System Architecture Design

**Change History**

| **Version** | **Date** | **Change Description / Reason** | **Author** |
| --- | --- | --- | --- |
| 1.0 | 2017-12-08 | Initial version | Hae-Min, Woo |
|  |  |  |  |
|  |  |  |  |

**Table of Contents**

[1. Purpose Description 4](#_Toc500323752)

[1.1 Purpose 4](#_Toc500323753)

[1.2 Main Description 4](#_Toc500323754)

[1.3 Result of Process 4](#_Toc500323755)

[2. Major Roles Acting in this Process 4](#_Toc500323756)

[3. Process 5](#_Toc500323757)

[3.1 Process Input – Output Definition 5](#_Toc500323758)

[3.2 Introducing Aspects 5](#_Toc500323759)

[3.3 Process Flow Chart 6](#_Toc500323760)

[3.3.1 Task 1: Establish Communication 7](#_Toc500323761)

[3.3.2 Task 2: Evaluate & describe system architecture 7](#_Toc500323762)

[3.3.3 Task 3: Develop a technical safety concept and necessary technical safety requirements 8](#_Toc500323763)

[3.3.4 Task 4: Specify system interfaces in detail 11](#_Toc500323764)

[3.3.5 Task 5: Ensure traceability 12](#_Toc500323765)

[3.3.6 Decision 1: Architecture consistent? 12](#_Toc500323766)

[3.3.7 Task 6: Develop verification criteria 12](#_Toc500323767)

[3.3.8 Task 7: Verify System architecture 12](#_Toc500323768)

[3.3.9 Task 8: Verify technical safety concept 13](#_Toc500323769)

[3.3.10 Decision 2: Architecture and technical safety concept accepted? 13](#_Toc500323770)

[4. Changes, References, Appendix, Terms 14](#_Toc500323771)

[4.1 References 14](#_Toc500323772)

[4.2 Template 14](#_Toc500323773)

# Purpose Description

## Purpose

The purpose of the system architecture design is to define the structure of the system to build, its interfaces, the overall behavior of the system and the allocation of requirements onto system elements in order to break down the development work into domains and structural elements.

## Main Description

The system architect defines the system structure that fulfills the requirements of the system requirements specification.

## Result of Process

The results of this process are

* The system structure
* All system requirements are allocated to elements of the architecture (as far as this is possible)
* All external and internal interfaces of every architecture element are defined
* All interfaces between the structure elements are defined
* The system architecture specification and the system interface specification are reviewed
* The technical safety concept is defined and reviewed (for safety classified devices)
* Consistency of the system architecture to all system requirements and the technical safety concept is verified

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 Sub-Suppliers?
* How are safety demands fulfilled?

# Major Roles Acting in this Process

|  |  |
| --- | --- |
| **Role** | **Contribution and Responsibilities** |
| System Architect | Defines the System architecture and allocates all requirements resulting from the system requirements specification to HW and SW elements of the architecture |
| System Analyst | Checks if System architecture is consistent to system requirements |
| Safety Manager | Creation of the technical safety concept |

# Process

## Process Input – Output Definition

The following process input is required:

|  |  |
| --- | --- |
| **Process input** | **From supplier** |
| System requirements specification (initial) | System Analyst |
| System interface specification (initial) | System Analyst |
| Functional safety concept | Customer / Safety Manager |
| Feasibility study | Project manager |
| Release plan | Project manager |

|  |  |
| --- | --- |
| **Process output** | **To customer** |
| System structure specification | Project Team |
| Technical safety concept | Project Team |
| System interface specification (detailed) | Project Team |
| System requirements specification (updated) | Project Team |

## Introducing Aspects

None

## Process Flow Chart



### Task 1: Establish Communication

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | Project Plan | | | | | |
| Output | | Project Plan (refined) | | | | | |
| D: |  | E: | Project Manager | S: |  | I: | All Major Roles |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

The Project Manager establishes all communication channels to supply the engineers involved in this process step with the needed information (documents, models, protocols, e.g.). The Project Manager ensures that changes of information are communicated to the according engineers.

The Project manager makes the system architecture available to all people involved (i.e. all sub-project architects and analysts, Quality Assurance, Test Laboratory etc.). In the case of changes to the system design, all people involved are notified.

Also it must be ensured that already existing information from the domains HW and SW is submitted to the system architect.

