Overview of the 2nd Edition of ISO 26262: Functional Safety – Road Vehicles

Rami Debouk

GM Research and Development

rami.debouk@gm.com

August 16th, 2018

Disclosures

- This presentation presents an overview of the ISO 26262 Functional Safety standard for road vehicles by conveying the content of the standard as it was released in its current FDIS version

- Permission was received from ISO to use content taken directly from the current FDIS and contained in this presentation

Outline

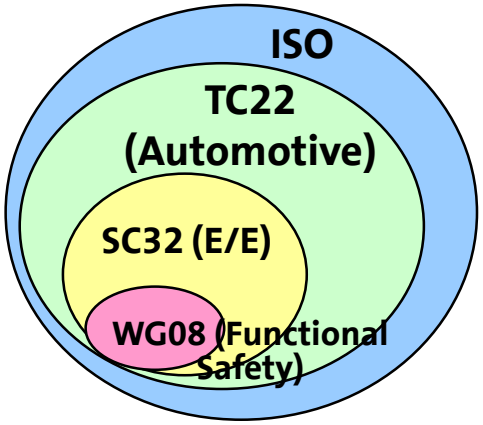
- ISO 26262 2nd Edition Development
- Definitions
- Functional Safety Management
- Hazard Analysis and Risk Assessment
- System, Hardware and Software Levels Requirements
- Supporting Processes
- Requirements for Motorcycles and Trucks and Buses
- Guidelines for Semiconductors
- Summary

What is ISO 26262?

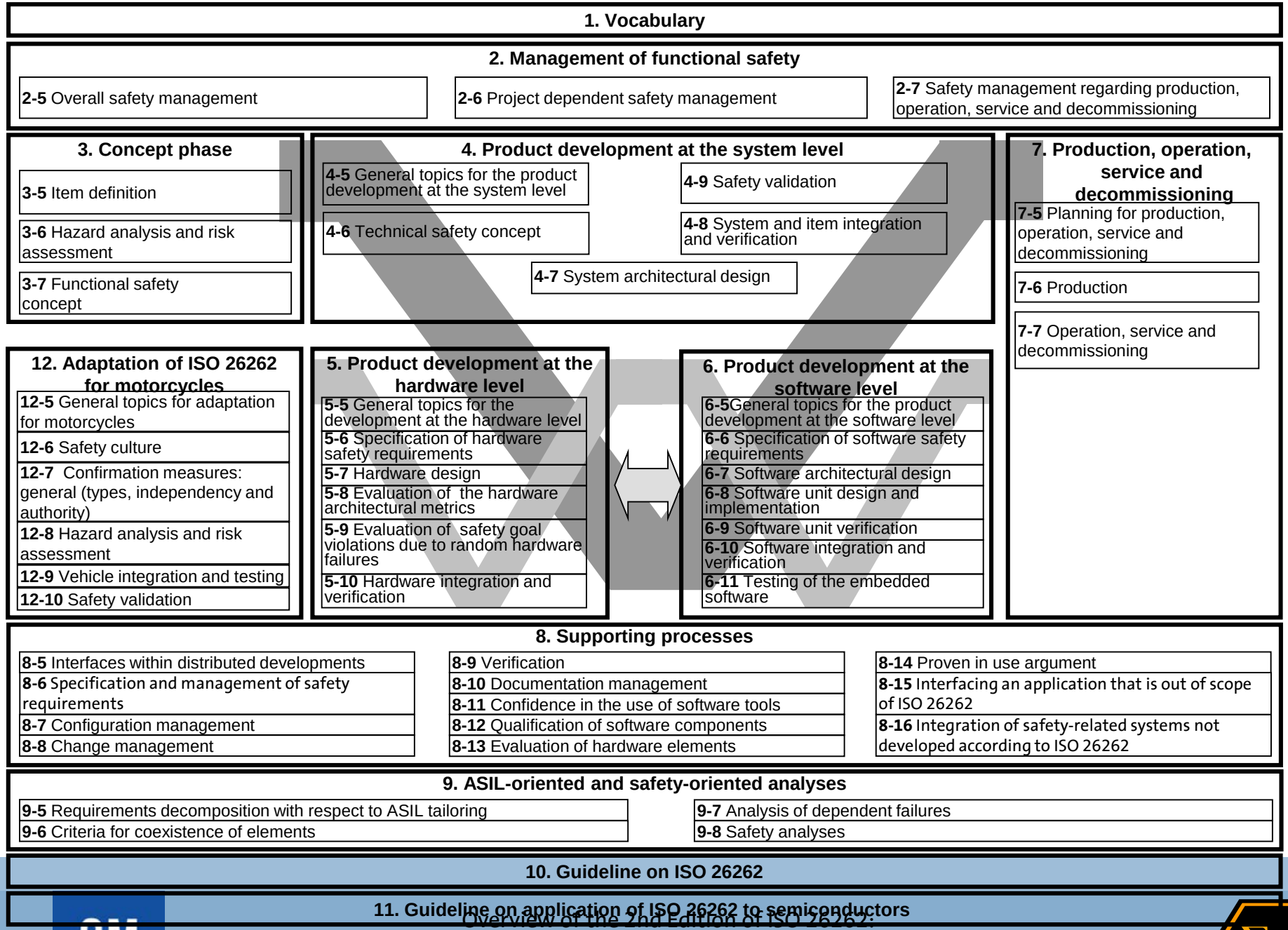
- Adaptation of IEC 61508 to comply with the specific needs of E/E systems within road vehicles
  - Specifies a functional safety life-cycle for automotive products

- Applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic, and software components
- Scope
  - Series production road vehicles excluding mopeds
- Does not apply to E/E systems in special vehicles
  - e.g., vehicles designed for drivers with disabilities

Development of ISO 26262



- ISO 26262 is developed under
  - TC 22 / SC 32 / WG 08
  - Comprised of 14 P-members
- First Edition was released in November 2011
- Due to the importance and the criticality of the automotive functional safety discipline, a review of the 1st Edition was initiated within 3 years (usually 5 years per ISO rules)
- Second Edition is at the Final Draft International Standard (FDIS) stage and expected to be released in 2018



Source ISO 26262 2nd Ed FDIS - Draft

Overview of the 2nd Edition of ISO 26262:
Functional Safety – Road Vehicles
ISSC 2018 Phoenix Arizona

ISO 26262 Terms

safety
absence of unreasonable **risk**

unreasonable risk
risk judged to be unacceptable in a certain context according to valid societal moral concepts

risk
combination of the **probability of occurrence** of harm and the **severity** of that **harm**

severity
estimate of the extent of harm to one or more individuals that can occur in a potentially hazardous situation

exposure
State of being in an operational situation that can be hazardous if coincident with the failure mode under analysis

harm
physical injury or damage to the health of persons

controllability
ability to avoid a specified harm or damage through the timely reactions of the persons involved, possibly with support from external measures

ISO 26262 Facts

- Focus is on possible hazards caused by malfunctioning behavior of E/E safety-related systems
  - failures or unintended behaviours of an item with respect to its design intent
  - random hardware failures as well as systematic failures
  - Includes interactions between E/E safety-related systems
- Corresponds to automotive product lifecycle
  - Development, validation, release for production vs. development, installation and commissioning, validation in IEC 61508
- Supports distributed development
  - e.g., division of work between OEMs/suppliers
- Includes “Controllability” in Risk Assessment

Safety Case

- Communicates a clear, comprehensive and defensible argument (supported by evidence compiled in work products) that a system is acceptably safe to operate in a particular context.

- A “safety argument” describes how the safety requirements have been interpreted, allocated, decomposed, etc., and fulfilled as shown by the supporting evidence from the work products.

