ISO 26262:2018 Overview for Functional Safety Engineers

Functional Safety Management System

OMNEX

© 2019, Omnex, Inc.

315 Eisenhower Parkway Suite 214
Ann Arbor, Michigan 48108
USA
734-761-4940
Fax: 734-761-4966

Third Edition

March 2019

Omnex provides training, consulting and software solutions to the international market with offices in the USA, Canada, Mexico, China (PRC), Germany, India, the Middle East, and SE Asia. Omnex offers over 400 standard and customized training courses in business, quality, environmental, food safety, laboratory and health & safety management systems worldwide.

Email: **info@omnex.com**

Web: **www.omnex.com**

Course Objectives

- Tailor the necessary activities to support automotive safety lifecycle management, development, production, operation, service and decommissioning
- Understand the integration of ISO 26262 with APQP and IATF 16949
- Understand functional safety aspects of the entire development process (requirements specification, design, implementation, integration, verification, validation and configuration)
- Understand the automotive-specific risk-based approach for determining risk classes Automotive Safety Integrity Levels (ASILs)
- Use ASILs for specifying the necessary safety requirements for achieving an acceptable residual risk
- Provide requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved

Course Agenda

Chapter 1: Introduction and Overview to ISO 26262

Chapter 2: Management of Functional Safety (Part 2)

Chapter 3: Production and Operation (Part 7)

Chapter 4: Safety Element out of Context (Part 10)

Chapter 5: Concept Phase (Part 3)

Chapter 6: ASIL-Oriented and Safety-Oriented Analyses (Part 9)

Chapter 7: System Level Development I (Part 4)

A BRIEF INTRODUCTION TO OMNEX

Omnex Introduction

- International consulting, training and software development organization founded in 1985.
- Specialties:
  - Integrated management system solutions.
  - Elevating the performance of client organizations.
  - Consulting and training services in:
    - Quality Management Systems, e.g., ISO 9001, IATF 16949, AS9100, QOS
    - Environmental Management Systems, e.g., ISO 14001
    - Health and Safety Management Systems, e.g., ISO 45001
- Leader in Lean, Six Sigma and other breakthrough systems and performance enhancement.
  - Provider of Lean Six Sigma services to Automotive Industry via AIAG alliance.

About Omnex

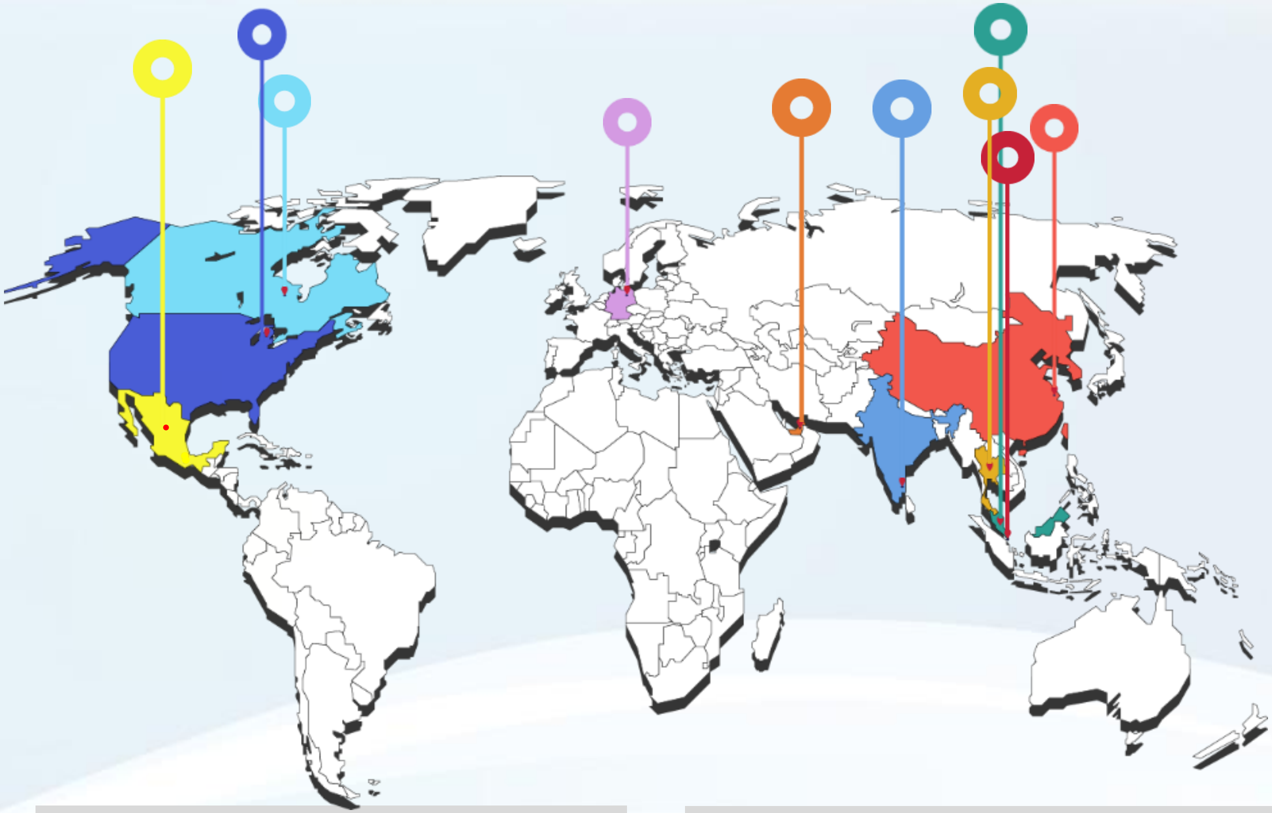
- Headquartered in Ann Arbor, Michigan with offices in major global markets.
- In 1995-97 provided global roll out supplier training and development for Ford Motor Company.
- Trained more than 100,000 individuals in over 30 countries.
- Workforce of over 400 professionals, speaking over a dozen languages.
- Former Delegation Leader of the International Automotive Task Force (IATF) responsible for ISO/TS 16949.
- Served on committees that wrote QOS, ISO 9001, QS-9000, ISO/TS 16949 and its Semiconductor Supplement, and ISO IWA 1 (ISO 9000 for healthcare).
- Former member of AIAG manual writing committees for FMEA, SPC, MSA, Sub-tier Supplier Development, Error Proofing, and Effective Problem Solving (EPS).

Omnex Worldwide Offices

Omnex is headquartered and operates from the United States through offices in Michigan.

The company maintains international operations in many countries to provide comprehensive services to clients throughout Western Europe, Latin America and the Pacific Rim.

www.omnex.com
info@omnex.com



- ● Omnex Global Head Quarters (Michigan, USA)
  West Coast Operations (San Jose, CA)
- ● Asia Pacific HQ (Chennai, Pune, Delhi, Bangalore)
- ● China (Shanghai, Guangzhou, Wuhan, Chengdu)
- ● Canada (Mississauga)
- ● Europe (Berlin, Germany)
- ● Middle East (Dubai, Saudi Arabia, Bahrain)
- ● Thailand (Bangkok)
- ● Mexico (Monterrey)
- ● Singapore
- ● Malaysia (Kuala Lumpur)

OMNEX

Rules of the Classroom

- ✓ Start and end on time
- ✓ Return from breaks and lunch on time
- ✓ All questions welcome
- ✓ Your input is valuable and is encouraged
- ✓ Don’t interrupt others
- ✓ One meeting at a time
- ✓ Listen – and respect others’ ideas
- ✓ No “buts” – keep an open mind
- ✓ Phones in Do Not Disturb (silent) mode
- ✓ No e-mails, texting or tweeting during class

If you must take a phone call or answer a text please leave the room for as short a period as possible

Icebreaker

- Instructor Information:
  - Name
  - Background

- Participant Introductions:
  - Name
  - Position / Responsibilities
  - What is your involvement in functional safety?
  - What are your experiences with functional safety?
  - *What do you expect to get out of this course?*
  - Please share something unique and/or interesting about yourself.

Chapter 1

Introduction and Overview to ISO 26262

ISO 26262: Functional Safety Management

Purpose of ISO 26262

- Safety is a key issue of automobile development.
- New functionalities and increasing content in electrical, electronics (E/E) and software requires increased focus on interface issues.
- With the increase in technological complexity, software content and mechatronic implementations there is an increase in systematic and random failures.

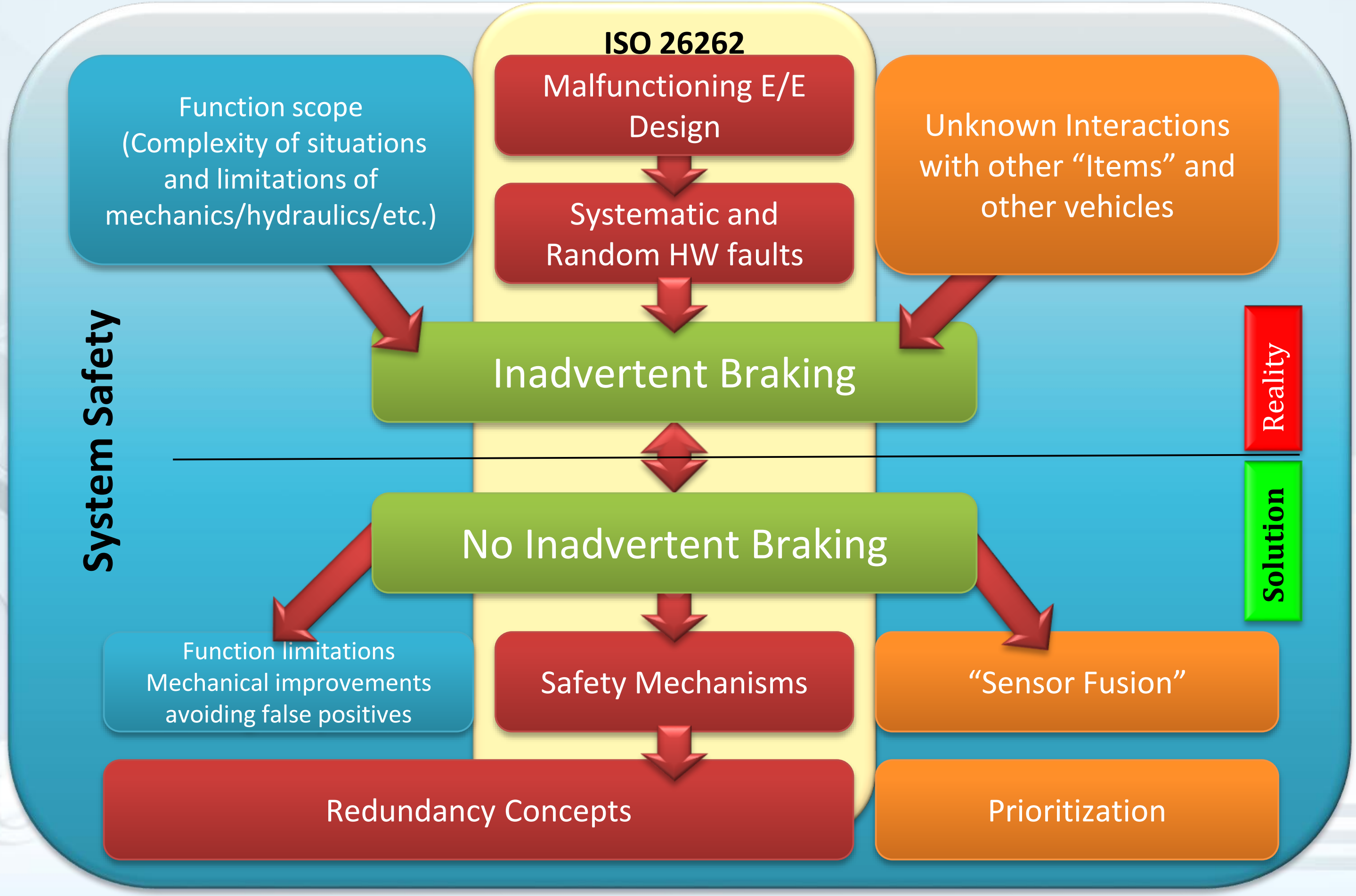
ISO 26262 provides a framework to enable Safety Management for E/E as well as other technologies

OMNEX

ISO 26262 Scope

- Addresses possible **hazards caused by malfunctioning behavior** of E/E safety-related systems including interaction of these systems that are installed in series production road vehicles, excluding mopeds.
  - It ***does not address*** hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless ***directly*** caused by malfunctioning behavior of E/E safety-related systems.
  - Not applied to address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.
- **However, ISO 26262 is *not* a system safety standard…**
  - It ***does not address*** the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems.

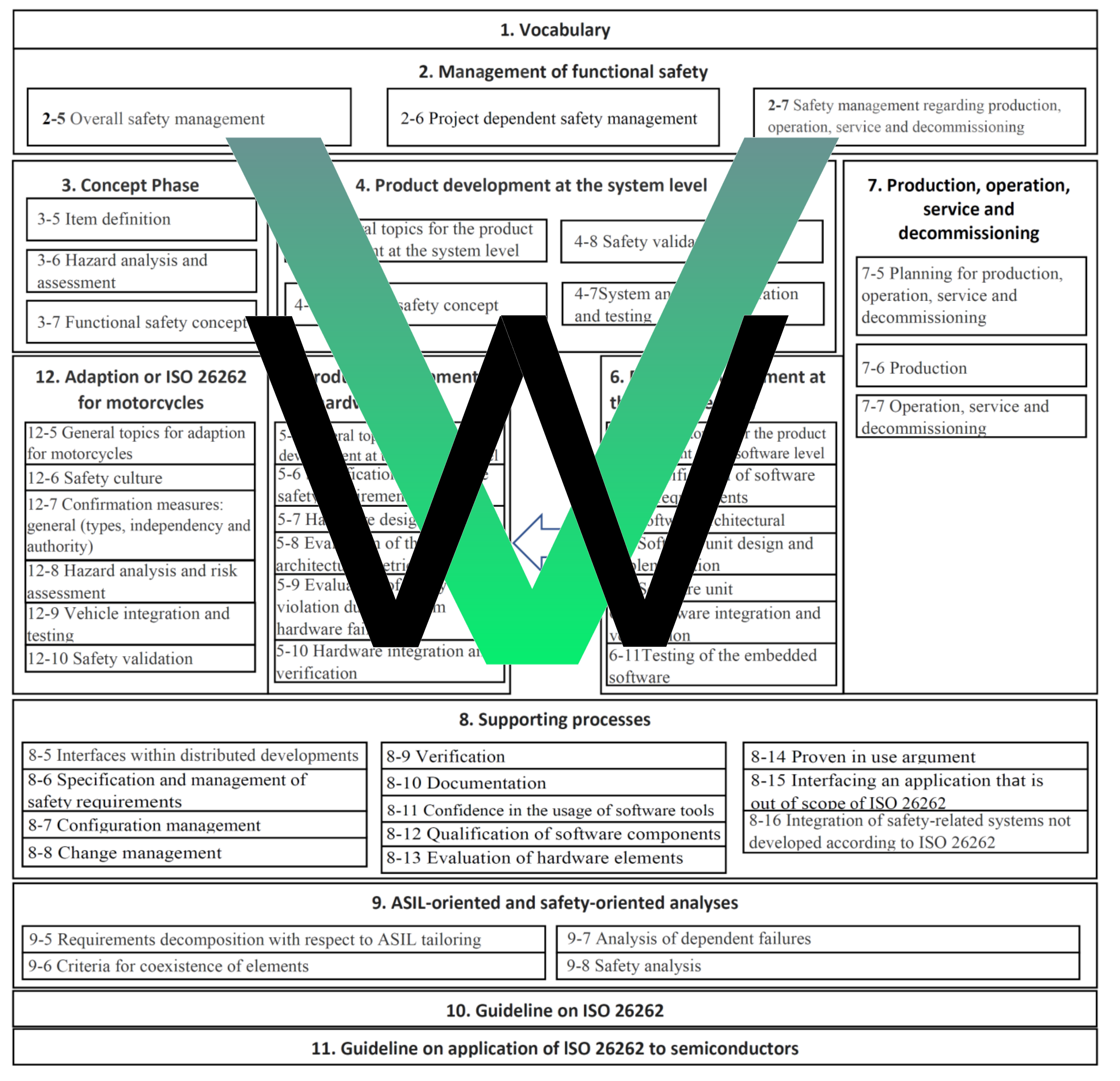
Addressing System Safety


ISO 26262
Function scope (Complexity of situations and limitations of mechanics/hydraulics/etc.)
Malfunctioning E/E Design
Systematic and Random HW faults
Unknown Interactions with other "Items" and other vehicles
System Safety
Inadvertent Braking
Reality
Solution
No Inadvertent Braking
Function limitations Mechanical improvements avoiding false positives
Safety Mechanisms
"Sensor Fusion"
Redundancy Concepts
Prioritization

ISO 26262 Framework

- Provides an automotive lifecycle that can be customized for your organizations (**tailoring**)
- Provides an automotive specific risk-based approach for determining safety integrity levels (Automotive Safety Integrity Levels (**ASILs**))
- Uses ASIL levels to prioritize application of risk prevention techniques
- Provides requirements of validation and confirmation measures to ensure a sufficient and acceptable level of safety is being achieved
- Provides requirements for supplier management / interface

ISO 26262 – 12 Parts



1. Vocabulary

2. Management of functional safety

- 2-5 Overall safety management
- 2-6 Project dependent safety management
- 2-7 Safety management regarding production, operation, service and decommissioning

3. Concept Phase

- 3-5 Item definition
- 3-6 Hazard analysis and assessment
- 3-7 Functional safety concept

4. Product development at the system level

- al topics for the product nt at the system level
- 4-8 Safety valida
- 4- safety concept
- 4-7System an ation and testing

7. Production, operation, service and decommissioning

- 7-5 Planning for production, operation, service and decommissioning
- 7-6 Production
- 7-7 Operation, service and decommissioning

12. Adaption or ISO 26262 for motorcycles

- 12-5 General topics for adaption for motorcycles
- 12-6 Safety culture
- 12-7 Confirmation measures: general (types, independency and authority)
- 12-8 Hazard analysis and risk assessment
- 12-9 Vehicle integration and testing
- 12-10 Safety validation

rod ment ardw

- 5- ral top dev ent at l
- 5-6 ication e safety iremen
- 5-7 Ha e desig
- 5-8 Eva n of th architectu etri
- 5-9 Evalua of y violation du m hardware fai
- 5-10 Hardware integration ar verification

6. ment at th e

- o r the product nt software level
- ifi of software eq ents
- oftw chitectural
- Soft unit design and plem ion
- S re unit
- ware integration and v ion
- 6-11Testing of the embedded software

8. Supporting processes

- 8-5 Interfaces within distributed developments
- 8-6 Specification and management of safety requirements
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Confidence in the usage of software tools
- 8-12 Qualification of software components
- 8-13 Evaluation of hardware elements
- 8-14 Proven in use argument
- 8-15 Interfacing an application that is out of scope of ISO 26262
- 8-16 Integration of safety-related systems not developed according to ISO 26262

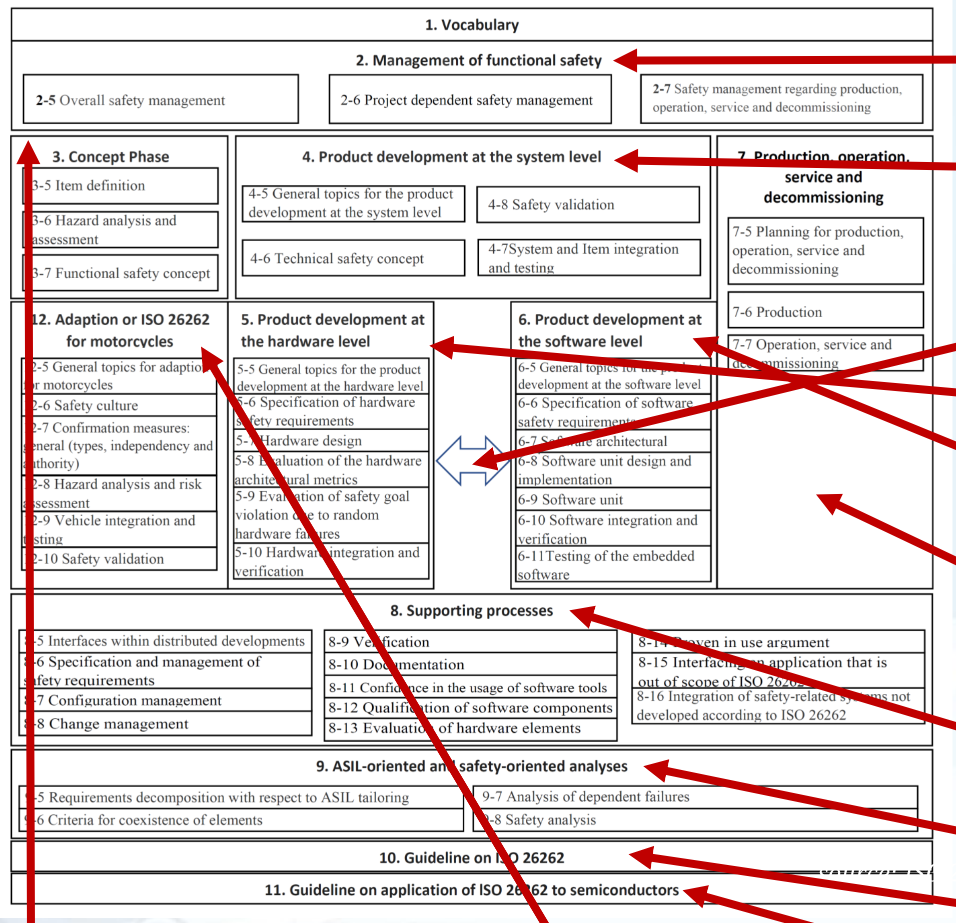
9. ASIL-oriented and safety-oriented analyses

- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of elements
- 9-7 Analysis of dependent failures
- 9-8 Safety analysis

10. Guideline on ISO 26262

11. Guideline on application of ISO 26262 to semiconductors

ISO 26262 — Parts 2 Through 12



1. Vocabulary

2. Management of functional safety

- 2-5 Overall safety management
- 2-6 Project dependent safety management
- 2-7 Safety management regarding production, operation, service and decommissioning

3. Concept Phase

- 3-5 Item definition
- 3-6 Hazard analysis and assessment
- 3-7 Functional safety concept

4. Product development at the system level

- 4-5 General topics for the product development at the system level
- 4-6 Technical safety concept
- 4-8 Safety validation
- 4-7System and Item integration and testing

7. Production, operation, service and decommissioning

- 7-5 Planning for production, operation, service and decommissioning
- 7-6 Production
- 7-7 Operation, service and decommissioning

12. Adaption or ISO 26262 for motorcycles

- 12-5 General topics for adaption for motorcycles
- 12-6 Safety culture
- 12-7 Confirmation measures: general (types, independency and authority)
- 12-8 Hazard analysis and risk assessment
- 12-9 Vehicle integration and testing
- 12-10 Safety validation

5. Product development at the hardware level

- 5-5 General topics for the product development at the hardware level
- 5-6 Specification of hardware safety requirements
- 5-7 Hardware design
- 5-8 Evaluation of the hardware architectural metrics
- 5-9 Evaluation of safety goal violation due to random hardware failures
- 5-10 Hardware integration and verification

6. Product development at the software level

- 6-5 General topics for the product development at the software level
- 6-6 Specification of software safety requirements
- 6-7 Software architectural
- 6-8 Software unit design and implementation
- 6-9 Software unit
- 6-10 Software integration and verification
- 6-11Testing of the embedded software

8. Supporting processes

- 8-5 Interfaces within distributed developments
- 8-6 Specification and management of safety requirements
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Confidence in the usage of software tools
- 8-12 Qualification of software components
- 8-13 Evaluation of hardware elements
- 8-14 Proven in use argument
- 8-15 Interfacing an application that is out of scope of ISO 26262
- 8-16 Integration of safety-related systems not developed according to ISO 26262

9. ASIL-oriented and safety-oriented analyses

- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of elements
- 9-7 Analysis of dependent failures
- 9-8 Safety analysis

10. Guideline on ISO 26262

11. Guideline on application of ISO 26262 to semiconductors

Part 2 – Functional Safety Management System

Part 4 – Technical Safety Concept, Testing, Validation and Integration – System

Parts 4-6 – Hardware-Software Interface

Part 5 – Hardware Safety Concept, Testing, Validation and Integration

Part 6 – Software Safety Concept, Testing, Validation and Integration

Part 7 – Process Control in Pre-production, Production, Service (maintenance and repair) and Decommissioning

Part 8 – Support Processes

Part 9 – ASIL-oriented and Safety-oriented Analysis

Part 10 – 26262 Guidelines

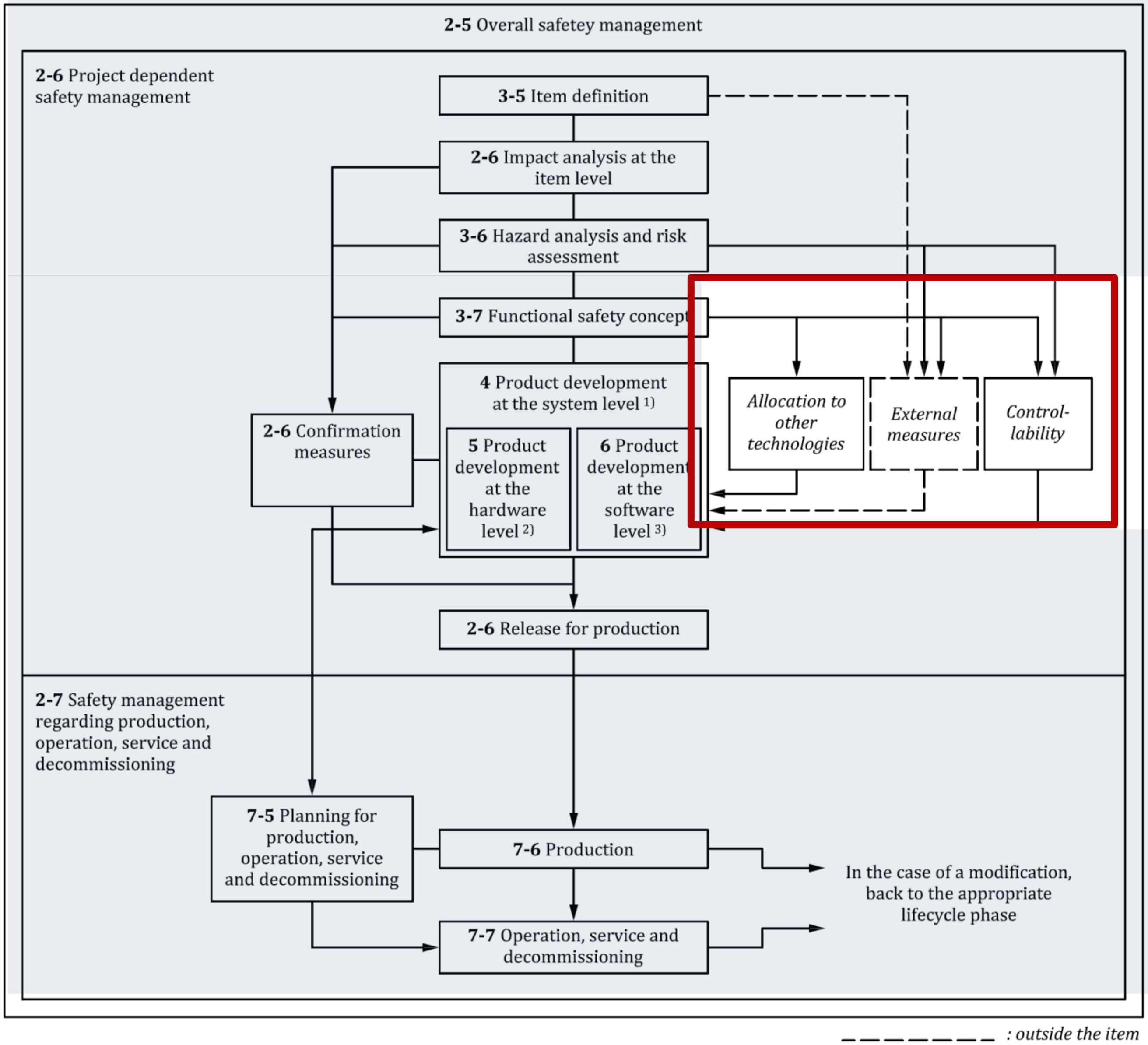
Part 11 – Semiconductor Guidelines

Part 3 – Item Definition Hazard Analysis and Risk Assessment and the Functional Safety Concept

Part 12 – Motorcycles

The Safety Lifecycle

Includes Allocation to Other Technologies



2-5 Overall safetey management

2-6 Project dependent safety management

3-5 Item definition

2-6 Impact analysis at the item level

3-6 Hazard analysis and risk assessment

3-7 Functional safety concept

4 Product development at the system level 1)

5 Product development at the hardware level 2)

6 Product development at the software level 3)

2-6 Confirmation measures

Allocation to other technologies

External measures

Control-lability

2-6 Release for production

2-7 Safety management regarding production, operation, service and decommissioning

7-5 Planning for production, operation, service and decommissioning

7-6 Production

7-7 Operation, service and decommissioning

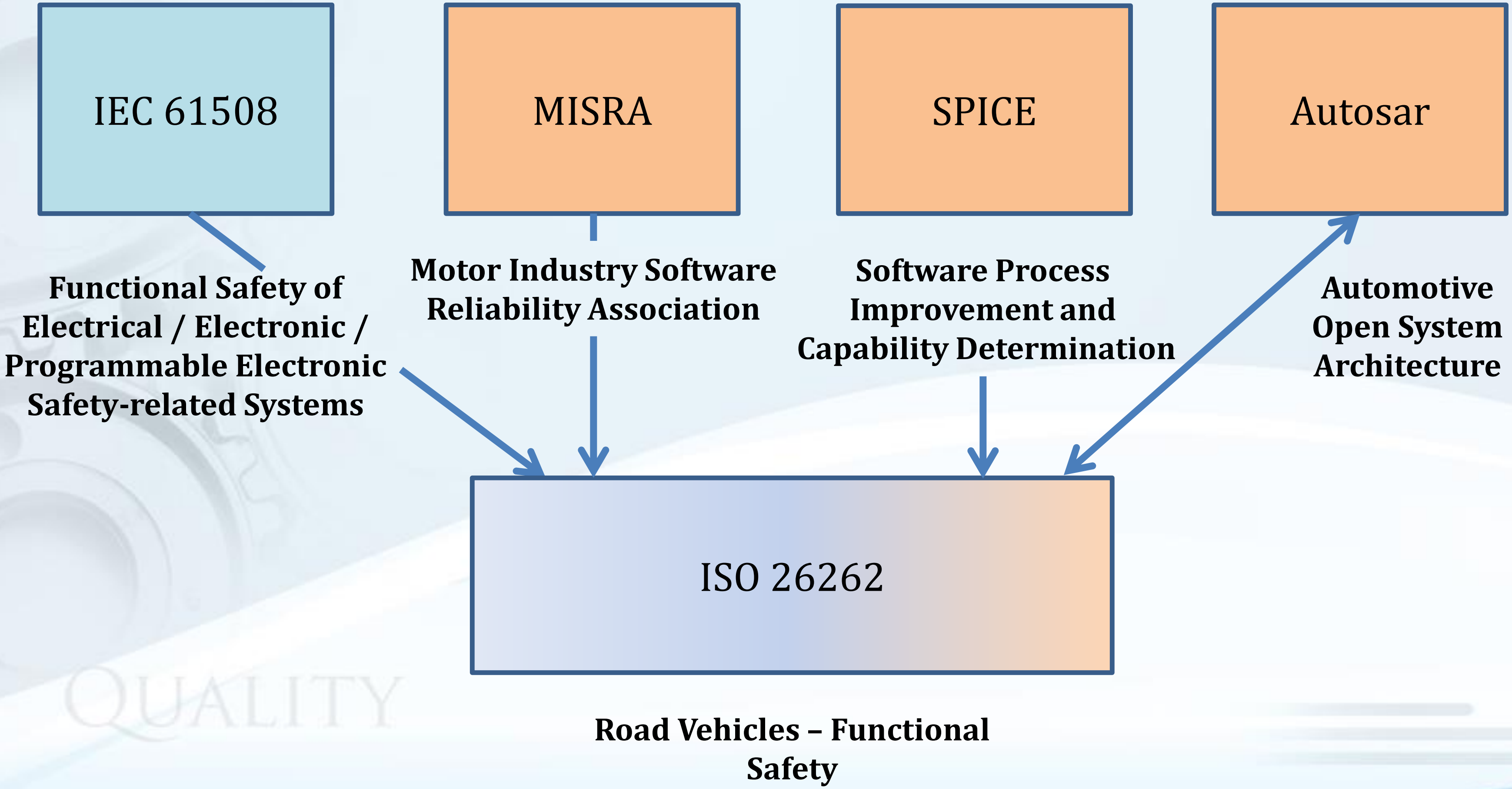
In the case of a modification, back to the appropriate lifecycle phase

: outside the item

source: ISO 26262 Part 2

OMNEX

ISO 26262 Influences



IEC 61508

Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems

MISRA

Motor Industry Software Reliability Association

SPICE

Software Process Improvement and Capability Determination

Autosar

Automotive Open System Architecture

ISO 26262

Road Vehicles – Functional Safety

ISO 26262 Drivers

Customers are driving ISO 26262

- Initially European Manufacturers:
  - BMW
  - Mercedes
  - VOLVO
  - Bosch
  - …etc.