### Task 2: Evaluate & describe system architecture

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | Release Plan  Feasibility Study  System Requirements Specification  System Interface Specification | | | | | |
| Output | | System Architecture Specification | | | | | |
| D: |  | E: | System Architect | S: | Safety Manager | I: |  |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

The system architecture is specified based on analysis of the requirements defined within the system requirements specification. By decomposing the whole system into its building blocks, the essential elements of the system and their interfaces are identified. The aims of simplicity and modularity are to be regarded. Measures for detection and control or mitigation of random hardware failures are to be specified. A guideline for this topic is available under this link.

Dynamic behavior depending or having impact on more than one block is to be specified (e.g. system states, start up behavior).

(Please note, that, external interfaces, already defined in the system interface specification are distinguished from internal interfaces which will subsequently be defined)

Each block realizing requirements must inherit the highest safety level of all requirements this block covers. If a block consists of several sub-blocks, all sub-blocks inherit the safety level of the master block. It is only possible to combine (sub-)blocks with different safety levels if evidence is made available that this combination cannot violate, directly or indirectly, any safety requirement allocated to the element, i.e. it cannot interfere with any safety-related sub-element of the element. Safety requirements of a certain ASIL level can be satisfied by several independent components of a lower safety class. For details of this ASIL decomposition please contact the project’s safety manager. In case an ASIL B2,C or D device is under development targets for single-point fault metric values, latent-point fault metric values and random hardware failures that are acceptable must be defined.

Every single block is to be annotated with its block class using the basic scheme:

* Class Low (e.g. simple block or no errors to be expected)
* Class Medium (e.g. block with average complexity)
* Class High (e.g. block with high complexity)

All non-functional system requirements (e.g. performance requirements, safety requirements, rules and regulations) must be analyzed and it must be documented if and how they impact any architectural design decisions.

The architecture must be suitable for each sample. E.g. it may be possible that the system requirements for different releases require different system architectures).

The results of feasibility studies and safety analyses must be considered. This means that causes of systematic and random failures are to be eliminated or their effects are to be mitigated.

Model-based methods may be used to assist traditional System architecture design techniques in defining, describing and detailing various functionalities of sub-system elements.

The system architecture specification must textually and/or graphically identify all elements and interfaces of the system architecture.

Consider re-use of existing components, concepts and/or methods. If an ASIL D device is under development it is to be justified if well trusted design principles are not re-used.

### Task 3: Develop a technical safety concept and necessary technical safety requirements

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | FS-FMEA  Functional Safety Concept  System Architecture Specification  System Requirements Specification  System Interface Specification | | | | | |
| Output | | Technical Safety Concept | | | | | |
| D: |  | E: | Safety Manager | S: | System Architect  HW Architect  SW Architect | I: |  |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

The technical safety concept (TSC) specifies how the safety goals will be met and how the safety integrity of the system will be ensured. By analyzing the relevant failure modes of the system architecture elements, the necessary safety mechanisms are determined to detect the occurrence of faults potentially affecting a safety goal, to prevent faults from being latent, to provide fault tolerance against undetected faults and to react safely upon detected faults.

The MHE default safety analyses for all ASILs are the FS-FMEA and the dependent fault analysis considering common cause / cascading faults. Additional deductive3 (e.g. FTA) and inductive (e.g. FMEA) analyses have to be performed as required (project-specific selection see Safety Plan/SafetyCase\_TaskPlan, depending on ASIL and customer requirements).

Errors that may lead to multiple-point failures are to be detected. Fault detection intervals for such failures are to be specified for each safety mechanism implemented for ASIL C and D devices. This is recommended for ASIL A and B devices also. Parameters to be considered for the definition of the fault detection interval are:

* The reliability of the hardware component with consideration given to its role in the architecture,
* The probability of exposure of the corresponding hazardous event(s),
* The specified quantitative target values for the maximum probability of violation of each safety
* Goal due to hardware random
* The assigned ASIL of the related safety goal.

Safety mechanisms the prevent multiple-point faults are also to be developed in compliance with the ASIL. If the multiple-point failure is assigned as ASIL D, the safety mechanism to prevent such a failure has to comply with ASIL B. If the multiple-point failure is assigned as ASIL B or C, the safety mechanism to prevent such a failure has to comply with ASIL A.

Due to the analysis results, modifications to the system architecture might be necessary (iteration loop with task 2) which could best be performed in a "safety architecture workshop".

For each safety mechanism that enables an item to achieve or maintain a safe state the following aspects must be specified:

1. The transition to the safe state,
2. The fault tolerant time interval;
3. The emergency operation interval, if the safe state cannot be reached immediately; and the measures to maintain the safe state.