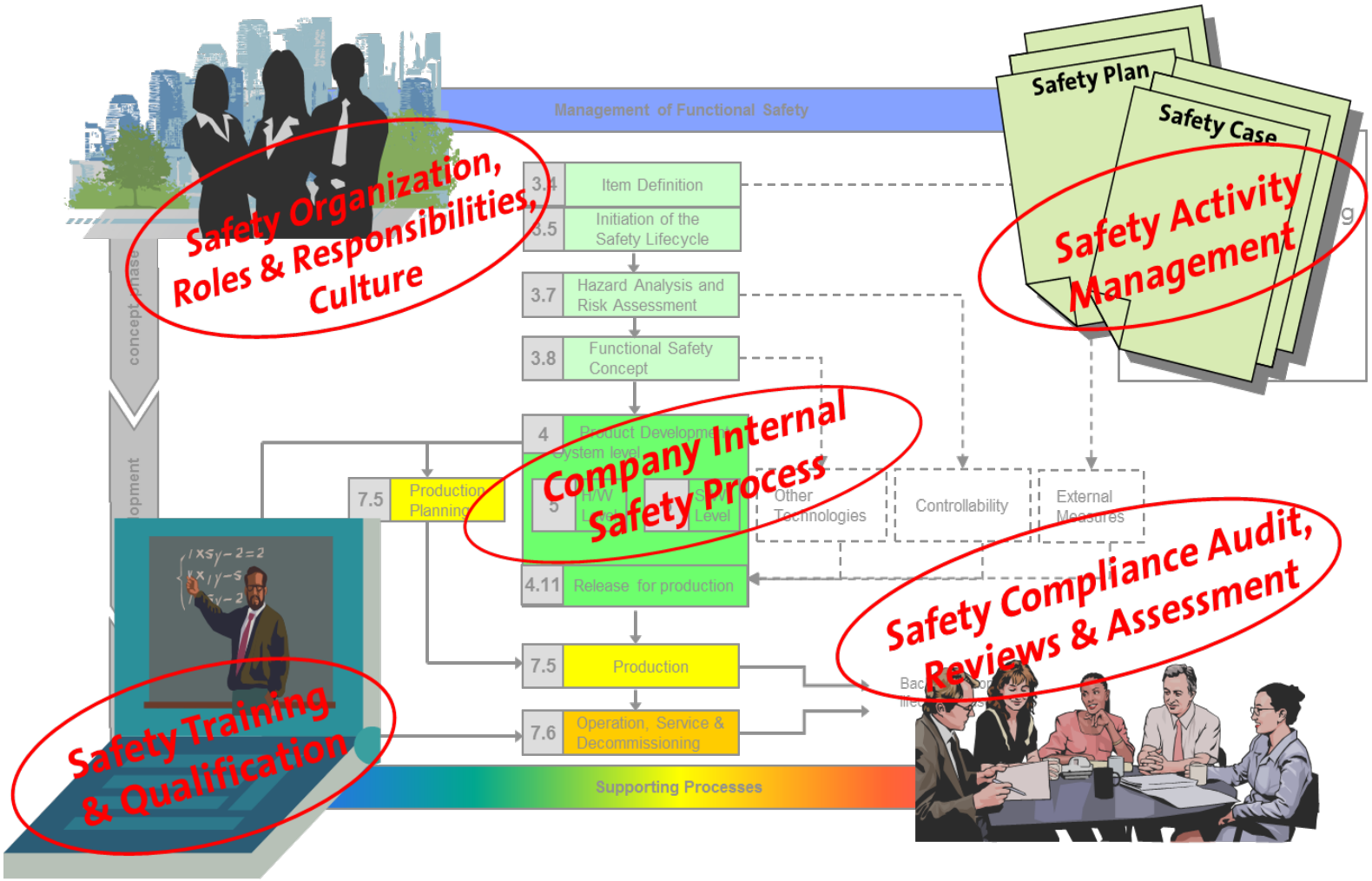
A work product is the documentation that results from an ISO 26262 requirement(s)

Functional Safety Management

- Planning, coordinating, and documenting activities related to functional safety

- Implementing management plan for all phases of the safety lifecycle, including:
  - Overall safety management
  - Project dependent safety management
  - Safety management for production, operation, service and decommissioning

Functional Safety Management



Hazard Analysis and Risk Assessment

- Item Definition
  - Vehicle, a vehicle system, or a vehicle function
  - Functional concept and operating modes; Operational and environmental constraints, Legal and applicable standard requirements, Expected behavior, Consequences of failures

- Situation Analysis & Hazard Identification
  - "Identify potential unintended behaviors of the item that could lead to a hazardous event."
    - Vehicle Usage
    - Environmental Conditions
    - Foreseeable driver use and misuse
    - Interaction between vehicle systems

