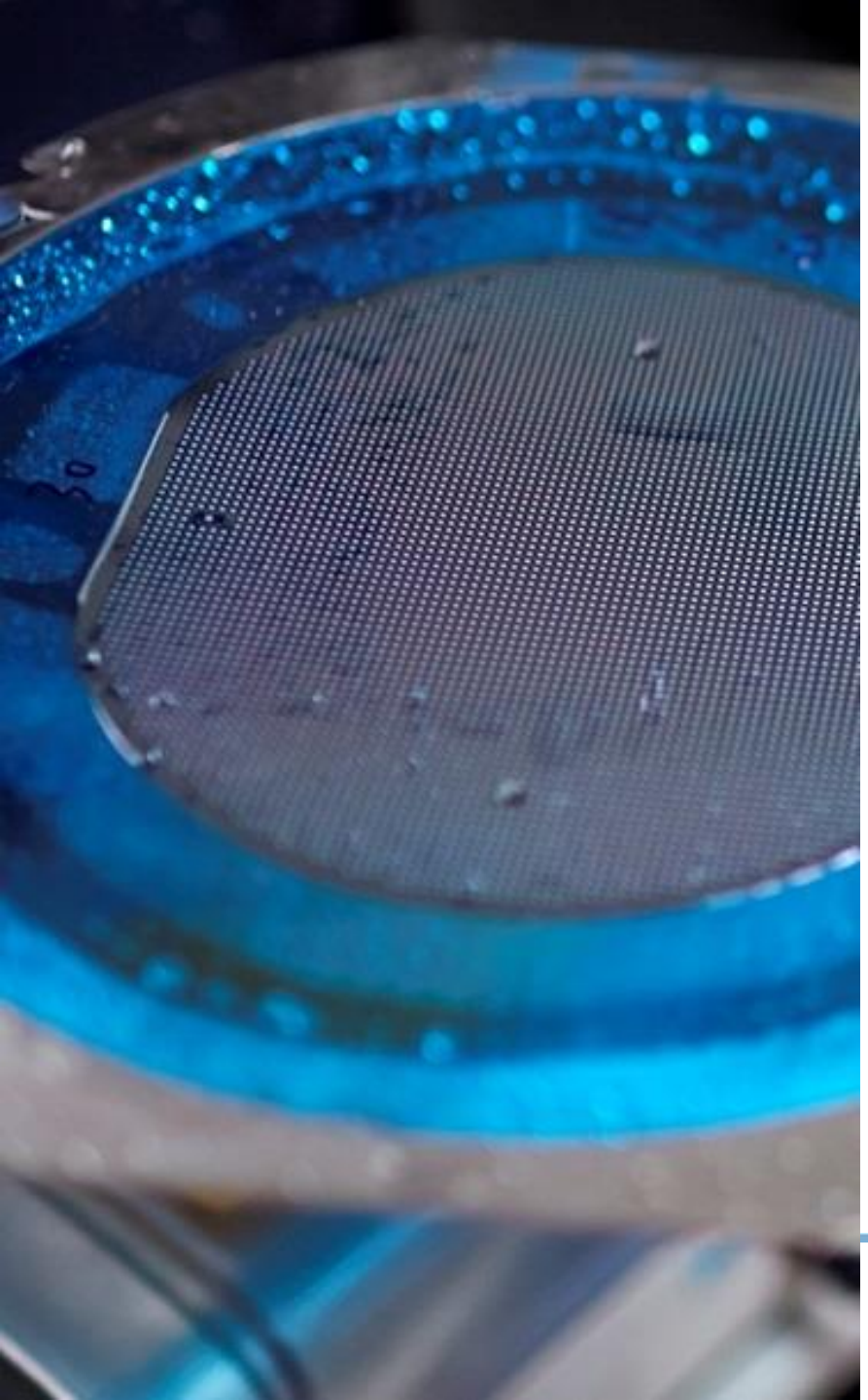
Compliance driven Integrated circuit development based on ISO26262