Now
- General Motors
- Ford
- FCA / Chrysler
- ….. etc.

- Europeans also believe that *litigation will drive more* *o.m.n.ex* *organizations toward conformance*.
  - Definition of "Published State of the Art" as it relates to Automotive Safety.
  - VDA in Germany has defined Best-Practice as IEC-61508 and ISO 26262.

The Need for 26262

Vehicle’s E/E systems are complex and are growing rapidly

Platform Golf IV (1998)	Platform Golf V (2003)	Platform Golf VI (2010)
	Central Gateway	Central Gateway
17 ECUs	35 ECUs	49 ECUs
2 CANs	5 CANs, 3 LINs	5 CANs, 7 LINs
147 CAN-Messages	307 CAN-Messages	704 CAN-Messages
434 CAN signals	2669 CAN signals	6516 CAN signals

Source: Lisa Whalen, *Making Products and Systems Functionally Safe*, 2012 CTi Conference on ISO 26262, Troy, MI

The Need for 26262

Complex Vehicle Software Size (lines of code)

F-22 Raptor
1.7 Million

F-35 Joint Strike Fighter
5.7 Million

Boeing 787 Dreamliner
6.5 Million
avionics and onboard support systems

2016 Ford GT
10 Million (mission critical)

2014 Mercedes S-Class
65 million lines of code

FROST & SULLIVAN

~200-300 Million
(predicted future)

General Requirements

When claiming compliance with the ISO 26262 series of standards, each requirement shall be met, unless one of the following applies:

- Tailoring of the safety activities in accordance with ISO 26262-2 has been performed that shows that the requirement does not apply,

– or –

- A rationale is available that the non-compliance is acceptable and the rationale has been evaluated in accordance with ISO 26262-2.

ASIL Notation

1. ASIL levels are A, B, C, and D
   - A QM designation denotes no additional requirements (other than the Quality Management System) to comply with ISO 26262.
2. The requirements or recommendation of each sub-clause shall comply with the ASIL Level of the corresponding Safety Goal.
3. **In the standard,** if an ASIL is shown in parentheses, such as **ASIL (A)** for example, the corresponding requirement shall be considered as optional for the ASIL.
4. If ASIL decomposition is used, each decomposed ASIL shall be marked by giving the ASIL of the safety goal in parenthesis.
   - The notation will be **ASIL B(D)** which indicates that the element can be developed as an ASIL B but confirmation measures must be in accordance with the ASIL of the safety goal, D;
   - Evidence for sufficient independence of the elements after decomposition shall be made available.

ASIL-Dependent Tables

In Parts 4 through 6 many requirements and methods are dependent on the determined ASIL for an element.

1. Tables are normative or informative depending on their context.
2. The different methods listed in a table contribute to the level of confidence in achieving compliance with the corresponding requirements. Each method in a table is either:
   a) A consecutive entry (marked by a sequence number in the leftmost column, e.g., 1, 2, 3); or
   b) An alternative entry (marked by a number followed by a letter in the leftmost column, e.g., 2a, 2b, 2c); or
   c) A combination of a and b.

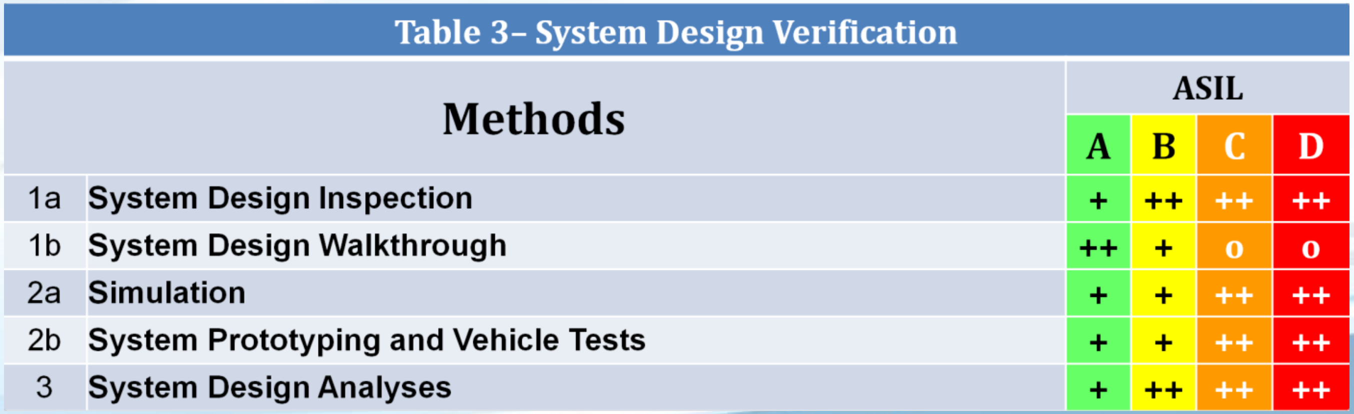


Table 3– System Design Verification

Methods		ASIL			
		A	B	C	D
1a	System Design Inspection	+	++	++	++
1b	System Design Walkthrough	++	+	o	o
2a	Simulation	+	+	++	++
2b	System Prototyping and Vehicle Tests	+	+	++	++
3	System Design Analyses	+	++	++	++

ASIL Driven Activities

Example: Table 3 – System Design Verification

Table 3– System Design Verification

Methods		ASIL			
		A	B	C	D
1a	System Design Inspection	+	++	++	++
1b	System Design Walkthrough	++	+	o	o
2a	Simulation	+	+	++	++
2b	System Prototyping and Vehicle Tests	+	+	++	++
3	System Design Analyses	+	++	++	++

For each method, the degree of recommendation to use the corresponding method depends on the ASIL and is categorized as follows:

++ The method is highly recommended for the identified ASIL.

+ The method is recommended for the identified ASIL.

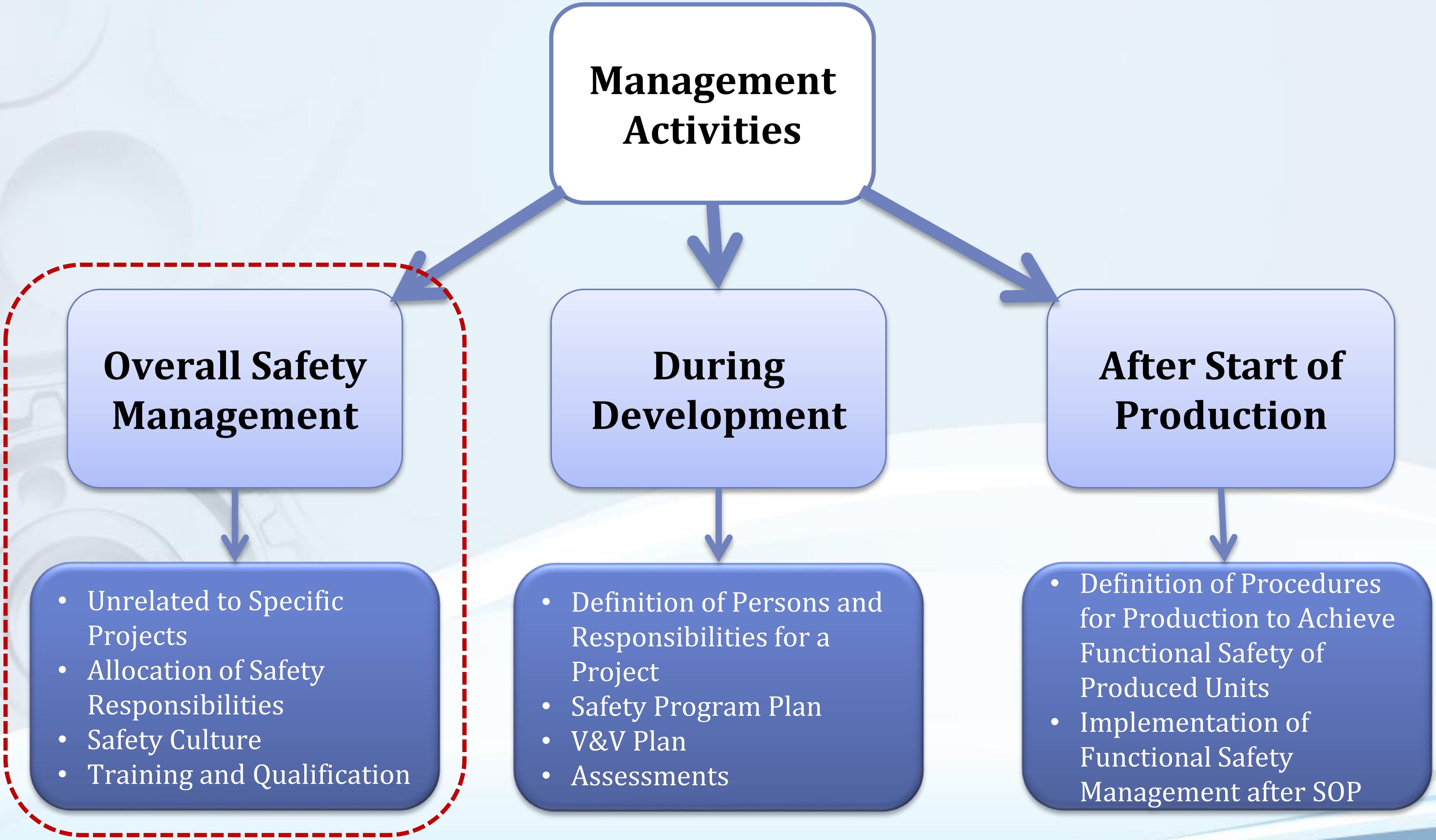
o The method has no recommendation for or against its usage for the identified ASIL.

Chapter 2

Management of Functional Safety (Part 2)

OMNEX

Functional Safety Management Activities



Management Activities

Overall Safety Management

- Unrelated to Specific Projects
- Allocation of Safety Responsibilities
- Safety Culture
- Training and Qualification

During Development

- Definition of Persons and Responsibilities for a Project
- Safety Program Plan
- V&V Plan
- Assessments

After Start of Production

- Definition of Procedures for Production to Achieve Functional Safety of Produced Units
- Implementation of Functional Safety Management after SOP

Overall Safety Management

Objectives

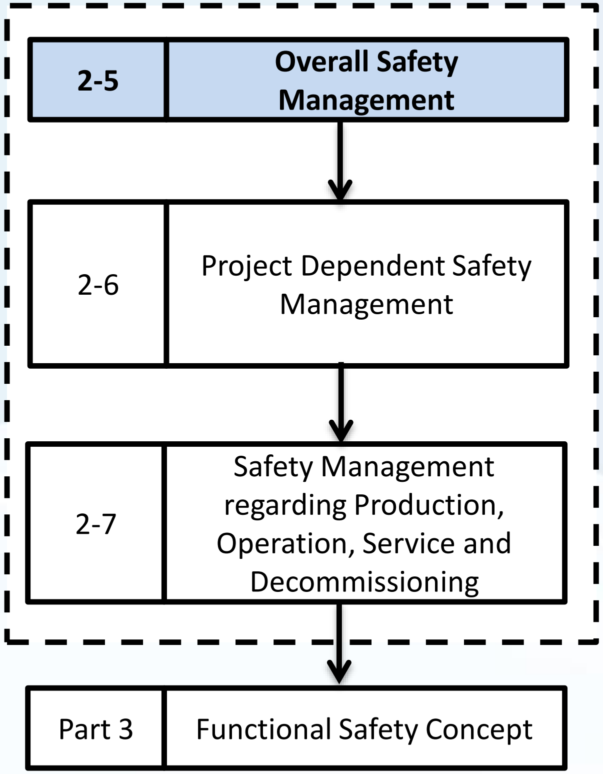
- Define the requirements for the organizations that are responsible for the safety lifecycle, or that perform safety activities in the safety lifecycle.
- Serve as a prerequisite to the activities in the ISO 26262 safety lifecycle.

Prerequisites

- None

Work Products

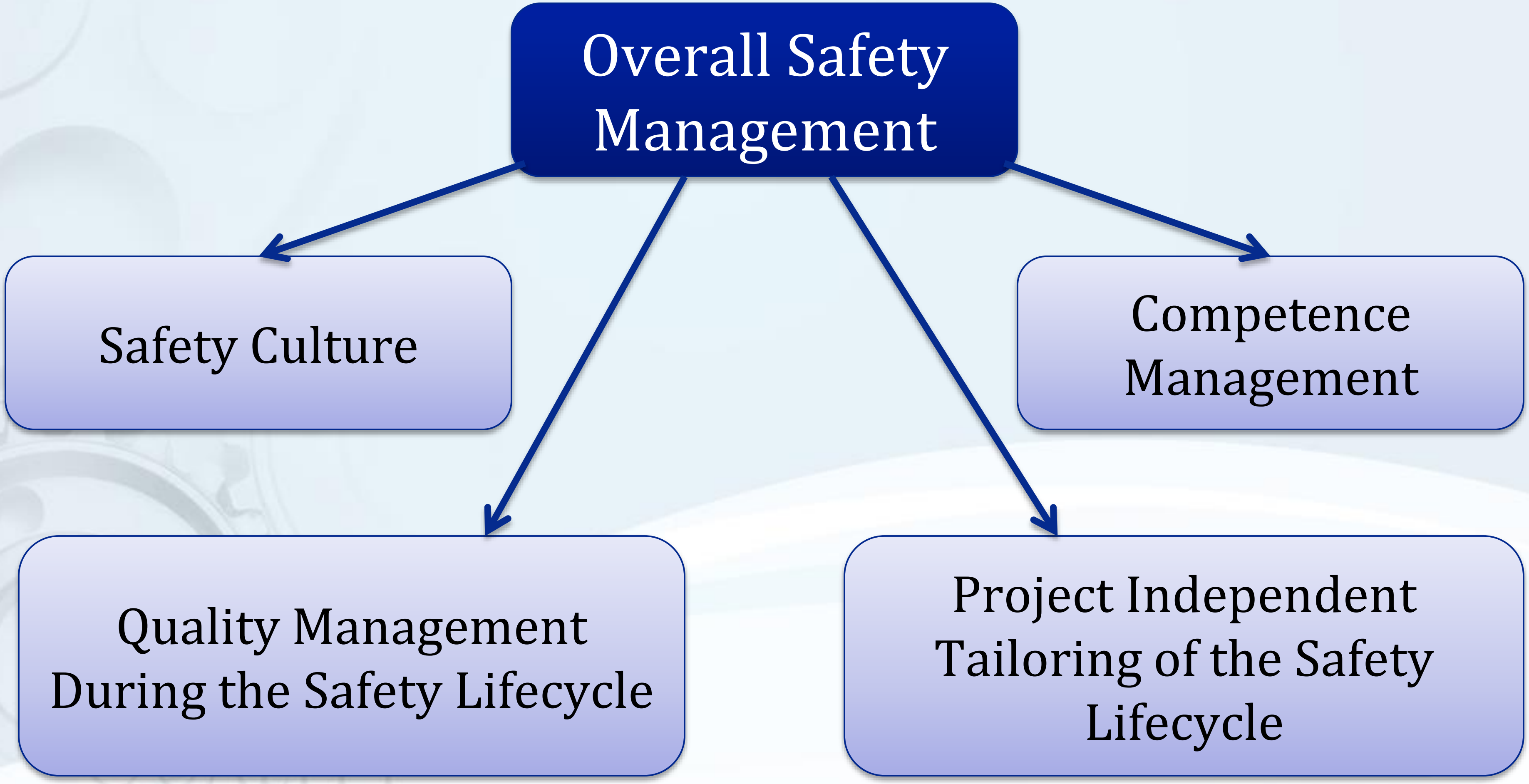
- Organization-specific rules and processes for functional safety
- Evidence of competence management
- Evidence of quality management system
- Identified safety anomaly reports


2-5
Overall Safety Management
2-6
Project Dependent Safety Management
2-7
Safety Management regarding Production, Operation, Service and Decommissioning
Part 3
Functional Safety Concept

Work Products

- A result of one or more associated requirements of the safety plan/ISO 26262.
  - Evidence of compliance to one or more system safety requirements.
- A work product is not required to be a separate document.
  - The information can be included in existing documentation, or several work products can be included in one document.
- Be sure to create a "roadmap" of where all required work products are located.
- Often referred to as "mapping" from what you have, to what is required, then noting your gaps to be filled.

Components of Overall Safety Management



Overall Safety Management

Safety Culture

Competence Management

Quality Management During the Safety Lifecycle

Project Independent Tailoring of the Safety Lifecycle

Overall Safety Management

- **5.4.2 Safety Culture**
  - **(5.4.2.1)** The organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety.
- **5.4.3 Management of Safety Anomalies Regarding Functional Safety**
- **5.4.4 Evidence of Competence**
  - Competence management in ISO 26262 will be satisfied by requirements in 6.2 in IATF 16949.
- **5.4.5 Quality Management System**
  - At a minimum ISO 26262 requires ISO 9001 conformance.
- **5.4.6 Project-independent Tailoring of the Safety Lifecycle**

Safety Culture

- In order to be able to develop safe systems,
  ISO acknowledged the need for a **Safety Culture**.
- Your vision should encompass safety, such as:

"To reduce accidents and save lives"

- **Safety culture is hard to fully understand, but there are ways to see if a company will succeed.**

Safety Culture

- **(5.4.2.1)** The organization shall create, foster, and sustain a safety culture that supports and encourages the effective achievement of functional safety.
  - Examples for evaluating a safety culture are given on the next slide.
- **(5.4.2.2)** The organization shall institute, execute and maintain organization-specific rules and processes to comply with the requirements of ISO 26262.
  - NOTE: Such organization-specific rules and processes can include the creation and maintenance of a generic safety plan and process description.

The Quality Culture of Safety Management — Examples

1. **Safety as a Top Priority**
   - In every business decision, give safety a high status in the business objectives.
2. **Management Commitment to Safety**
   - Leadership by example. Challenge unsafe behavior.
3. **Increasing Visibility Around Safety**
   - Conducting safety audits and safety workarounds. Demonstrates commitment.
4. **Report on Safety**
   - Frontline reporting of safety issues (e.g., accidents, near misses and safety concerns).
   - Professional public relations management (if required) regarding actions taken.
   - Promptly react to incidents in a positive learning way.
   - Take strong corrective actions. Send clear message to eliminating the next injury.

The Quality Culture of Safety Management — Examples

5. **Staff Involvement**
   - Active employee participation is essential towards preventing and controlling hazards.
   - Providing effective training and forums to assist employees in personal safety contribution.
   - Easy feedback mechanism to report concerns.
6. **Create a Learning Curve**
   - Learn what a good safety performance means in your job and contribute ideas for improvement.
7. **Provide Recognition**
   - Recognize the achievements of employees who improve safety in the organization.

The Quality Culture of Safety Management — Examples

8. **Open Culture**
   - Encourage the reporting of issues or concerns without fear of personal blame.
   - Create an open door policy for safety issues.
9. **Effective Communication**
   - Clearly communicate the safety policy in a visible way.
   - Communicate major incidents.
10. **Safety Management System**
    - Assign a Safety Coordinator and Top Level Management Sponsor.
    - Monitor performance and make it transparent.

Safety Culture

- **(5.4.2.3)** The organization *shall institute and maintain effective communication channels* between functional safety, **cybersecurity**, and other disciplines that are related to the achievement of functional safety**.**
- **(5.4.2.4)** During the execution of the safety lifecycle, the organization shall perform the required safety activities, including the creation and management of the associated documentation in accordance with **ISO 26262-8:2018, Clause 10 (Documentation Management**).
- **(5.4.2.5)** The organization shall provide the resources required for the achievement of functional safety.
  - NOTE: Resources include human resources, tools, databases, guidelines and work instructions.

Safety Culture

- **(5.4.2.6)** The organization shall institute, execute and maintain a ***continuous improvement process***, based on:
  - Learning from the experiences gained during the execution of the safety lifecycle of other items, including field experience; and O-M-N-E-X
  - Derived improvements for application on subsequent items.
- **(5.4.2.7)** The organization shall ensure that the persons responsible for achieving or maintaining functional safety, or for performing or supporting the safety activities, are given sufficient authority to fulfil their responsibilities.

Management of Safety Anomalies Regarding Functional Safety

- **(5.4.3)** The organization shall institute, execute and maintain processes to ensure that:
  - **(5.4.3.1) I**dentified safety anomalies are explicitly communicated to the persons responsible for achieving or maintaining functional safety during the safety lifecycle.
  - **5.4.3.2** (safety anomaly resolution process) Identified safety anomalies are analyzed, evaluated, resolved and managed to closure in a timely and effective manner.
- **(5.4.3.3)** A safety anomaly shall only be considered as managed to closure if:

a) an adequate safety measure is implemented that resolves the safety anomaly, based on a rationale; and the effectiveness of the safety measure is verified, or external measures (e.g. measures outside the scope of the ISO 26262 series of standards).

b) the safety anomaly is evaluated as not constituting an unreasonable risk and is closed, based on a rationale.

Management of Safety Anomalies Regarding Functional Safety

- **(5.4.3.4)** The rationale for a safety anomaly managed to closure, in accordance with **5.4.3.3**, shall be documented; and shall be reviewed.
  - The rationale can be reviewed as part of the functional safety assessment.
- **(5.4.3.5)** Safety anomalies that are not managed to closure shall be escalated to the persons responsible for functional safety, such as the project manager in the case of a safety anomaly regarding product development.

Competence Management

(5.4.4) The organization shall ensure that the persons involved in the execution of the safety lifecycle have a sufficient level of skills, competence and qualification corresponding to their responsibilities.

- Training and qualification program:
  - Safety practices and concepts in design;
  - ISO 26262 and other applicable standards;
  - Organization-specific rules for functional safety;
  - Functional safety processes.
- Previous professional activities including
  - Domain knowledge of the item;
  - Expertise on the environment of the item;
  - Management experience.

Example Skills:

- **Fault Tree Analysis**
- **FMEA**
- **Development of a HARA**
- **ASIL Determination**
- **Application of Safety Mechanisms**
- **ASIL Decomposition**
- **Development of Safety Case**
- **Reliability Analysis**
- **Development of Test Cases**
- **Testing for Reliability**
- **Structural Metrics Analysis**
- **Etc.**

Quality Management System

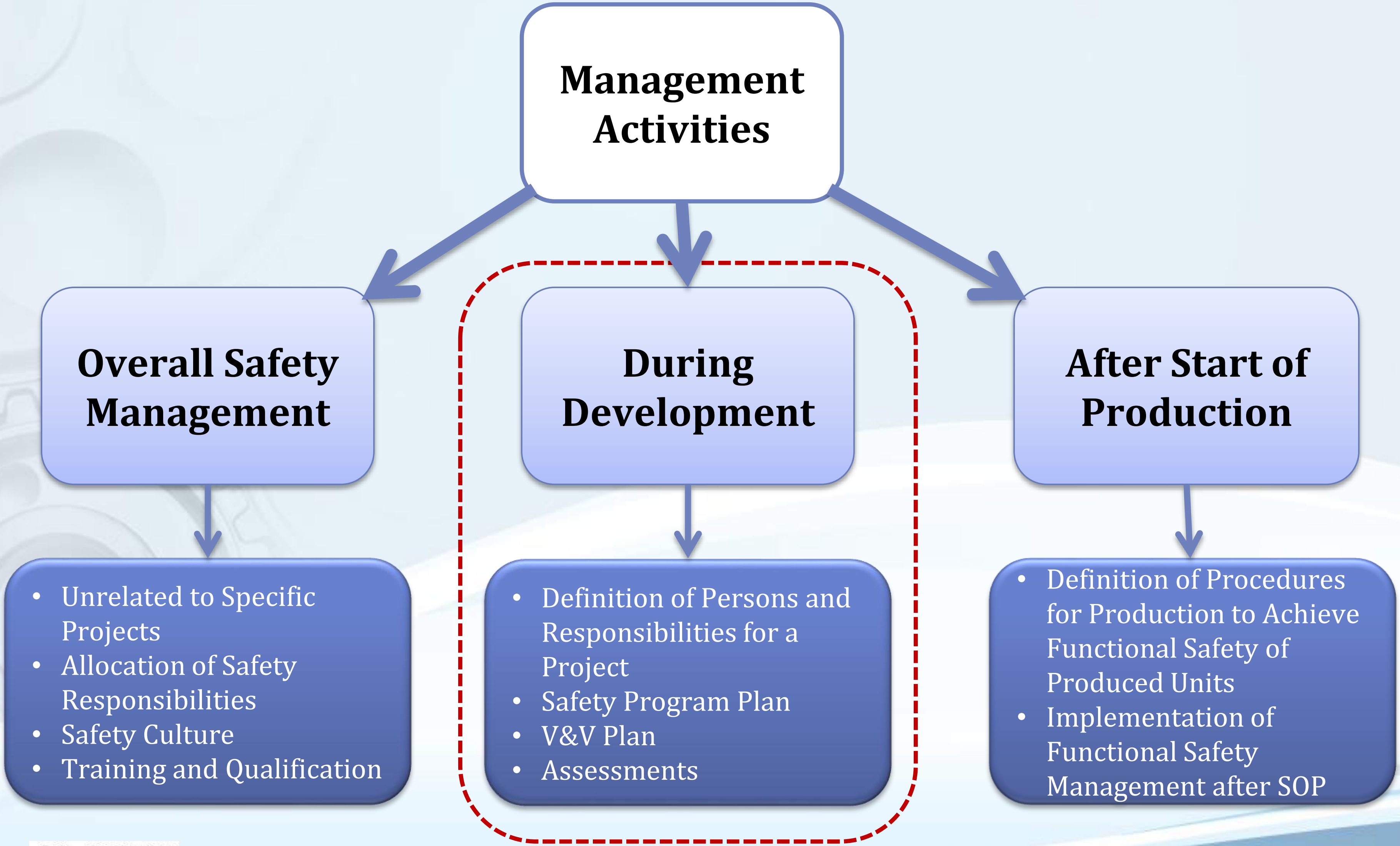
(5.4.5.1) The organization shall have a quality management system that supports achieving functional safety and complies with a quality management standard, such as IATF 16949 in conjunction with ISO 9001, or equivalent.

Project-Independent Tailoring of the Safety Lifecycle

(5.4.6.1) The organization may tailor the safety lifecycle for application across items or elements, i.e. apply a project-independent tailoring, but only if such a tailoring is limited to:

- Combining or splitting sub-phases, activities or tasks,
- Performing an activity or task in a different phase or sub-phase,
- Performing an activity or task in an added phase or sub-phase,
- Iterating phases or sub-phases,
- Performing safety activities concurrently with safety activities of other phases, or sub-phases, provided that 6.4.7.1 is complied with, or
- Omitting a phase or sub-phase that is not applicable to the organization, based on a rationale.

Functional Safety Management Activities



Management Activities

Overall Safety Management

- Unrelated to Specific Projects
- Allocation of Safety Responsibilities
- Safety Culture
- Training and Qualification

During Development

- Definition of Persons and Responsibilities for a Project
- Safety Program Plan
- V&V Plan
- Assessments

After Start of Production

- Definition of Procedures for Production to Achieve Functional Safety of Produced Units
- Implementation of Functional Safety Management after SOP

Project Dependent Safety Management

Objectives

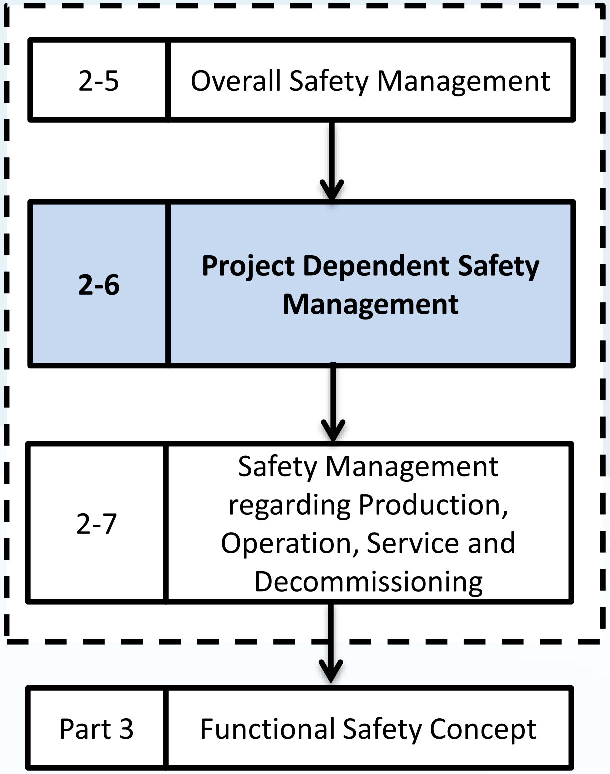
- Define the safety management roles and responsibilities.
- Define the requirements for safety management during the concept phase and the development phases, including the planning and coordination of the safety activities, the progression of the safety lifecycle, the creation of the safety case, and the execution of the confirmation measures.

Prerequisites

- Organization specific rules and processes for functional safety
- Evidence of competence management
- Evidence of quality management

Work Products

- Impact Analysis at the Item Level
- Impact Analyses at Element Level
- Safety Plan / Project Plan (refined)
- Safety Case
- Confirmation Measures Reports
- Release for Production Report


2-5
Overall Safety Management
2-6
Project Dependent Safety Management
2-7
Safety Management regarding Production, Operation, Service and Decommissioning
Part 3
Functional Safety Concept

New Product Development Roles

Project Manager: manages the entire product launch conducts project reviews including Phase Gate Reviews.

- **(6.4.2.2)** The project manager shall be given the responsibility and the authority, to ensure that:
  - a) the safety activities required to achieve functional safety are performed; and
  - b) compliance with ISO 26262 is achieved.
- **(6.4.2.3)** The project manager shall verify that the organization has provided the required resources for the safety activities.
- **(6.4.2.4)** The project manager ***shall ensure that the safety manager is appointed*** in accordance with 5.4.4.
  - NOTE: The role of the safety manager can be fulfilled by the project manager.

New Product Development Roles

Safety Manager: responsible for the planning and coordination of the functional safety activities.

- Not necessarily a position
- Maintains the safety plan and monitor progress of the safety activities against the safety plan
- Safety activities include item integration and testing plan, validation plan, software verification plan, and functional safety assessment plan
  - NOTE 1: The role of the safety manager can be fulfilled by the project manager.
  - NOTE 2: As the term “safety manager” is defined as a role (see ISO 26262-1), its assignment can be split between different persons depending on the organization.
  - NOTE 3: In the case of a distributed development, safety managers are appointed at the customer and at the suppliers that develop one or more elements intended to be integrated.

Impact Analysis at Item Level

- **(6.4.3.1)** At the beginning of the-safety lifecycle, an impact analysis at the item level shall be performed ***to determine whether the item is a new development, a modification of an existing item or an existing item with a modified environment***.

- **(6.4.3.2)** In the case of a modification of an item or its environment, the impact analysis at the item level shall identify and describe the modifications applied to the item, including:
  a) modifications to the design;
  b) modifications of the implementation; and
  c) modifications related to the environment

- **(6.4.3.3)** An impact analysis at the item level shall:
  a) evaluate the implications of the modifications with regard to functional safety; and
  b) identify and describe the safety activities to be performed, based on the impact of the modifications.