Hazard Analysis and Risk Assessment

For each identified hazardous scenario, evaluate …

Severity

S0	S1	S2	S3
No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Exposure

E0	E1	E2	E3	E4
Incredible	Very low probability	Low probability	Medium probability	High probability

Controllability

C0	C1	C2	C3
Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

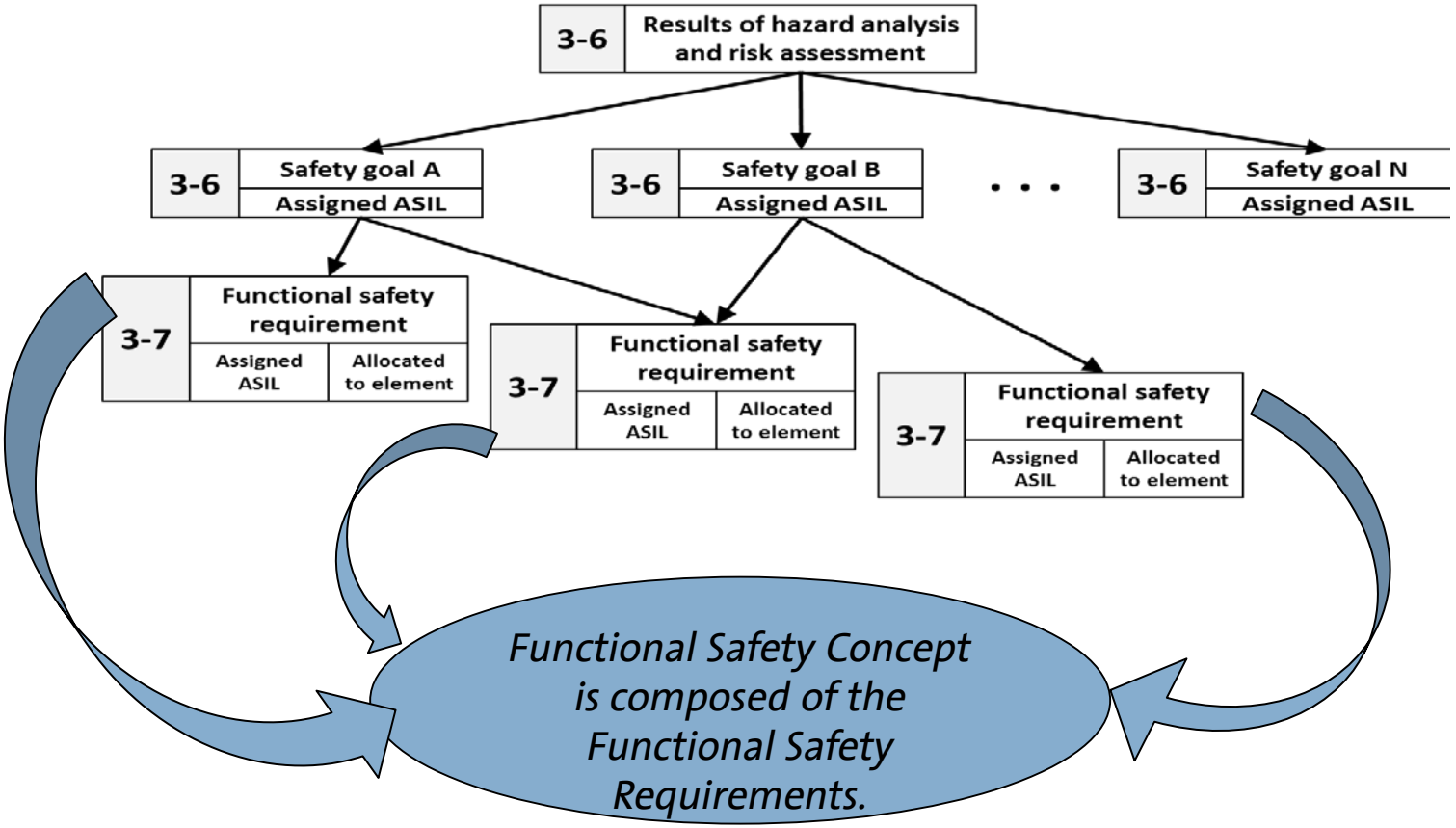
Hazard Analysis and Risk Assessment