The Technical safety requirements shall specify the response of the system to stimuli that affect the achievement of safety goals. This includes failures and relevant combinations of stimuli in combination with each relevant operation mode and defined system states.

The specification of the technical safety requirements shall be derived from the functional safety concept taking into account the preliminary architectural design of the item. The ASIL of the technical safety requirements based on the ASIL of the corresponding functional safety requirements is to be assigned to technical safety requirement.

Besides the technical safety requirements, the following design decisions and system properties shall be defined:

* Interfaces, such as communication and user interfaces, if applicable
* Restrictions concerning environmental conditions

The technical safety requirements shall be traceable and consistent with the functional safety concept and the preliminary architectural design.

The technical safety concept shall specify all safety related or other relevant dependencies between system elements.

The technical safety concept shall at least describe requirements on safety measures, which include at least the following:

* Measures related to the detection, indication and control of faults in the system itself (self-monitoring of the system)
* Measures related to the detection, indication and control of faults in the peripheral devices as other electronic control units, sensors, actuators and communication systems
* Measures that enable the system to achieve or maintain a safe state
* Specification of the measures to detail and implement the warning and degradation concept
* Specification of the measures which prevent faults from being latent
* Measures related to tests of the above mentioned functions during power up (predrive checks), operation, power down (postdrive checks) and in maintenance
* Measures for detection and control of corruption of safety-related data

Each measure listed above shall have an ASIL as attribute.

Acceptance criteria for the system safety verification of the technical safety requirements and validation criteria for safety of the item shall be specified.

All additional hazards identified during product development at system level shall be appended to the hazard and risk analysis (see MHE-PE-21).

**Target Values for HW architectural metrics**

Target values for HW failure metrics shall be defined within the context of the Technical safety concept (Normally, target values are defined at vehicle level and are given as part of the customer requirements specification). These target values need to be taken over and/or refined during evaluation of the TSC. They are then part of the technical safety requirements within the System architecture specification.

The definition of target values shall be done according to the following restrictions:

**Single-point fault metric**

For each safety goal, a quantitative target value for the "single-point fault metric" shall be based on one of the following sources of reference target values:

* derived from the HW architectural metrics calculation applied on similar well-trusted design principles, or from the following table:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ASIL** | | |
| **B** | **C** | **D** |
| **Single-point fault metric** | ≥ 90 % | ≥ 97 % | ≥ 99 % |

**Latent-fault metric**

For each safety goal, a quantitative target value for the "latent-fault metric" shall be based on one of the following sources of reference target values:

* derived from the HW architectural metrics calculation applied on similar well-trusted design principles, or from the following table:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ASIL** | | |
| **B** | **C** | **D** |
| **Latent fault metric** | ≥ 60 % | ≥ 80 % | ≥ 90 % |

**Random hardware failure target value**

Quantitative target values for the maximum probability of the violation of each safety goal due to random hardware failures shall be defined using one of the following sources:

* derived from field data from similar well-trusted design principles, or
* derived from quantitative analysis techniques applied to similar well-trusted design principles using failure rates in accordance with failure rate definitions for HW architectural metrics, or
* Derived from the following table:

|  |  |
| --- | --- |
| ASIL | **Random hardware failure target values** |
| D | < 10-8 h-1 |
| C | < 10-7 h-1 |
| B | < 10-7 h-1 |
| NOTE These quantitative target values described in this table can be tailored to fit specific uses of the item (for instance if the item is able to violate the safety goal for durations longer than the typical use of a passenger car). | |

The above mentioned target values are values that must be fulfilled on vehicle level for each safety relevant function/safety goal.

Depending on the scope of the MHE order, the target values to be fulfilled must normally be given by the vehicle manufacturer as part of the Customer requirements specification or the Development Interface agreement, since the overall target values given in the table above are subdivided and allocated to the different parts of the overall vehicle level architecture (item).

Since MHE normally does NOT deliver a complete (vehicle-level) system, the target values for MHE will normally be lower than those in the table above.

This process step can be omitted if the system under development has no ASIL classification.

### Task 4: Specify system interfaces in detail

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | System Architecture Specification  System Interface Specification | | | | | |
| Output | | System Interface Specification | | | | | |
| D: |  | E: | System Architect | S: | HW Architect  SW Architect | I: |  |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

The external and internal interfaces of the system are listed and described in detail. MHE Form 8382 is to be used to specify the system interfaces (including the HW/SW interfaces).