Reuse of an Existing Element

(6.4.4) In the case an existing element is reused, an impact analysis at element level shall be performed, which shall:

- Identify the modifications to the operational context, including resulting modifications of the element;
- Evaluate whether the reused element, with or without modifications, is able to comply with the allocated safety requirements that result from the item, or element, in which the considered element is to be integrated;*
- identify the safety activities to be performed based on an evaluation of the implications of the modifications, including implications on the validity of previously made assumptions; and
- Evaluate whether the existing safety-related documentation regarding the reused element is sufficient to support the integration of the element into the item, or element, in which the considered element is to be integrated.

***Modifications of the element can be planned, for example, to enable the integration of the existing element**

Tailoring of the Safety Activities

(6.4.5.1) A safety activity with regard to a specific item development may be tailored i.e. omitted or performed in a different manner than prescribed in the reference ISO 26262 lifecycle. If such a safety activity is tailored, then

a) The tailoring shall be ***defined in the safety plan***; and

b) A ***rationale*** as to why the tailoring is appropriate and sufficient to achieve functional safety shall be available.

Tailoring of the Safety Lifecycle

Tailoring is the modification of standard criteria to best fit the needs of the organization and project.

- **Project-independent Tailoring** is limited to applying one or more of the following:
  1. Sub-phases, activities or tasks may be combined or split;
  2. An activity or task may be performed in a different phase or sub-phase;
  3. An activity or task may be performed in an added phase or sub-phase;
  4. Phases or sub-phases may be iterated.
- **Project-related Tailoring** includes the customization of ASIL tables and safety-related activities.

- The Tailoring shall be defined in the Safety Plan.
  - *A rationale shall be available for all changes*.

Tailoring of the Safety Activities – Specific Clauses

- **(6.4.5.2)** If a safety activity is tailored as a result of an ***impact analysis*** then the tailoring shall comply with **ISO 26262-2:2018, 6.4.6.7**.

- **(6.4.5.3)** If a safety activity is tailored as a result of a ***proven in use argument***, then the tailoring shall comply with **ISO 26262-8:2018, Clause 14**.

- **(6.4.5.4)** If a safety activity is tailored because of an evaluation of ***hardware elements***, the tailoring shall comply with **ISO 26262-8:2018, Clause 13**.

- **(6.4.5.5)** If a safety activity is tailored because of a qualification of ***software components***, the tailoring shall comply with **ISO 26262-8:2018, Clause 12**.

- **(6.4.5.6)** If a safety activity is tailored based on a rationale that considers the ***confidence in the usage of software tools***, then the tailoring shall comply with **ISO 26262-8:2018, Clause 11**.

Tailoring of the Safety Activities – SEooC

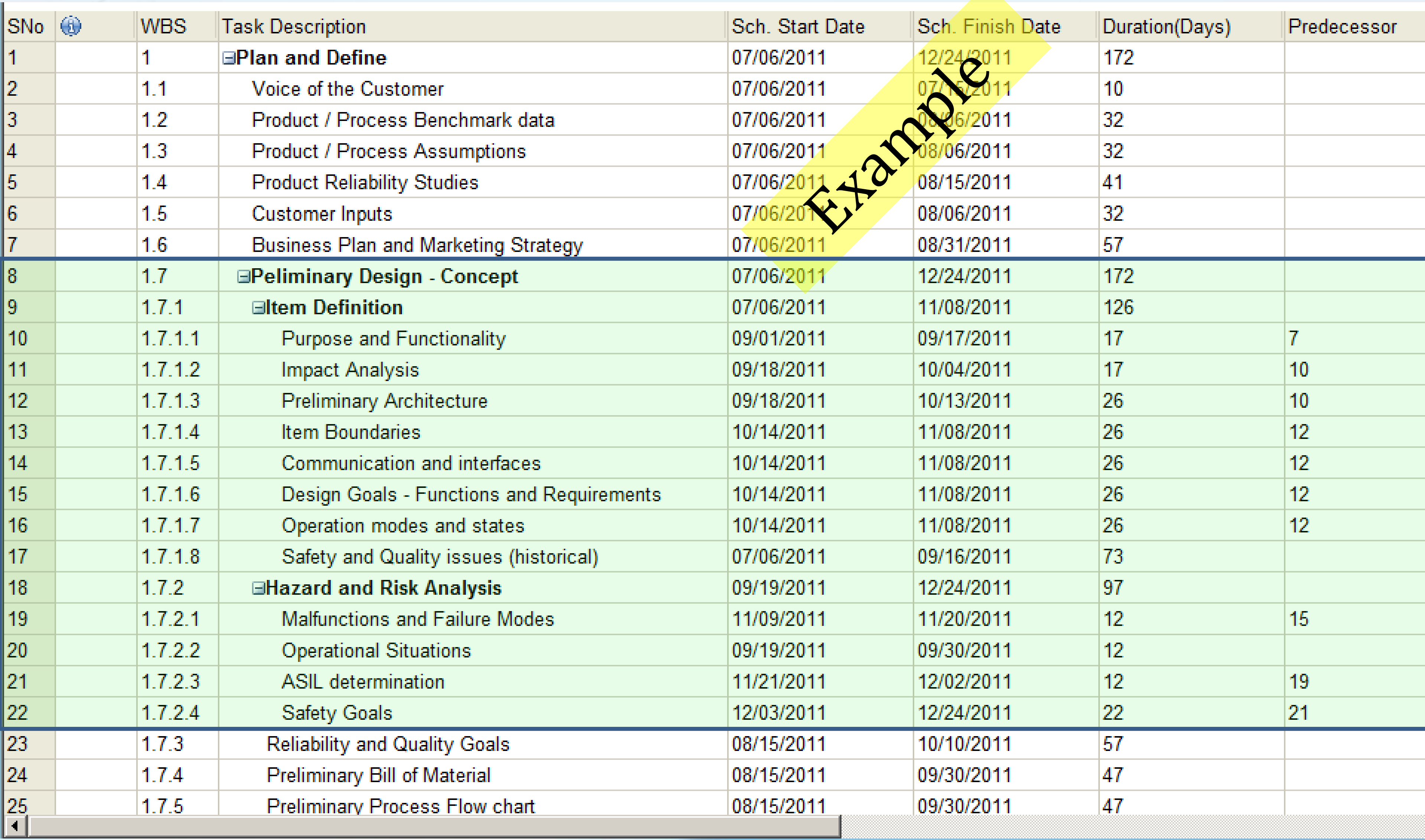
- **(6.4.5.7)** If the safety activities are tailored because an element is developed as a **Safety Element out of Context ("SEooC")**, then
  - The development of the safety element out of context shall be based on a requirement specification that is ***derived from assumptions*** on an intended use and context, including its external interfaces; and
  - The assumptions on the intended use and context of the safety element out of context shall be ***validated*** when the element is integrated ***in its target application***.

Planning and Coordination of the Safety Activities

- **(6.4.6.1 and 6.4.6.2)** The safety manager shall be responsible for the planning and coordination, and for maintaining and monitoring the safety plan.
- **(6.4.6.3 to 6.4.3.5)** All the responsibilities and activities need to be planned and detailed, and the safety plan can be referenced or included in the project plan.
- **(6.4.3.6)** The planning of a safety activity shall include describing
  a) the objective;
  b) the dependencies on other activities or information;
  c) the resource responsible for performing the activity;
  d) the required resources for performing the activity;
  e) the starting point in time and duration; and
  f) the identification of the corresponding work product.

6.5.2 Project Plan (refined)

(with integrated Safety Plan; ref 6.4.3.4)



SNo	ⓘ	WBS	Task Description	Sch. Start Date	Sch. Finish Date	Duration(Days)	Predecessor
1		1	⊟**Plan and Define**	07/06/2011	12/24/2011	172	
2		1.1	Voice of the Customer	07/06/2011	07/15/2011	10	
3		1.2	Product / Process Benchmark data	07/06/2011	08/06/2011	32	
4		1.3	Product / Process Assumptions	07/06/2011	08/06/2011	32	
5		1.4	Product Reliability Studies	07/06/2011	08/15/2011	41	
6		1.5	Customer Inputs	07/06/2011	08/06/2011	32	
7		1.6	Business Plan and Marketing Strategy	07/06/2011	08/31/2011	57	
8		1.7	⊟**Peliminary Design - Concept**	07/06/2011	12/24/2011	172	
9		1.7.1	⊟**Item Definition**	07/06/2011	11/08/2011	126	
10		1.7.1.1	Purpose and Functionality	09/01/2011	09/17/2011	17	7
11		1.7.1.2	Impact Analysis	09/18/2011	10/04/2011	17	10
12		1.7.1.3	Preliminary Architecture	09/18/2011	10/13/2011	26	10
13		1.7.1.4	Item Boundaries	10/14/2011	11/08/2011	26	12
14		1.7.1.5	Communication and interfaces	10/14/2011	11/08/2011	26	12
15		1.7.1.6	Design Goals - Functions and Requirements	10/14/2011	11/08/2011	26	12
16		1.7.1.7	Operation modes and states	10/14/2011	11/08/2011	26	12
17		1.7.1.8	Safety and Quality issues (historical)	07/06/2011	09/16/2011	73	
18		1.7.2	⊟**Hazard and Risk Analysis**	09/19/2011	12/24/2011	97	
19		1.7.2.1	Malfunctions and Failure Modes	11/09/2011	11/20/2011	12	15
20		1.7.2.2	Operational Situations	09/19/2011	09/30/2011	12	
21		1.7.2.3	ASIL determination	11/21/2011	12/02/2011	12	19
22		1.7.2.4	Safety Goals	12/03/2011	12/24/2011	22	21
23		1.7.3	Reliability and Quality Goals	08/15/2011	10/10/2011	57	
24		1.7.4	Preliminary Bill of Material	08/15/2011	09/30/2011	47	
25		1.7.5	Preliminary Process Flow chart	08/15/2011	09/30/2011	47	

Progression of the Safety Lifecycle

- **(6.4.7.1)** In the case of a lack of information from the pertinent preceding sub-phases, ***a subsequent sub-phase shall only start if the lack of information does not cause an unreasonable risk regarding functional safety***.
  - NOTE: For cases where the lack of information can jeopardize the project, the issue is escalated.

- **(6.4.7.2)** The work products required by the safety plan shall be subject to configuration management, change management and documentation.

SAFETY CASE

ISO 26262

3rd Party Certification

Most management standards required by the OEMs include 3rd party certification. That is a supplier’s implementation is required to be recognized by Independent, third-party agency, as demonstrating that a product or service complies with all standard requirements.

Why Do Companies Seek / Require 3rd Party Certification?

- To demonstrate compliance with national or international standards and regulations.
- To demonstrate independent validation and verification of their commitment to safety and quality.
- To increase credibility and acceptance with retailers, consumers and regulators.

➔ Benefit from enhanced product quality and safety.

Safety Case

- ISO 26262 does ***NOT*** include provisions for 3rd Party registration or certification.
- Instead, the standard requires the development of a Safety Case.
  - A safety case requires communicating a clear, comprehensive and defensible argument (supported by evidence) that a system is free of unreasonable risk to operate in a particular context.

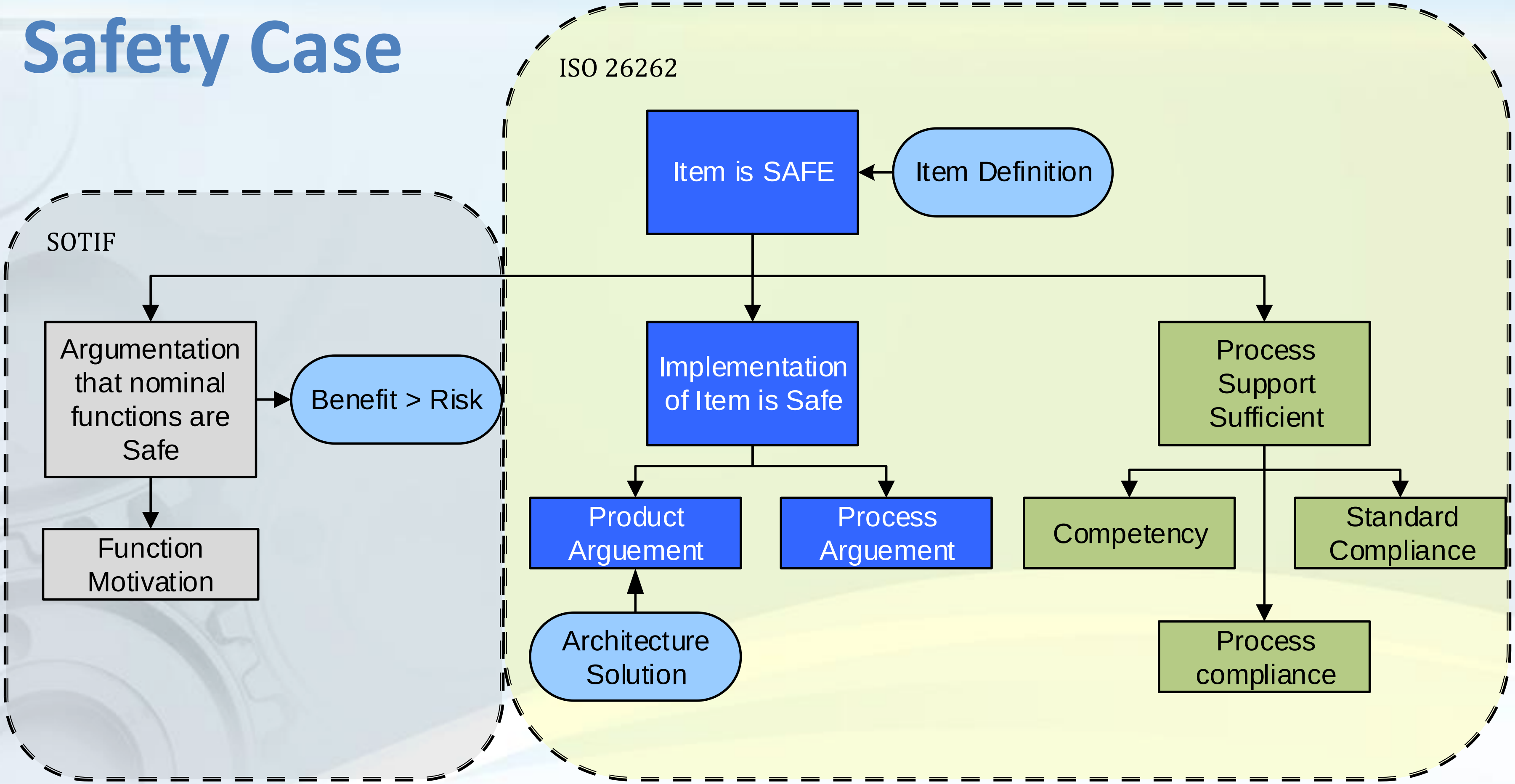
Safety Case

- The following are important considerations for the purpose of developing a safety case:
  - Above all, the safety case exists to communicate an argument.
  - It is used to demonstrate how it is possible to ***reasonably*** conclude that a system is free of ***unreasonable*** **risk** based on the available evidence.
  - A safety case is a device for communicating ideas and information, usually to a third party.
- There are three principal elements of a safety case, namely:
  - the requirements;
  - the argument; and
  - the evidence.
- The safety case should progressively compile the work products that are generated during the safety lifecycle.

Breakout Exercise 1: Safety Case

- As teams, identify what should be contained in a Safety Case; what should the Table of Contents include?

Safety Case



Safety of the Intended Function

The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF).

Safety Case

Common types of safety arguments

- **Product Argument:** direct appeal to features of the implemented product (e.g. the behavior of a timing watchdog).
- **Process Argument:** appeal to features of the development and assessment process (e.g. the design notation adopted).

- The safety case development can not be left as an activity to be performed towards the end of the safety lifecycle.
  - e.g., Behavior of user might change over time because of widespread use and familiarity to new safety systems.
- Safety cases are, by their nature, often **subjective**; the objective of the safety case development, therefore, is to obtain mutual acceptance of this subjective position.

CONFIRMATION MEASURES

Audits, Assessments and Reviews (Part 2, Clause 6)

Reviews, Audits and Assessments

- **Review:** Examination of a ***work product***, for achievement of the intended work product goal, according to the requirements of ISO 26262.
  - NOTE: Reviews can be supported by checklists.
- **Audit:** Examination of an ***implemented process***.
- **Assessment:** Examination of *the* ***achieved functional safety*** of an item or element.
  - NOTE: A level of independence, of the party or parties performing the assessment, is associated with each assessment.

Reviews, Audits and Assessments

Confirmation activity	Confirmation review	Functional safety audit	Functional safety assessment
Result	*Confirmation review report*[a]	*Functional safety audit report*[a]	*Functional safety assessment report*
Subject for evaluation	Work product	Implementation of the processes required for functional safety.	Item as described in the “Item definition” (see ISO°26262-3, Clause°5).
Responsibility of the persons that perform the confirmation measure	Evaluation of the compliance of the work product with the corresponding requirements of ISO 26262.	Evaluation of the implementation of the required processes.	Evaluation of the achieved functional safety. Provision of a recommendation for acceptance, a conditional acceptance or a rejection.
Timing during lifecycle	After completion of the corresponding safety activity. Completion before the release for production.	During the implementation of the required processes.	Progressively during development, or in a single block. Completion before the release for production.
Scope and depth	Planned prior to the review, in accordance with the safety plan.	Implementation of the processes against the definitions of the activities referenced or specified in the safety plan.	The work products required per the safety plan, the implementation of the required processes and a review of the implemented safety measures that can be assessed during the item development.

[a] can be included in functional safety assessment report

Confirmation Measures	Degree of Independency applies to:					Scope
		ASIL				
	QM	A	B	C	D	
Impact Analysis at Item Level	13					Judgment of whether the impact correctly identified the item status
Hazard Analysis and Risk Assessment	I3					The scope of this review shall include the correctness of the determined ASILs, and QM ratings of the identified hazards for the item, and a review of the safety goals
Safety Plan	-	-	I1	I2	I3	Applies to the highest ASIL among the safety goals of the item
Functional Safety Concept	-	I0	I1	I2	I2	
Technical Safety Concept	-	I0	I1	I2	I2	
Item Integration and Test Strategy	-	I1	I1	I2	I3	
Safety Validation Specification	-	-	I0	I1	I1	
Safety Analyses and the Dependent Failure Analyses	-	I0	I1	I2	I3	
Safety Case	-	I0	I1	I2	I3	
Functional Safety Audit	-	-	I0	I2	I3	
Functional Safety Assessment	-	-	I0	I2	I3	

source: ISO 26262 Part 2

Confirmation Review

source: ISO 26262 Part 2

The notations: --, I0, I1, I2 and I3 are defined as:

- no requirement and no recommendation for or against regarding this confirmation measure;

I0 the confirmation measure ***should*** be performed; however, if the confirmation measure is performed, it shall be performed by a *different person*;

I1 the confirmation measure ***shall*** be performed, by a *different person*; O$M$$N$E$X

I2 the confirmation measure **shall** be performed, by a *person from a different team*, i.e. not reporting to the same direct superior;

I3 the confirmation measure **shall** be performed, by a *person from a different department or organization*, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.

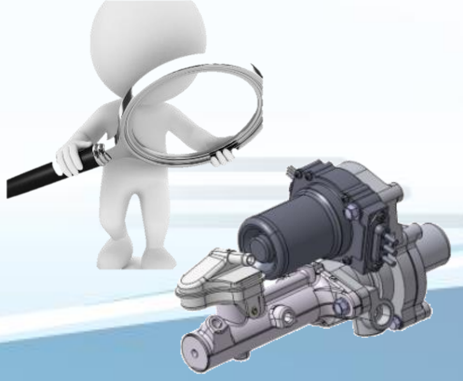
Note: software tool development is outside the item's safety lifecycle whereas the qualification of such a tool is an activity of the safety lifecycle

Functional Safety Audits

- The Functional Safety Audit is required when the highest ASIL of the item’s safety goals is ASIL (B) C, or D.
- One or more persons shall be appointed to carry out one or more Functional Safety Audits.
- A report shall be provide that contains an evaluation of the implementation of the processes required for functional safety.

Functional Safety Assessment

- A Functional Safety Assessment shall be carried out when the highest ASIL is (B), C, or D.
- The Safety Manager is responsible for planning the Safety Assessment.
- An agenda shall be prepared for performing the Safety Assessment.
- One or more person(s) shall be appointed to carry out a Functional Safety Assessment
- The scope of the Safety Assessment shall include:
  - The work products required by the safety plan;
  - The processes required for functional safety; and
  - Reviewing the appropriateness and effectiveness of the implemented safety measures.



Functional Safety Assessment

- A Functional Safety Assessment shall consider:
  - The planning of the other confirmation measures;
  - The results from the confirmation reviews and functional safety audit(s);
  - The recommendation(s) resulting from the previous functional safety assessment(s), if applicable.
- A Functional Safety Assessment Report shall include a recommendation for acceptance, conditional acceptance, or rejection of the functional safety of the item.
  - If the recommendation is a conditional acceptance, the corrective actions should be carried out.
  - If the recommendation is a rejection, then adequate corrective actions shall be initiated; ***and the functional safety assessment shall be repeated.***

Confirmation Measure Reports

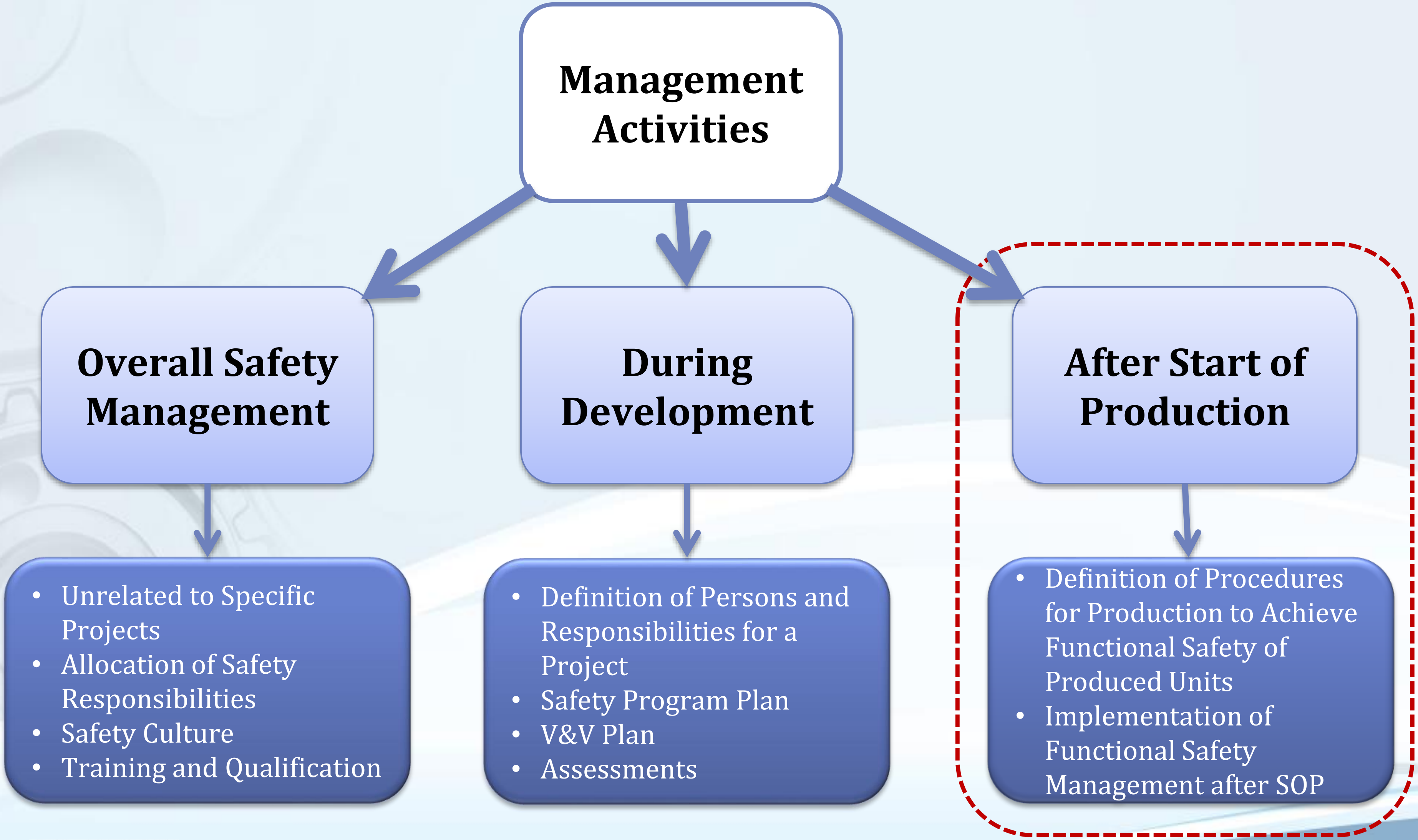
- Reports are required for the three types of Confirmation Measures.

- As part of the **Management of Functional Safety (ISO 26262-2, Clause 6)**, a comprehensive review and report of the Functional Safety Assessment, including the Safety Case will be made

Release for Production

- **(6.4.13.1)** The safety case shall be available prior to the release for production.
- **(6.4.13.2)** The applicable confirmation measure reports shall be available prior to the release for production.
- **(6.4.13.3)** The release for production of the item, or elements, shall only be approved if there is sufficient evidence for confidence in the achievement of functional safety.
- **(6.4.13.4)** The documentation of functional safety for release for production shall include the following information:
  a) the name and signature of the person responsible for the release;
  b) the versions of the released item or elements;
  c) the configuration of the released item or elements; and
  d) the release date.
- **(6.4.13.5)** At the release for production, a baseline for the embedded software, including the calibration data, and a baseline for the hardware shall be available and shall be documented.

Functional Safety Management Activities



Management Activities

Overall Safety Management

- Unrelated to Specific Projects
- Allocation of Safety Responsibilities
- Safety Culture
- Training and Qualification

During Development

- Definition of Persons and Responsibilities for a Project
- Safety Program Plan
- V&V Plan
- Assessments

After Start of Production

- Definition of Procedures for Production to Achieve Functional Safety of Produced Units
- Implementation of Functional Safety Management after SOP

OMNEX

Safety Management Regarding Production, Operation, Service and Decommissioning

Objectives

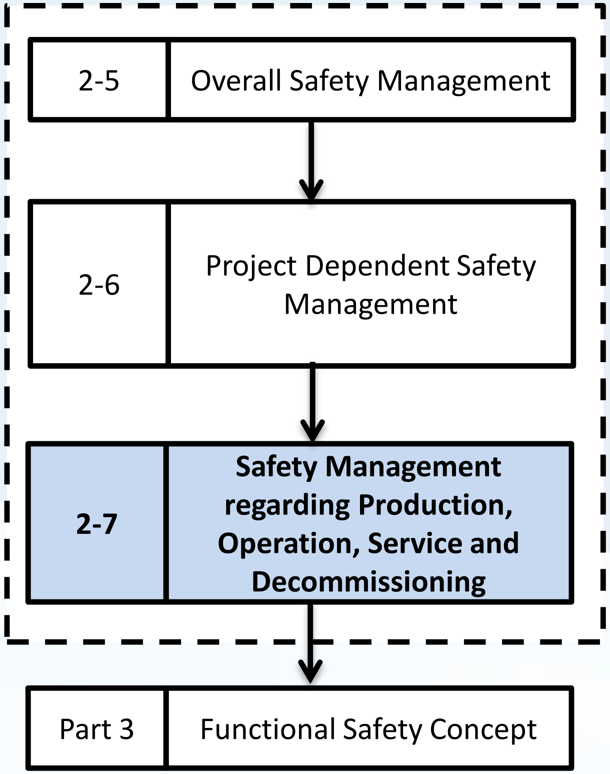
- Define the responsibilities of the organizations and persons responsible for functional safety after the item's release to production. This relates to the general activities for ensuring the required functional safety of the item during the lifecycle sub phases after the release for production.

Prerequisites

- Organization specific rules and processes for functional safety
- Evidence of competence management
- Evidence of quality management
- Release for Production Report

Work Products

- Evidence of safety management regarding production, operation, service and decommissioning


2-5
Overall Safety Management
2-6
Project Dependent Safety Management
2-7
Safety Management regarding Production, Operation, Service and Decommissioning
Part 3
Functional Safety Concept

Responsibilities, Planning and Required Processes

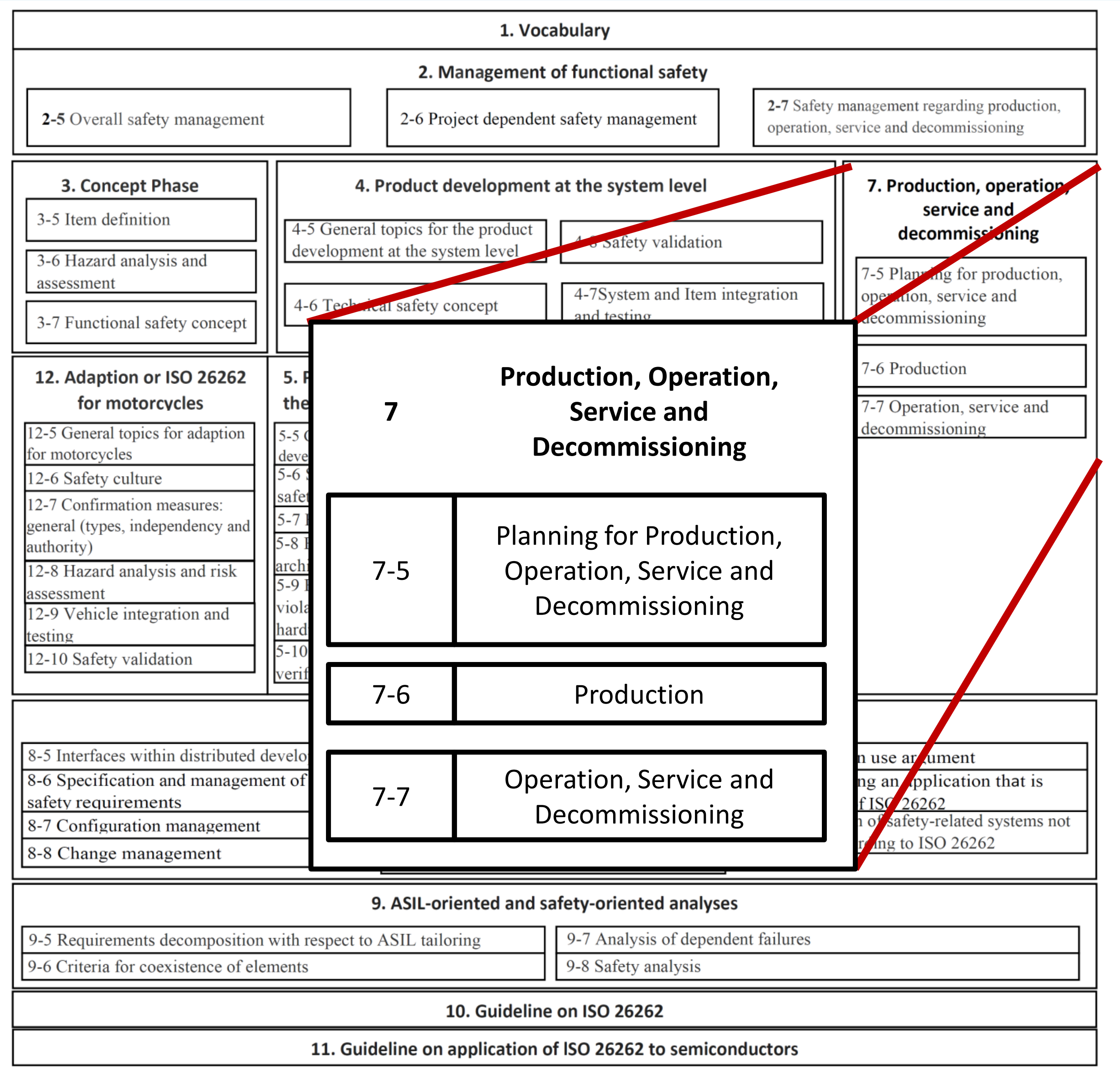
- **(7.4.2.1)** The organization shall appoint persons responsible to maintain the functional safety regarding production, operation, service and decommissioning.
- **(7.4.2.2)** The activities for ensuring the functional safety of the item regarding production, operation, service and decommissioning:
  a) shall be planned in accordance with **ISO 26262-7:2018, Clause 5**;
  b) shall be initiated during the product development at the system level in accordance with **ISO 26262-4**; and
  c) shall be executed in accordance with **ISO 26262-7:2018, Clauses 6 and 7.**
- **(7.4.2.3)** The organization shall institute, execute and maintain processes in order to achieve and maintain the functional safety of the item regarding production, operation, service and decommissioning.
  – NOTE This includes a field monitoring process with respect to the item's functional safety. Refer to **ISO 26262-7**.

