinction has to be outlined between the system (e.g. control unit) and the external devices of the vehicle which interact with the own system in any way. The functions of the own system and functions of the external systems which interact with the own system must be described.*

## External Interfaces Description

*The interfaces between the MHE system and the vehicle (or other external systems) are to be described (e.g. data flow and directions of data flow on communication channels, meaning of data exchange, mechanical interfaces, environment influences). Only a rough description may be made here.*

*The details of the interface descriptions must be defined in “System interface specification”.*

### System Interfaces

### Test Interfaces

*Usually test interfaces are designed to support in the development phase. These interfaces should be described here separated from the "normal" system interfaces. (E.g. also test interfaces like CCP/XCP should be desribed here.)*

# General System Concepts

## Common Scope

### Product and Platform Strategy

*Aspects to be considered:*

* reusability *(e.g. reuse of concepts, standard modules from former projects)*
* *modularity*
* *expandability*
* *technologies*

 *OEM constraints (e.g. requirements from customer on the architecture, AUTOSAR, etc.)*

 *MHE constraints*

*Examples for descriptions:*

 *Required technology/standard*

 *Re-Use of components (e.g. from former series project)*

 *Integration of system (HW and/or SW and/or MD) modules from other suppliers*

* *Definition and justification on general concepts and design decisions (e.g. which microcontroller will be used)*

### Product Life Cycle

*Aspects to be considered:*

* *Development (development, system test)*
* *Production*
* *OEM production (pre- assembly; UB disconnect)*
* *Configuration*
* *Usage*
* *failing environment*
* *flashen (incl. Subsystems)*
* *spare parts (umbrella parts)*
* *Configuration; wrong signal environment*
* *recycling and disposal*

*Examples for descriptions:*

* Flashing of SW containing components (µC, Co-µC, DSP) via external bus interface.*

* Extended liftetime (e.g. component/technology availability)*

* Umbrella part for replacement*

#### Flash and Programming concept

*The concept should be described and visualized with a graphical representation to identify the affected modules.*

*(This representation can also be included in or reference to the System architecture diagram).*

*Details of the concept should be defined with use of sequence charts/flow diagrams/state diagrams.*

### Variants

*Aspects to be considered:*

 *Variants and equipment definition*

* *configurations*
* *system-family concepts*

*Examples for description:*

* *Design variants*
* *Assembly variants*

## Environment Scope

### Power Supply

*The following aspects**need to be considered:*

* Power line dimensions (incl. Fuses, cables) on vehicle level*

* Redundant power supply concept*

* Max. Current scenarios (one path, overall, SW current limited outputs)*

* Quiescent current*

*Examples for description:*

* Max. allowed supply current*

* Redundant power supply (monitoring, failure behaviour)*

* Dedicated power supplies (eg. KL 30N, load supply)*

### Environmental Conditions

*Aspects to be considered:*

* Power dissipation*

* Physical requirements*

* Optical requirements*

* Acoustic requirements*

* Magnetic requirements*

* EMC requirements*

*Examples for descriptions:*

* Power dissipation reduction*

* *Component level: concept (HW, SW, MD)*
* *Vehicle level: partitioning*
* *Asynchronous switching of loads*

* Camera and coloured windshield*

* No usage of relays due to acoustical effects (driver annoying)*

* *Operating temperature (full/reduced performance)*

### Partitioning

*Aspects to be considered:*

* system-partitioning*

* accessibility*

* Logistic concept*

* different production sites*

* transport*

* final assembly*

*Examples for descriptions:*

* mounting of sub-components (e.g. switches) in line-production*

* accessibility of external components (e.g. fuses)*

## Functionality Scope

### Safety

*Aspects to be considered:*

* distributed safety concept*

* component classification*

* redundancy concepts*

*Examples for descriptions:*

* ASIL classified functions*

* Fail-safe states of outputs in case of voltage drop*

* Valid stored data in case immediate voltage drop (data storage concept: internal power supply buffer, data storage architecture)*

