Requirement Driven Safety Verification

Ranga Kadambi, Vladimir Litovtchenko,
Jens Rosenbusch, Antonio Vilela

Infineon Technologies AG

accellera SYSTEMS INITIATIVE

2016 DESIGN AND VERIFICATION™ DVCON CONFERENCE AND EXHIBITION EUROPE

Agenda

- Introduction and Scope
- Requirement driven development and verification
- Verification goals and coverage
- SysML modelling and example
- Conclusion

© Accellera Systems Initiative

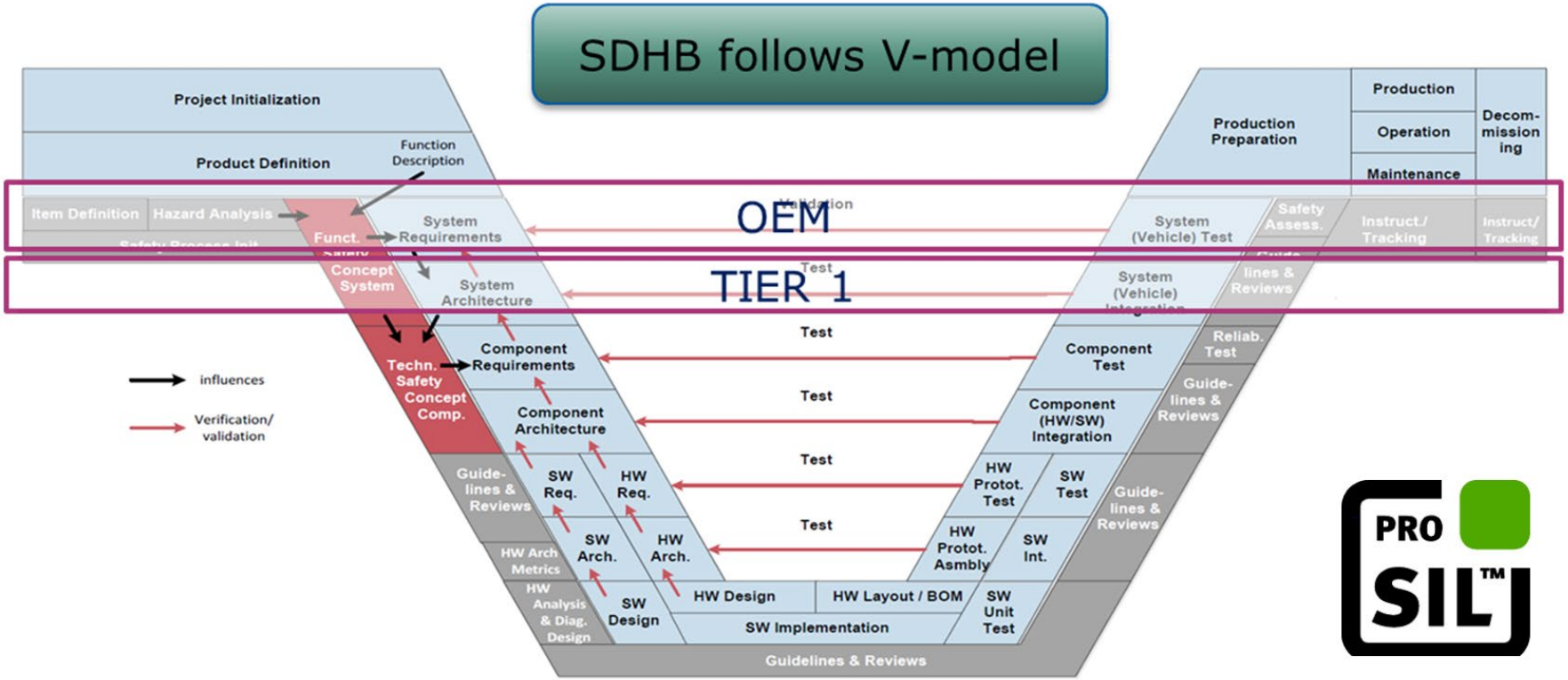
Introduction and Scope

- Standard ISO26262 [1] was introduced in 2011 to address functional safety in modern automotive systems
- Addresses all development steps: ISO26262 covers whole lifetime of products used in automotive E/E systems
- Compliance to safety requirements: 130 work products for whole V-model
- RDDF: ISO26262 widely utilizes safety requirements at all abstraction level for all its work packages
- RDDF usage by Infineon: HW and SW development, verification and validation for Aurix™ MCUs
- Scope:
  - Aurix™ MCUs development according to ISO26262 Part 4 and Part 5
  - Requirements capturing and refinement
  - Modelling at different abstraction levels
  - Safety verification based on RDDF