HARIDAS VILAKATHARA
Oct, 2015

NXP Semiconductors

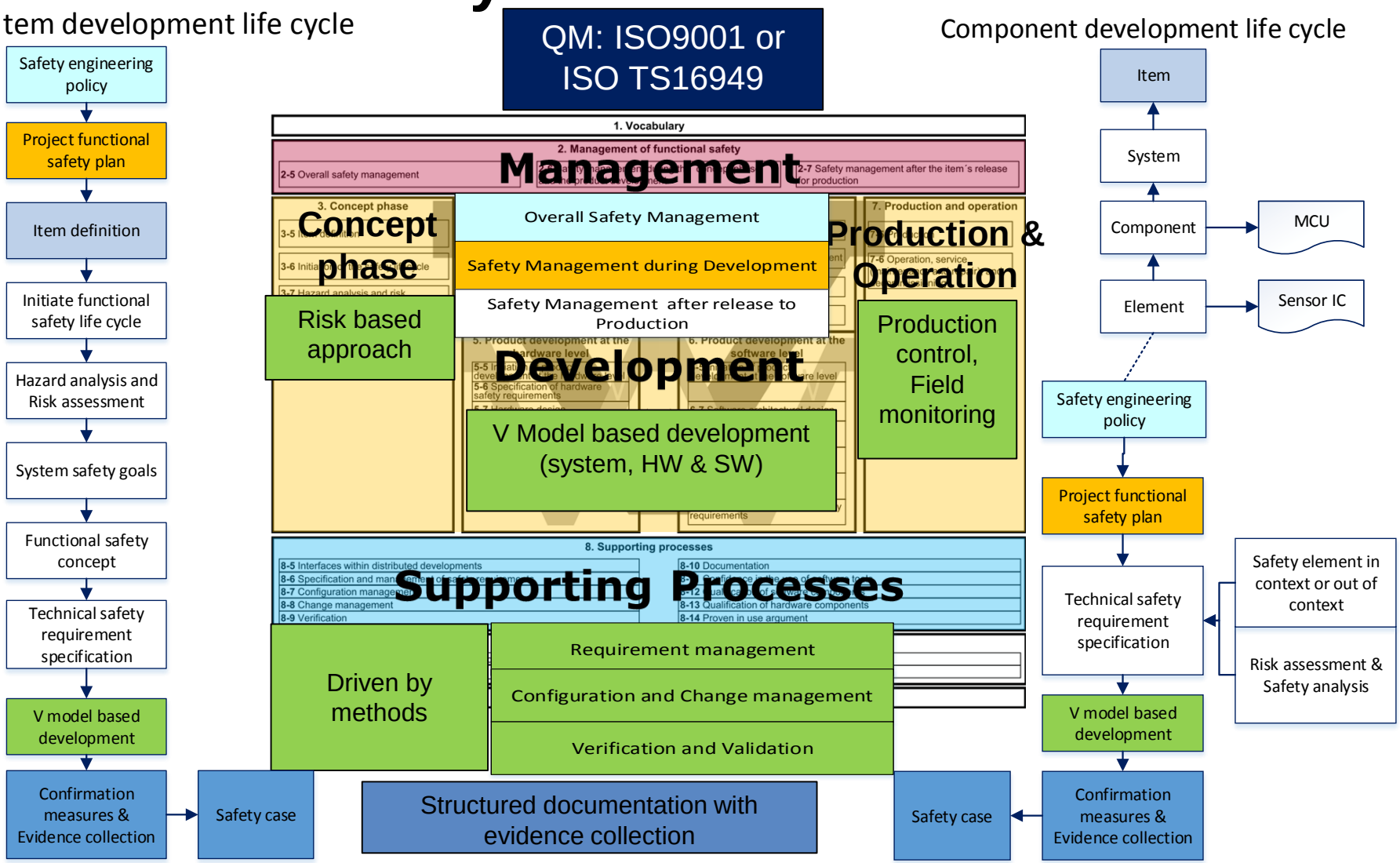
NXP
SECURE CONNECTIONS FOR A SMARTER WORLD



Outline

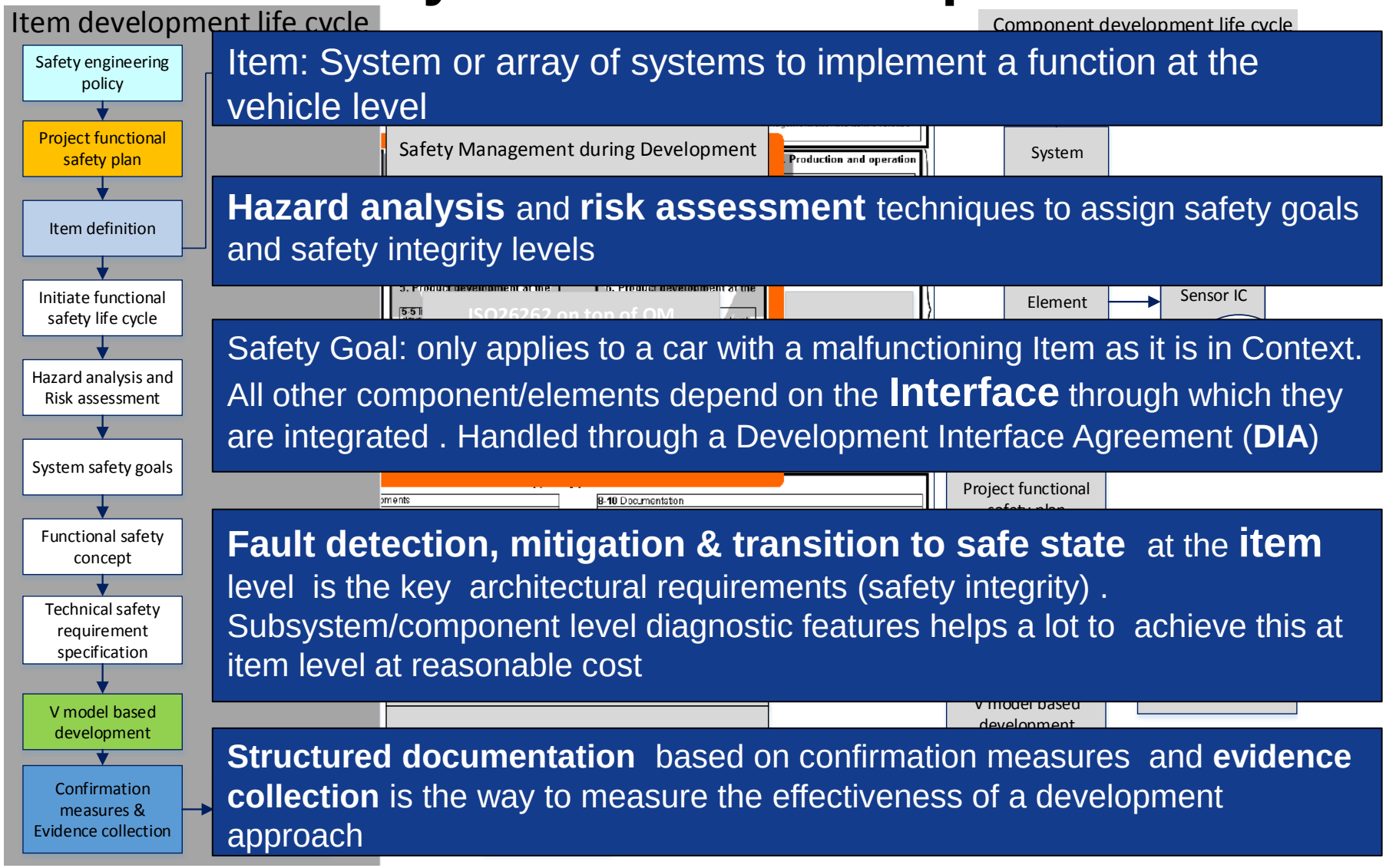
- ISO26262 life cycle overview
  - Item development
  - Component development
- Compliance driven development process
  - V model with safety extension
  - Safe requirement management
  - HW risk assessment and safety analysis
  - Requirement driven verification
  - Tool qualification
- Questions?