* Selftest concept*

#### Reset Strategy and Watchdog concept

*The concept should be described and visualized with a graphical representation to identify the affected modules.*

*(This representation can also be included in or reference to the System architecture diagram).*

*Details of the concept should be defined with use of sequence charts/flow diagrams/state diagrams.*

### Performance

*Aspects to be considered:*

* Real-time requirements*

* Startup requirements (e.g. valid CAN bus messages after wake-up within a limited time)*

*Examples for descriptions:*

* Overall propagation delay for brake lights (e.g. 50ms)*

* Execution requirements for integrated SW task (e.g. 5 MIPS, 10ms cycle)*

* valid CAN bus messages after wake-up within a limited time*

### Communication

*Aspects to be considered:*

* communication interface types (serial, proprietary, …)*

* bus-load estimation*

*Examples for descriptions:*

* Infrastructure: low-speed CAN I/F, optional high-speed I/F.*

* Intra-ECU communication*

### Diagnostics

*Aspects to be considered:*

* Network diagnostics concept (e.g. Multiadress-Diagnostics , Subsystem-Diagnostics )*

* Self diagnostics concept (e.g. co-controller, asics, …)*

* Load diagnostics (robustness)*

*Examples for descriptions:*

* Diagnostics address allocation*

* Selftest*

### Dynamic Behaviour

Describe the behaviour that tackles more than one defined module. This can be done supported by models and/or UML diagramms. Time sequence diagramms are necessary for the most important functional flows.

#### Mode management

*Aspects to be considered:*

* vehicle state management (e.g., … -> Kl30, Kl30N, …)*

* Power-Up/Down procedures*

*Examples for descriptions:*

* run mode, sleep mode*

* production mode (test support)*

* transport mode*

##### Startup and Power-Down Concept

###### Startup Behaviour

*The concept should be described and visualized with a graphical representation to identify the affected modules.*

*(This representation can also be included in or reference to the System architecture diagram).*

*Details of the concept should be defined with use of sequence charts/flow diagrams/state diagrams.*

###### Power-Down Behaviour

*The concept should be described and visualized with a graphical representation to identify the affected modules.*

*(This representation can also be included in or reference to the System architecture diagram).*

*Details of the concept should be defined with use of sequence charts/flow diagrams/state diagrams.*

##### Quiescent Current concept

*The concept should be described and visualized with a graphical representation to identify the affected modules.*

*(This representation can also be included in or reference to the System architecture diagram).*

*Details of the concept should be defined with use of sequence charts/flow diagrams/state diagrams.*

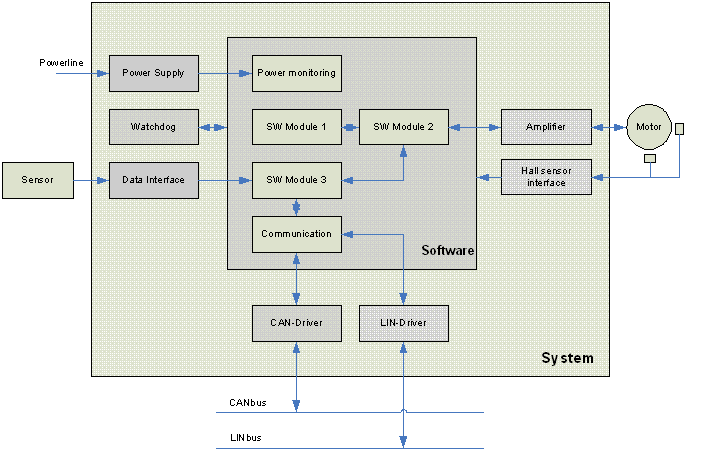
# Technical system architecture

## Graphical representation

*Insert a block diagram with the graphical representation of the technical architecture elements.*

*The block diagram must be described. Eventually insert a link to a Visio-diagram.*

### System architecture



### Hardware architecture

*Only a short description should be given here.*

*Usually insert a link to a Visio-diagram or the corresponding document as a reference for details.*

