# Requirement Driven Safety Verification

Ranga Kadambi, Vladimir Litovtchenko, Jens Rosenbusch, Antonio Vilela
Infineon Technologies AG,
Am Campeon 1-12,
85579 Neubiberg, Germany

***Abstract*-Evaluation of hardware architecture against the requirements of fault handling as represented by the hardware architectural metrics is one key objective for safety verification. We propose a requirement driven design and verification flow which takes into consideration the special needs of ISO26262 compliant verification.**

**Keywords -- ISO26262; safety verification, SysML, requirements driven development**

## I. INTRODUCTION

Standard ISO26262 [1] was introduced in 2011 to address one of the key area of the road vehicles with the maximum gross mass up to 3500 kg: functional safety in modern automotive systems (car manufacturers and their suppliers including chip providers). Starting from hazards analysis standard covers whole lifetime of products used in automotive electric/electronic systems and therefore also addresses all development steps. It is required to show compliance to safety requirements with 130 work products for concept, development (system, hardware, software) phases according to a V-model, production and operation until decommissioning, and supporting processes like defining responsibilities, configuration and change management, or documentation.

ISO26262 widely utilizes safety requirements at all abstraction level for all its work packages. From other side, functional /nominal requirements are also driving product development and therefore well fit processes defined by the ISO26262 standard. This can be applied to all aspects of product development from car level down to the smallest hardware parts and software units.

In our paper we introduce and explain the usage of a requirement driven development flow used by Infineon. This flow covers hardware as well as software development. The scope of this paper is to show the flow used for hardware side and especially concentrating on aspects related to verification and validation of microcontroller products for functional safety. The paper also shows analysis and development flow used for Aurix™ MCUs starting from SysML-based high-level abstraction models down to verification and validation flow.

## II. SCOPE OF THIS PAPER IN TERMS OF ISO26262

Standard ISO26262 defines the term “functional safety” as: Absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems.
This paper has intention to show how Infineon Technologies AG analyses, designs and verifies functional safety within AURIX™ product family.
AURIX™ products are microcontroller units which belong as hardware parts to ISO26262 Chapter 5 Product development at the hardware level.
OEM define System Requirements and TIER1 define System Architecture for their products, but AURIX™ microcontroller products are used in several different systems and we partly use also ISO26262 Chapter 4 Product development at the system level to formulate Application Assumptions (AA) and Technical Safety Requirements (TSR).
Additionally to hardware parts also software is developed together with AURIX™ products, this software is not further in the scope of this paper than to formulate Assumptions of Use (AoU) which have to be fulfilled.

Functional safety for hardware parts means to follow technical safety concept (specification of the technical safety requirements and their allocation to system elements for implementation by the system design).