Chapter 3

Production and Operation (Part 7)

OMNEX

26262 Framework



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Project dependent safety management

2-7 Safety management regarding production, operation, service and decommissioning

3. Concept Phase

3-5 Item definition

3-6 Hazard analysis and assessment

3-7 Functional safety concept

4. Product development at the system level

4-5 General topics for the product development at the system level

4-8 Safety validation

4-6 Technical safety concept

4-7System and Item integration and testing

7. Production, operation, service and decommissioning

7-5 Planning for production, operation, service and decommissioning

7-6 Production

7-7 Operation, service and decommissioning

12. Adaption or ISO 26262 for motorcycles

12-5 General topics for adaption for motorcycles

12-6 Safety culture

12-7 Confirmation measures: general (types, independency and authority)

12-8 Hazard analysis and risk assessment

12-9 Vehicle integration and testing

12-10 Safety validation

5. P

the

5-5 (

deve

5-6 S

safe

5-7 I

5-8 I

archi

5-9 I

viola

hard

5-10

verif

8-5 Interfaces within distributed develo

8-6 Specification and management of safety requirements

8-7 Configuration management

8-8 Change management

n use argument

ng an application that is

f ISO 26262

n of safety-related systems not

ring to ISO 26262

7	**Production, Operation, Service and Decommissioning**
7-5	Planning for Production, Operation, Service and Decommissioning
7-6	Production
7-7	Operation, Service and Decommissioning

9. ASIL-oriented and safety-oriented analyses

9-5 Requirements decomposition with respect to ASIL tailoring

9-6 Criteria for coexistence of elements

9-7 Analysis of dependent failures

9-8 Safety analysis

10. Guideline on ISO 26262

11. Guideline on application of ISO 26262 to semiconductors

Overview of Production and Operation Phase

Clause 5 — Planning for Production, Operation, Service and Decommissioning
Objectives

- Develop and maintain a production process for safety-related elements or items that are intended to be installed in road vehicles.
- Develop the necessary information concerning operation, service (maintenance and repair) and commissioning for users who interface with the safety-related items or elements in order to ensure that functional safety is achieved throughout the lifecycle of the vehicle.

Prerequisites

- Requirements Specification for Production, Operation, Service & Decommissioning
- Specification of Dedicated Measures for Hardware – ***this includes the identification of all SC/CCs related to the product***
- Warning and Degradation Strategy, included in the functional safety concept

Overview of Production and Operation Phase

Work Products

- **5.5.1 Safety-related Content of the Production Plan, including *identification of all related SC/CCs***
- **5.5.2 Safety-related Content of the Production Control Plan, including test plan**
- **5.5.3 Specification on the Producibility at System, Hardware or Software Development, e.g. error-proofing**
- **5.5.4 Assessment Report for Capability of the Production Process**
- **5.5.5 Safety-related Content of the Service Plan**
- **5.5.6 Safety-related Content of the Service Instructions**
- **5.5.7 Safety-related Content of the Information Made Available to the User**
- **5.5.8 Safety-related Content of the Decommissioning instructions**
- **5.5.9 Operation, Service and Decommissioning Requirements Specification**
  - NOTE This specification can be included in the relevant documentation of the corresponding phases.
- **5.5.10 Safety-related Content of the Rescue Services Instructions**

Overview of Production and Operation Phase

Clause 6 — Production

Objectives

- Achieve functional safety during the production process by relevant manufacturer or the person or organization responsible for the process (vehicle manufacturer, supplier, sub-supplier, etc.).

Prerequisites

- Release for Production Report
- Safety-related Content of the Production Plan, including the test plan and producibility requirements specification, if applicable
- Production Process Capability Report

Work Products

- 6.5.1 Control Measures Report
- 6.5.2 Assessment Report for Capability of the Production Process

Overview of Production and Operation Phase

Clause 7 — Operation, Service (Maintenance and Repair) and Decommissioning Objectives

- Ensure functional safety is achieved during the operation, service (maintenance and repair) and decommissioning sub-phases of the vehicle lifecycle.

Prerequisites

- Release for Production Report
- Safety-related Content of the Service Plan
- Safety-related Content of the Information Made Available to the User
- Safety-related Content of the Decommissioning Instructions
- Operation, Service and Decommissioning Requirements Specification, if applicable
- Safety-related Content of the Rescue Services Instructions

Work Products

- Field Observation Instructions

Part 7 Production and Operation

- Assure conformance of Production Plan to ISO 26262:
  - Production process flow
  - Production tools
  - Implementation of traceability measures
- Ensure that required functional safety is achieved during the production process
- Include all safety-related special characteristics
  - Such as, temperature range for specific processes, material characteristics, expiration date, fastening torque, production tolerance and configuration
- Planning of operation, service (maintenance and repair), and decommissioning
- Field monitoring process
- Activities addressing safety issues before disassembly

Chapter 4

Safety Element out of Context (Part 10 (Informative))

Types of Elements

Elements (components) can be developed in one of three ways:

1. **Standard Component:** Development is independent of use as a safety element. If used as such, it must be qualified (see part 8).
   – Qualification of components is to provide evidence of the suitability of intermediate level components and parts for their use as part of items, systems or elements, developed in compliance with ISO 26262, concerning their functional behavior and their operational limitations for the purposes of the safety concept.

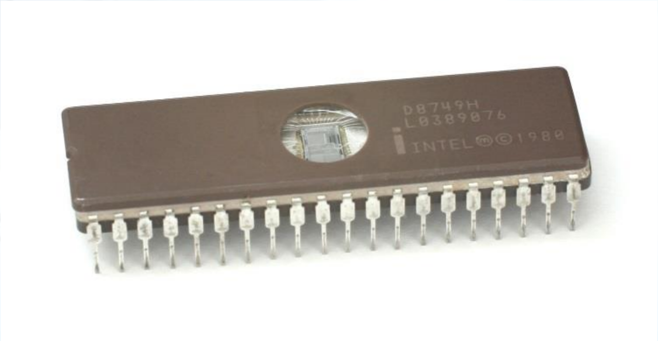
2. Development of elements ***in context***; i.e. elements developed to satisfy specific safety requirements as provided or derived from the OEM development activities.
   – The context is the Item to be supported.

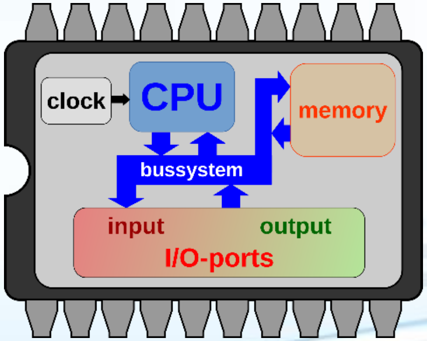
3. Development of elements ***out of context***; i.e. there is no specific OEM or item (context) that provides the specific safety requirements of the component.

Safety Element out of Context

- SEooCs differ from qualified components.
- The SEooC concept deals with the **development** of elements in accordance with ISO 26262 that are intended to…
    1. Provide for safety requirements; and
    2. Be **reusable**

under specified assumptions documented by the supplier.





Safety Element out of Context

Definition: A Safety Element out of Context is a safety element for which an item does not exist at the time of its development.

Essential Observations:

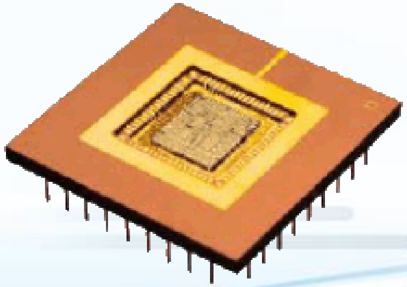
- Typically, the correct **implementation** of the assumed requirements is **verified** during development of the SEooC, but the **validation** takes place during the item development.

- The development of an SEooC starts at a certain level of requirements and design, and all information on requirements or design prerequisites is pre-determined with the status “assumed”.

Safety Element out of Context

Some typical examples of a Safety Element out of Context include:

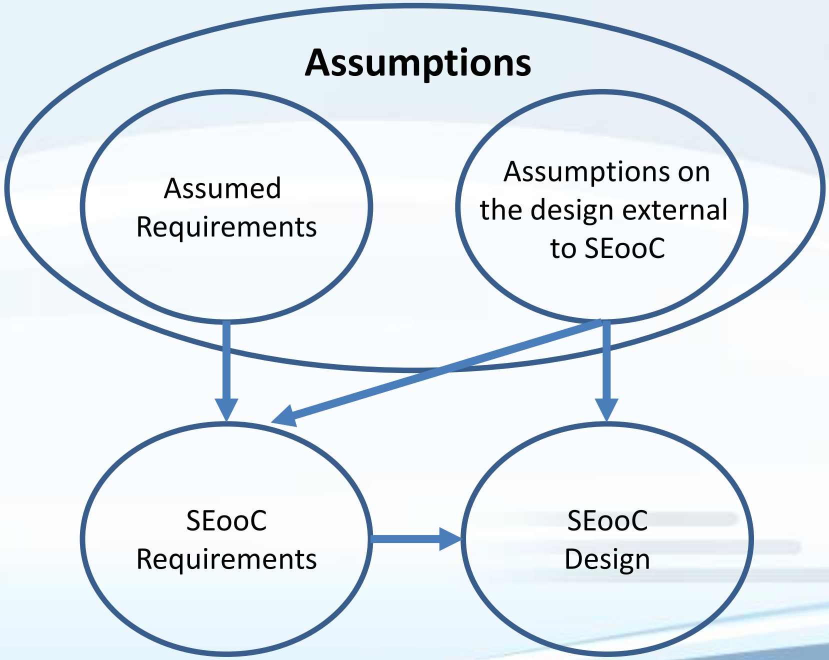
- **A hardware ECU** (Engine Control Unit) developed for certain types of Engine Management Systems (EMS) applications (low-end, medium or high-end vehicles) with the corresponding basic software that includes hardware build-in tests.
- **An ASIC** (Application Specific Integrated Circuit) that implements ECU monitoring functions and ensures the cut-off of essential actuators in case of severe failure.
- **A module** that provides the ECU with the engine synchronization.



An ASIC is a typical SEooC

SEooC

- The development of an SEooC involves making assumptions on the prerequisites of the corresponding phase in the product development.
  - It might not be necessary to make assumptions on all prerequisites, e.g. safety plan.



Development of an SEooC

System Development

By Supplier

- Step 1a – Assumptions on the Scope of SEooC and its Related Item
- Step 1b – Assumption on Functional Safety Requirement of the SEooC
- Step 2 – Execution of SEooC Development
- Step 3 – Provision of Work Products to System Integrator

By Customer

- Step 4 – Establish Validity of Assumptions
- Step 5 – SEooC Integration in the Item

Caution

Remember: Safety is a System Level Property

An SEooC is *not* a black box!

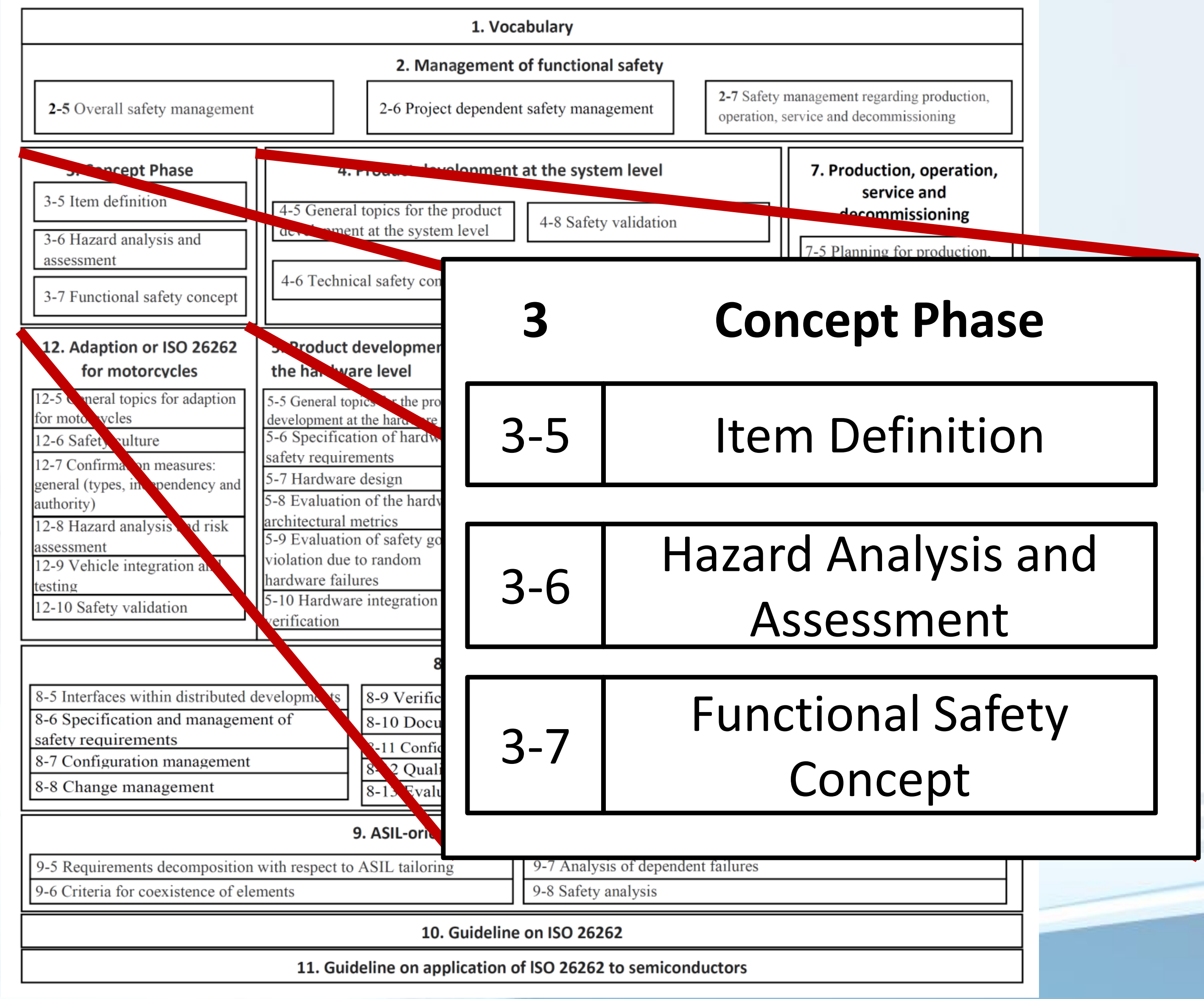
- The SEooC developer needs to:
  - Declare and document assumptions
  - Perform a complete analysis of SEooC components, parts or sub-parts
  - Produce and deliver all the applicable work products
  - Provide results in such a way that the item's integrator is able to adapt them with respect to the system analysis
- The item developer needs to:
  - Validate assumptions and work products
  - Provide feedback to the SEooC developer

An SEooC must be transparent with respect to integration

Chapter 5

Concept Phase (Part 3)

Concept Phase



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Project dependent safety management

2-7 Safety management regarding production, operation, service and decommissioning

3. Concept Phase

3-5 Item definition

3-6 Hazard analysis and assessment

3-7 Functional safety concept

4. Product development at the system level

4-5 General topics for the product development at the system level

4-8 Safety validation

4-6 Technical safety con

7. Production, operation, service and decommissioning

7-5 Planning for production,

12. Adaption or ISO 26262 for motorcycles

12-5 General topics for adaption for motorcycles

12-6 Safety culture

12-7 Confirmation measures: general (types, independency and authority)

12-8 Hazard analysis and risk assessment

12-9 Vehicle integration and testing

12-10 Safety validation

5. Product developmen the hardware level

5-5 General topics for the pro development at the hardware

5-6 Specification of hardw safety requirements

5-7 Hardware design

5-8 Evaluation of the hardw architectural metrics

5-9 Evaluation of safety go violation due to random hardware failures

5-10 Hardware integration verification

8

8-5 Interfaces within distributed developments

8-6 Specification and management of safety requirements

8-7 Configuration management

8-8 Change management

8-9 Verific

8-10 Docu

8-11 Confi

8-12 Quali

8-13 Evalu

9. ASIL-ori

9-5 Requirements decomposition with respect to ASIL tailoring

9-6 Criteria for coexistence of elements

9-7 Analysis of dependent failures

9-8 Safety analysis

10. Guideline on ISO 26262

11. Guideline on application of ISO 26262 to semiconductors

3	Concept Phase
3-5	Item Definition
3-6	Hazard Analysis and Assessment
3-7	Functional Safety Concept

Item Definition – Terminology

- An **item** is an E/E system that implements a function **at vehicle level**.
  - relates at least a sensor, a controller, and an actuator with each other.
- An **item** refers to the entire scope under consideration and is a (array of) system(s) to implement a function at the vehicle level.
  - A system is a set of **elements** that relate.
  - An **element** is any sub-unit of an item, and might or might not be further divided into constituent elements.
    - An element that cannot be divided into further elements is a hardware part of software unit.
    - A divisible element can be labelled as a system, a subsystem, or a component.
    - The term subsystem would typically be used when it is important to emphasize that the element is part of a larger system.
  - A component is a non-system level, logically and technically separable element.
    - Often the term component is applied to an element that is only comprised of parts and units.

Item Definition

- The item definition should collect all information relevant to the analysis and design for the item:
  - Purpose and description;
  - Function(s) and relations between functions;
  - Requirements for each function;
  - Draft architecture/outline;
  - Additional nonfunctional constraints;
  - Borders or interfaces to other items/systems;
  - Legal requirements;
  - ...

The base functionalities of the Item; does not include Safety Measures

Item Definition

(Systems Perspective)

The boundary of the item, its interfaces, and the assumptions concerning its **interaction with other items** and elements, shall be defined considering:

a) the elements of the item;

NOTE: The elements could also be based on other technology

b) the assumptions concerning the effects of the item's behavior on **other items or elements**, that is the environment of the item;

c) **interactions** of the item with other items or elements;

d) functionality required by **other items**, elements and the environment;

e) functionality required from **other items**, elements and the environment;

f) the use of functions among the involved systems and **allocation and distribution** elements; and

g) the operating scenarios which impact the functionality of the item.

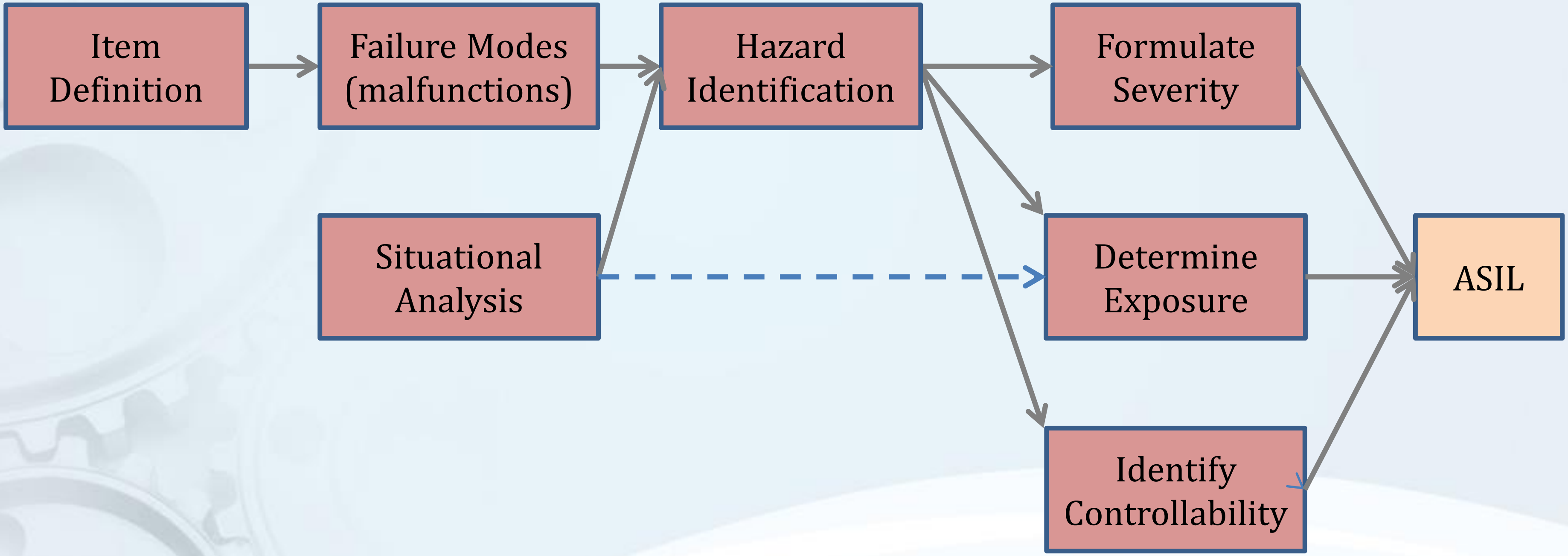
Breakout Exercise 2: Item Definition

Using the information in the Breakout handout booklet:

- Identify which information should be included in the Item Definition.
  - Purpose and Functionality
  - Impact Analysis
- Draw a preliminary architecture (Boundary Diagram) for the item.
  - Identify Item Boundaries
- Identify the basic functions and requirements of the system.

Reference : ItemDefinition-handout.xlsx

Hazard Analysis



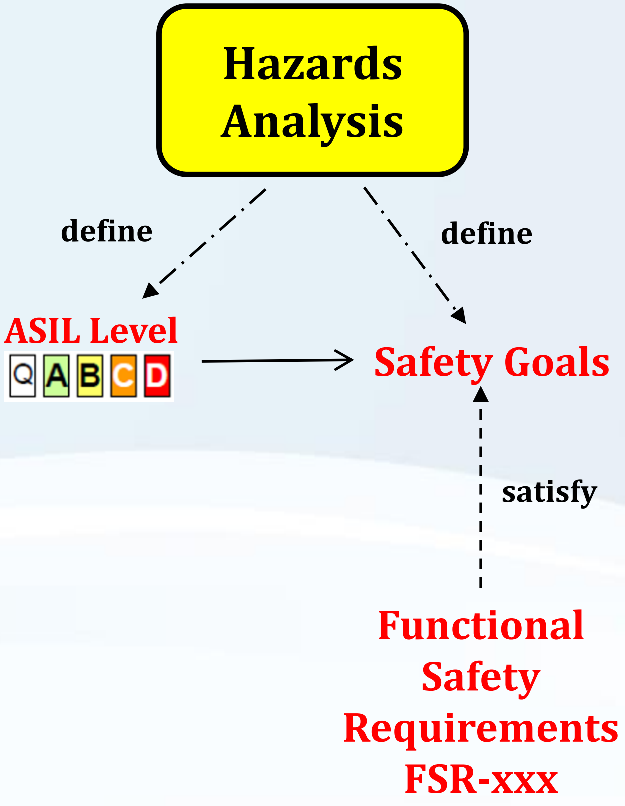
The objective is to define the functional safety after an item's release for production.

This relates to the general activities for ensuring the required functional safety of the item during the lifecycle of the product and including the release for production

Objectives

Hazard Analysis and Risk Assessment consists of three fundamental steps:

1. **Hazard Identification**
   - Determine the Malfunctions Possible for the Item
   - Situation Analysis
     - identify the potential unintended behaviors of the item that could lead to a hazardous event.
2. **Hazard Classification**
   - Determine the **Severity (S)**, the **Exposure (E)** and the **Controllability (C)** associated with the considered hazard of the item.
3. **ASIL Determination**
   - Determine the **required Automotive Safety Integrity Leve**l.



Hazard 🡐 Malfunction + Operational Situation

Initiation of the HARA

- **6.4.1.1:** The hazard analysis and risk assessment shall be based on the item definition.

- **6.4.1.2:** The item ***without internal safety mechanisms*** shall be evaluated during the hazard analysis and risk assessment,
  - i.e. safety mechanisms intended to be implemented or that have already been implemented in predecessor items shall **not** be considered in the hazard analysis and risk assessment.

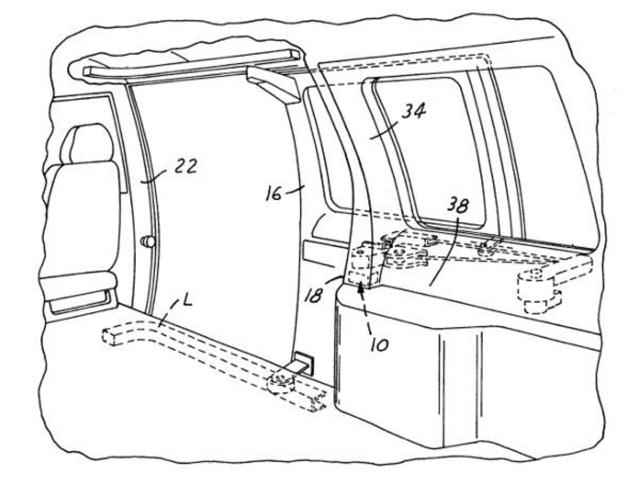
If there are hazards identified in this clause that are outside of the scope of ISO 26262, these hazards shall be addressed according to organization-specific procedures

Malfunctions

- Failure or unintended behavior of an item with respect to its design intent (functional requirements)
- Malfunction with specificity ➔ Failure Mode
- Typical Malfunction categories:
  - NO function
  - REVERSE function
  - MORE/LESS function
  - PARTIAL function
  - function EARLY
  - function LATE
  - Unexpected
  - etc.

Stay in Scope

- The ISO 26262 standard only concerns hazards that arise from malfunctioning behavior of an item that are observable **at the vehicle level**.
  - Need to consider expected use ***and*** expected misuse.
- "Unexpected" driver or passenger misuse of a correctly functioning item is outside of the scope of the standard.
  - e.g., a passenger manually overrides the safety mechanisms on a power sliding door and opens the door at high speed.



A power sliding door can be misused even if it works correctly

Operational Situations

Road Conditions

All operational situations that are relevant are identified

- Factors to be considered for situation analysis and hazard identification may include:
  - Vehicle usage scenarios, for example high speed driving, urban driving, parking, off-road;
  - Environmental conditions, for example road surface friction, side winds;
  - Reasonably foreseeable driver use and misuse;
  - Interaction between operational systems.

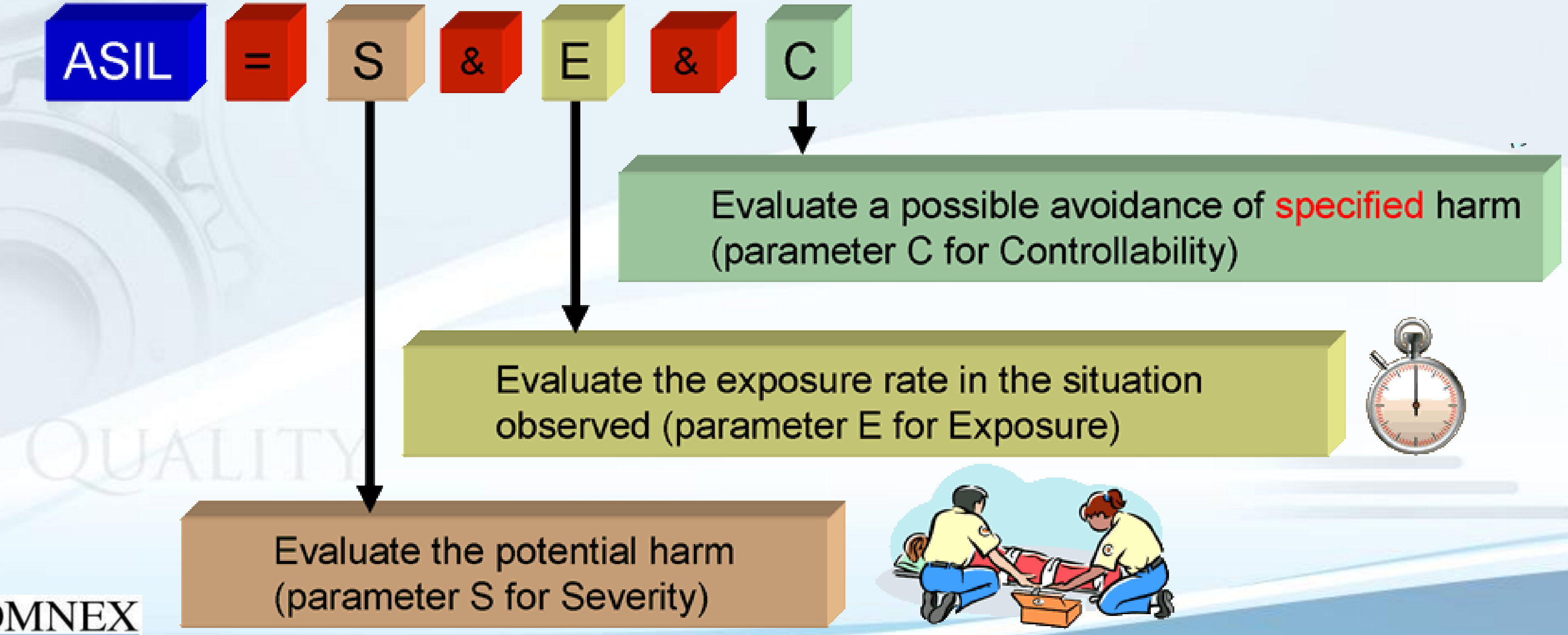
Environmental conditions

Usage scenarios

Parking

Hazard Classification

- Hazard classification involves three categories
  - Severity (S)
  - Exposure (E)
  - Controllability (C)
- Together they lead to the **Automotive Safety Integrity Level** (ASIL)



Evaluate a possible avoidance of specified harm (parameter C for Controllability)

Evaluate the exposure rate in the situation observed (parameter E for Exposure)

Evaluate the potential harm (parameter S for Severity)

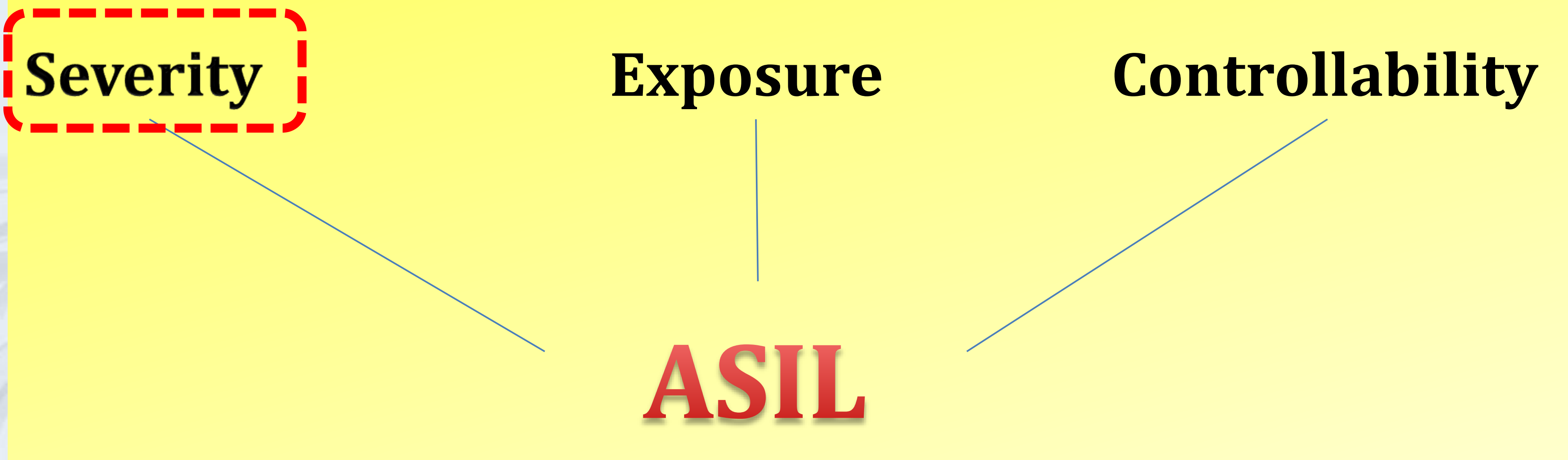
ASIL Factors

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

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

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

Severity Level (S)



Severity

7.4.3.2: The severity of potential harm shall be estimated based on a defined rationale for each hazardous event.

- The risk assessment of hazardous events focuses on the harm to each ***person*** potentially at risk:
  - Driver
  - Passengers
  - Pedestrians
  - Cyclists
  - Passengers in other vehicles

Damage to **<u>things</u>** is out of scope of ISO 26262!