ISO 26262 Life cycle Overview



Functional safety (ISO26262) : A**bsence of unreasonable risk** due to hazards caused by malfunction behavior of E/E/EP systems in passenger cars

ISO 26262 life cycle : Item Development



ISO 26262 life cycle: Component Development

Components/elements depend on the **Interface** through which they are integrated at item level . This is handled through a Development Interface Agreement (DIA)

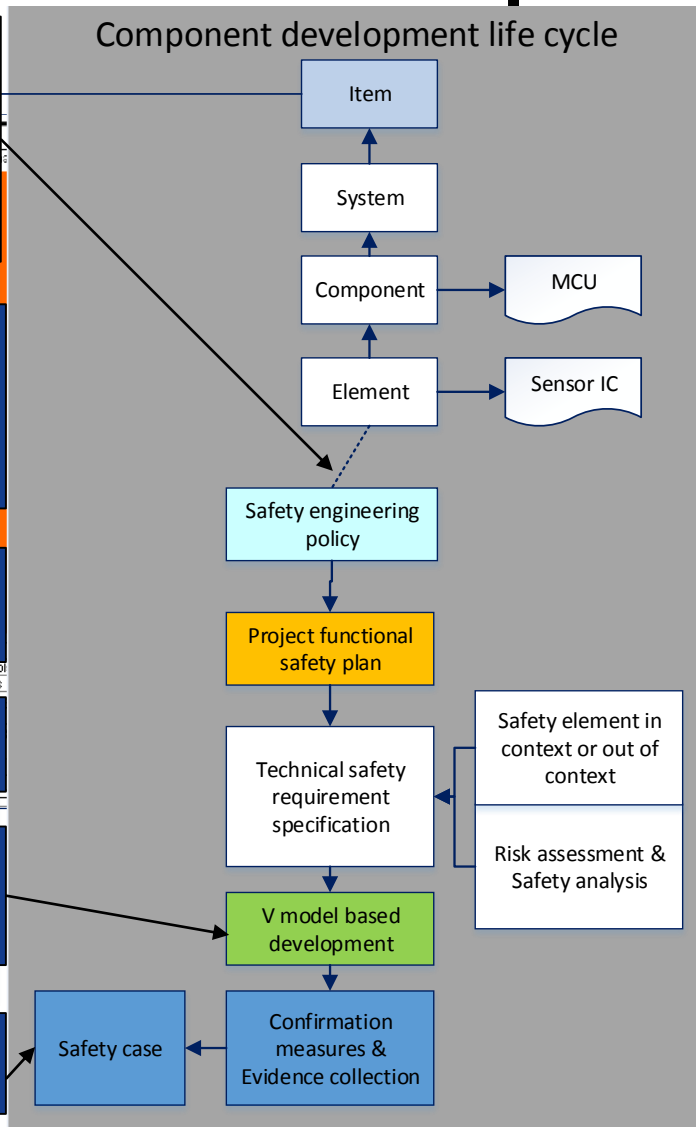
For generic component development standard recommends a **safety element out of context methodology** (e.g. MCU)