© Accellera Systems Initiative

Introduction and Scope

- IFX SDHB: System Development Hand Book



Requirement driven flow

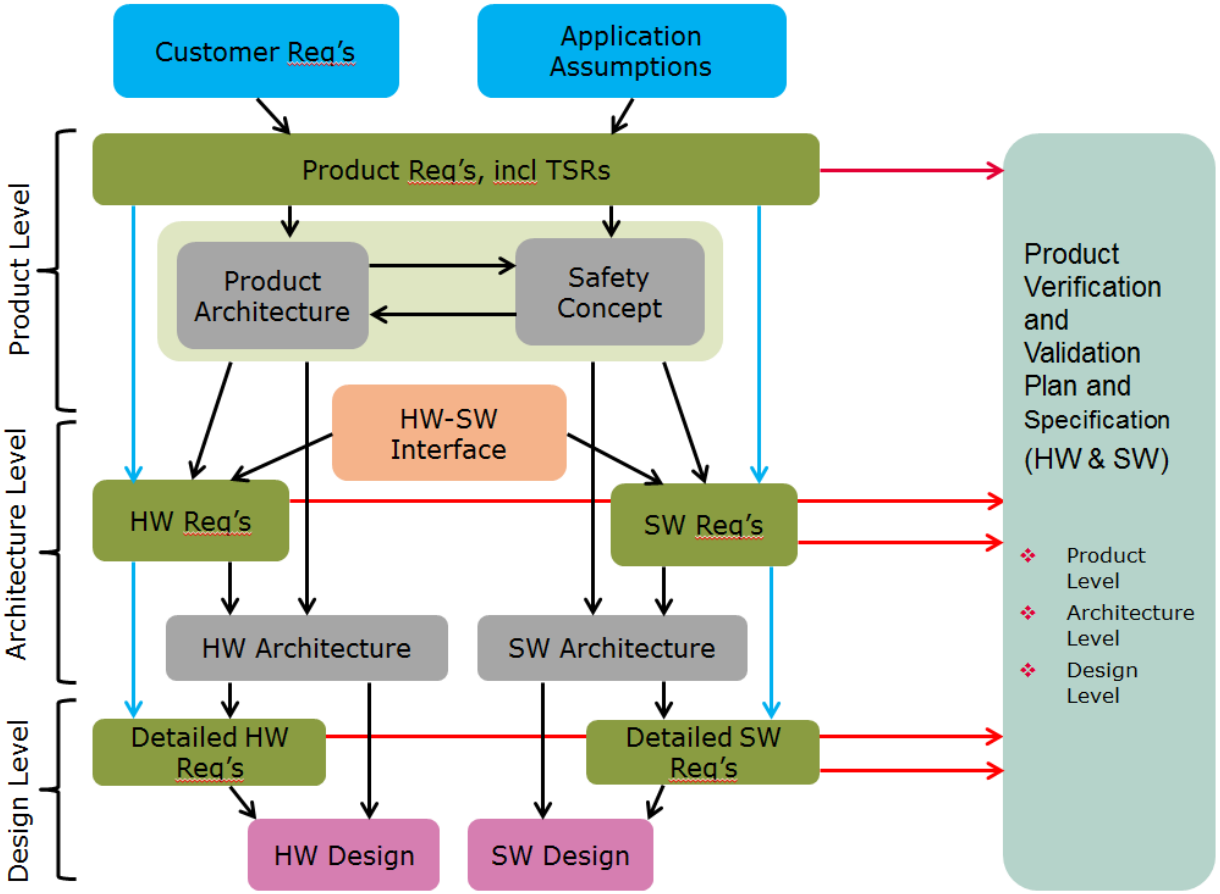
- ISO26262 Requirement Flow
  - Based on requirements: the standard considers work packages to be generated during product development at two levels: system and hardware
    - Technical Safety Requirements (TSRs) for System level and Hardware Safety Requirements (HSRs) for Hardware level,
    - TSRs and HSRs are required 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.
  - TSRs and HSRs are key for all further steps of development: TSRs for the System-level, HSRs for Hardware-level Development and Verification.
- Requirement Driven Development Flow (RDDF) and ISO26262
  - RDDF is not developed only to be conformant with standards like ISO26262 and IEC61508
  - Systematic and discipline approach to systems development 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