### Software architecture

*Only a short description should be given here.*

*Usually insert a link to a Visio-diagram or the corresponding document as a reference for details.*

## Description of single subsystems/modules

*The main requirements (described in "System Requirement Specification") have to be linked to the subsystems/modules where they are realized/implemented to ensure Traceability in a sensible granularity.*

### ECU

*Add a brief description of sub-system n. What are the main tasks of the sub-system?*

*As stated in the introduction in this subchapter in principle the scopes defined in chapter 3 are "repeated" here, i.e. which solutions are derived from the system concepts for the realized modules.*

*They should be used as a kind of checklist for the description of each module.*

#### Power supply

##### Description

###### Standard Scopes

Functionality

Example:

The power supply is responsible for transforming the power and voltage delivered from the power plug to the power and voltage needed by the rest of the system.

The following voltages are provided:

* +5,0V
* +12,0V
* ...

Re-Use

Variants

Safety

Diagnostics

Mode Management

###### Additional Scopes

*Examples:*

* *Performance*
* *Communication*
* *Environmental conditions*
* *Partitioning*
* *Product Life Cycle*
* *...*

##### Interfaces

Example:

A SPI interface connects the watchdog to the µC.

#### <Module n>

##### Description

###### Standard Scopes

Functionality

Module classification

Re-Use

Variants

Safety

Diagnostics

Mode Management

###### Additional Scopes

*Examples:*

* *Performance*
* *Communication*
* *Environmental conditions*
* *Partitioning*
* *Product Life Cycle*
* *...*

##### Interfaces

### <Subsystem n>

*Examples for Systems which consists of different Subsystems from MHE point of view:*

* *Keyless Entry System (ECU, Remote-Key, Antennas)*
* *Advanced Frontlighting System (ECU, Actuators, Sensors)*

*Add a brief description of sub-system n. What are the main tasks of the sub-system?*

*As stated in the introduction in this subchapter in principle the scopes defined in chapter 3 are "repeated" here, i.e. which solutions are derived from the system concepts for the realized modules.*

*They should be used as a kind of checklist for the description of each module.*

#### <Module n>

##### Description

###### Standard Scopes

Functionality

Re-Use

Variants

Safety

Diagnostics

Mode Management

###### Additional Scopes

*Examples:*

* *Performance*
* *Communication*
* *Environmental conditions*
* *Partitioning*
* *Product Life Cycle*
* *...*

##### Interfaces

* A SPI interface connects the watchdog to the µC.

## Internal Interfaces description

Internal system interfaces include also ECU to ECU interfaces if the system to build includes more than one ECU.

The interfaces between the different subsystems/modules are described on a high abstraction level in the corresponding chapters.

A detailed definition is done in additional documents:

* System Interfaces Module (Doors)
* Pure HW interfaces are described in detail in the “module interface specification of each module”. Insert a link to the HW module interface specifications.
* Hardware/Software interfaces are to be mentioned and defined in the “Hardware/Software interface specification”, which may be started here. But the details of the HW/SW interface can only be specified during module design. Insert a link to the HW/SW-Interface specification.

# Technical Safety Concept

## System Safety Integrity Measures (SSI)

*“system” denotes further on only the ordered subsystem.*

*SSI includes the "common (basic) functions like processor, RAM, ROM, watchdog etc.*

### System safety architecture block diagram

*Include block diagram showing the safety-goal-independent overview of the system to be delivered with ASIL allocated to each block.It should show the µC, RAM/ROM, the external watchdog, busses, relevant IO, power supply etc.*

*The block diagram should be explained.*

**Figure** Object ID**: Block diagram**

*< insert diagram here >*

### Safety Goal independent system modes

*To ensure that the specifications cover all relevant operating modes and system states, list them here, (possibly derived from the System requirement specification).*

**Table: List of operating modes**

|  |  |  |
| --- | --- | --- |
| Operating mode | Safety relevant | Comment |
|  |  |  |