Driver

Passengers

Pedestrians

Estimating Severity?

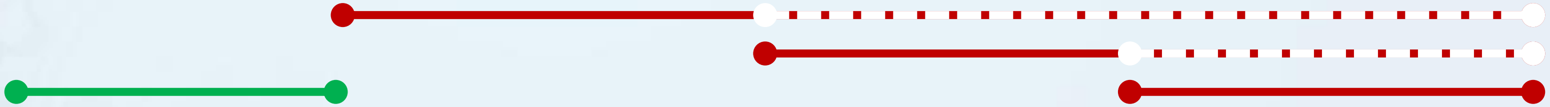
- Accident statistics can be used to determine the distribution of injuries that can be expected to occur in different types of accidents.
- ISO 26262 provides an approach based on results in automotive medicine: **The Abbreviated Injury Scale (AIS)**
  - Expected severity based upon previous accident analyses.
  - Statistics on distribution of injuries expected to occur in different types of accidents.
  - The use of internationally recognized **injury scales** based upon the current state of medical research in the automotive domain.

AIS represents a categorization of injury classes, but only for single injuries. Instead of AIS, other categorizations such as Maximum AIS (MAIS) and Injury Severity Score (ISS) can be used.

ISO 26262 and AIS

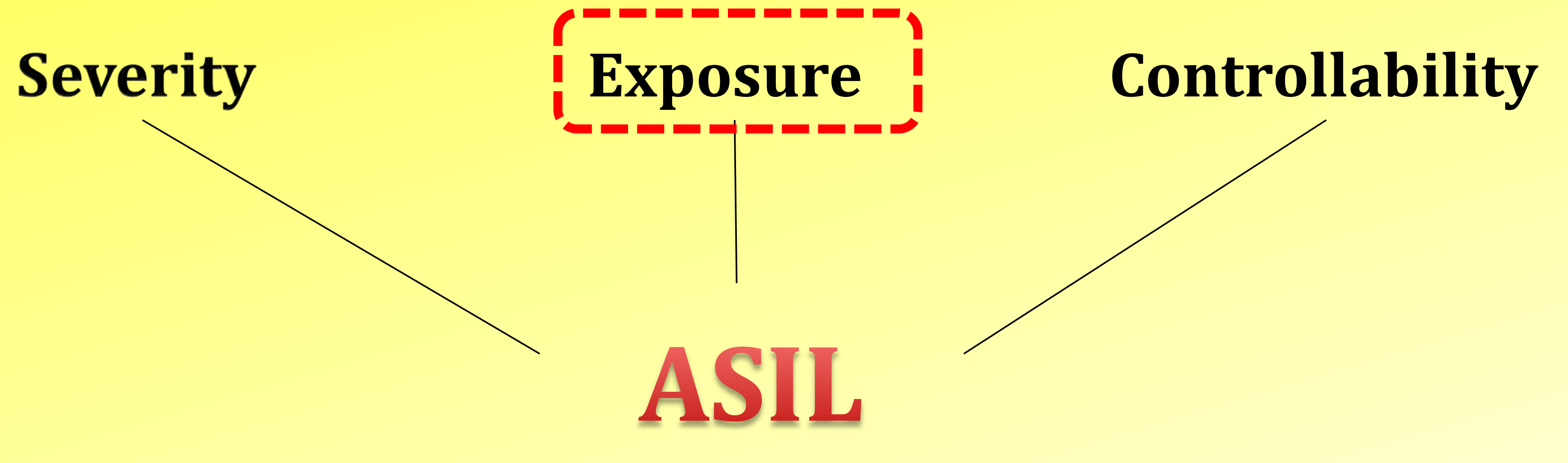
ISO 26262 covers Abbreviated Injury Scale (AIS) in a simpler manner, “collapsing” seven levels into only four:

- S1 covers “at least minor to moderate injuries, AIS 1-2”
- S2 covers “at least serious to severe injuries, AIS 3-4”
- S3 covers “critical and unsurvivable injuries, AIS 5-6”



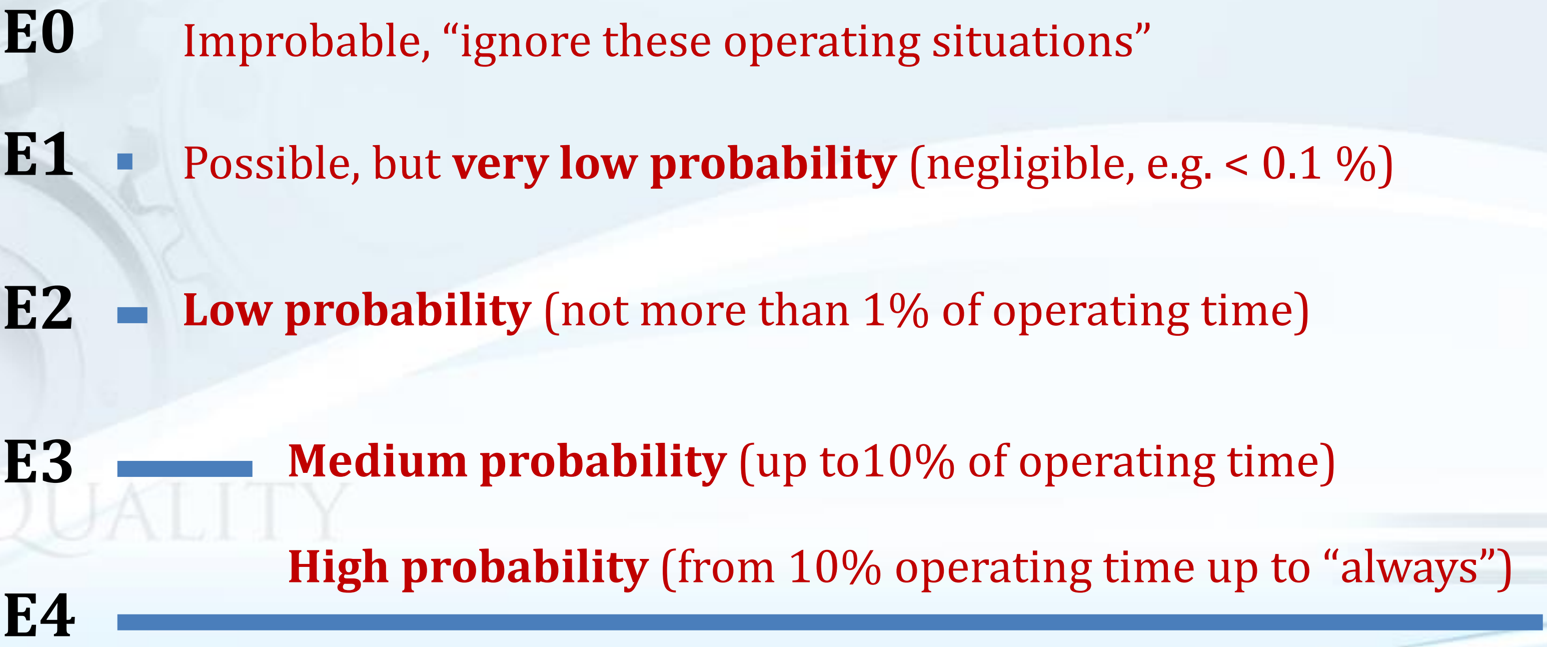
ISO 26262 Class	S0	S1	S2	S3
Description	No Injuries	Light and moderate injuries	Severe injuries, possibly life-threatening, survival probable	Life-threatening injuries (survival uncertain) or fatal injuries
Reference for Single Injuries (from AIS)	AIS-0 (No safety related damage)	Not S2 or S3 and > 10% probability of AIS 1-6 (safety-related damage)	Not S3; > 10% probability of AIS 3-6 (severe injuries+)	> 10% probability of AIS 5-6 (critical injuries+)

Exposure (E)



The Scale of Exposure

- Related to the Operational Situation
- A simplified four-level classification scheme is used for probability of **exposure**
- Each level is an **order of magnitude** (i.e. 10 times previous level)



E0 Improbable, “ignore these operating situations”

E1 Possible, but **very low probability** (negligible, e.g. < 0.1 %)

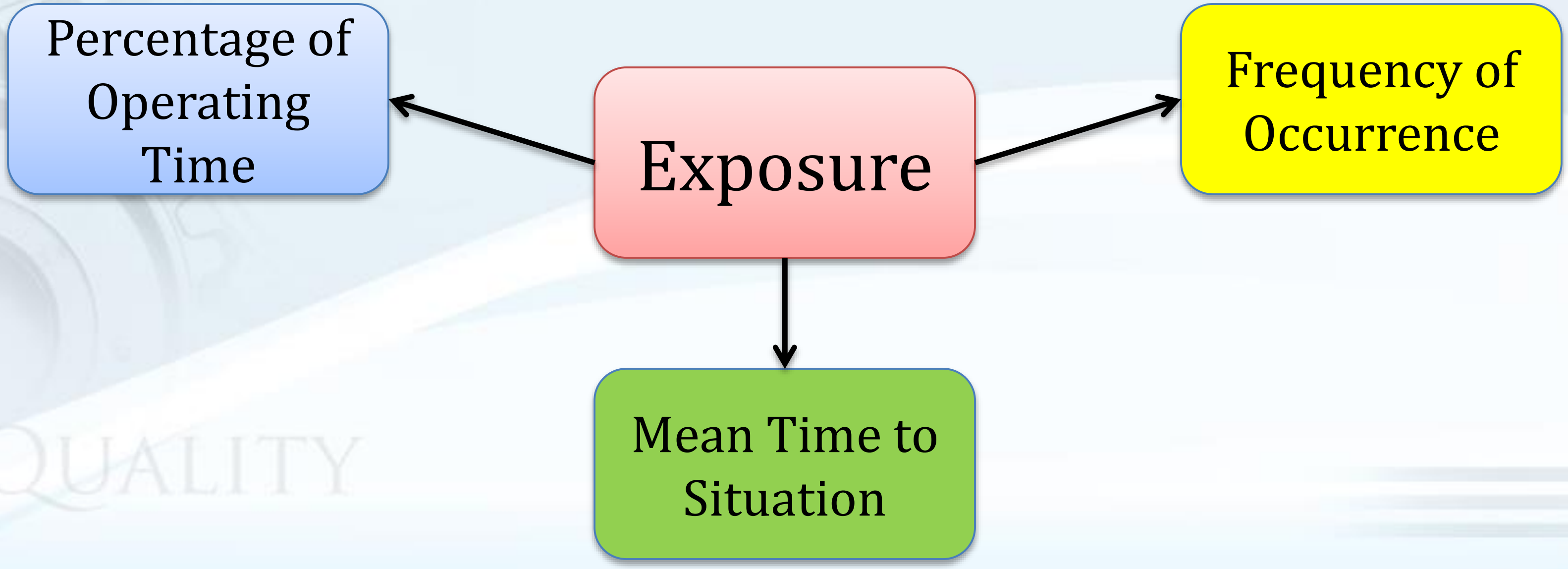
E2 **Low probability** (not more than 1% of operating time)

E3 **Medium probability** (up to10% of operating time)

E4 **High probability** (from 10% operating time up to “always”)

Estimation Strategies for Exposure

- The estimation of probability of exposure is difficult at best.
- Depending on the scenario, different approaches can be used as appropriate.



Exposure

Percentage of Operating Time

Frequency of Occurrence

Mean Time to Situation

Operating Time Examples (Table B.2)

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time	Not specified	<1%	1%-10%	>10%
Examples for Road Layout	—	– Country road intersection – Highway exit ramp	– One-way street (city street)	– Highway – Country road
Examples for Road Surface	—	– Snow/ice on road – Slippery leaves on road	– Wet road	—
Examples for Vehicle in Stationary State	– Vehicle during jump start – In repair garage	– Trailer attached – Roof rack attached – Vehicle being refuelled	– Vehicle on a hill (hill hold)	—
Examples for Maneuver	– Driving downhill with engine off (mountain pass)	– Driving in reverse – Overtaking – Parking (with trailer attached)	– Heavy traffic (stop and go)	– Accelerating – Decelerating – Stopping at traffic light (city street) – Lane change (highway)

Frequency Examples (Table B.3)

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Frequency of Situation	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Examples for Road Layout	—	– Mountain pass with unsecured steep slope	—	—
Examples for Road Surface	—	– Snow/ice on road	– Wet road	—
Examples for Vehicle in Stationary State	– Stopped, engine requiring restart (at railway crossing) – Vehicle being towed	– Roof rack attached	– Vehicle being refuelled – Vehicle on a hill (hill hold)	—
Examples for Maneuvre	—	– Evasive maneuvre, deviating from desired path	– Overtaking	– Shifting transmission gears – Executing a turn (steering) – Using indicators – Driving in reverse

OMNEX

T&B Examples

The tables on the next slides (Table B.4 and B.5) provide examples for trucks, buses, trailers and semi-trailers (T&B).
Different types of base vehicles are considered in the tables:

- **Long Haul (LH):** for long distance transporting goods
- **Distribution (DI):** for distributing goods
- **Vocational (VO):** for performing specific work functions, e.g. dumper truck, concrete mixer, dustcart
- **City Bus (CB):** for urban and suburban use
- **Interurban Bus (IB):** for interurban transport
- **Coach (CO):** for long distance journeys

T&B Operating Time Examples (Table B.4)

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time	Not specified	<1%	1%-10%	>10%
Driving in Reverse	—	LH, CB, CO, IB	DI, VO	—
Overtaking Another Truck or Bus with Small Speed Difference (with lane change to oncoming lane)	LH, DI, VO, CO, IB	—	—	—
Driving with Trailer Attached	—	—	DI, CO, IB	LH, VO
Semi-trailer Tractor w/o Trailer Attached (on public road)	—	LH, DI, VO	—	—
Driving on Construction Site (vehicle is driving directly on construction site, not only for delivering goods to construction site)	LH	DI	—	VO
Steep Slope	LH, CB	DI, CO, IB	VO	—
Standing at a Bus Stop	—	—	CO	CB, IB
Entering/Driving Off From Bus Stop	—	CO	CB, IB	—

Table B.2 can be applied to T&B, but are considered on a case-by-case basis. For situations occurring in both Tables B.2 and B.4, B.4 is considered more appropriate for T&B.

T&B Frequency Examples(Table B.5)

Class	E1	E2	E3	E4
Description	Very low probability	Low probability	Medium probability	High probability
Duration (% of average operating time	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average
Driving in Reverse	—	—	CB	LH, DI, VO, CO, IB
Overtaking Another Truck or Bus with Small Speed Difference (with lane change to oncoming lane)	—	—	LH, DI, VO, CO, IB	—
Driving with Trailer Attached	—	—	DI, CO, IB	LH, VO
Semi-trailer Tractor w/o Trailer Attached (on public road)	—	DI, VO	LH	—
Driving on Construction Site (vehicle is driving directly on construction site, not only for delivering goods to construction site)	LH	DI	—	VO
Steep Slope	LH, CB	DI, CO, IB	—	VO
Standing at/Entering/Driving off a Bus Stop	—	—	—	CB, CO, IB

Table B.3 can be applied to T&B, but are considered on a case-by-case basis. For situations occurring in both Tables B.3 and B.5, B.5 is considered more appropriate for T&B.

Right Level of Granularity

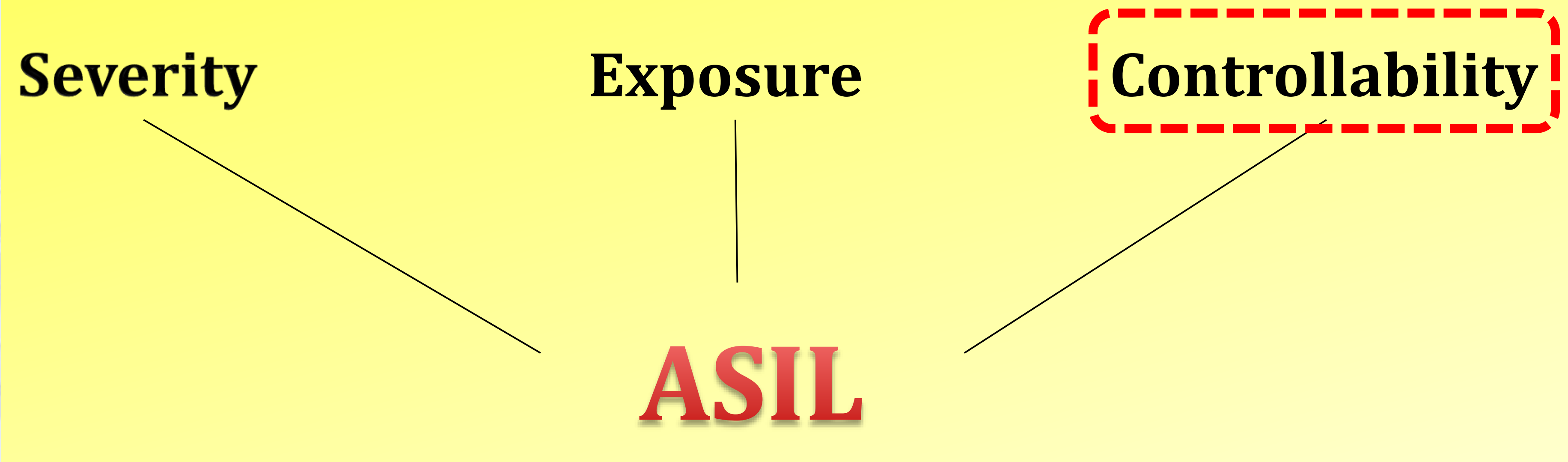
How to arbitrarily lower the ASIL values

- Create a fine level of granularity in the scenarios. This makes it easier to allocate **severity (S)** and **controllability (C)** levels.
- **But** it creates many, small probabilities of occurrence of each scenario and **artificially lowers the probability of exposure (E)**.
  - **With E1, all ASILs are QM except with S3 and C3.**
- Beware of creating too many detailed operational scenarios! This not only makes the hazard analysis more time consuming and it will probably not be acceptable to the customer.

Operational Scenarios

....
City driving – driving backwards
City driving – parking situation
Country road – crossing
Country road – snow and ice
Country road – slippery/leaves
Highway – entering
Highway – exit
Highway – congestion
Highway – xxx
Highway – yyy
Highway – zzz
Highway – ...
...

Controllability (C)



Severity

Exposure

Controllability

ASIL

What is Controllability?

Controllability is an estimate of the probability that the *driver or other endangered persons* are able to gain control of the hazardous event that is arising and able to avoid the specific harm.

- Assumptions:
  - Driver is in normal condition to drive
  - Driver is complying with laws and regulations
  - Driver is trained (has proper driver's license)

Class of Controllability

There are four classes:

C0 – Controllable in general

C1 – Simply controllable

C2 – Normally controllable

C3 – Difficult to control or uncontrollable

- The selection of classification is based on assumptions about the control actions necessary **by the individuals involved in the hazard** scenario to retain or regain control of the situation, as well as the representative driving behaviors of the drivers involved (which may be related to the target market, individuals' age, eye-hand coordination, driving experience, cultural background, etc.)
  - Some "reasonably foreseeable misuse" might be appropriate in the analysis in some cases.

Controllability

	C0	C1	C2	C3
Driving Factors and Scenarios	Controllable in General	99% or more of all drivers or other traffic participants are usually able to avoid harm	90% or more of all drivers or other traffic participants are usually able to avoid harm	Less than 90% of all drivers or other traffic participants are usually able, or barely able to avoid harm
Unexpected radio volume increase	Maintain intended driving path			
Fault adjustment of seat position while driving		Brake to slow/stop vehicle		
Failure of ABS during emergency braking			Maintain intended driving path	
Failure of brakes				Brake to slow/stop vehicle

Controllability Notes

- For C2, a feasible test scenario is accepted as adequate:
  - “Practical testing experience revealed that a number of 20 valid data sets per scenario can supply a basic indication of validity”. If each of the 20 data sets complies with the pass-criteria for the test, a level of controllability of 85 % (with a level of confidence of 95 % which is generally accepted for human factors tests) can be proven. This is appropriate evidence of the rationale for a C2-estimate.
- For C1, a test to provide a rationale that 99% of the drivers “pass” the test in a certain traffic scenario might not be feasible because a large number of test subjects would be necessary as the appropriate evidence for such a rationale. Decision can be based on expert judgment.
- As no controllability is assumed for category C3, it is not relevant to have appropriate evidence of the rationale for such a classification.

ASIL Allocation

Severity	Exposure	Controllability		
		C1 (Simple)	C2 (Normal)	C3 (Difficult or Uncontrollable)
S1 Light and moderate injuries	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 Severe and life threatening injuries (survival probable)	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 Life threatening / fatal injuries	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

Application of Severity, Exposure and Controllability

Example: Cruise Control

- Hazard: "Unintended Acceleration: Cruise Control is not deactivated when the driver is braking" (and speed > 30 mph on suburban roads).
  - Severity → **S2 =** Severe injuries, possibly life-threatening
  - Exposure → **E4 =** More than 10% of operating time
  - Controllability → **C3 =** Difficult to control or uncontrollable

ASIL = C

ASIL Classification

Category QM – Lowest

ASIL A

ASIL B

ASIL C

ASIL D – Highest

- QM denotes no additional requirements (other than the Quality Management System) to comply with ISO 26262.
- Safety Goals are determined for each (non-QM) ASIL evaluated.

ASIL Impact on Requirements

ASIL	Example	Sample Ranking	Sample requirement: Diagnostic coverage / dedicated measures	Identified as ++ in tables of part 4, 5, 6
A	Cruise control: failure to decelerate	S1, C2, E4	none / some	~ 50
B	Cruise control: deceleration outside design limits	S1, C3, E4	90% single-point, 60% latent / more	~ 80
C	Passenger Airbag wrong deployment	S3, C3, E1	97% single-point, 80% latent / even more	~ 130
D	Electric Steering, Wrong assist EPB, lock rear wheels SCS, wrong intervention	S3, C3, E4	99% single-point, 90% latent / most	~ 150

Higher ASILs require increased effort

T&B Considerations with HARA

(6.4.5.2) The following variances shall be considered when conducting a hazard analysis and risk assessment for a T&B vehicle:

a) type of base vehicle;

b) the T&B vehicle configuration; and

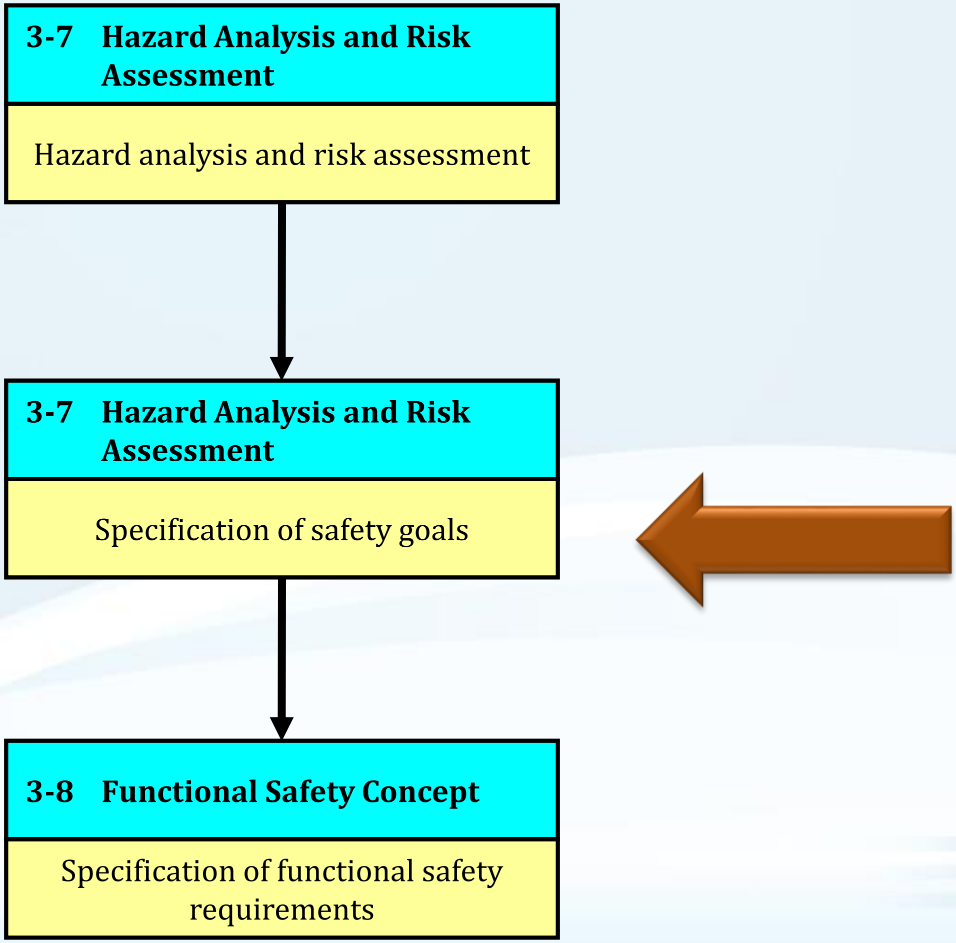
c) the T&B vehicle operation.

NOTE Engineering judgement is appropriate when selecting variance types for the analysis.

T&B Considerations with HARA

- **(6.4.5.3)** When conducting a hazard analysis and risk assessment each relevant type of base vehicle shall be considered.
- **(6.4.5.4)** The number of vehicles of a given type of base vehicle shall not be considered when estimating the probability of exposure.
- **(6.4.5.5)** The number of vehicles equipped with a specific configuration shall not be considered when estimating the probability of exposure.
- **(6.4.5.6)** When conducting a hazard analysis and risk assessment the variances in operational situations that have impact on technical parameters shall be considered.

Safety Goals



3-7 Hazard Analysis and Risk Assessment

Hazard analysis and risk assessment

3-7 Hazard Analysis and Risk Assessment

Specification of safety goals

3-8 Functional Safety Concept

Specification of functional safety requirements

Safety Goals

- Safety Goals are top-level safety requirements for the item.
  - The concept of a safety goal is expressed in terms of functional objectives, ***not technological solutions***.
- A Safety Goal is determined for each hazardous event with an ASIL evaluated in the hazard analysis.
- If similar Safety Goals are determined, they may be combined into a single Safety Goal.
- The ASIL determined for the hazardous event shall be assigned to the corresponding Safety Goal.
- If similar Safety Goals are combined into a single one, the highest ASIL shall be assigned to the combined Safety Goal.

Example of Safety Goal

- **Item:** Electrical Park Brake (EPB) systems
  - The EPB system, when activated by a specific driver command, brakes the vehicle rear wheels to prevent unintended vehicle movement during parking.
- **Function:** brakes the vehicle rear wheels on demand
- **Malfunction:** Function Unintended
- **Failure Mode:** Unintended EPB activation; i.e., without demand
- **Operational Situations:**
  - High Speed
  - Taking a bend
  - Low Adherence
  - Medium-low speed **AND** High Adherence

Example of Safety Goal

Failure Mode	Specific Situation	HAZARD	ASIL	Safety Goal	Safe State
Unintended parking activation	High Speed OR Taking a bend OR Low Adherence	Unexpected deceleration (± 0.2 g over a 200 msec) with loss of vehicle control	Higher ASIL	The Parking function shall not be activated with moving vehicle	Parking function activation inhibition over a TBD threshold speed
Unintended parking activation	Medium-low speed AND High Adherence	Unexpected deceleration (± 0.2 g over a 200 msec) with possible crash with following vehicle	Lower ASIL	The Parking function shall not be activated with moving vehicle	Parking function activation inhibition over a TBD threshold speed

A Management View

Another view of the safety goal:

The safety goal is the top-management safety requirement.

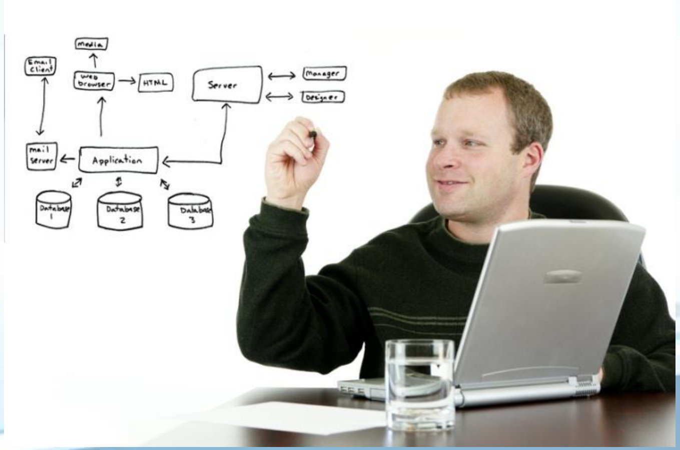
- It is the job of the manager to know the safety goals.

This perspective on safety goals underlines an essential characteristic:

Safety goals are descriptive, not technical.

- They must be understandable to a manager, and not prescribe a technological approach.