Safety requirement through risk assessment & safety analysis

Requirement management with **traceability**

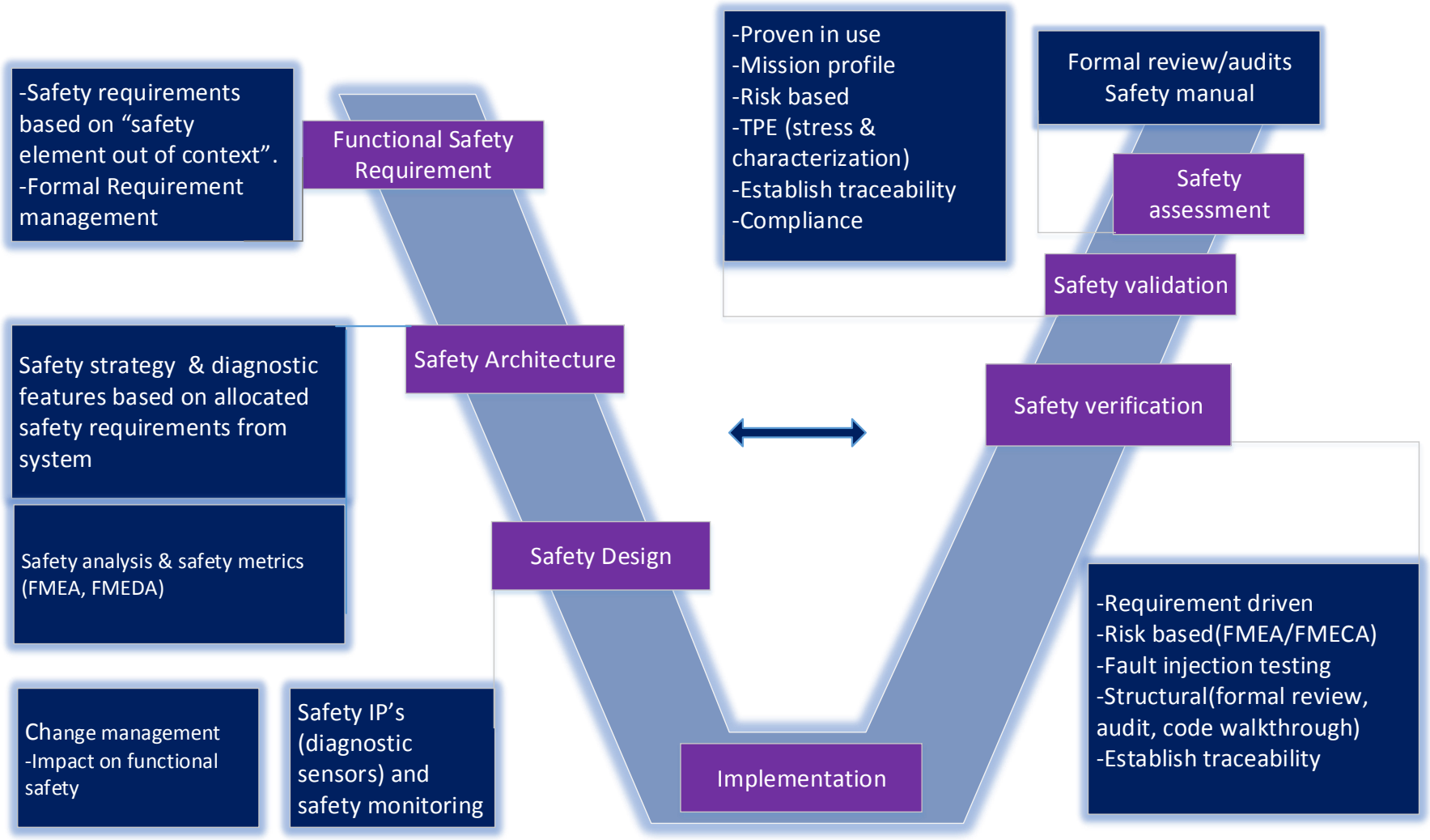
Verification and Validation at every stage and are **driven by methods**