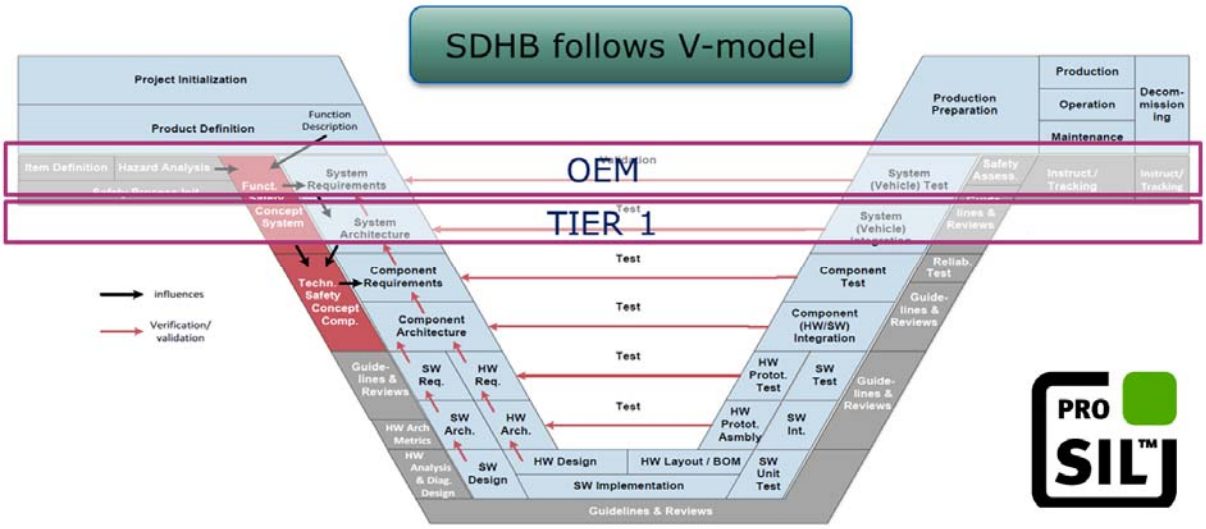


**Figure 1: V model of development flow**

Figure above shows the V-model according SDHB (system development hand book) which is a guideline for our development flow. Each abstraction level in concept and design phase has a corresponding verification level to prove fulfillment of given requirements.

This paper explains in chapter III how requirements are derived at several abstraction levels. Number or requirements in complex microcontroller products can easily reach several hundred. So an automated flow to handle requirements and the relationships between them is a key to efficient work and reaching reasonable time to market. Automated requirement handling also includes interface to and feedback from verification which is the topic in chapter IV.
A practical example shows how model driven system engineering builds a framework to connect different abstraction levels for requirements and their verification in chapter V. Goal is to support the argumentation about completeness of requirements and collect evidences for the correctness of implementation as well as to easy for verification to determine correct condition and scenarios for test environment.
Example in chapter V shows how Functional Safety Concept defines safety requirements for the microcontroller which are based on ISO26262 and the application needs. SysML representation of hardware failure modes are extracted from System Architecture. Technical Safety Requirements are result of safety analysis in SysML and safety mechanisms are selected to cover hardware failure modes. Verification can now use the same framework to define scenarios for test.

## III. Requirement Driven Development and Verification

- ISO26262 Requirement Flow

ISO26262 development flow is based on requirements. The standard considers work packages to be generated during product development at two levels: system and hardware development levels. These two levels are based on requirements: System Development level needs Technical Safety Requirements (TSRs) and Hardware Development level is based on Hardware Safety Requirements (HSRs). The TSRs and HSRs are needed not only for product development but also for safety verification and validation steps at the related levels. Both types of requirements are also a crucial part necessary for the Functional Safety assessment of the product. But first of all those requirements are the key for all further steps of development: TSRs are required for the System-level and the HSRs for the Hardware-level Development and Verification.

- Requirement Driven Development Flow (RDDF) and ISO26262

RDDF is not developed only to be conformant with standards like ISO26262 “Road vehicles – Functional safety” and IEC61508 “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems”. The RDDF allow very systematic and discipline approach to systems development and related activities at all levels:

- Customer requirements collection and documentation
- System definition and documentation
- Planning of activities at all levels
- Compliance with standards like ISO26262
- Verification and validation at all levels including reviews
- Evidence collection
- Traceability at all levels

The approach used by Infineon to address RDDF flow is shown on the figure below.