© Accellera Systems Initiative

Requirement driven flow

RDDF workflow: 3 requirements databases are created.

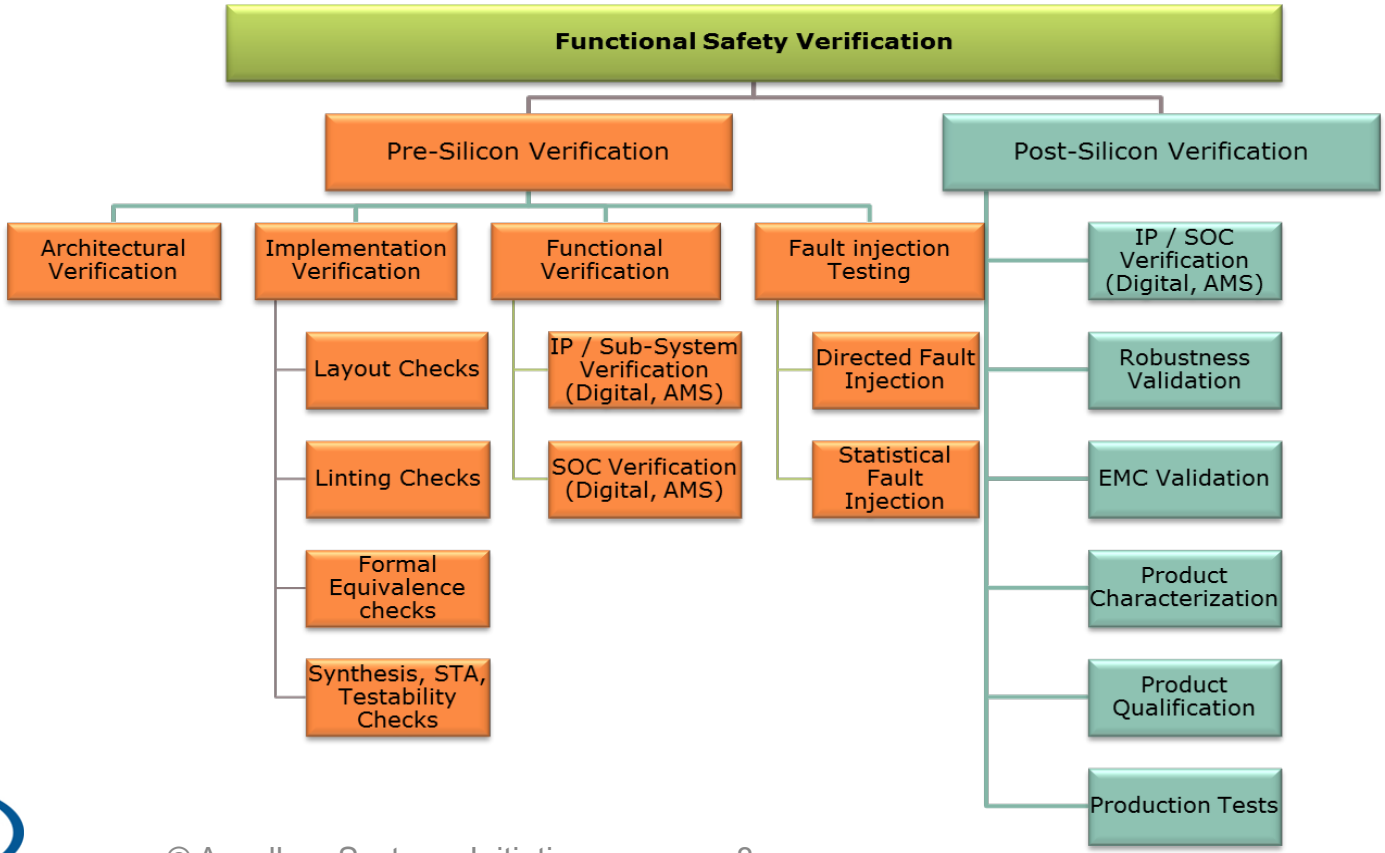
- Further used in verification and validation flows also at three levels: Product, Architecture and Design.