**Table: List of system states**

|  |  |  |
| --- | --- | --- |
| System states | Safety relevant | Comment |
|  |  |  |

### SSI constraints and analysis

*The standard System Safety Integrity (SSI) measures should be generated, based on the typical measures collected in the FS database, by means of the FS-FMEA and other analysis methods referenced below.*

*The project specific SSI measures contain the measures for the safety goal (SG) independent HW.*

Reset Strategy and Watchdog concept *should be described and visualized with a graphical representation to identify the affected modules (see items No 2 and 5 of table below).*

*(This representation can also be included in or reference to the System architecture diagram).*

*Details of the concept should be defined with use of sequence charts/flow diagrams/state diagrams.*

**Table: SSI items to be analysed to define suitable measures**

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Keyword | Keyword explanation | Project comment |
| 1. | *SSI measures* | *The standard SSI measures are generated out of the FS register (DOORS:DB1/MHE-GE/Central/HW-FS/FuSi SA SW/ SSI Measures for ASIL A and ASIL B).*  *The constraints (µC with ECC, MPU, …) are described as “descriptions” in the requirement engineering system (e.g. DOORS).* |  |
| 2. | *external watchdog* | *If there are more than 1\* µC the µC can include the watchdog function for another µC.* |  |
| 3. | *power supply* | *Provide a list of all required voltages together with the impact of under and over-voltage and their control.* |  |
| 4. | *reference voltage* | *A candidate for dependent faults.* |  |
| 5. | *reset* | *Consider the reset behavior of the µC and IO drivers to check, if hazardous states of the IO signals could occur* |  |
| 6. | *safestate powered* | *Special attention is required if the safestate is powered.*  *e.g. emergency light* |  |
| 7. |  |  |  |

*The ISO26262 does not mandate particular measures, but specifies fault assumptions, which shall be controlled by appropriate measures. Use of standard measures helps to ease the analysis.*

*MHE provides defined standard measures, which are often suitable and do not require detailed analysis. If one of these standard measures is not easy to implement by the project, a project specific analysis can be done.*

#### SSI Measures against random HW failures (FS-FMEA)

*For a checklist which parts could be relevant to analyse and demonstrate, see ISO26262-5, table D.1:*

*Import and refine results from FS-FMEA in this section.*

*Note: SG specific measures are specified in sections "*TSC to achieve individual safety goals".

#### Dependent fault analysis

*The analysis of dependent failures aims to identify the single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal.*

*Dependent fault analysis is always required.*

*The “Dependent\_Fault\_Analysis\_template.xls” lists the requirements for system, HW and SW.*

#### Generic SSI Requiremenets

Insert Generic SSI Requirements from DOORS Database:

Module name: "**SSI Measures for ASIL A and ASIL B**"

Link to the module: doors://MHEDOORS1.dc.MHE.com:36681/?version=2&prodID=0&view=00000002&urn=urn:telelogic::1-3d50b3905e72333b-M-0004ba42

**-> space for resulting DOORS requirements**

## TSC to achieve individual safety goals

### Measures for SG\_01 <name of Safety Goal>

*The architecture to safety goal should be built out of one or more safety goals which could be handled together without confusing case differentiations.*

***note:*  template (for "Measures for SG\_01 <name of Safety Goal>") repeated n-times (for each SG)**

*e.g. different SG for flasher / turn indication should be grouped together.*

*e.g. if the light functions (without flasher) should be handled together will be project dependent*

*The block diagram should demonstrate the architecture to a top safety goal / hazard*

#### Introduction, Basic Conditions

*Copy or short description of the TSC relevant parts of the item definition*

*If the TSC for this SG is based on assumptions which are not part of the FSC requirements they shall be listed here and adressed to the customer.*

*FSC requirements shall be referenced here additionally*

* *if they are important for the chosen concept or*
* *if they are important for reuse of the TSC of the SG*