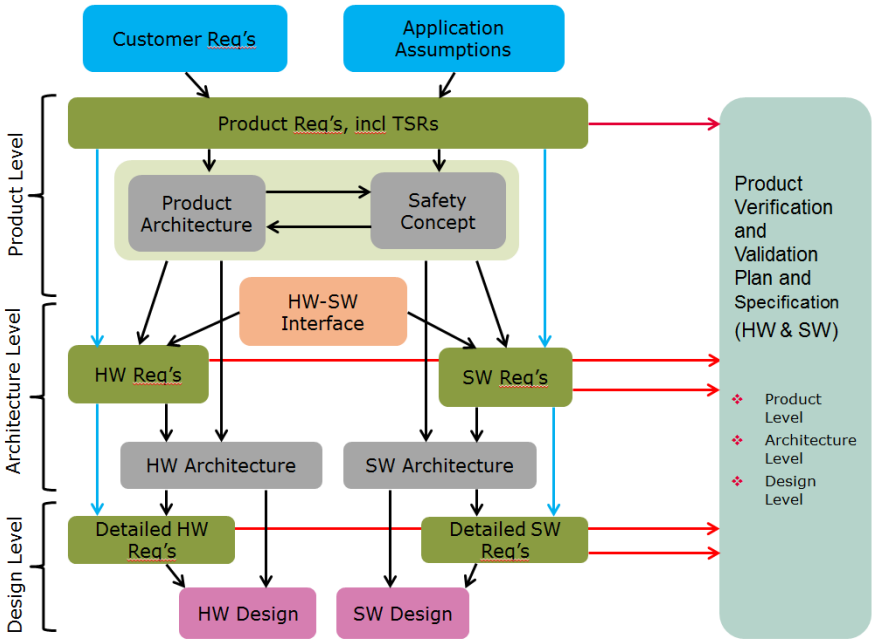


**Figure 2: Requirement Driven Development Flow**

Product Requirements are extracted from the Customer Requirements and also from Application Assumptions and created a base for the Product Architecture (PA) definition. The PA is used for the safety analyses required to create a Safety Concept (SC) for a product. SC also has influence on the PA for its refinement according to ISO26262 requirements and flow. PA and SC can also be used to define the HW-SW interface so that all three blocks can be used to formulate HW and SW Requirements at architecture level. The final products at this level are HW and SW Architectures. Those architectures are used at Design level and refined in Detailed HW as well as SW Requirements. The HW and SW designs are based on those requirements and must be done according to the HW and SW architecture definitions.
This RDDF workflow allows creating three requirements databases which are further used in the verification and validation flows also at three levels: Product, Architecture and Design level. Therefore the RDDF allows systematic and very discipline approach in product development at all levels as well as product verification and validation.

## IV. VERIFICATION GOALS AND VERIFICATION COVERAGE

The main goal of the functional safety verification is to ensure that the safety requirements as applicable are verified for its correctness and completeness. The evidence and argumentation are collected in a structured format. As previously described the ISO26262 recommends the usage of the V model at each stage development of the product.

The functional safety verification at different stages can be broadly described as show in the below figure

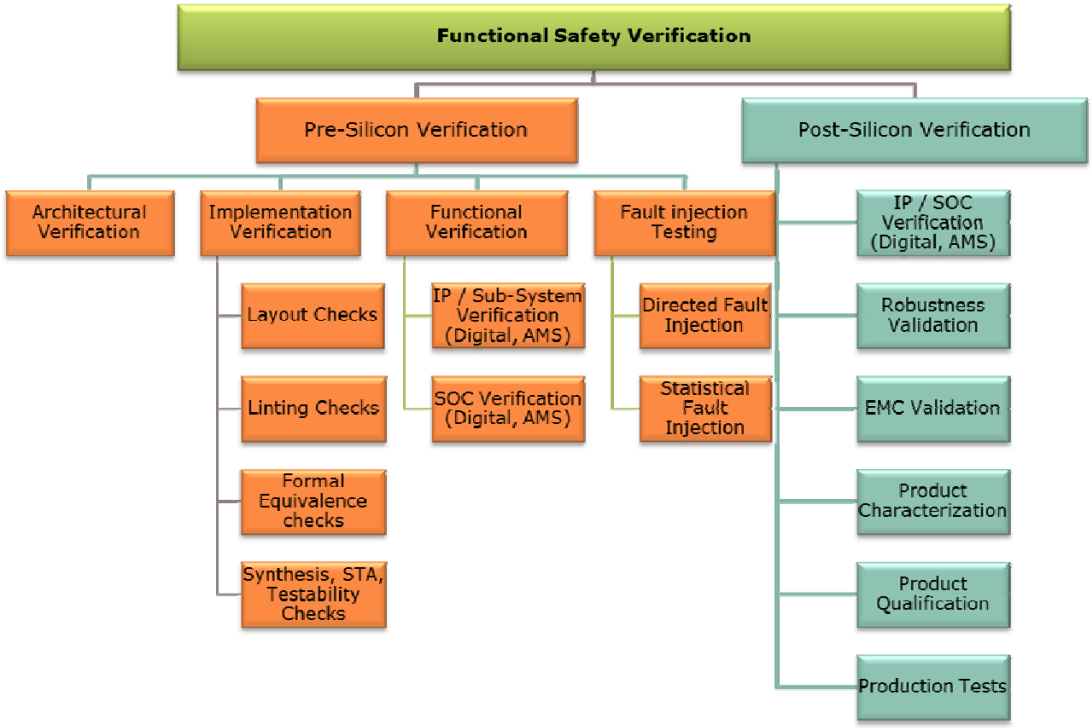


**Figure 3: Overview functional safety verification**

The main **objective** of the **Functional Safety Verification and Validation** is to verify the HW Part, SEooC based on the Safety requirements as applicable up to ASIL D for its correctness and completeness taking into consideration **ISO26262-5, Table 3, 10, 11, 12 and ISO26262-10 Annex A, Table A.8 7.4.4 – Verification of HW design** recommendations.