Verification goals and coverage

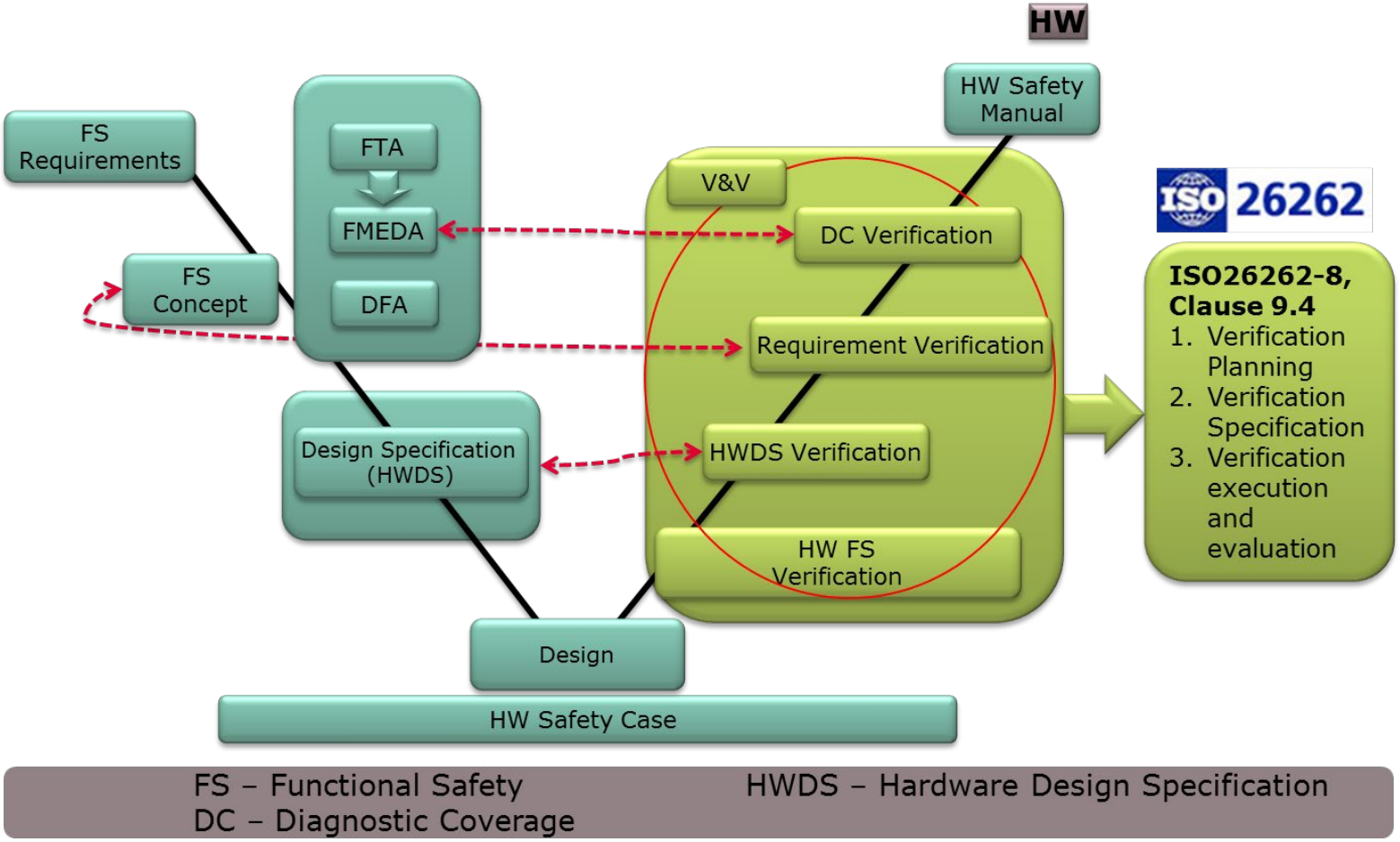
FuSa Verification and Validation main objective:

- Verify the HW Part/SEooC based on the Safety requirements (up to ASIL D) for its correctness and completeness
- Considering **ISO26262-5, Table 3, 10, 11, 12 and ISO26262-10 Annex A, Table A.8 7.4.4 – Verification of HW design** recommendations.



© Accellera Systems Initiative

Verification goals and coverage



SysML modelling and example

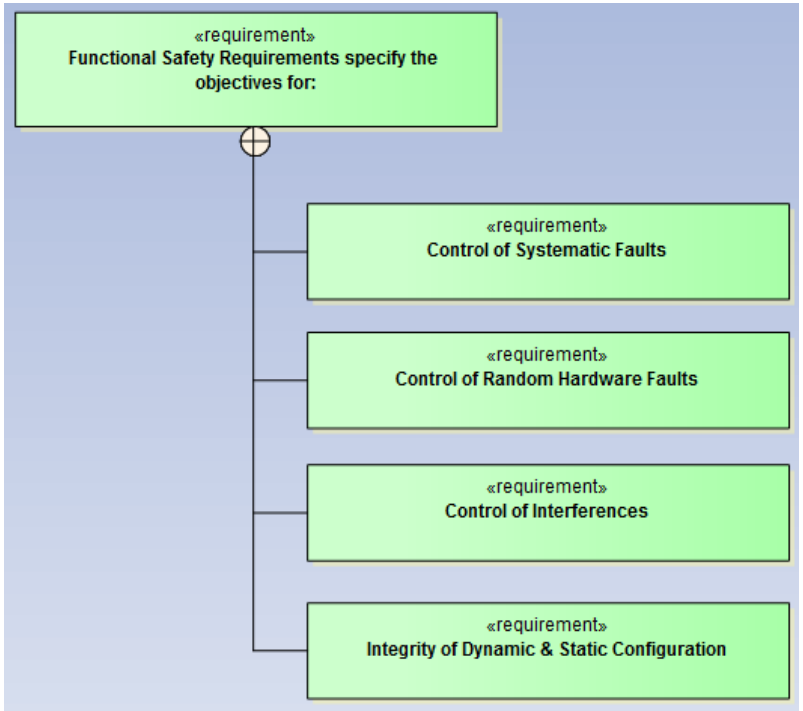
- Model driven systems engineering is gaining momentum in the automotive industry.
- Initially focused on UML for SW components modelling the trend is now to use the SysML extensions.
- SysML enables to model different aspects of HW and SW and especially their interactions.
- The key advantage of using SysML: 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.
- Advantages:
  - Functional safety verification can take advantage of the richness of the modeling to build scenarios that are representative of the safety claims.
  - SysML model itself provides the rules to verify consistency and completeness of the information.

© Accellera Systems Initiative

SysML modelling and example

- SysML model for safety system has different viewpoints:
  - Failure behavior: essential aspect that drives the technical decisions.
  - The failure analysis is hierarchical: from behavioral aspects down to architectural and design descriptions.

- SysML modelling allows to:
  - Build a safety argumentation and
  - Enable argumentation verification,
  - Understand the chain of analysis and how a given artifact is supporting a requirement specification (a rationale).