Use Severity, Exposure, Controllability to set ASIL

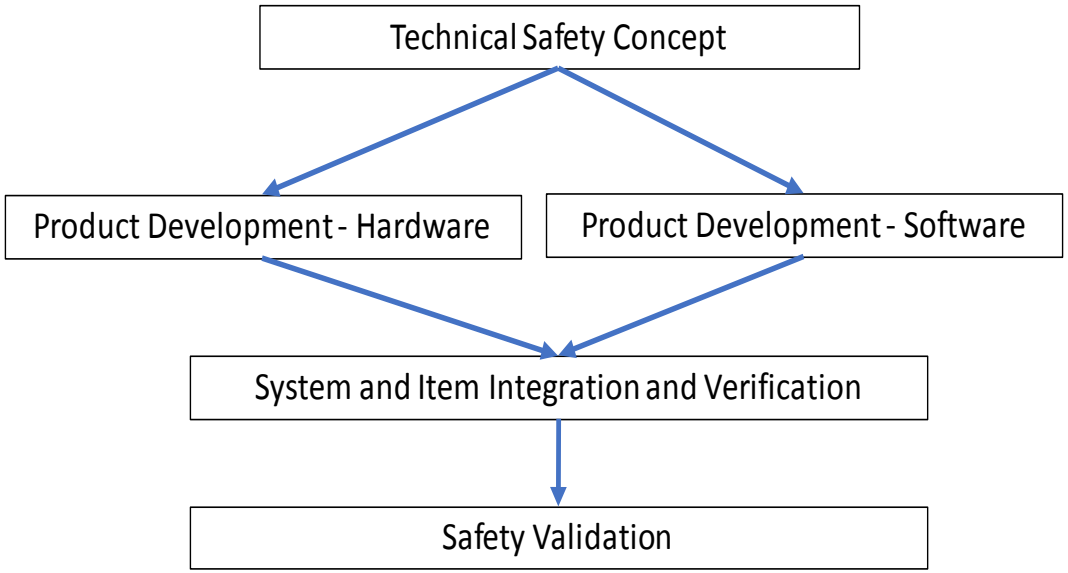
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

Functional Safety Concept

Source ISO 26262 2nd Ed. FDIS - Draft



Requirements at System Level



Technical Safety Concept

- Technical safety requirements
- Refinement of functional safety requirements defining mechanisms to detect faults and mitigate or control failures (inherit the ASIL)
- Defines system architectural design