Structured documentation with evidence collection



MCU: Micro controller unit

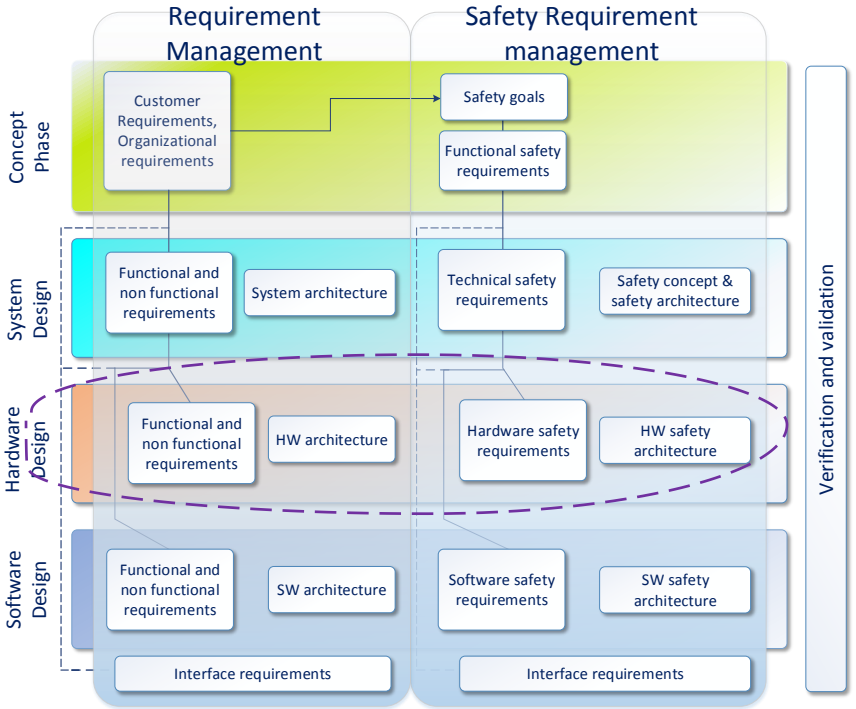
V Model with Safety Extension



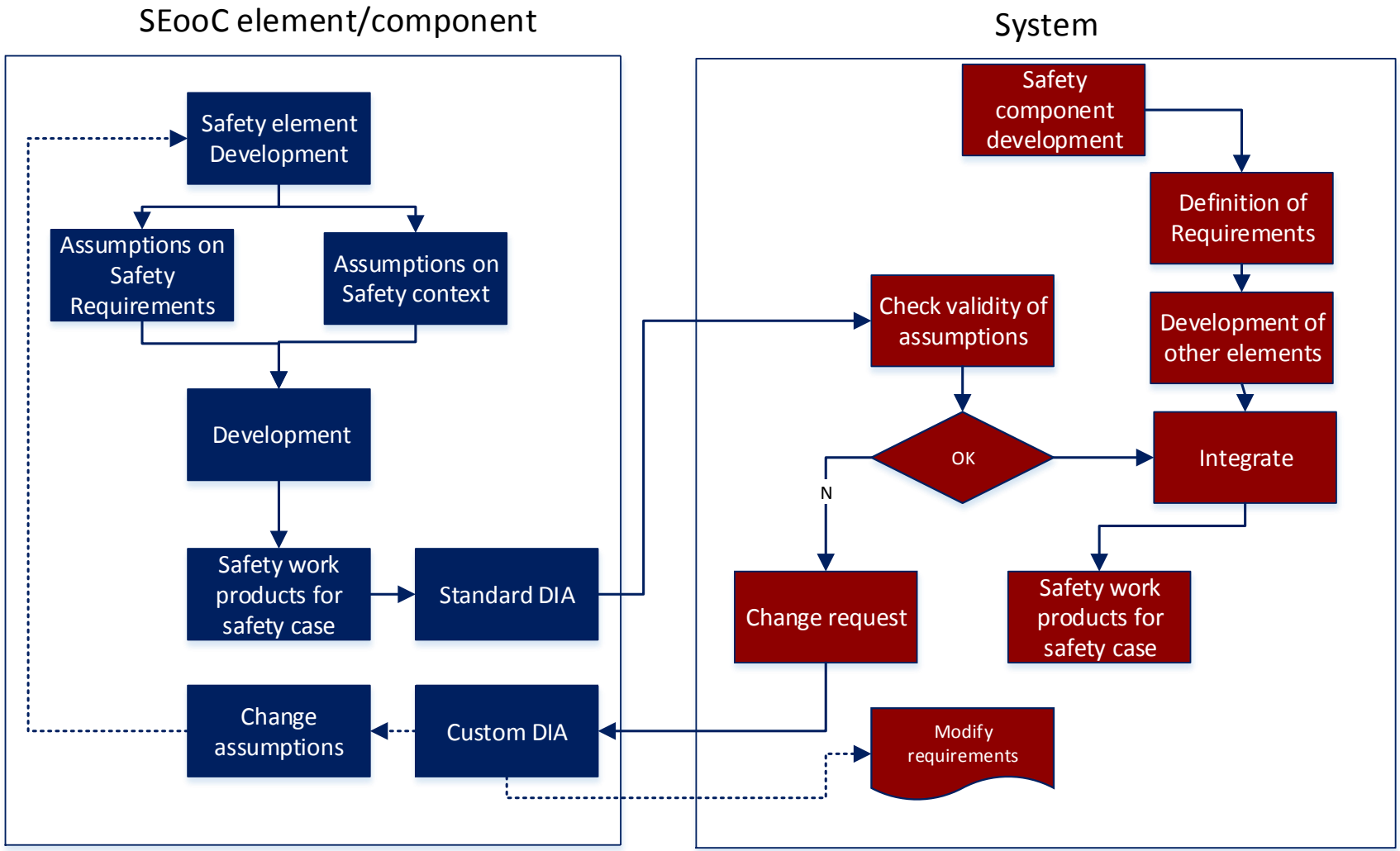
FME(C)A: Failure mode and effects (criticality)analysis
FMEDA: Failure mode and effects & diagnostic analysis
TPE: Test and production, IP: Intellectual property

Component level Safety Goals and Requirements

- A Component always interacts through an **interface** through which it connected to the rest of the system
- Direct assignment of safety goals to a component not easy. However…
- Derived safety requirements can be allocated to a component & an **interface** through which it interact with rest of system
- The interactions with other systems and components can be handled through
  - Interface control document (technical interface)
  - Development interface agreement (process interface)
  - Safety manual (assumptions on use)