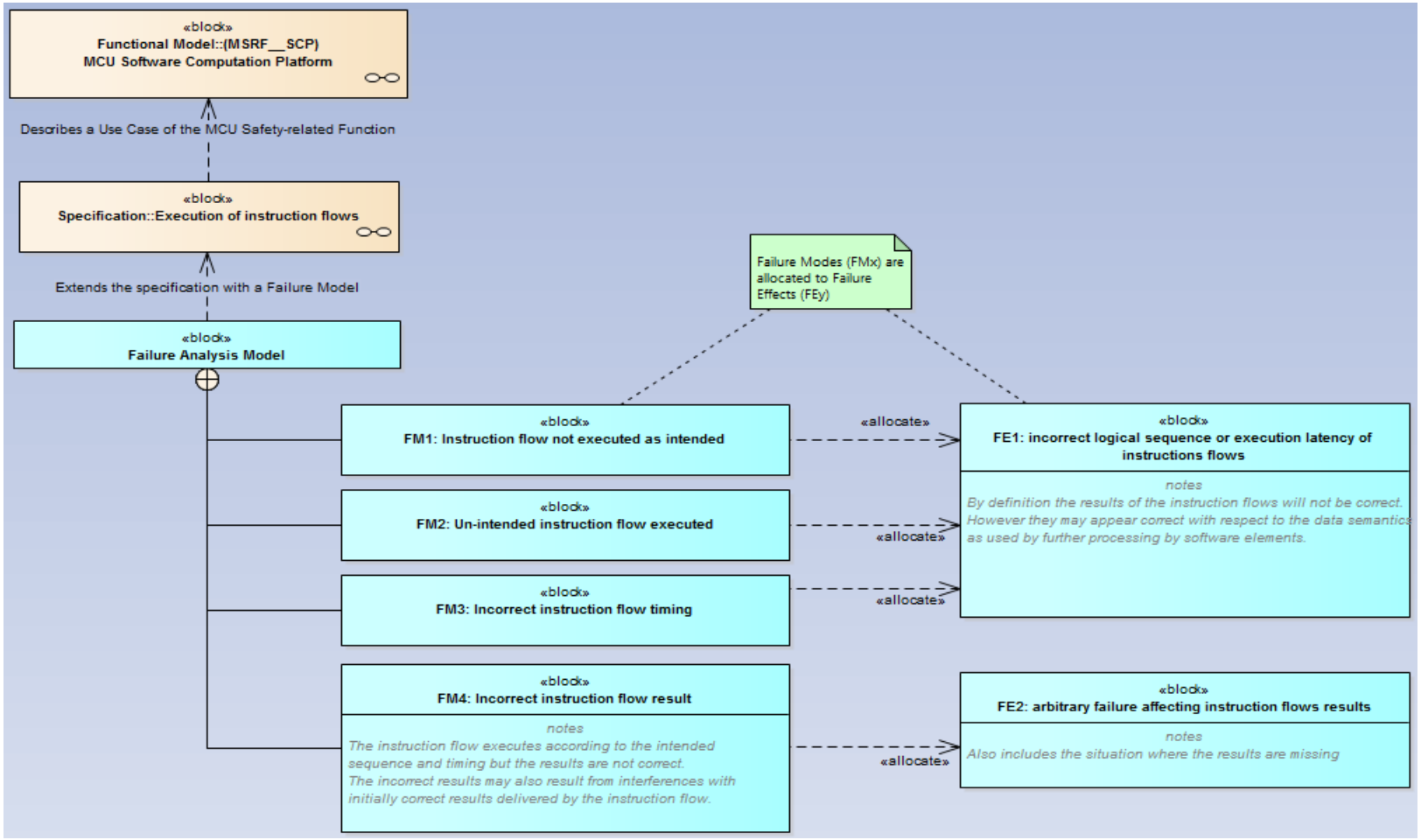


Example of requirements structuring model that can be enforced at the different levels of the architecture.