**-> space for resulting DOORS requirements concerning "Basic Conditions"**

#### Block diagram with ASIL allocation

*A block diagram of the safety goal with ASIL allocation is input and updated a result of the safety architecture workshop.*

*The structure of the FMEA should mirror the block diagramm. For details see FS-Guideline FSI-07.*

**Figure** Object ID**: Technical safety concept block diagram**

*Description of the block diagram and the ASIL allocation.*

*Rationale for allocation. Strategy for the ASIL allocation or decomposition, if not evident by first view*

*Documentation of the architectural decisions done in the architectural process.*

#### Safety concept for implementation

*Description of the implementation concept --* overall explanation of the safety concept for this SG, based on the block diagram

*If the implementation concept is not evident, the rationale shall be given that the assumable fault assumptions will be detected in the required time.*

*If different safety concepts have been discussed, the arguments 'pro' and 'contra' shall be documented here.*

#### Refinement into Safety Functions

*If the implementation of the SG requires a lot of requirements it is necessary to structure the requirements in a way that an overview is given and a review to completeness and other goals is possible.*

*A hierarchical structure is desirable because it increase reuse.*

*The transformation from the SG down to the requirements (HW, SW, …) shall be done stepwise by so-called Safety Functions (SF\_xx) .*

*Reasons:*

 *hierarchy ease and demonstrate traceability*

 *reuse of abstract levels for different implementations*

 *reuse of SF for different safety goals*

 *level for interface to disciplines (HW / SW)*

 *help to break down the safety goals to the implemented requirements.*

*The Safety Functions should*

 *represent blocks of the block diagram*

 *mirror (or preset) the FMEA function structure.*

*Note: In the FS-FMEA the right side of level 2 should match the safety functions.*

***Each SF\_xx typically corresponds to one block of the block diagram.***

*Example (for a light function low beam):*

 *SF\_01: read inputs (light switch, KL15, …)*

 *SF\_02: read bus input (read, check CRC, alive counter, monitor if signal is valid, …)*

 *SF\_03: input plausibility checks (e.g. if the light inputs are coded 1oo4 (one out of 4))*

 *SF\_04: logic*

 *SF\_05: write outputs (switch light ON, …)*

 *SF\_06: read-back outputs (read HW back,...)*

 *SF\_07: verify outputs (compare to set value, check short cut, check open load)*

 *SF\_08: goto safestate (inform driver, set emergency light)*

##### SF\_01: Safety Function <...>

*Description of SF\_01*

##### SF\_xx: Safety Function <...>

*Description of SF\_xx*  **(template repeated xx-times (for each SF))**

#### Safety analysis

##### Hazardous events (input for the analysis)

*The list of hazardous events due to the chosen architecture (do not confuse with the H&R hazards on the higher level of vehicle functions!) shall include the events which can cause the hazard as single-point or especially as multiple-point fault e.g. implemented as decomposition. It is important that especially for ASIL C and D the multiple-point faults are listed and tested. The list of hazardous events shall be a base for requirements and test of the measures.*

**Table: List of hazardous events**

|  |  |  |
| --- | --- | --- |
| System states | Safety relevant effect | Comment |
|  |  |  |

*Example ESCL:*

*The ASIL D hazard is “ESCL locks during drive”*

*Implementation dependent hazardous events are e.g.:*

 *KL30 power for ESCL during drive*

 *KL31-lock connection for ESCL during drive*

 *Lock command to ESCL during drive*

##### Measures against random HW failures (FS-FMEA)

*If it is not obvious, the rationale shall be given here, that in the FS-FMEA all assumable faults are analysed.*

*The measures of the FS-FMEA shall be analysed, (refined in more detail and split, if necessary) phrased as requirements and assigned to the domains or other subsystems (e.g. customer).*

**-> space for resulting DOORS requirements**

##### Measures to deal with systematic faults

*Consider aspects like timing, program flow monitoring (PFM), potential resource conflicts, coverage of all possible operating modes, ...*

**-> space for resulting DOORS requirements**

##### Dependent fault analysis

The analysis of dependent failures aims to identify the single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal.