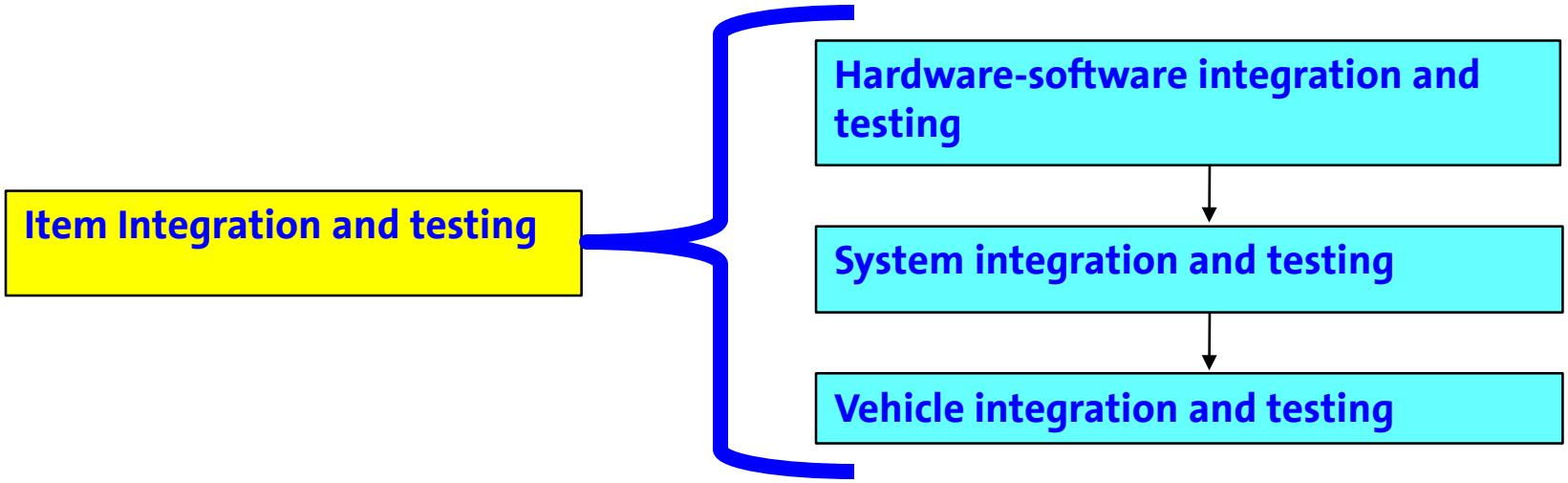
Requirements at Hardware Level

- Hardware implementation of the technical safety concept involves identification of hardware requirements
- Assignment from technical safety requirements to hardware elements given the system architectural design
- Suitability of the system architectural design is checked using
  - Assessment of single fault metric and latent fault metric. Both metrics have target values depending on the ASIL of the requirements being implemented, or
  - Evaluation of the probability of safety goals violation. Also dependent on the ASIL of the safety goal.

Requirements at Software Level

- Software safety requirements are derived from the technical safety concept and the system architectural design specification (inherit the ASIL)
- Software architectural design suitable to satisfy the software safety requirements with their respective ASILs and
- Software architectural design supports the implementation and verification of the software being developed.
  - Software unit design
  - Implementation and verification
  - Software integration and verification
  - Testing of the resulting embedded software.

Integration and Testing and Validation



- Validation of safety goals is applied to the item integrated at the vehicle level
- Validation plan includes test procedures for each safety goal with pass/fail criteria

Production, Operation, Service and Decommissioning Requirements

- Some technical safety requirements address safety concerns related to production, operation, service and decommissioning

- Develop a production process for safety-related systems to be installed in road vehicles that includes all necessary information and documentation regarding operation, maintenance and repair, and decommissioning
  - to be used by whomever is interfacing with the safety-related systems

- Field monitoring process needs to be established

Supporting Processes

Consolidate common requirements to maintain consistency

Supporting Processes

- Interfaces within distributed developments
- Specification and management of safety requirements
- Configuration management
- Change management
- Verification
- Documentation management
- Confidence in the use of software tools
- Qualification of software components
- Evaluation of hardware elements
- Proven in use argument
- Interfacing an application that is out of scope of ISO 26262
- Integration of safety-related systems not developed according to ISO 26262

Motorcycles

- Requirements of Parts 2 through 9 apply to motorcycles, however some tailoring is required
  - Requirements in Part 12 supersedes the corresponding requirements in the other parts

- The major adaptation of requirements in the case of motorcycles applies to the development of the hazard analysis and risk assessment and the determination of the S, E, and C parameters
  - Introduction of Motorcycle Safety Integrity Level
  - MSIL is mapped to the ASIL
  - Safety goals are assigned to the mapped ASIL

MSIL	ASIL
QM	QM
A	QM
B	A
C	B
D	C

Trucks and Buses

- Similar to motorcycles, requirements of Parts 2 through 9 apply to Trucks and Buses

- Any specific requirements for T&B are listed within the parts of the standard wherever they apply.

- Additional requirements are listed under

  – Functional safety management – supporting processes
  – Hazard analysis and risk assessment
  – System level validation environment
  – Production, operation, service and decommissioning

Guidelines for Semiconductor

- A necessary extension of ISO 26262 to provide guidelines for semiconductors used in automotive application.
  - Informative Part

- Semiconductor components can be developed as
  - Part of the item – safety analysis performed per Part 5 requirements
  - Safety Element out of Context (SEooC) – development is based on assumptions to be verified at integration

- Guidelines on semiconductor components

- Guidelines on semiconductor technologies

Summary

- 2nd Edition of ISO 26262 is currently on track for publication by the end of 2018

- Many improvements/additions have been implemented