The pre-silicon verification mainly consists of Architectural, Implementation, Functional and fault injection verification and the post-silicon verification includes the functional, Product characterization, qualification, production tests, EMC and failure mode verification for robustness.

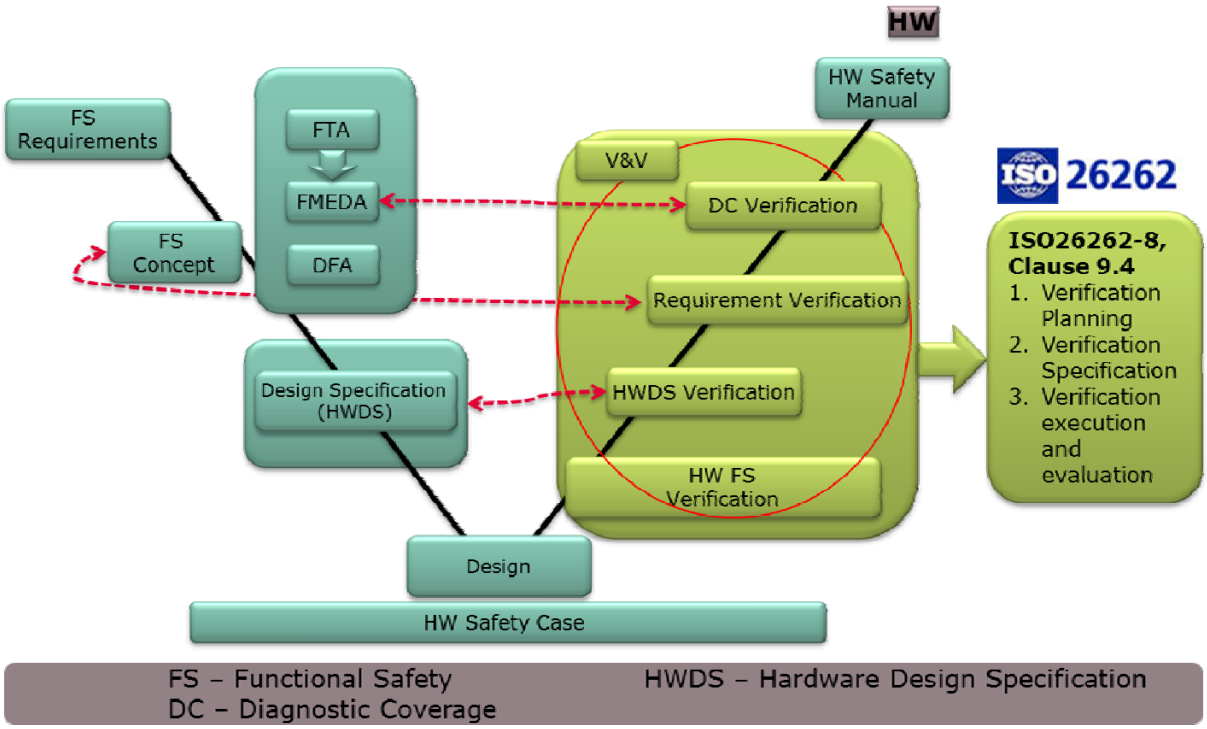


**Figure 4: V Flow functional safety verification**

Based on the ISO-26262-8 Clause 9.5, following Work Products are required

- ISO-26262-8 Clause 9.5.1 : Verification planning
- ISO-26262-8 Clause 9.5.2: Verification specification
- ISO-26262-8 Clause 9.5.3: Verification execution and evaluation

Addressing the following according to ISO-26262-8 Clause 9.4.1.1

a) The objective and content of the work products to be verified
b) The methods used for verification
c) The pass and fail criteria for the verification
d) The verification environment, if applicable
e) The tools used for verification, if applicable
f) The actions to be taken if anomalies are detected
g) The regression strategy

The functional Concept outlines the requirements including safety related requirements and needs to be verified by pre and post Silicon Verification methods and called as Requirements Verification.