In case on board flashing is required the system architect must also ensure that the corresponding template (F-8529) including the necessary information for the production facility is filled out.

Usually the first step of defining the system interfaces is performed by the HW developer (see also MHE-PE-07). Then the SW developer introduces his information and finally a workshop is performed in order to complete missing information.

### Task 5: Ensure traceability

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | System Requirements Specification  System Architecture Specification | | | | | |
| Output | | Traceability record | | | | | |
| D: |  | E: | System Architect | S: |  | I: |  |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

All system requirements must be assigned to individual elements of the entire architecture. This also applies to technical safety requirements. At least one assignment to the hardware and software must be apparent.

It must be obvious what system element satisfies which requirement. This should be accomplished by establishing bilateral traceability between the system requirements and architectural elements that satisfy these requirements (also known as the allocation of requirements to architectural elements).

### Decision 1: Architecture consistent?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | |  | | | | | |
| Output | |  | | | | | |
| D: | Safety Manager | E: |  | S: | System Architect | I: |  |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

It must be decided, whether the consistency of the system architecture to the technical safety concept is sufficient.

### Task 6: Develop verification criteria

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | System Architecture Specification | | | | | |
| Output | | System Architecture Specification | | | | | |
| D: |  | E: | System Architect | S: | System Analyst | I: |  |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

A description of what must be tested to guarantee the correct fulfillment of a requirement and/or model element by the architecture must be defined and documented. A trace to the requirement and/or model element must be given.

### Task 7: Verify System architecture

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | System Architecture Specification  System Interface Specification | | | | | |
| Output | | Review Checklist System Architecture Specification  Review Checklist System Interface Specification | | | | | |
| D: |  | E: | System Architect | S: | System Analyst  HW Architect  SW Architect  Safety Manager  System Integration Tester | I: | SW Quality Planner  HW Quality Planner |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

The System architecture must be reviewed. Review criteria should be i.e.: completeness, reusability, modularity, expandability, etc. Main focus of the review is if the demanded and required output of the process step is reached.

The review includes the check of the system interface specification.

The customer must be involved in the review, if he has prescribed that specific architectural elements be included.

It is recommended to perform a real time analysis of the system architecture in order to verify the timing behavior and the usage of the available resources (see guideline for real-time simulation in confluence).

### Task 8: Verify technical safety concept

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | | Technical Safety Concept | | | | | |
| Output | | Review Checklist Technical Safety Concept | | | | | |
| D: |  | E: | Safety Manager | S: | System architect | I: | Project Manager |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

It shall be shown that the technical safety concept is consistent with the functional safety concept and the architectural design. This is to be achieved by a review meeting, a simulation (recommended for ASIL A and B and mandatory for ASIL C and D), by use of system prototyping and vehicle tests (recommended for ASIL A and B and mandatory for ASIL C and D).

It shall be checked whether the system design introduces new possible hazards. In case new hazards are identified the hazard and risk analysis must be updated concerning these new hazards.

The correctness of the FS-FMES must be verified using the corresponding review checklist (F-8788).

Additionally a release of the technical safety concept by the customer may be conducted (to be decided by the project).

This process step can be omitted if the system under development has no ASIL classification.

### Decision 2: Architecture and technical safety concept accepted?

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Input | |  | | | | | |
| Output | |  | | | | | |
| D: | Project Manager | E: | System Architect | S: | Safety Manager | I: | Project Manager |
| D = Decision | | E = Execution | | S = Support | | I = Information | |

It must be decided based upon the outcome of the System architecture (including the system interface specification) and the technical safety concept, if the current proposal is sufficient or if a modification or redesign of the System architecture is necessary. It may be useful in this phase to create alternate System architecture proposals and assess them using the same review criteria as used in Task 7: .

# Changes, References, Appendix, Terms

## References

|  |  |  |
| --- | --- | --- |
| **Category** | **Document Name** | **Document Number** |
| Process | System architecture design | AD-PE1-1-02 |

## Template

|  |  |  |
| --- | --- | --- |
| **Category** | **Document Name** | **Document Number** |
| Template | System architecture specification | 8303 |
| Template | Review-Checklist System architecture specification | 8332 |
| Template | System interface specification | 8382 |
| Template | Review-Checklist system interfaces | 8333 |
| Template | Technical safety concept | 8487 |
| Template | Review Checklist Technical safety concept | 8488 |
| Template | HW/SW Interface Specification for standard μCs | 8618 |
| Template | On board programming | 8529 |