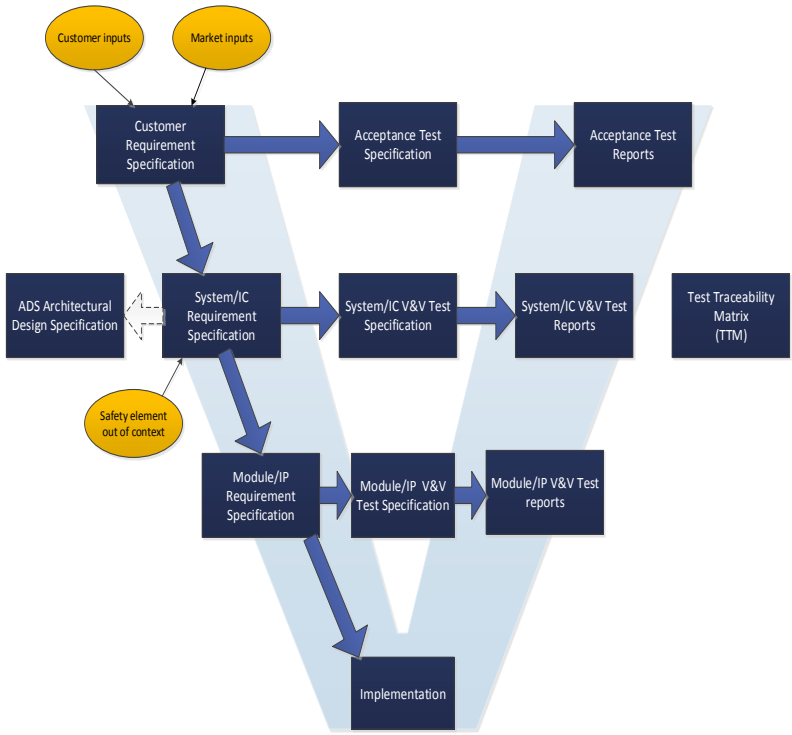


Component level (SEooC) Interface Agreement



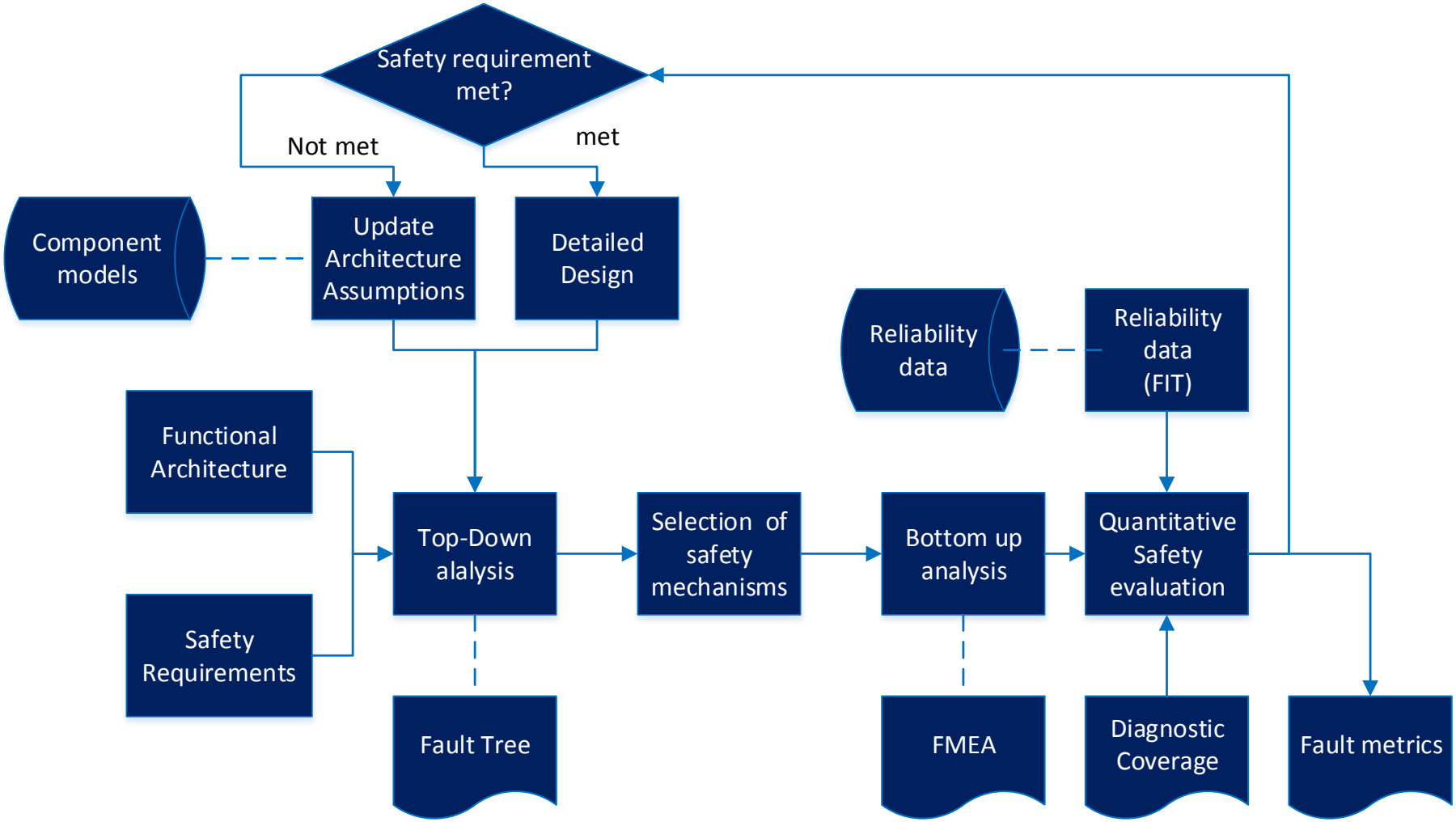
(Safe) Component level Requirement Management