SAFETY GOAL



Safe States

- The **safe state** is a key concept in all safety-related standards
  - ***"A safe state is a state of the system without any unacceptable risk caused by the system"***
- **Note that this does not mean acceptable item functionality i.e. the *"desired state"***
  - A vehicle that is standing still is (usually) safe, but it is not necessarily in the desired state (e.g. running well).
- It is important that if a particular safety goal can be **achieved by transitioning to a safe state within the fault reaction time interval (FRTI)** , then there must be a corresponding requirement specified, e.g. how long do you have…

Situations Greatly Expanded with ISO 26262:2018

- From cars and light trucks
- To large trucks with many configurations possible, semi-tractors and trailers, buses, and motorcycles
- Extreme variables in terms of weight, operating parameters, and driver training requirements

Cruise Control Example

SAFETY GOAL: **"Cruise Control is deactivated when the driver is braking"**

SAFE STATE: Remain in 'Off state'

Breakout Exercise 3: Hazard and Risk Analysis

Using the information in the Breakout handout booklet:

- Identify the malfunctions for each function of the system
- Determine relevant Driving situations for the item
  - determine the exposure values (E) for these situations
- Combine the situations with the item‘s malfunctions
  - identify the potential hazards
- Determine the harm induced by the hazards
  - potential effects and severity (S)
  - determine the controllability (C)
- Assign ASIL values to the hazardeous events
- Create safety goals for all ASILs larger than QM

Reference: ItemDefinition-handout.xlsx

HARA Verification

(6.4.6.1) The hazard analysis and risk assessment including the safety goals shall be verified in accordance with ISO 26262-8:2018, Clause 9, to provide evidence for the:

a) appropriate selection with regard to operational situations and hazard identification (and T&B vehicle configuration);

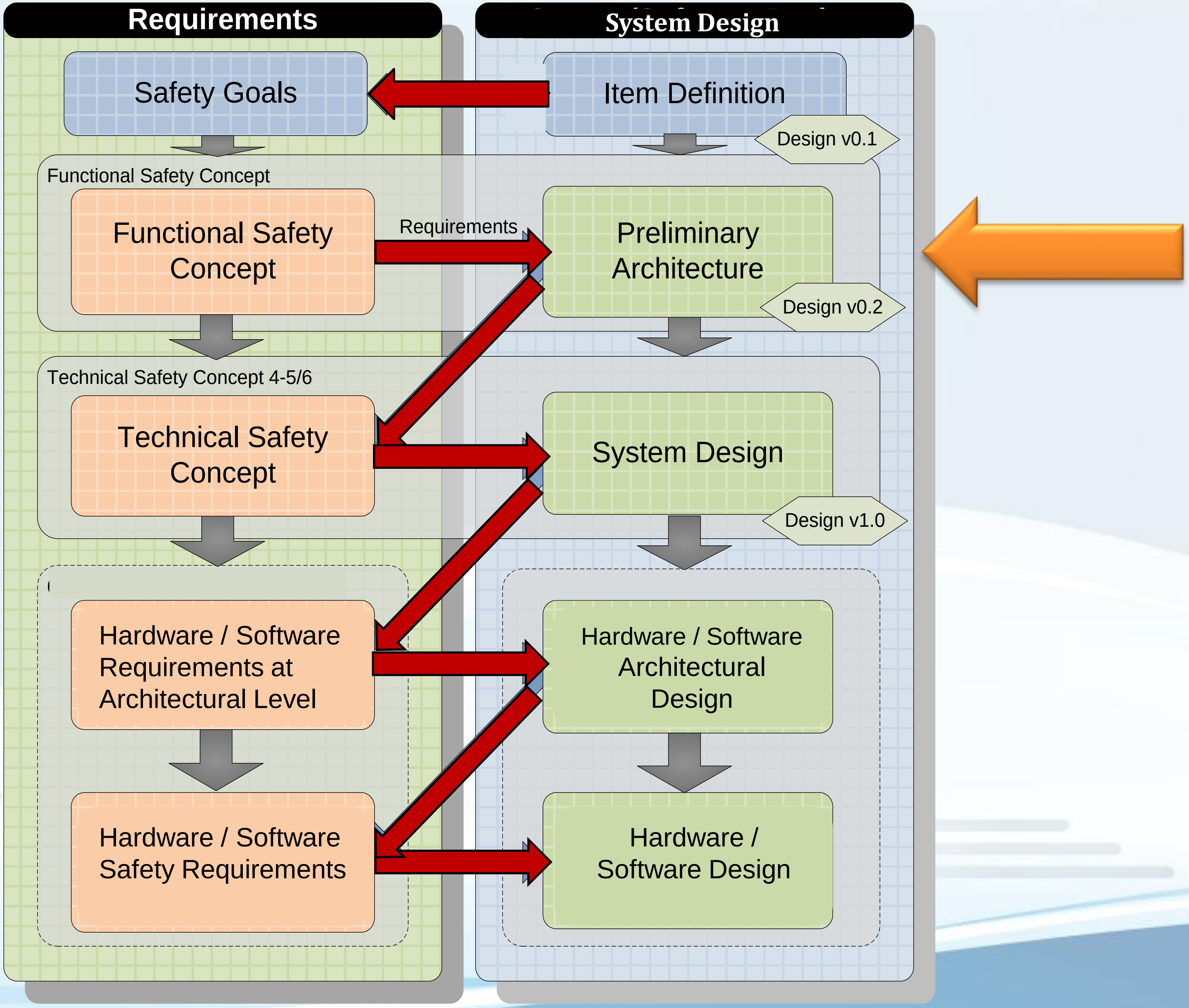
b) compliance with the item definition;

c) consistency with related hazard analyses and risk assessments of other items;

d) completeness of the coverage of the hazardous events; and

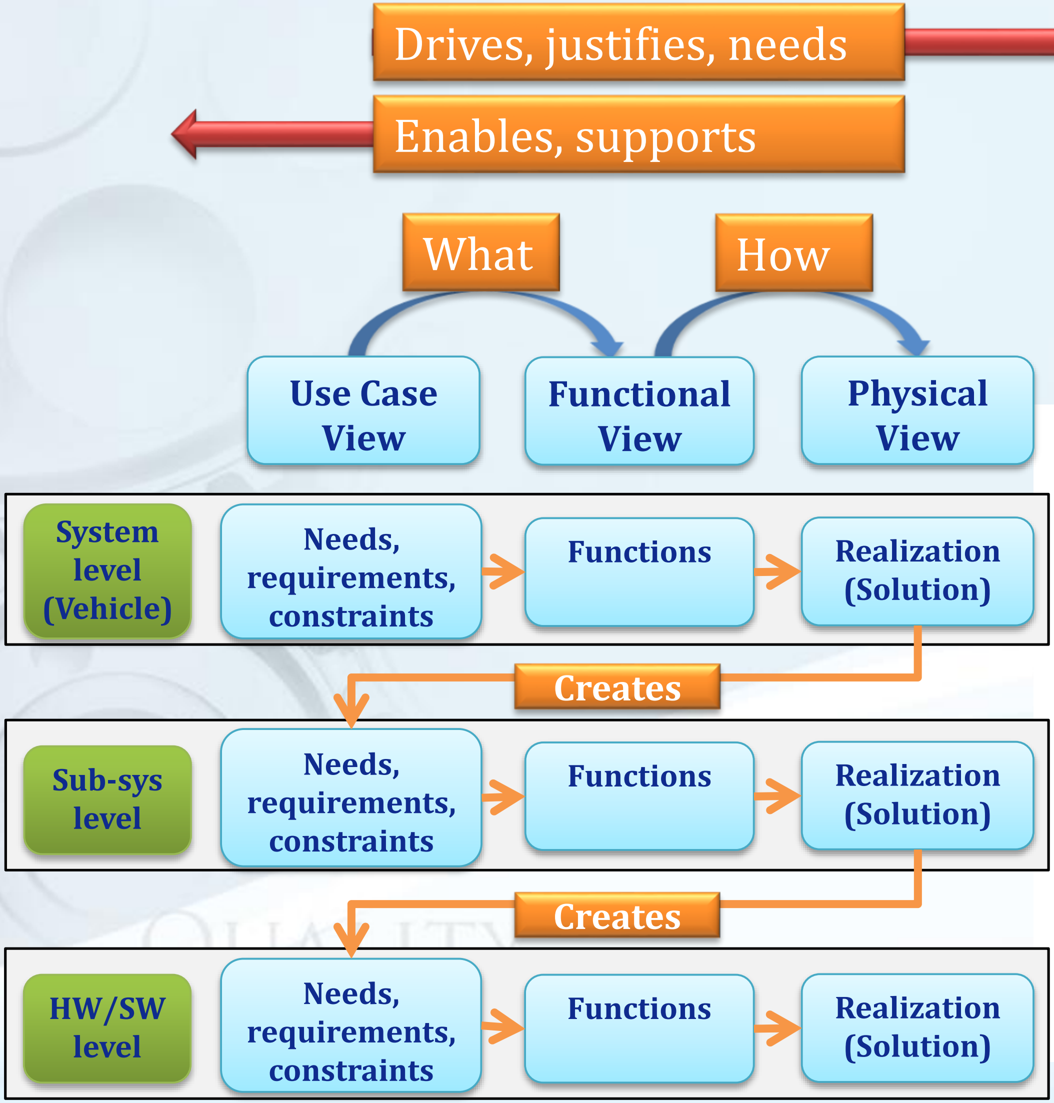
e) consistency of the safety goals with the assigned ASILs and the corresponding hazardous events.

ISO 26262 Development Flow


Requirements
System Design
Safety Goals
Item Definition
Design v0.1
Functional Safety Concept
Functional Safety Concept
Requirements
Preliminary Architecture
Design v0.2
Technical Safety Concept 4-5/6
Technical Safety Concept
System Design
Design v1.0
Hardware / Software Requirements at Architectural Level
Hardware / Software Architectural Design
Hardware / Software Safety Requirements
Hardware / Software Design

Recommended development flow from Requirements to Design (solution) throughout the system hierarchy

Development Flow Principles



Drives, justifies, needs

Enables, supports

What

How

Use Case View

Functional View

Physical View

System level (Vehicle)

Needs, requirements, constraints

Functions

Realization (Solution)

Creates

Sub-sys level

Needs, requirements, constraints

Functions

Realization (Solution)

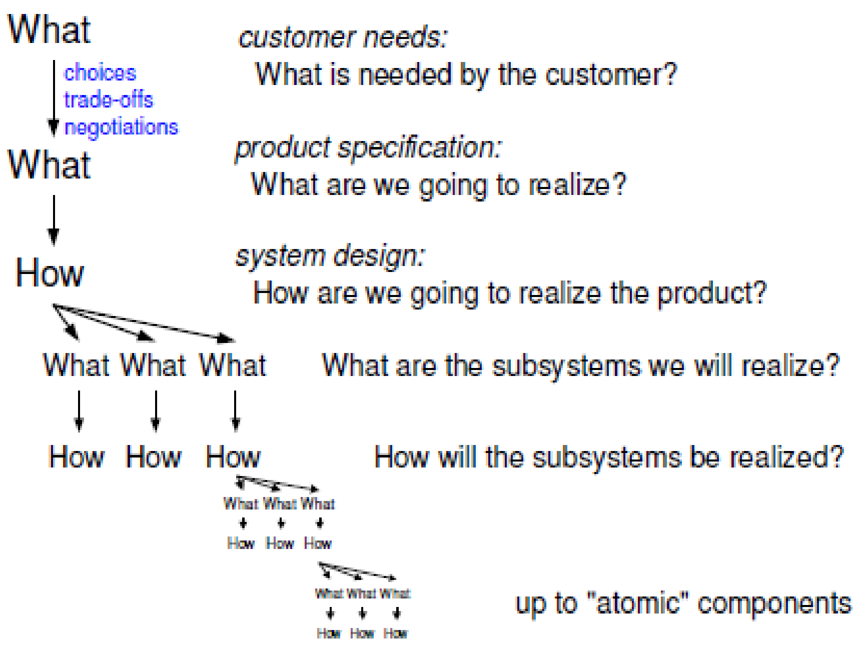
Creates

HW/SW level

Needs, requirements, constraints

Functions

Realization (Solution)



What

choices
trade-offs
negotiations

customer needs:
What is needed by the customer?

What

product specification:
What are we going to realize?

How

system design:
How are we going to realize the product?

What What What

What are the subsystems we will realize?

How How How

How will the subsystems be realized?

up to "atomic" components

OMNEX

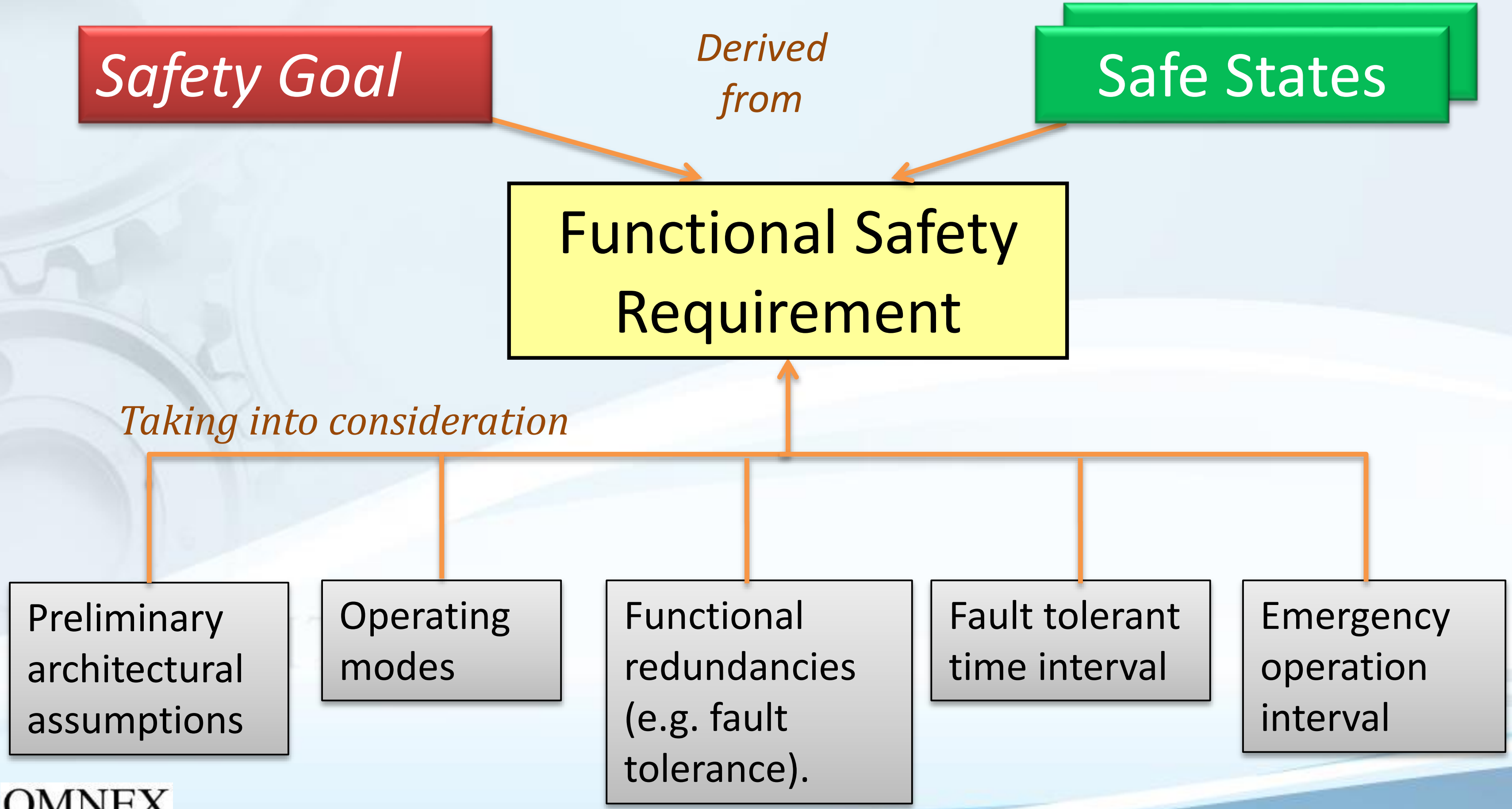
Requirements

- A ***Functional*** Requirement will address a deficiency in the design that will result in a violation of a ***Functional*** Goal
- A ***Safety*** Requirement will address a deficiency in the design that will result in a violation of a ***Safety*** Goal

That is, a Functional Safety Requirement is fundamentally a Functional Requirement that also addresses a Safety Goal.

Requirement Derivation

(8.4.2.1) The functional safety requirements shall be derived from the safety goals and safe states, taking into account the preliminary architectural assumptions.



Safety Goal

Derived from

Safe States

Functional Safety Requirement

Taking into consideration

Preliminary architectural assumptions

Operating modes

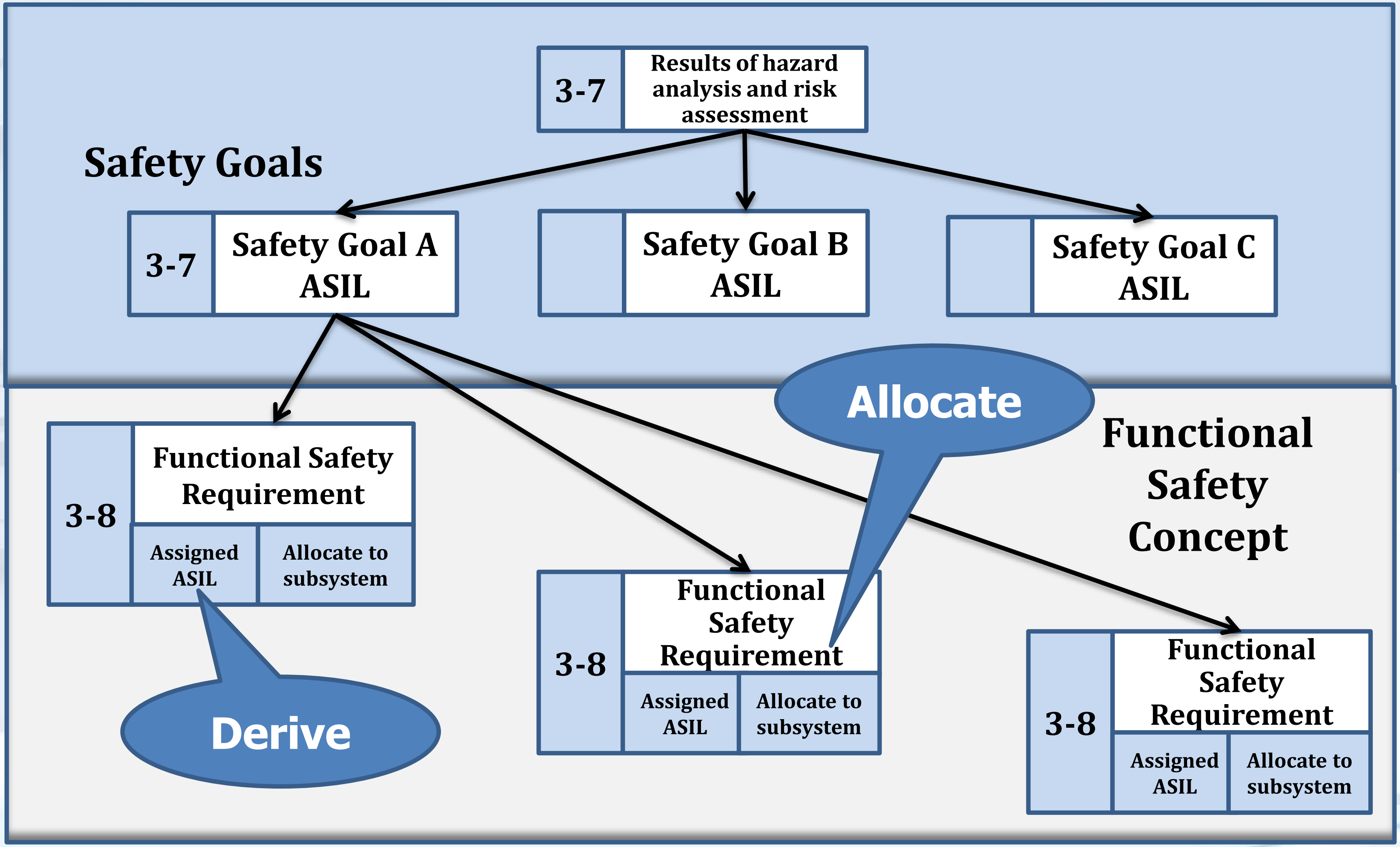
Functional redundancies (e.g. fault tolerance).

Fault tolerant time interval

Emergency operation interval

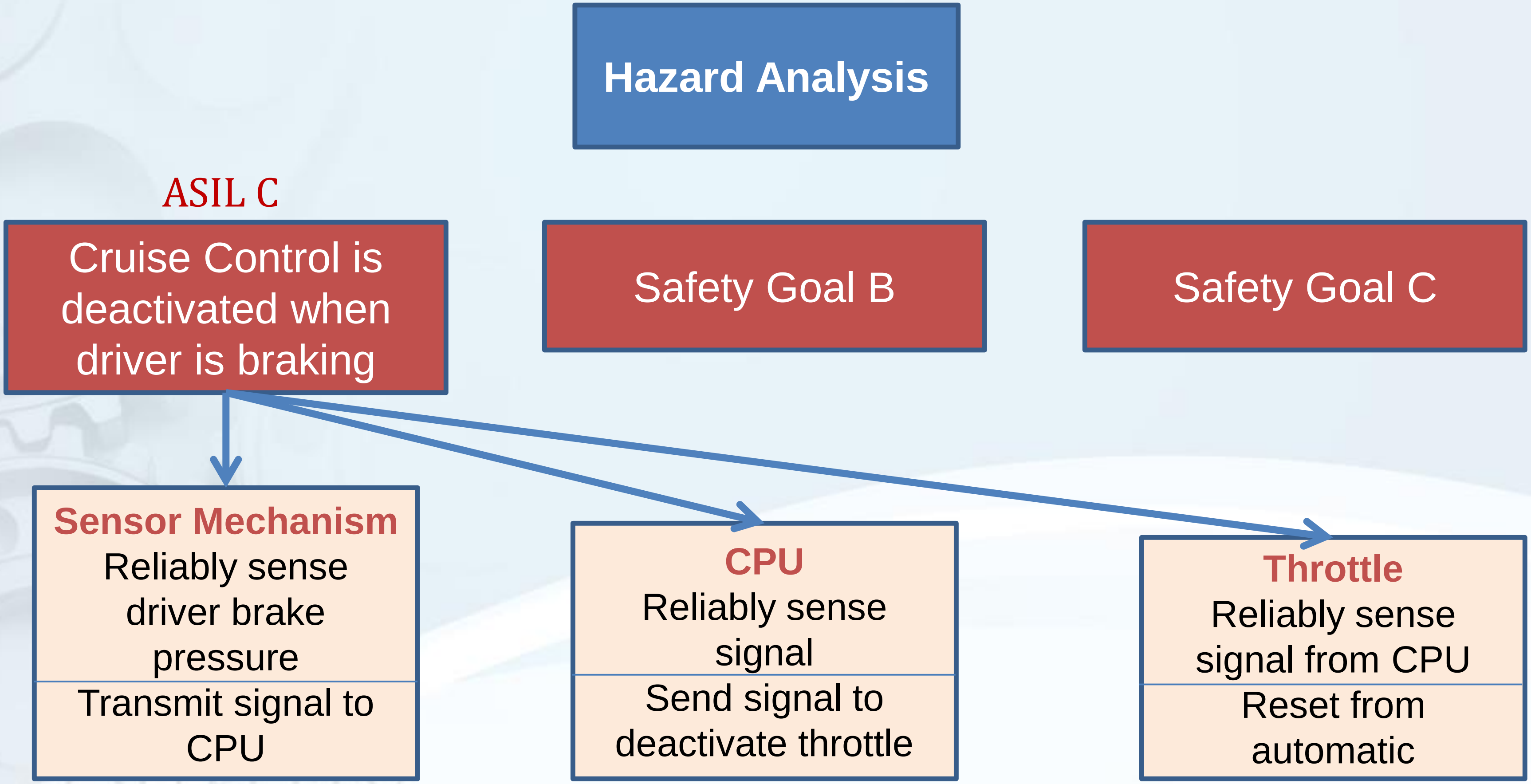
OMNEX

Functional Safety Requirements



OMNEX

Safety Goals and Requirements – Cruise Control



Hazard Analysis

ASIL C

Cruise Control is deactivated when driver is braking

Safety Goal B

Safety Goal C

Sensor Mechanism

Reliably sense driver brake pressure

Transmit signal to CPU

CPU

Reliably sense signal

Send signal to deactivate throttle

Throttle

Reliably sense signal from CPU

Reset from automatic

Functional Safety Concepts

Characteristics of Safety Requirements

Safety requirements must:

- Be unambiguously identifiable as safety requirements
- Inherit the ASIL from the safety requirements from which they are derived
- Be allocated to an item or an element
- Have the following characteristics:
  - Unambiguous
  - Complete / Comprehensible
  - Atomic
  - Internally Consistent / Correct
  - Feasible
  - Verifiable
  - Traceable

Breakout Exercise 4: FSR

Using the information in the Breakout handout booklet:

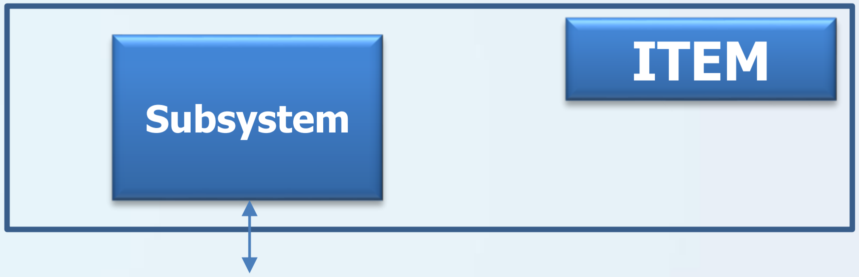
- Determine how the product could violate the Safety Goal with the “Unintended” malfunction; i.e. “Activates without demand“.
  - Use a fault tree analysis to identify negative events
- Determine what design changes are needed to eliminate, mitigate, or monitor/control negative events
- Develop Functional Safety Requirements
- Develop a safety architecture
- Develop Functional Safety Concepts

Reference: Functional Safety Concept - handout.xlsx

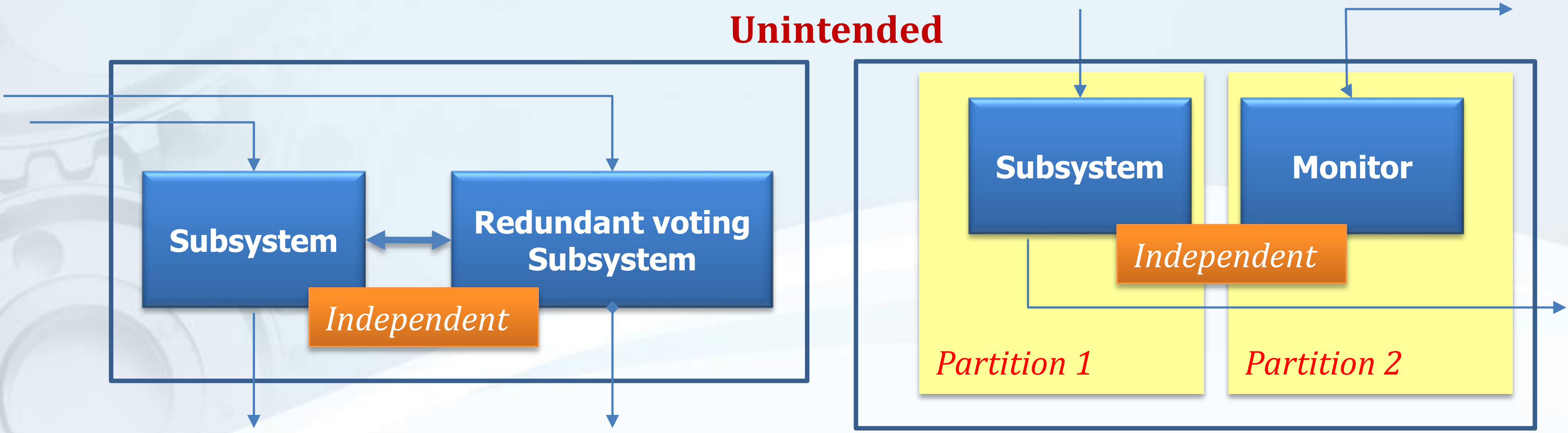
Preliminary Safety Architecture

Original Architecture

Block diagrams are sufficient for showing preliminary architectural assumptions



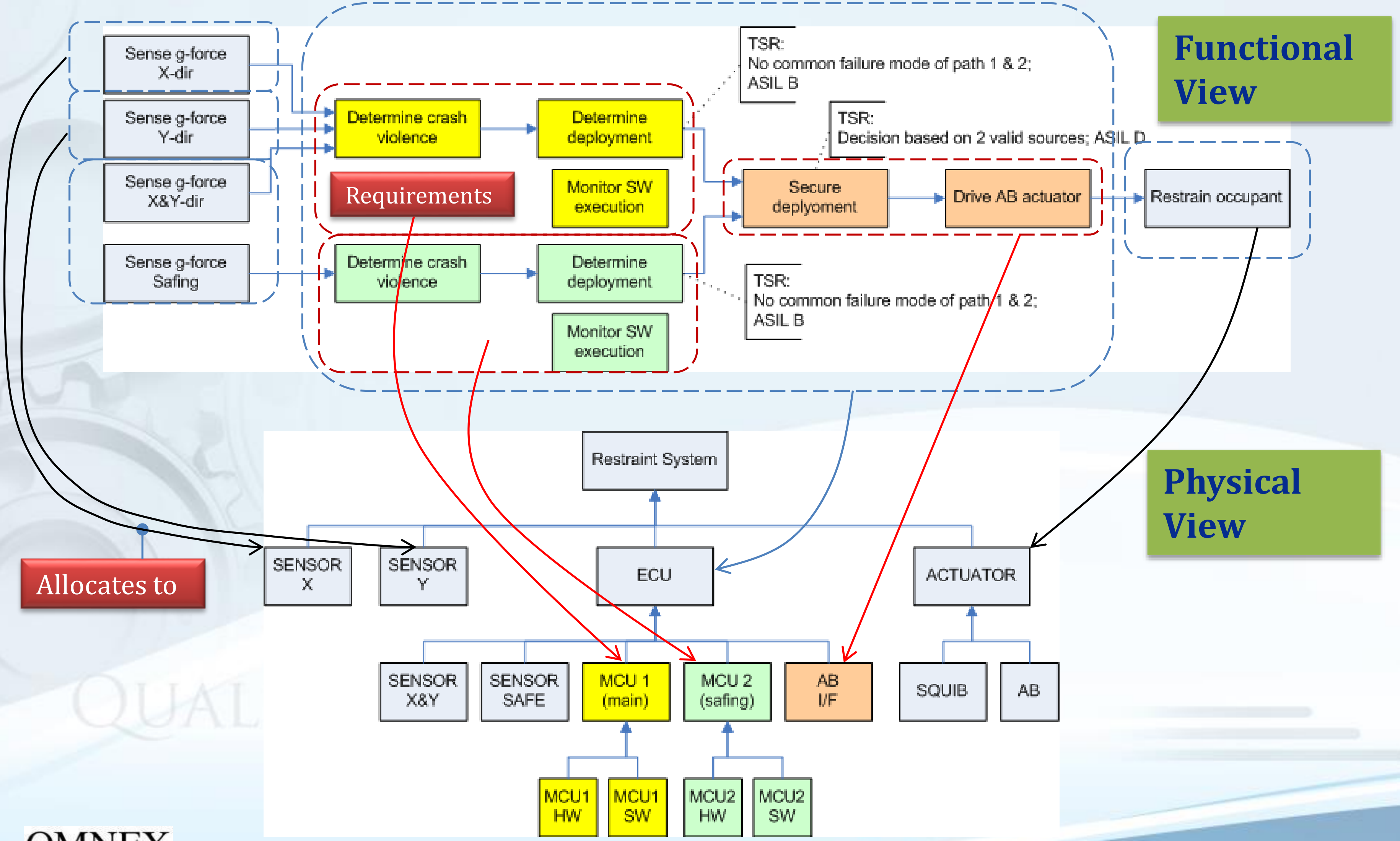
Unintended



- **Why <u>safety</u> architecture?**
  - Because it includes your **<u>basic</u>** concepts for ensuring safety such as redundancy and independence.

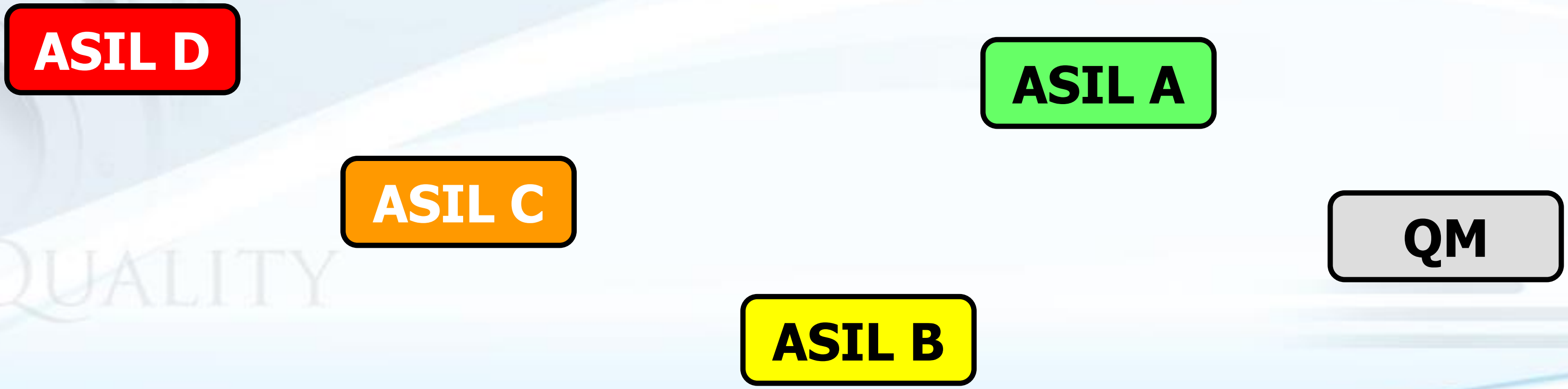
Requirements Allocation

Example 1: Restraint System (ECU with 2 MCU:s)



ASIL Assignment

- The basic principles for assigning ASILs to the allocated requirements are:
  - Inheritance
  - Highest level
  - Decomposition (detailed in Part 9)



ASIL D

ASIL C

ASIL B

ASIL A

QM

Safety Validation / Verification

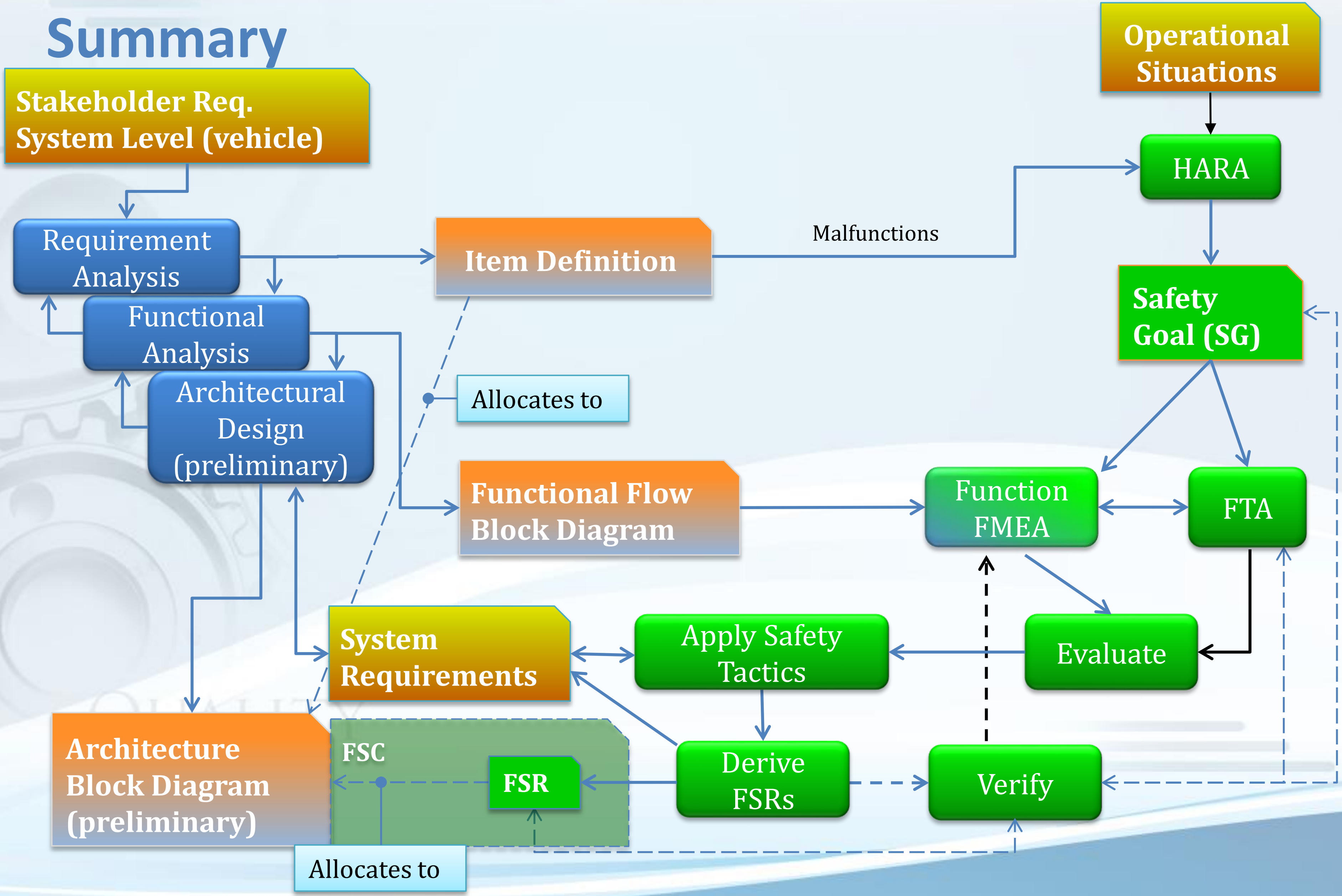
- **(7.4.3.1)** The acceptance criteria for safety validation of the item shall be specified based on the functional safety requirements and the safety goals.
  - Safety validation of the safety goals is addressed on the upper right of the V cycle **but is included in the activities during development and not only performed at the end of development.**
- **(7.4.4.1)** The functional safety concept shall be verified in accordance with ISO 26262-8:2018, Clause 9, to provide evidence for:

  a) its consistency and compliance with the safety goals; and

  b) its ability to mitigate or avoid the hazards.