The Hardware Design Specification (HWDS), where the failure modes and the intended safety mechanisms to protect the safety related logic is described by the Designer are verified for its correctness during the early phases of the IP / product development. The Error Detection Time is defined as the point from where the fault is deemed dangerous to the point when an alarm is raised by the intended Safety Mechanism is measured during this exercise.

Finally, the FMEDA is verified using the failure mode and statistical fault injection verification is applied as one of the methods to gather and support the evidence for the Diagnostic coverage claims in the FMEDA.

With the above verification strategies, the ISO26262-8, Clause 9.4 Work Products are derived enabling the correctness and completeness of the requirements and evidences collected.

## V. SysML Modelling example

Model driven systems engineering is gaining momentum in the automotive industry. Initially focused on UML for the development of software components the trend is now to use the SysML extensions that enable to model the different aspects of hardware and software and especially their interactions. The key advantage of using SysML is that requirements, structural, behavioral, temporal, state models exist under a global system model and follow a logical decomposition that enables to capture the overall interactions and dependencies of the system. In that context the functional safety verification can take advantage of the richness of the modeling to build scenarios that are representative of the safety claims.
Another aspect is that the model itself provides the rules to verify consistency and completeness of the information. The picture below shows a requirements structuring model that can be enforced at the different levels of the architecture.