- Safety requirements are allocated to a component through
  - Allocated from next higher level system
  - Through risk assessment and safety analysis
- Formal requirement management with traceability is mandatory
  - All requirements can be tracked to a design, verification and validation item
  - No design element in repository without an assigned requirement
  - Any PR raised can be tracked to a corresponding requirement ID
  - Impact on existing requirements can be identified for CR
- Formal process to track
  - Customer requirements
  - Allocated requirements from system or through risk assessment



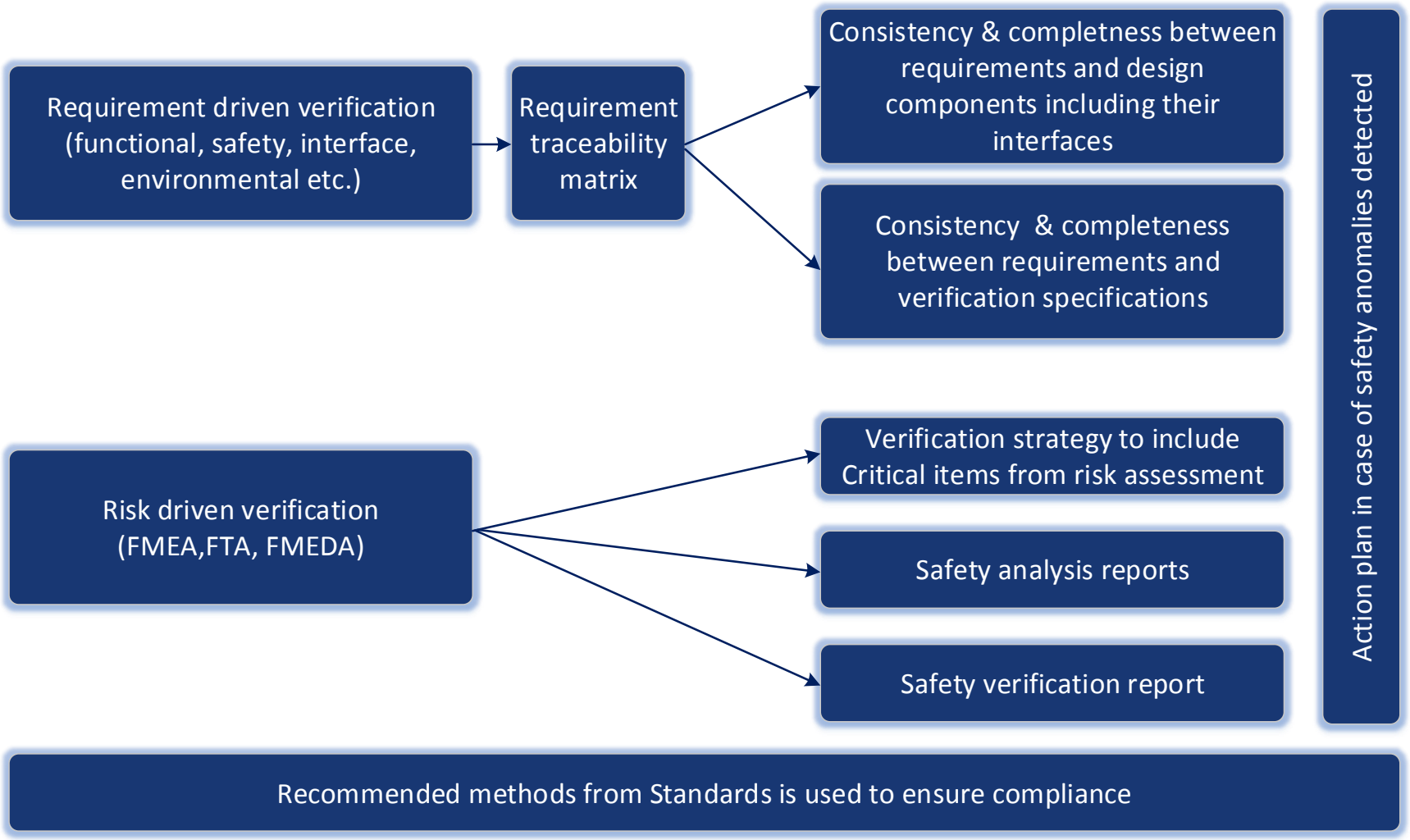
PR: Problem report, CR: Change request, ID: Identification Number