© Accellera Systems Initiative

SysML modelling and example

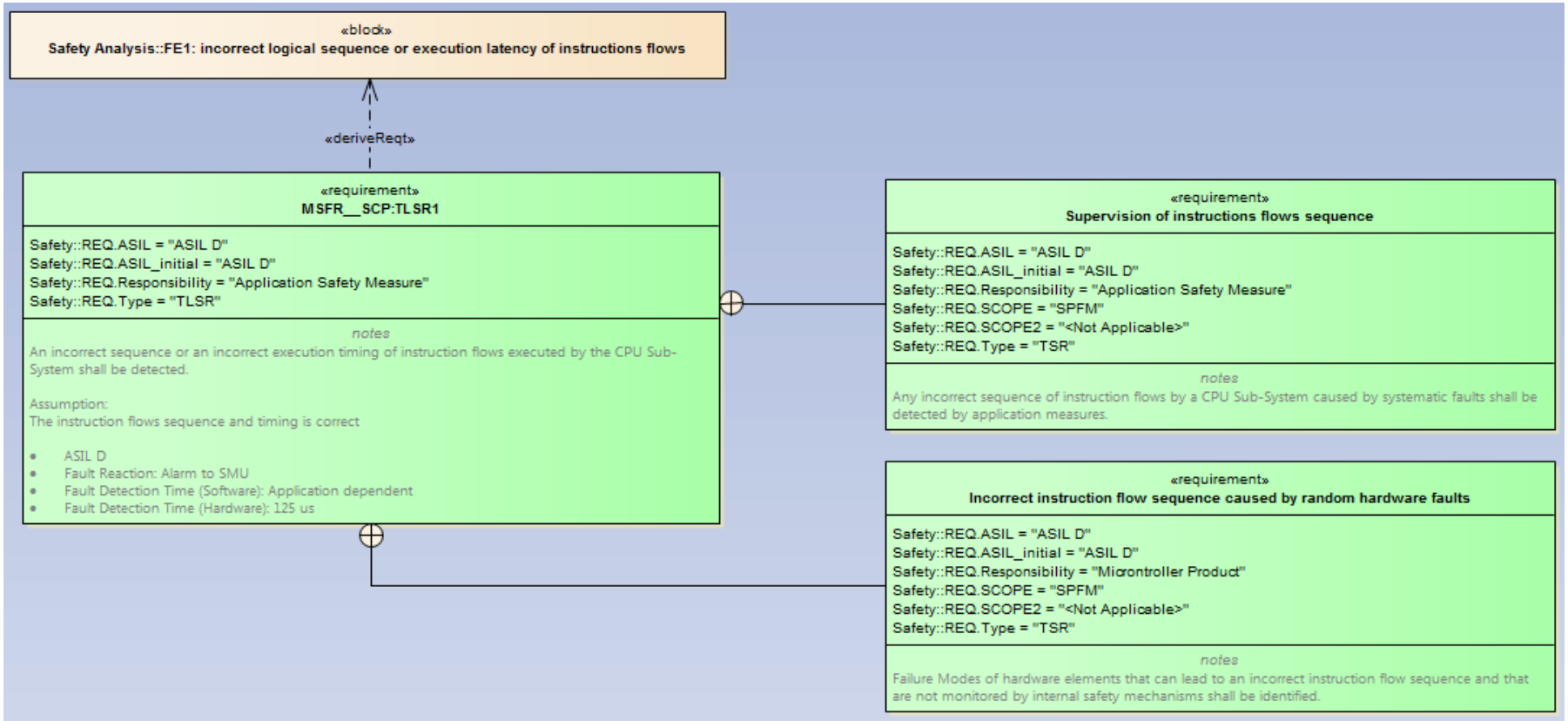
Further modelling stages allow extraction of requirements from the results of the failure analysis.



SysML modelling and example

Using SysML from verification viewpoint modeling allows to:

- Verify that the requirement is properly implemented and also
- Create verification scenarios that check requirements are sufficient and complete for all Failure Modes



© Accellera Systems Initiative

Conclusion

- Efficient development and verification approaches are necessary
  - to address increasing complexity in automotive HW products,
  - together with requirements from ISO26262 standard.
- Advantages of requirement driven development flow
  - uses functional models to represent use cases and resulting requirements.
    - These requirements are then refined at lower levels and
    - Proven for correct implementation on all abstraction levels by verification.
  - Verification can start before hardware is implemented and available
    - Requirements on high abstraction levels are available very early in development process.
    - Allows to avoid expensive and time consuming rework.
  - RDDF flow enables almost parallel development at all levels and
  - 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
    - Requirements capturing and finally
    - Product verification and validation to proof its compliancy to ISO26262 already at early development stages.

© Accellera Systems Initiative

Many thanks for your attention!

Questions