The verification (carried out during the concept phase) can be based on the same methods that are used for safety validation; however, the safety validation undertaken cannot be based on concept studies alone (e.g. prototypes)

Functional Safety Concept Development – Summary



Copyright 2019 Omnex, Inc. All Rights Reserved

Chapter 6

ASIL-Oriented and Safety-Oriented Analyses (Part 9)

OMNEX

Requirements Decomposition with Respect to ASIL Tailoring

Objectives

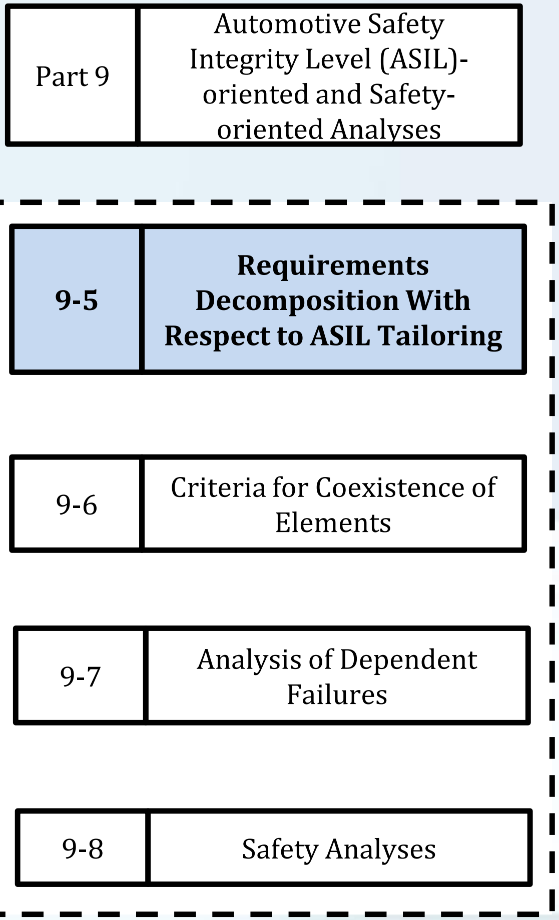
- Provide rules and guidance to decomposing safety requirements into functionally redundant safety requirements to allow ASIL tailoring at the next level of detail.

Prerequisites

- The safety requirements at the level at which the ASIL decomposition is to be applied; system, hardware, or software.
- The architectural information at the level at which the ASIL decomposition is to be applied; system, hardware, or software.

Work Products

- Update of Architectural Information
- Update of ASIL as attribute of safety requirements and elements



Part 9	Automotive Safety Integrity Level (ASIL)-oriented and Safety-oriented Analyses
9-5	**Requirements Decomposition With Respect to ASIL Tailoring**
9-6	Criteria for Coexistence of Elements
9-7	Analysis of Dependent Failures
9-8	Safety Analyses

General

- The method of ASIL Tailoring during the design process is also called “***ASIL Decomposition.***”
- Benefits can be obtained from architectural decisions including the existence of sufficiently independent architectural elements. This offers the opportunity:
  - To implement safety requirements redundantly by those independent architectural elements, and
  - To assign a potentially lower ASIL to these decomposed safety requirements.
- If the architectural elements are not sufficiently independent, then the redundant requirements and the architectural elements inherit the initial ASIL.

Basic Principles

- An element implemented to address a given safety goal, with a given ASIL may be decomposed *into* ***two independent*** elements, with possibly lower ASIL.
  - Each must address the **same safety goal.**
  - And each must take on the **same safe state.**
- Can be used in the following phases:
  - Functional Safety Concept
  - System Design
  - Hardware Design
  - Software Design
- ASIL decomposition is a **qualitative** concept, more addressing systematic issues (architecture) than random errors (hardware reliability)
  - It can be a way of making architectures more robust.
  - Similar to 61508 fault-tolerant architecture concepts.

Requirements and Recommendations

- ASIL decomposition shall consider each initial safety requirement individually.
- The initial safety requirement shall be decomposed to redundant safety requirements implemented by sufficiently independent elements.
- Each decomposed safety requirement shall comply with the initial safety requirement by itself.
- The requirements on the evaluation of the hardware architectural metrics and evaluation of safety goal violations due to random hardware failures shall remain unchanged by ASIL decomposition.

Requirements and Recommendations

- In the case of ASIL Decomposition resulting in redundant safety requirements being implement with hardware elements, how does this help to meet the architectural metrics and probability of failure due to random hardware failures?
  1. Eliminates Single Point Failures – only dual point failures will result in the violation of a safety goal.
  2. Failure due to random hardware failures requires that there be two random hardware failures – the **probability is the product of the probability of the two independent failure rates**.
- For ASIL decomposition applied at the software level, sufficient independence between the elements shall be checked at the system level and appropriate measures taken at the software level, or hardware level, or system level to achieve sufficient independence

Requirements and Recommendations

- When ASIL decomposition of an initial safety requirement results in the allocation of decomposed requirement to the intended functionality and an associated safety mechanism, then:
  - The associated safety mechanism should ***be assigned the highest decomposed ASIL.***
  - A safety requirement shall be allocated to the intended functionality and implemented applying the corresponding decomposed ASIL.
- If a violation cannot be prevented by switching off the element, then adequate availability of the sufficiently independent elements implementing the decomposed safety requirements shall be shown.

Requirements and Recommendations

- When applying ASIL Decomposition, then:
  a) ASIL decomposition shall be applied according to the next slide;
  b) ASIL decomposition may be applied more than once;
  c) Each decomposed ASIL shall be marked by giving the ASIL of the safety goal in parenthesis.

Example:
If an ASIL D requirement is decomposed into one ASIL C requirement and one ASIL A requirement, then these are marked as “ASIL C(D)” and “ASIL A(D)”.

If the ASIL C(D) requirement is further decomposed into one ASIL B requirement and one ASIL A requirement, then these are also marked with the ASIL of the safety goal as “ASIL B(D)” and “ASIL A(D)”.

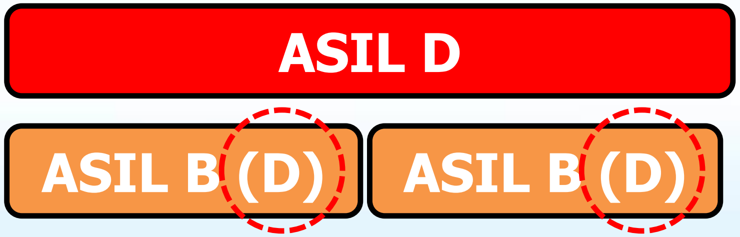
ASIL Decomposition

ASIL D	ASIL D		ASIL D		ASIL D	
	ASIL C (D)	ASIL A (D)	ASIL B (D)	ASIL B (D)	ASIL D (D)	QM (D)
ASIL C			ASIL C		ASIL C	
			ASIL B (C)	ASIL A (C)	ASIL C (C)	QM (C)
ASIL B			ASIL B		ASIL B	
			ASIL A (B)	ASIL A (B)	ASIL B (B)	QM (B)
ASIL A					ASIL A	
					ASIL A (A)	QM (A)

Table of valid combinations for ASIL decomposition

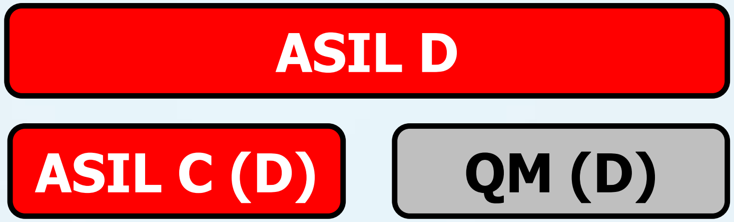
Original ASIL

- Note that after ASIL decomposition, the original ASIL is kept in parentheses.
  - Why keep the original ASIL in parentheses?
- **Answer:** because the overall requirements on the function remain the same and must be fulfilled **according to the original Safety Goal's ASIL.**
  - "Confirmation measures"
  - Hardware metrics (single-point fault metric, latent-fault metric)
  - Measure of probability of violating the safety goal (random failures; reliability)
  - Integration / Testing Activities



Separation of Concerns

A closer look at:



- The last column in the table is special; an ASIL is split into two elements:
  - One element has the same ASIL.
  - The other element is QM.
- What is the logic behind this?
  - This is **separation of concerns**: the purely functional aspects are separated from the safety-related aspects.
- Increases possibilities for reuse, lowers production costs, etc.
  - But may not always be possible if an element is handling several functions with different ASIL, or because it may be too expensive to separate the safety related functions from the other ones.

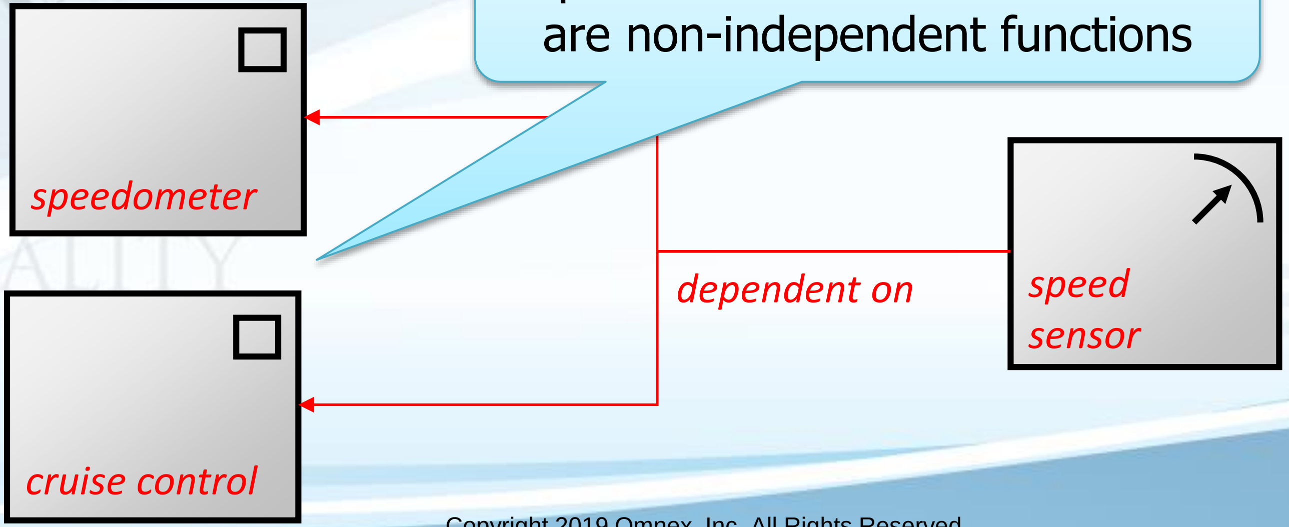
Coexistence

- It is not enough to simply decompose an element into two sub-elements with a lower ASIL.
  - You must make a convincing argument that these sub-elements can safely **co-exist**.
- This essentially means showing their total **independence** from each other.
- This means:
  - The obvious part: **operational independence**
  - The less obvious part: **no common cause dependencies**
  - The non-obvious part: **freedom from interference**

?
independent?

Operational Independence

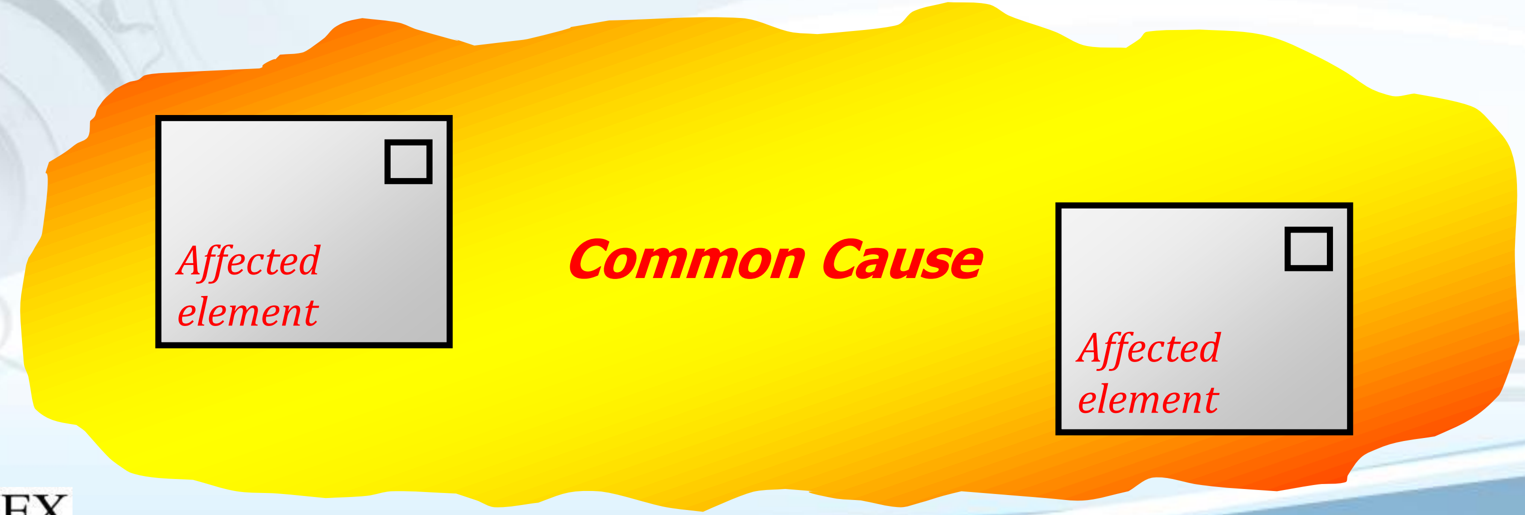
- Consider two functions such as a speedometer and a cruise control.
- Assume that they both rely on a speed sensor to receive the inputs necessary for their operation.
- They may seem to be independent elements, but in fact they are not, because they both depend upon the same sensor.
- If the sensor fails, their operation is at risk.



Speedometer and cruise control are non-independent functions

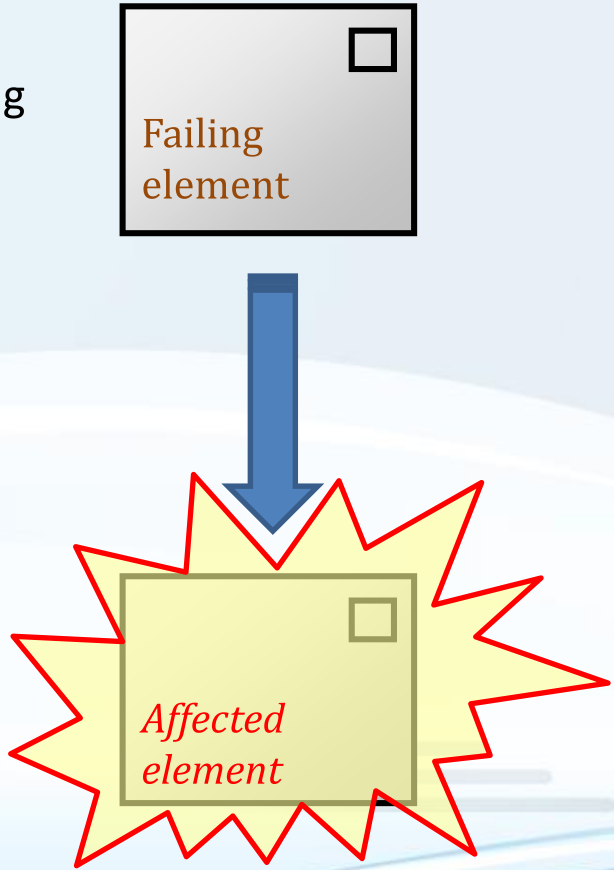
Common Cause Failures

- Elements can be operationally independent from each other but still be subject to outside forces that cause them to fail.
  - Example: strong electromagnetic signals that cause elements each to fail in their own specific ways.
- These elements are subject to failures due to a **common cause.**
  - And therefore they are not truly independent from each other.



Freedom from Interference

- Functional independence by itself doesn’t guarantee total independence.
- Even two functionally independent elements can affect each other through erroneous behavior.
  - An element “gone wild” can create so-called cascading errors, where it causes the failure of other elements.
- **Freedom from interference** means that an element is unable to make another element fail through erroneous behavior.
  - In other words, the failing element does not interfere with the other element.



Requirements and Recommendations

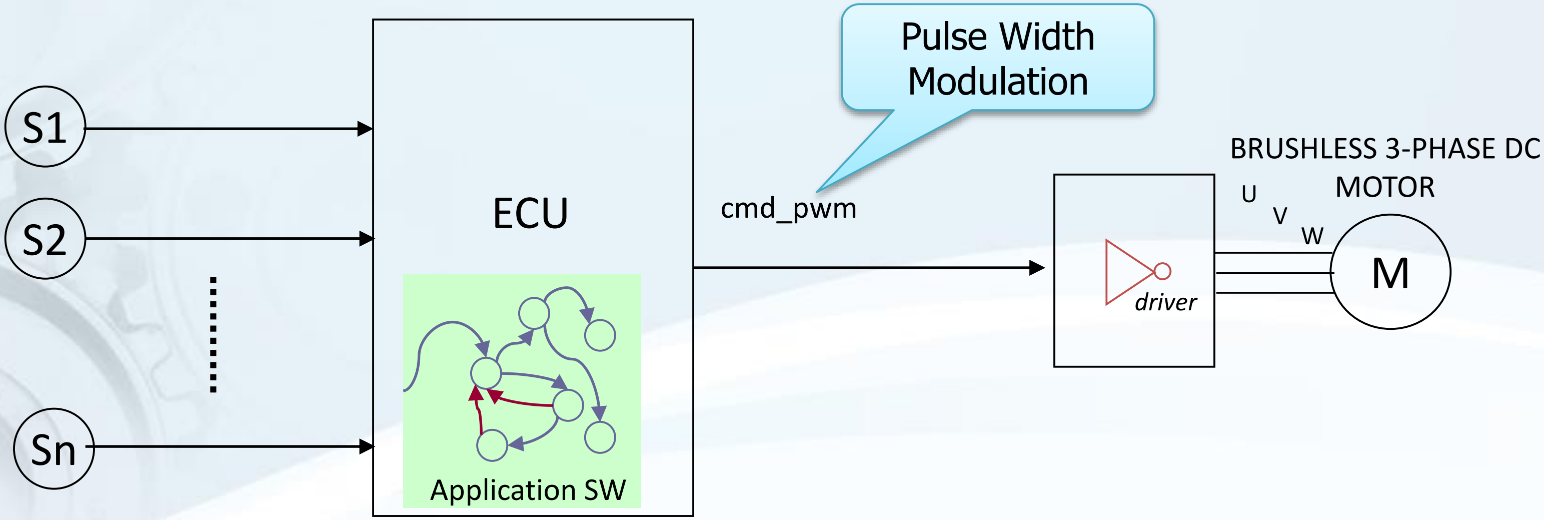
- The following shall be used with any of the decomposition schemes:
  a) Confirmation measures shall be applied according to the ASIL of the Safety Goal.
  b) Evidence for sufficient independence of the elements after decomposition shall be made available.

- When a decomposition scheme for ASIL D, then:
  – The same software tools shall be considered as software tools for developing ASIL D items or elements.

EXAMPLE — SCENARIO

Problem Description

- Consider a function **F** which, upon input from a combination of sensors **S1, S2**, ... **Sn** issues an activation command to actuator **M** ("Motor"):
  - Suppose that the Safe State for F is "**M deactivated**".
  - Suppose that Hazard and Risk Analysis has determined **ASIL C** for the function F.

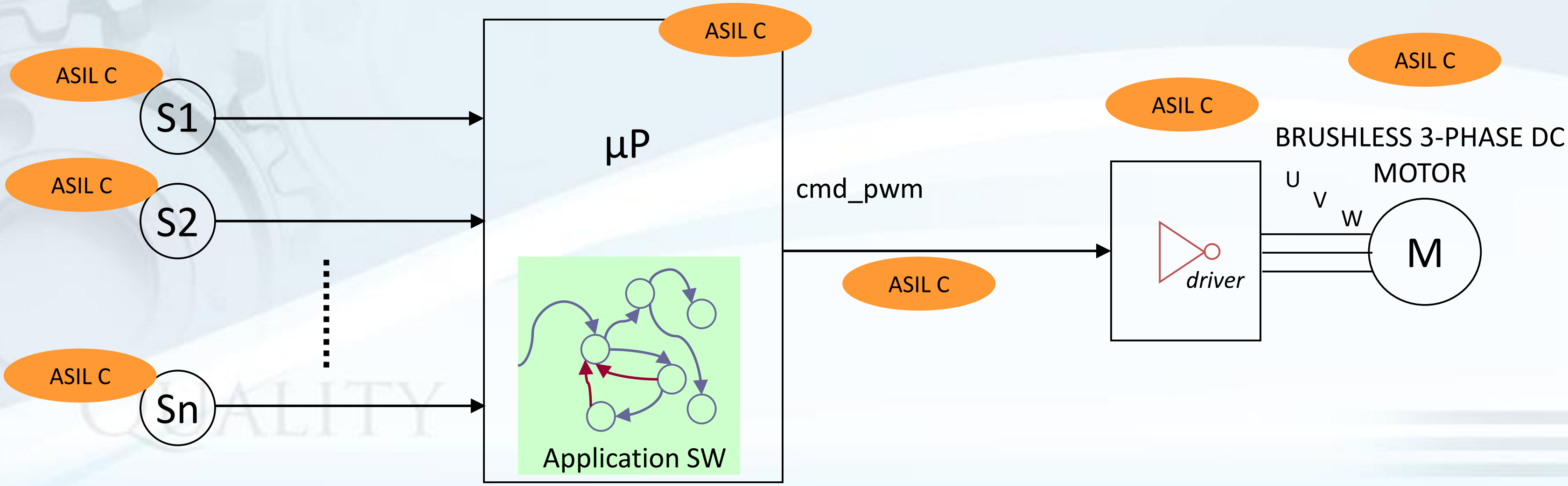


- Suppose that we have identified the following safety goal:

  "**Avoid the undesired activation of M**"
  - Whereby "undesired" means "as a result of an incorrect combination of sensors S1, S2, ... Sn"

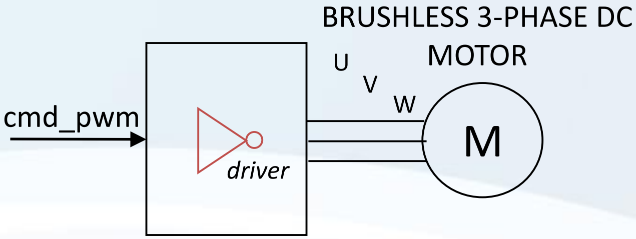
ASIL Allocation

- Suppose further that sensor **S1, S2, … Sn** measures some different value.
  - That is, the sensors are independent of each other and non-redundant.
- Further more, in this scenario we assume that ***each*** of these sensors could ***by itself*** cause the safety goal to be violated.
  - The ASIL theory of the standard says that therefore each of the sensors must also inherit the ASIL C allocated to the function F.



First Analyses

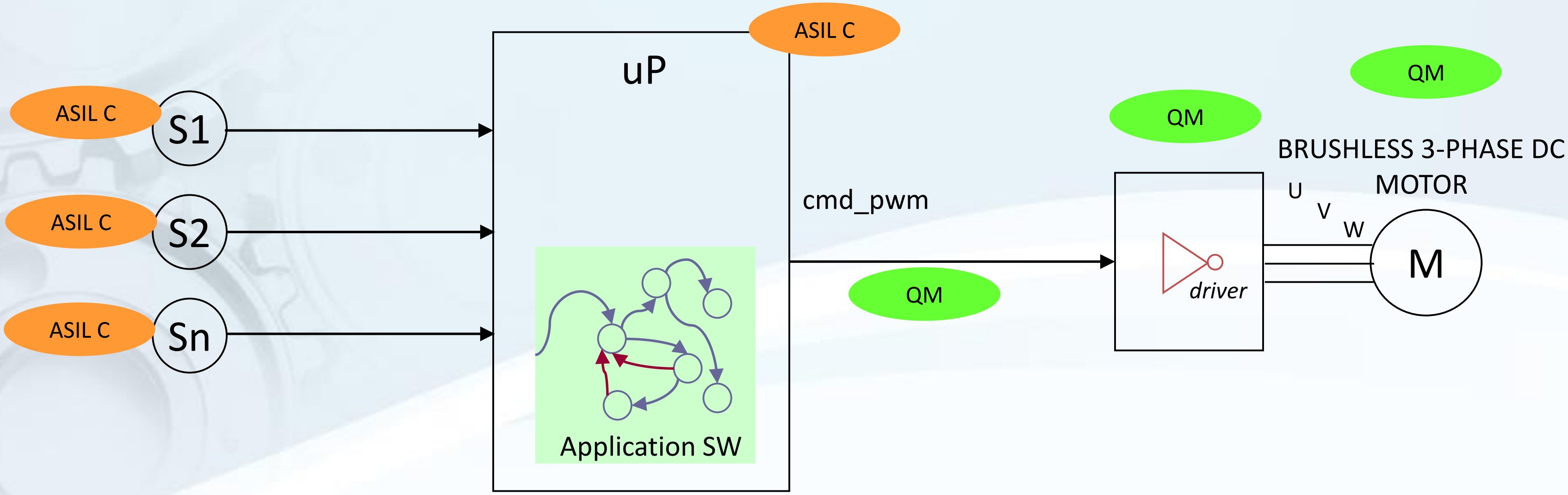
- At this point, we begin to analyze our architecture, reasoning about which elements of the architecture in reality have the capability of violating the safety goal.
  - This may exploit specific knowledge of the technology involved.
- In this example, we know from the theory of the control of brushless 3-phase DC motors that the three phases need signals that are precisely defined in time.
  - Therefore an error in some of the components (e.g., the driver and its associated command channel) could not possibly produce the precise signals necessary to erroneously activate M.
  - And therefore they are incapable ***by themselves*** of violating the safety goal.



Brushless 3-phase DC motor technology needs precise input signals – impossible for a malfunctioning driver to produce

Lowering ASIL

- As a result of this analysis, we are justified in lowering the ASIL of the driver, motor, and command channel to QM.
  - Note that this depends entirely on the technology; if the motor were based on continuous technology, it would not have been possible to lower the ASIL to QM.



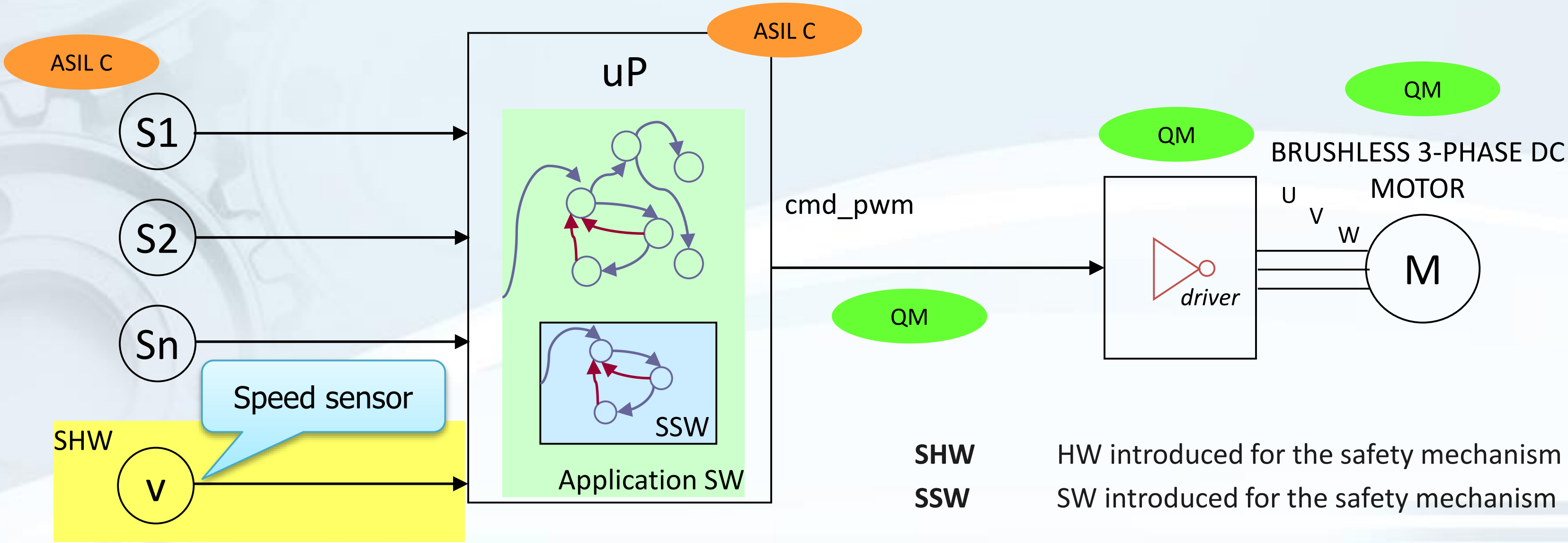
Lesson Learned: Sometimes through examining the technology and its potential for safety goal violation, we can influence ASIL allocation. Sometimes a project might even change its technologies after such analyses.

Exploiting the H&R Analysis

- We now look for ways to improve the safety architecture, by exploiting the results of the **hazard and risk (H&R) analysis.**
- In its current form, the architecture considers only “erroneous sensor inputs”, regardless of the operational scenario.
  - But suppose that the H&R analysis distinguished operational scenarios, such as the speed of the vehicle? (this is typical).
- Suppose that the H&R analysis yielded the result that undesired activation of M was only dangerous at a speed greater than some threshold?
  - (As another example, consider undesired deployment of an airbag – its effect depends on the velocity of the vehicle).
  - Other typical examples of operational scenarios might be “driver-side door open” or “temperature of engine greater than some threshold”.
- The results of this H&R analysis yield information that we can exploit to introduce a **safety mechanism** in our architecture.