The dependent fault analysis includes the common cause analysis and the cascading fault analysis.

*Dependent fault analysis is always required.*

*The “Dependent\_Fault\_Analysis\_template.xls” lists the requirements for system, HW and SW*

**-> space for resulting DOORS requirements**

##### Safety analysis by FTA

***FTA requirement:***

 *required for ASIL C - D;*

 *required if the OR view of the FMEA is not sufficient*

 *if decomposition is used*

*Note-1: A qualitative FTA shall be reviewable for completeness of the handled part.*

*Note-2: A quantitative FTA shall demonstrate diagnosis with the diagnostic coverage, which requires the &-gate for the detected faults and no &-gate for the resumed (not detected) faults.*

**-> space for resulting DOORS requirements**

## Safety Integrity Summary

### Safety I/O safestate summary

For the digital, analog and bus I/O the safestate shall be defined.

-> *Insert the following table (and/or a specific requirements template).*

**Table: I/O safestate**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| signal **typ** | **signal name** | **safestate** | **related SG / SFxx**  points out if I/O are used for different SG, SFxx, which shall be analysed for potential common cause faults or different safestates | **comment**  Safestate shall be guaranteed for all assumable faults e.g. open.  Arguments shall be provided if a safestate is not safety relevant e.g. because the fault will be detected by plausibility |
| DI | dgital inputs | low or high |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| AI | analog inputs |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| bus inputs |  |  |  | safestate shall be used during   initialization, reset   input signal time out |
|  |  |  |  |  |
|  |  |  |  |  |
| DO |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| AO |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| bus outputs |  |  |  | safestate shall be sent as long as no valid output signal exists |
|  |  |  |  |  |
|  |  |  |  |  |

**-> space for resulting DOORS requirements**

### Safety functions cross reference

*The safety functions of the several safety goals shall be sampled here for work out reuse and define the required ASIL of the SF\_xx.*

*(***important for re-use and for ASIL allocation check***)*

**Table: Safety function cross reference**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | SF\_01 | SF\_02 | SF\_03 | SF\_04 | SF\_05 | SF\_06 | SF\_07 | SF\_08 |  |
| SG01 |  |  |  |  |  |  |  |  |  |
| SG02 |  |  |  |  |  |  |  |  |  |
| SG03 |  |  |  |  |  |  |  |  |  |
| max. ASIL |  |  |  |  |  |  |  |  |  |
| resulting ASIL (1) |  |  |  |  |  |  |  |  |  |

(1) If decomposition is used, ASIL of this part of the decomposition

#### SF\_01\_Requirements

**-> space for resulting DOORS requirements**

#### SF\_XX\_Requirements

**-> space for resulting DOORS requirements**

### Safety diagnosis summary

*This table should contain all diagnosis (part of SafetyFunctions SFxx) from SSI and of the SGs. (***important for overview by SIM, reviewer and discussion with customer***)*

*This table contains the summary of the diagnosis worked out in TSC – used for proof of appropriate and sufficient diagnoses.*

**Table: List of safety diagnosis**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Diag\_ID | Diag\_Name | Description | Execution (per cycle, per ignition cycle) | Reaction | Demature, Rehabilitation |
| *D01* | *ROM Test* | *CRC area, adress, signature,* | *once per ignition cycle* | *DTC, Reset, Safe state after 3 resets during ignition cycle* | *with next ignition cycle* |
| *D02* | *Brakelight monitoring* | *Output of Brakelight application has to be checked* | *cyclicly, 100ms* | *DTC, Reset, safestate acc to xxx* | *with next ignition cycle* |
| *D03* | *High side driver T1* | *The right On/Off status of Highside driver (T1) must be monitored:* | *cyclicly,*  *1sec* | *DTC, Reset, safestate acc to xxx* | *with next ignition cycle* |
|  |  |  |  |  |  |

## Further safety requirements

**-> space for resulting DOORS requirements**