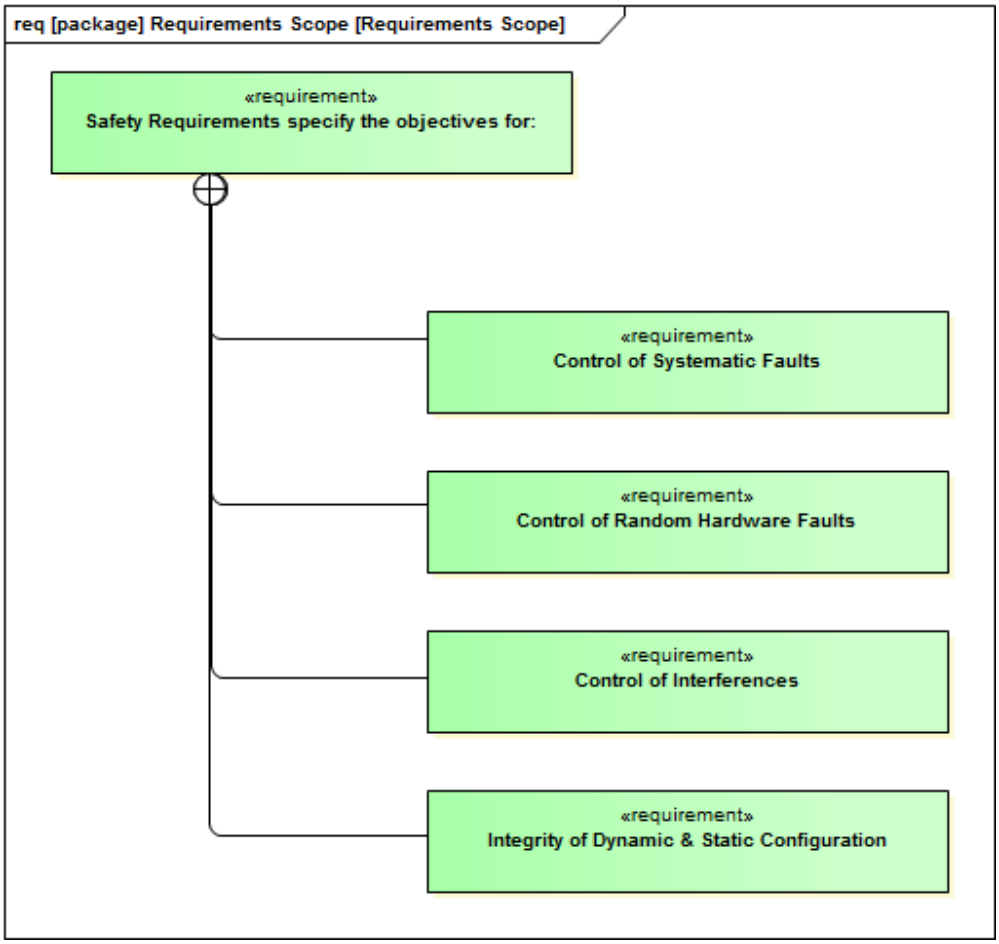


**Figure 5: Functional safety requirements**

In a safety system different viewpoints are created as mentioned before, one of them is the failure behavior that is an essential aspect that drives the technical decisions. The failure analysis is performed in a hierarchical manner starting from behavioral aspects down to architectural and design descriptions. To build a safety argumentation and to be able to verify it is it necessary to understand the chain of analysis and understand at each step how a given artifact is supporting a requirement specification (a rationale). This is illustrated below by a failure analysis that is linked and extends a functional specification model.

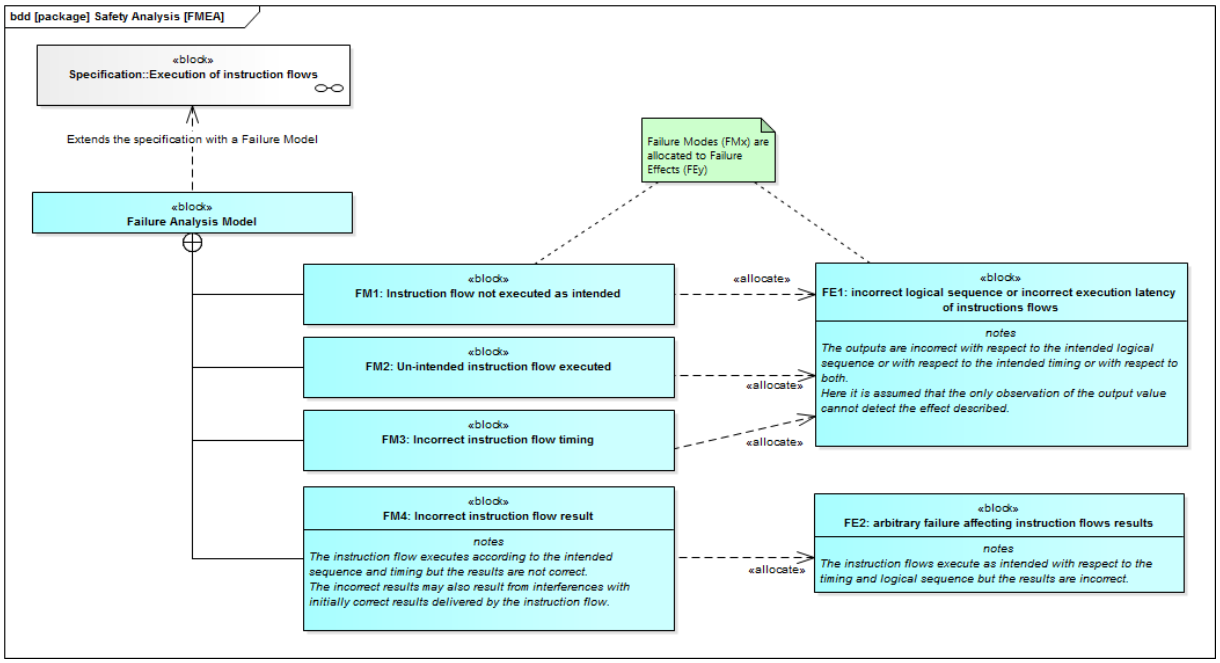


**Figure 6: Failure Analysis Model**

In a further stage the elicitation of the requirements is derived from the results of the failure analysis.