HW Risk Assessment and Safety Analysis



FME(C)A: Failure mode and effects (criticality)analysis
FIT: Failure in time

Requirements and Risk driven Verification

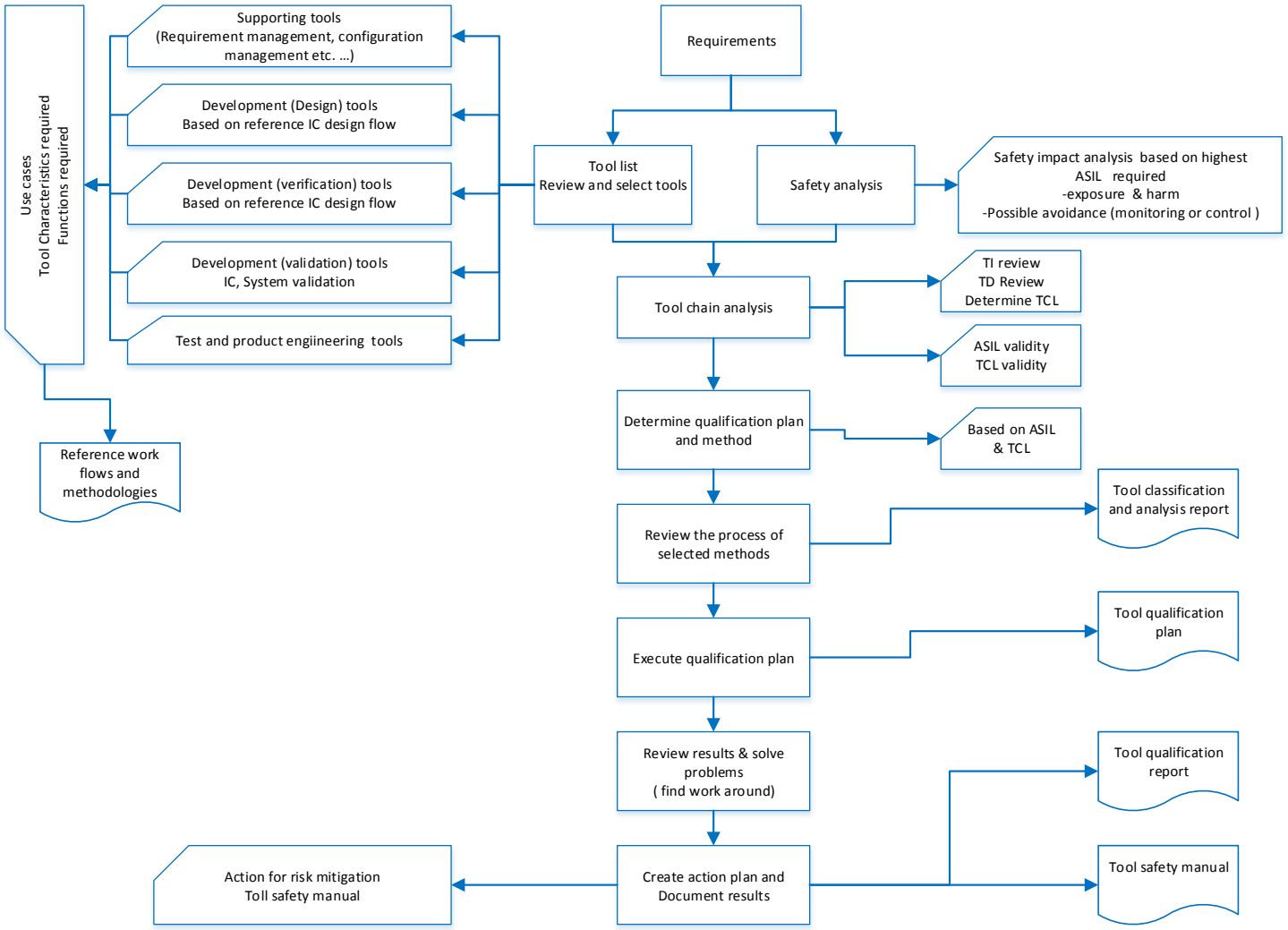


FME(C)A: Failure mode and effects (criticality)analysis
FMEDA: Failure mode effect and diagnostic analysis
FTA: Fault tree analysis

Tool Qualification

- Why tool qualification
  - IC design involves many translation process, and tool in general has the capacity to introduce error during various translation process
  - e.g. RTL-> Synth netlist -> post layout
- Verification tools may fail to detect errors in the hardware items
- Tool qualification makes sure that tool correctly functions (improve confidence in tool function)
- The library components and different views used during the design translation process also need to be of mature quality and qualified one
- Recommended practice is to deploy a validated reference design flow (RDF) at organizational level

Tool Qualification Flow



Conclusion

- Component development always need to be taken through a Development Interface Agreement both from process & product point of view.
- Direct assignment of a safety goal at a component level is not always possible.
  - Risk assessment and safety analysis at component level shall be used as a key instrument in deriving the safety requirements
  - Risk assessment shall be performed based on assumed safety context
- Requirement driven and risk oriented verification shall be employed as a verification approach
  - ISO 26262 standard provides a set of recommended methods to achieve the verification goals
- Tool confidence and tool qualification is a critical item from the ISO 26262 standard
  - Recommendation is to use a validated reference design flow at organization level as a reference

QUESTIONS ??

Impact on Methodologies & Tools

Requirement management	-Vertical traceability up-to **design** & Horizontal traceability (DOORS) -Traceability shall support **impact analysis (DOORS)** - Method driven (Risk analysis) approach for **safety** requirement capture
Verification & Validation	-Requirement driven - Fault injection - Proven in use argument generation - Verification in every phase of development (follow V model)
Configuration management	According to ISO/TS 16949, ISO 10007 and ISO/IEC 12207 All safety work products under configuration control
Change management	Procedure driven approach Evaluation of change request through Impact analysis (use DOORS)
Confirmation measures	Review: Results of a safety work product Audit: Process and procedures Assessment: Achievement of functional safety against safety plan
Tools	SW tool qualification based on tool impact on safety work products and detectability
Documentation	Structured documentation on all the above into safety case with argumentation

Safety work flow (Safety component or element)