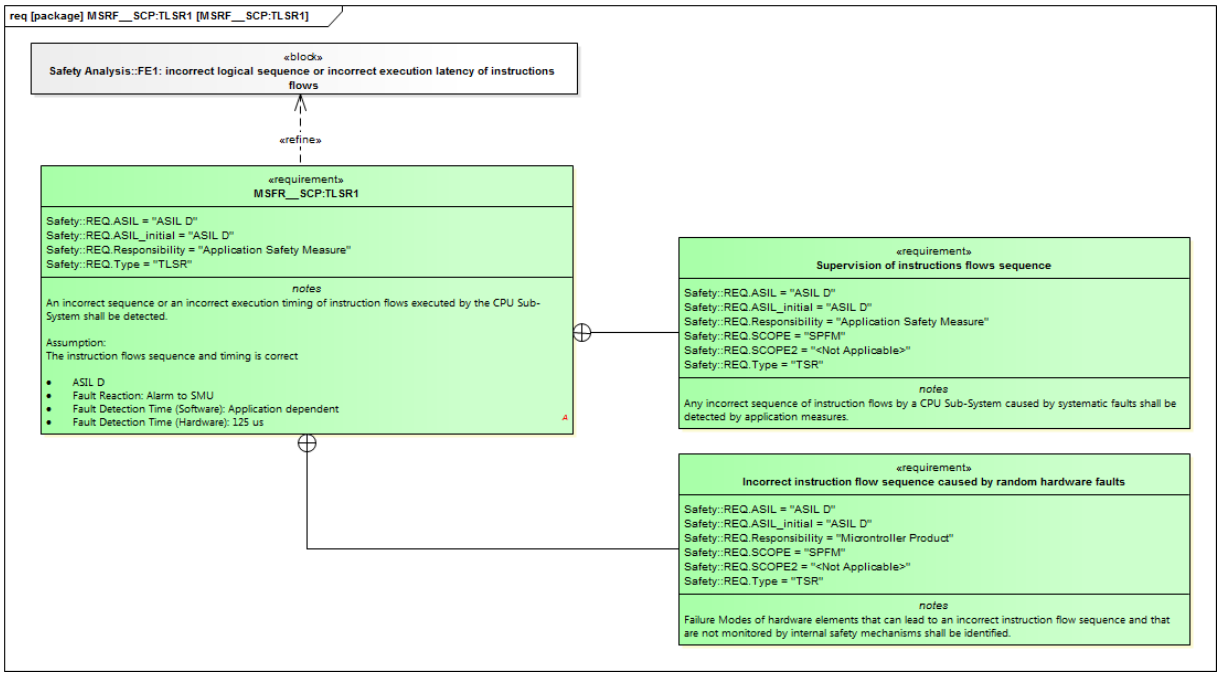


**Figure 7: Safety Analysis**

From a verification viewpoint this provides the capability not only to verify that the requirement is properly implemented but to create the verification scenarios that are representative of the requirement and from that perspective bring an additional level of safety insurance where for instance it can be detected that the requirement as expressed is not sufficient (complete) to cover the failure scenarios.

## VI. Conclusion

Efficient development and verification approaches are necessary to address increasing complexity in automotive hardware products together with requirements coming from ISO26262 standard. Our requirement driven development flow uses functional models to represent use cases and resulting requirements. These requirements are then refined at lower levels and also proven for correct implementation on all abstraction levels by means of verification.

Since requirements on high abstraction levels are available very early in development process the corresponding verification can start already before hardware is implemented and available. This allows to avoid expensive and time consuming rework. From other hand the RDDF flow enables almost parallel development at all levels as well as it delivers crucial evidence required by the ISO26262 standard necessary for product functional safety assessment and certification. This flow perfectly fits product definition and modelling at high level with SysML as well as requirements capturing and finally product verification and validation to proof its compliancy to ISO26262 already at early development stages.

## References


[1] ISO 26262 Std. Road vehicles, Parts. 1-10, 15 Nov. 2011.
[2] Infineon Technologies AG, Aurix Safety V&V Concept, V1.0, 2015-04
[3] Infineon Technologies AG, Documentation Tree, Edition V4.0, 2015-12-22
[4] Infineon Technologies AG, System Development Handbook (SDHB), 2016
[5] OMG Systems Modeling Language (OMG SysML™) Version 1.4, September 2015
[6] Requirements-driven Verification Methodology for Standards Compliance, Serrie-justine Chapman (TVS), Mike Bartley (TVS), Darren Galpin (Infineon), DVCON 2014
[7] Compliance driven Integrated circuit development based on ISO26262, Haridas Vilakathara, NXP Semiconductors, Manikandan panchapakesan, NXP Semiconductors, DVCON 2014