Introducing a Safety Mechanism

- We now introduce a safety mechanism: “The function M must not be activated when vehicle speed **is greater than** a specified threshold”.
  - This is effectively introducing a kind of “AND” gate to lower the probability of M being erroneously activated.
  - The undesired activation of M can only occur now if F and safety mechanism fail *and* v > threshold.



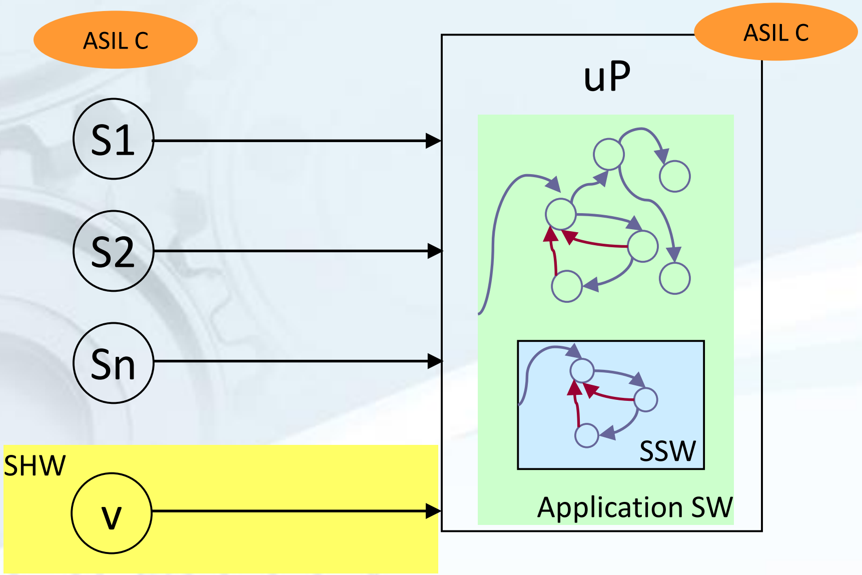
SHW HW introduced for the safety mechanism

SSW SW introduced for the safety mechanism

Lesson Learned: By careful examination of the Hazard and Risk Analysis and sufficiently detailed analysis of operational scenarios, we can discover possibilities for the introduction of safety mechanisms in the architecture.

Safety Mechanism ASIL?

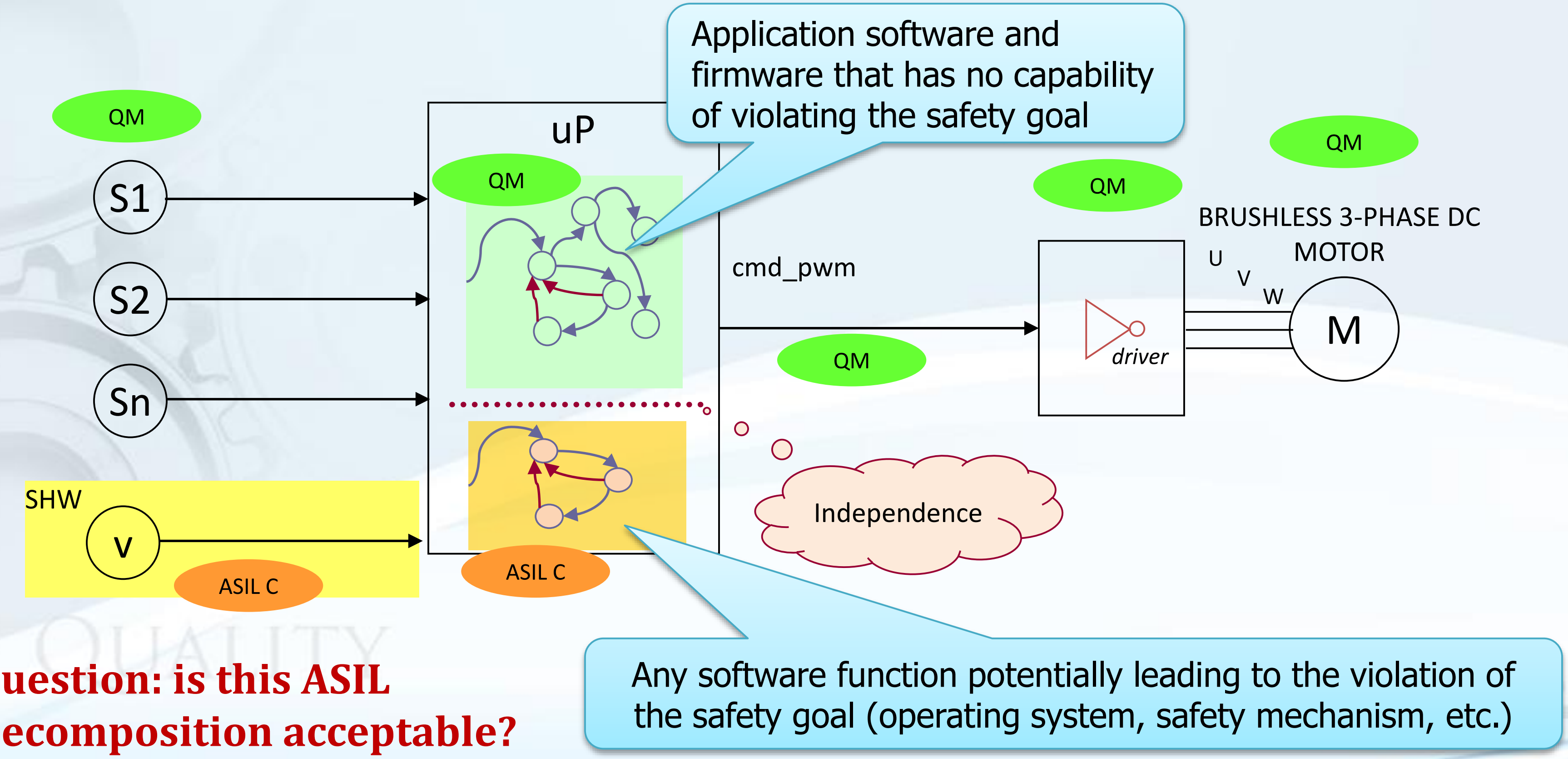
- Note that we have actually changed the architecture now:
  – We have introduced a new sensor V.
  – We have introduced new software.



- But have we changed the ASIL allocation?
  – The answer is “**No**”.
  – The mere addition of a safety mechanism *by itself* does not change the ASIL allocation.

SW ASIL Decomposition?

We find ASIL C for our system software to be too high, but we don't want to introduce hardware redundancy into the control logic, so we decide to apply **ASIL Decomposition at the software level.**



Application software and firmware that has no capability of violating the safety goal

Any software function potentially leading to the violation of the safety goal (operating system, safety mechanism, etc.)

Question: is this ASIL Decomposition acceptable?

Independence?

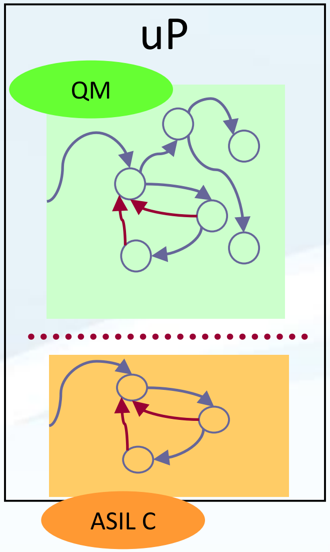
Answer: the proposed software-level ASIL decomposition is acceptable **only if the criteria of independence are satisfied.**

- This includes not only examining the software but also the hardware.

Furthermore: What about the hardware metrics?

Do they become ASIL QM, or ASIL C? Or some combination based on percentages?

Answer: hardware metrics are not affected, so they are still ASIL C!

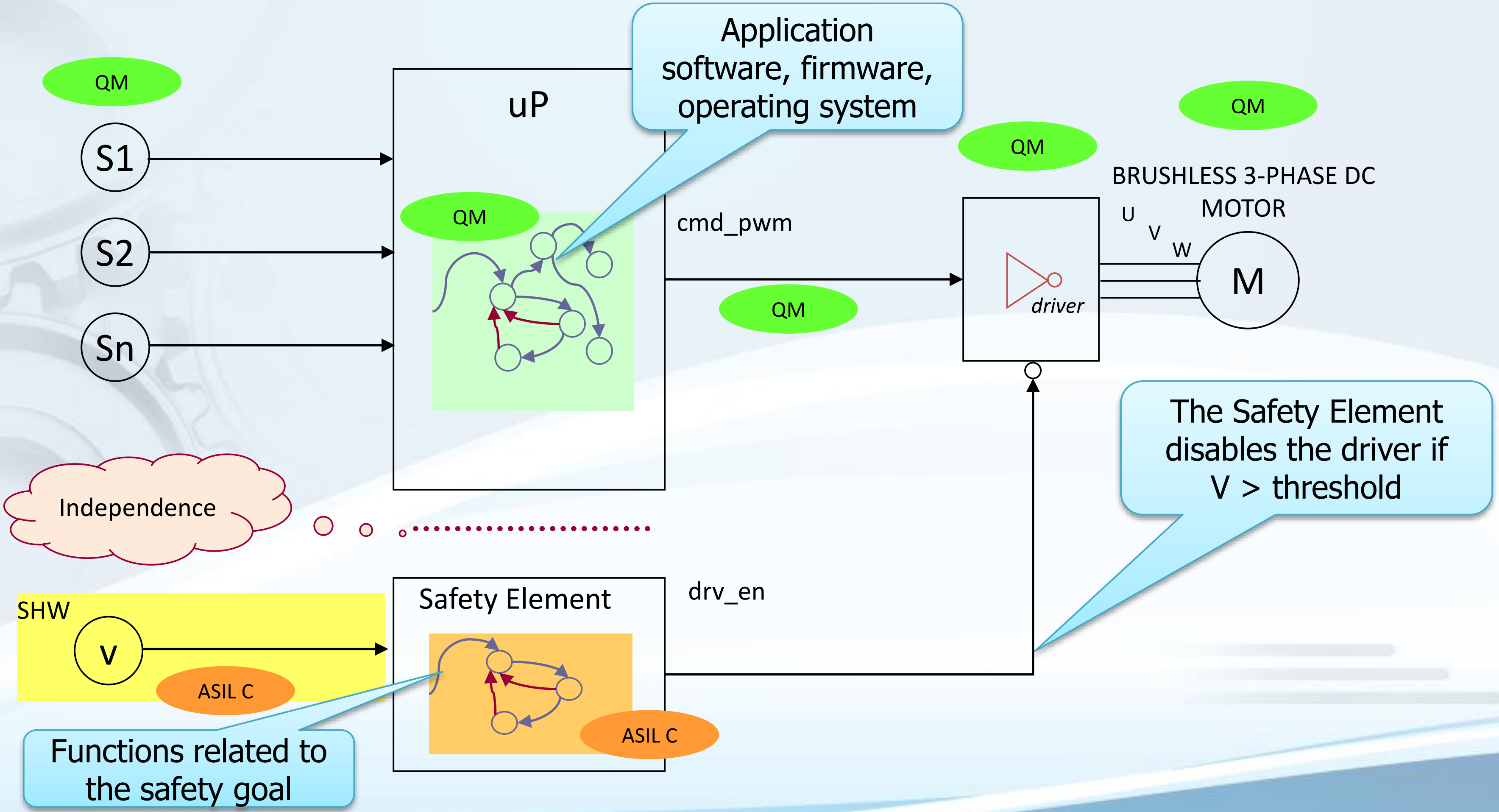


- There are several issues:
  - What about sharing of software resources like the underlying operating system?
  - Sharing of firmware?
  - What about sharing of hardware resources like memory, ALU, etc.?

Lesson Learned: Software level ASIL decomposition involves a careful analysis of *both* software and hardware independence. Hardware metrics are not affected by ASIL decomposition at the software level.

HW-Level Decomposition

Our analysis of software level decomposition determines that there are too many issues, and we decide to do a HW-level decomposition.



Application software, firmware, operating system

The Safety Element disables the driver if V > threshold

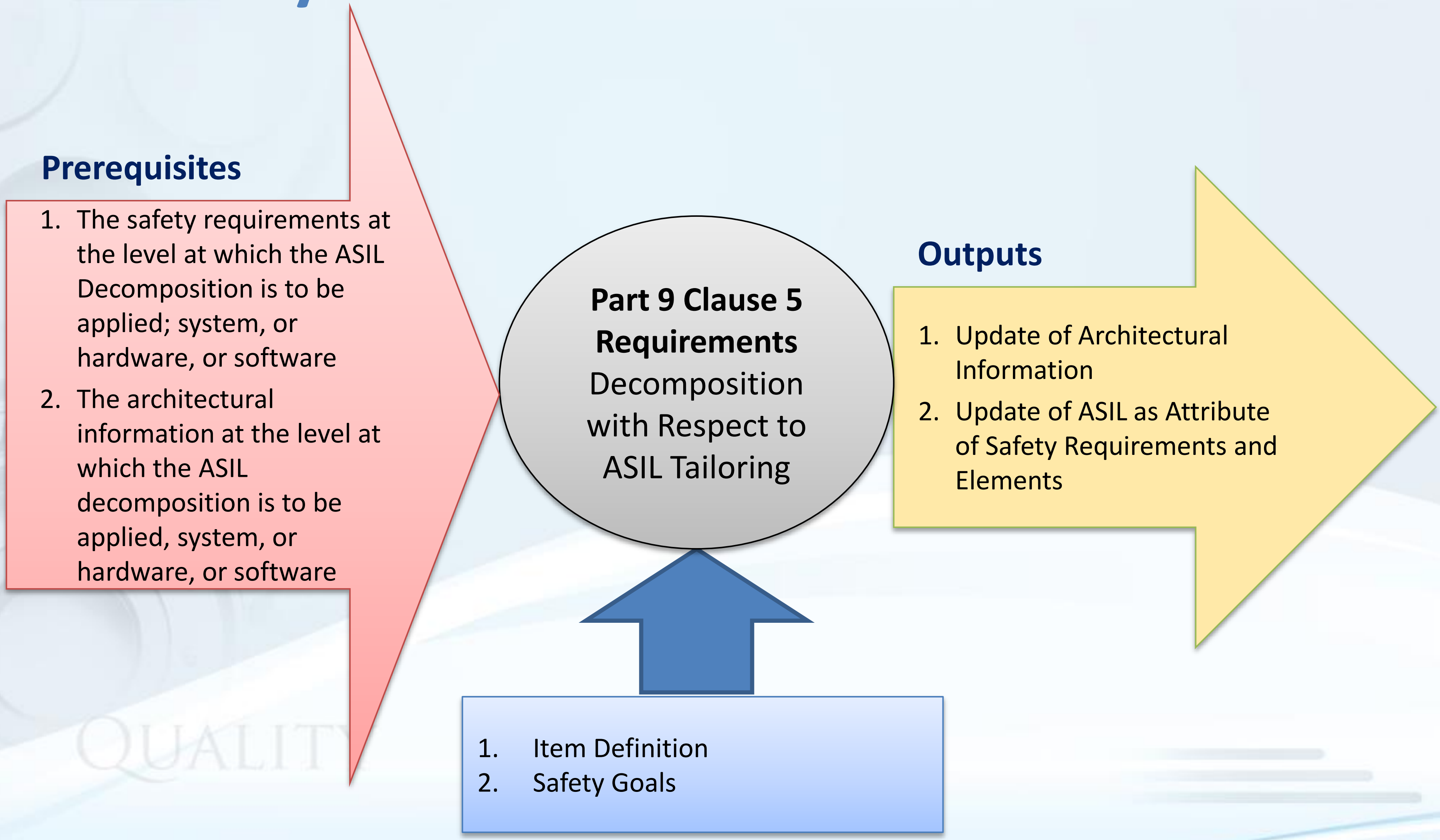
Functions related to the safety goal

The Safety Element

- What exactly is the Safety Element in terms of hardware?
  - This doesn’t have to be a full microprocessor.
  - It can be a programmable gate array, essentially just a state machine, programmed only one time, with no operating system.
  - They cost only one-tenth of a full micro, and are very reliable, with their own clock, power supply, easy to manage.
- There is little embedded logic – so there is little software.
  - This has consequences for the ISO 26262 safety process.
  - There is much less to handle in Part 5.
- That is why it is only called a safety element.
  - It depends on the safety function to be carried out.

Lesson Learned: Hardware level ASIL decomposition involves deep knowledge of the characteristics of the available hardware, so that independence, functionality, and costs are all correctly balanced.

Summary



Prerequisites

1. The safety requirements at the level at which the ASIL Decomposition is to be applied; system, or hardware, or software
2. The architectural information at the level at which the ASIL decomposition is to be applied, system, or hardware, or software

Part 9 Clause 5 Requirements
Decomposition with Respect to ASIL Tailoring

Outputs

1. Update of Architectural Information
2. Update of ASIL as Attribute of Safety Requirements and Elements

1. Item Definition
2. Safety Goals

Supporting Information

SAFETY ANALYSES IN ISO 26262

Safety Analyses in ISO 26262

- **Safety analyses** are an important part of any safety-related development process.
  - Over the years, many types of analyses have been developed in many industries (military, space, automotive, industrial manufacturing, etc.)
  - Various standards promote the use of various types of analyses.
- But in addition to the question of the **types** of analyses to perform, there is the equally important question of **where** in the development lifecycle these analyses are to be performed.
  - 26262 also provides both normative and informative information the "what" and "where" of safety analyses.

ISO 26262 Part 9.8 — Safety Analyses

- ISO 26262 has introduced an entirely new, separate section dedicated to safety analyses.
  - This section provides a useful explanation of the types and purposes of safety analyses that are recommended by the standard.
  - Makes it possible to identify the differences to the IEC 61508 “mother” standard.
- This section outlines where the safety analysis are to be performed:
  - They are performed at the **system** level (ISO 26262 Part 4)
  - They are performed at the **hardware** level (ISO 26262 Part 5)
  - They are performed at the **software** level (ISO 26262 Part 6)
  - They may be performed at the **concept** level (ISO 26262 Part 3)
  - They are planned at the functional safety **management** level (ISO 26262 Part 2)

The "What"

ISO 26262 Part 9.8 describes the recommended safety analyses.

- Distinction between **qualitative** and **quantitative** analyses:
  - **Qualitative:** these are mainly **investigative**, searching for faults, failures, and problems with the design.
  - **Quantitative:** these are generally hardware-related, linked to failure rates, fault models, quantitative targets – used for random errors, not systematic errors.
  - NOTE: the same type of analysis method can often be employed for both qualitative and quantitative analyses (the same approach is used, whereby the necessary quantitative values and formulas are added in the case of quantitative analysis).
- Distinction between **inductive** and **deductive** analyses:
  - What are these?

Types of Reasoning

- The deductive and inductive types of safety analyses in ISO 26262 get their names from their counterparts in logic.
  - **Deductive reasoning**: a conclusion necessarily follows from a premise (“All men are mortal; Socrates is a man; Socrates is mortal”).
  - **Inductive reasoning**: start with a set of observed facts, search for a hypothesis that covers all of them (“The sun rose every day for the past week; therefore the sun rises every day, always”).
- The ISO 26262 use of the terms is not perfectly analogous.
  - **Deductive**: start from effect, seek possible causes (“top-down”).
  - **Inductive**: start from causes, seek possible effects (“bottom-up”).

ISO 26262 Analysis Methods

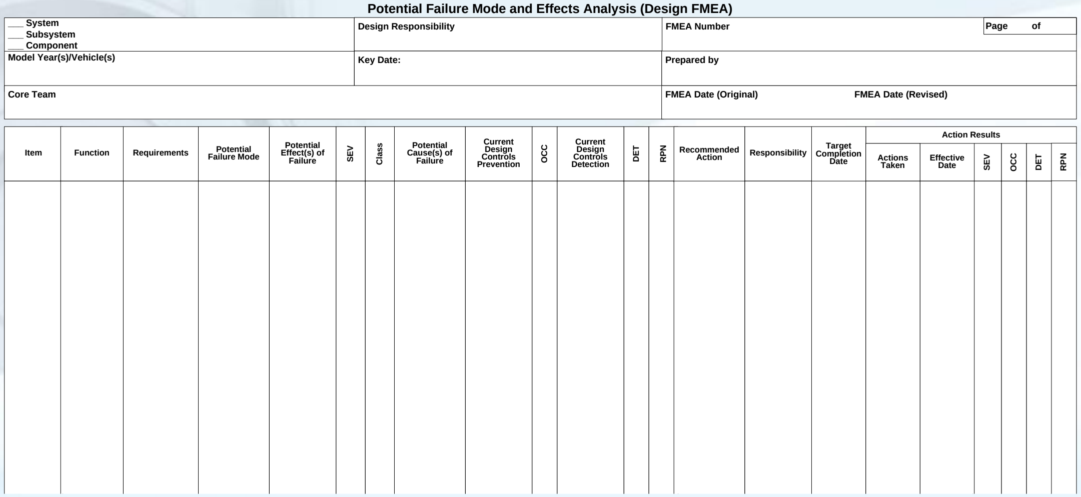
These are the safety analyses explicitly mentioned in ISO 26262

	Inductive	Deductive
Qualitative	• Qualitative **FMEA** • Qualitative **ETA** • **HAZOP**	• Qualitative **FTA**
Quantitative	• Quantitative **FMEA** • Quantitative **ETA** • **Markov modeling**	• Quantitative **FTA** • **Reliability block diagrams**

Note that variants of the same method (e.g., FMEA) can sometimes be used for both qualitative and quantitative analyses

FMEA and FTA

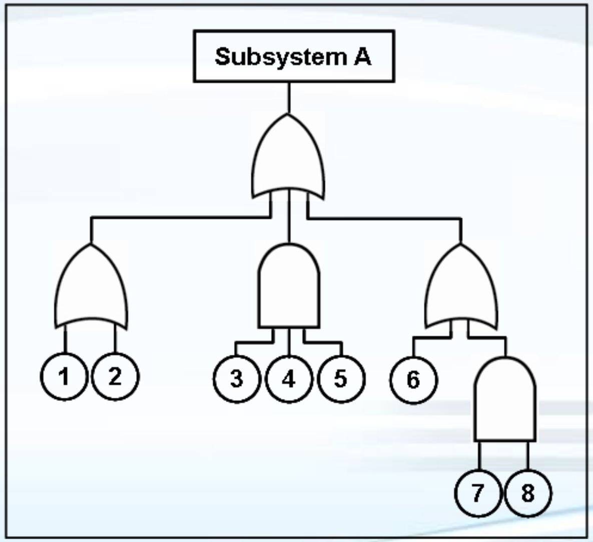
- By far the most popular methods for safety analysis, with the most support both in terms of standards and tools, are Failure Modes and Effects Analysis (**FMEA**) and Fault Tree Analysis (**FTA**).
  - As inductive and deductive methods they complement each other well.
  - There are industry standards (e.g., from SAE for FMEA).
  - This course has complete modules on FMEA and FTA.



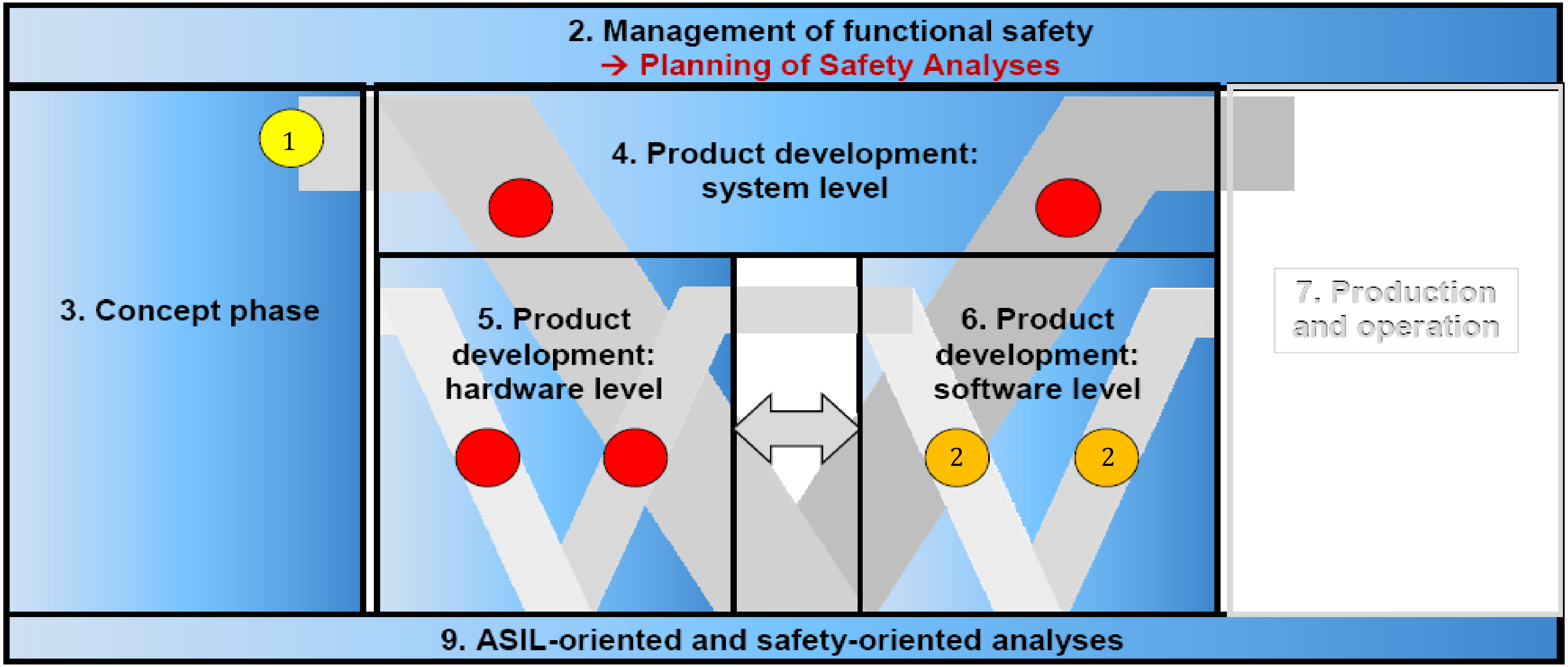
Potential Failure Mode and Effects Analysis (Design FMEA)

___ System ___ Subsystem ___ Component	Design Responsibility	FMEA Number	Page of
Model Year(s)/Vehicle(s)	Key Date:	Prepared by	
Core Team		FMEA Date (Original)	FMEA Date (Revised)

Item	Function	Requirements	Potential Failure Mode	Potential Effect(s) of Failure	SEV	Class	Potential Cause(s) of Failure	Current Design Controls Prevention	OCC	Current Design Controls Detection	DET	RPN	Recommended Action	Responsibility	Target Completion Date	Action Results					
																Actions Taken	Effective Date	SEV	OCC	DET	RPN



The “Where”


2. Management of functional safety
→ Planning of Safety Analyses
3. Concept phase
1
4. Product development: system level
5. Product development: hardware level
6. Product development: software level
2
2
7. Production and operation
9. ASIL-oriented and safety-oriented analyses

🔴	Normative + ASIL-dependent methods
2	Normative + methods may be chosen
1	Optional + methods may be chosen

This overview shows where safety analyses are addressed in the lifecycle by the standard

ASIL-Dependent Analyses

At system level, safety analyses are ASIL-dependent.

Table 4-1 – System Design Analysis

	Methods	ASIL			
		A	B	C	D
1	**Deductive analysis (FTA)**	o	+	++	++
2	**Inductive analysis (FMEA)**	++	++	++	++

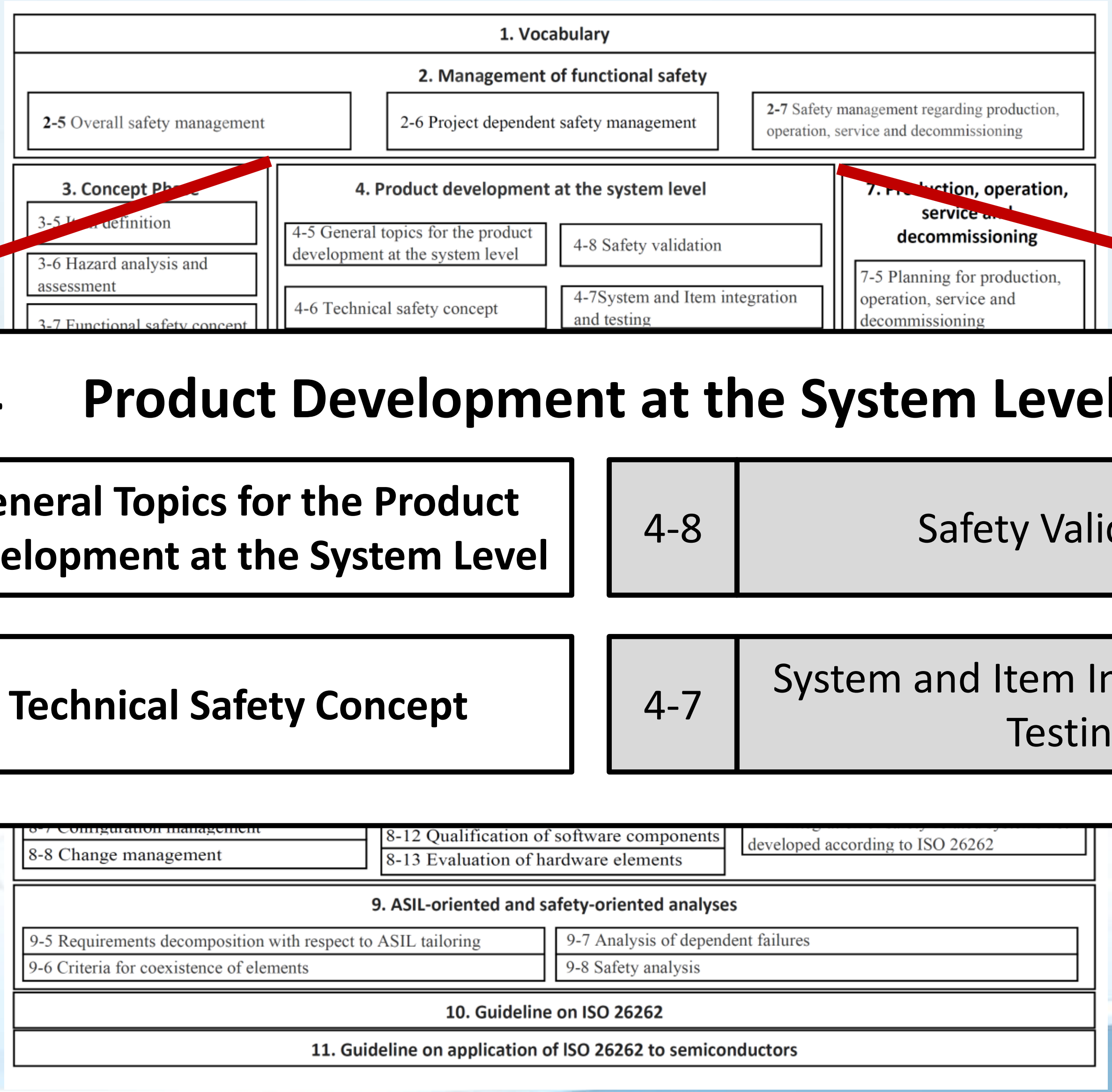
Inductive analyses are always highly recommended, for any ASIL. Deductive analyses are more selectively recommended.

These recommendations are generally accompanied by further recommendations regarding either **qualitative** or **quantitative** analysis.

Chapter 7

System Level Development I (Part 4)

System Level Development



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Project dependent safety management

2-7 Safety management regarding production, operation, service and decommissioning

3. Concept Phase

3-5 Item definition

3-6 Hazard analysis and assessment

3-7 Functional safety concept

4. Product development at the system level

4-5 General topics for the product development at the system level

4-8 Safety validation

4-6 Technical safety concept

4-7System and Item integration and testing

7. Production, operation, service and decommissioning

7-5 Planning for production, operation, service and decommissioning

8-7 Configuration management

8-8 Change management

8-12 Qualification of software components

8-13 Evaluation of hardware elements

developed according to ISO 26262

9. ASIL-oriented and safety-oriented analyses

9-5 Requirements decomposition with respect to ASIL tailoring

9-6 Criteria for coexistence of elements

9-7 Analysis of dependent failures

9-8 Safety analysis

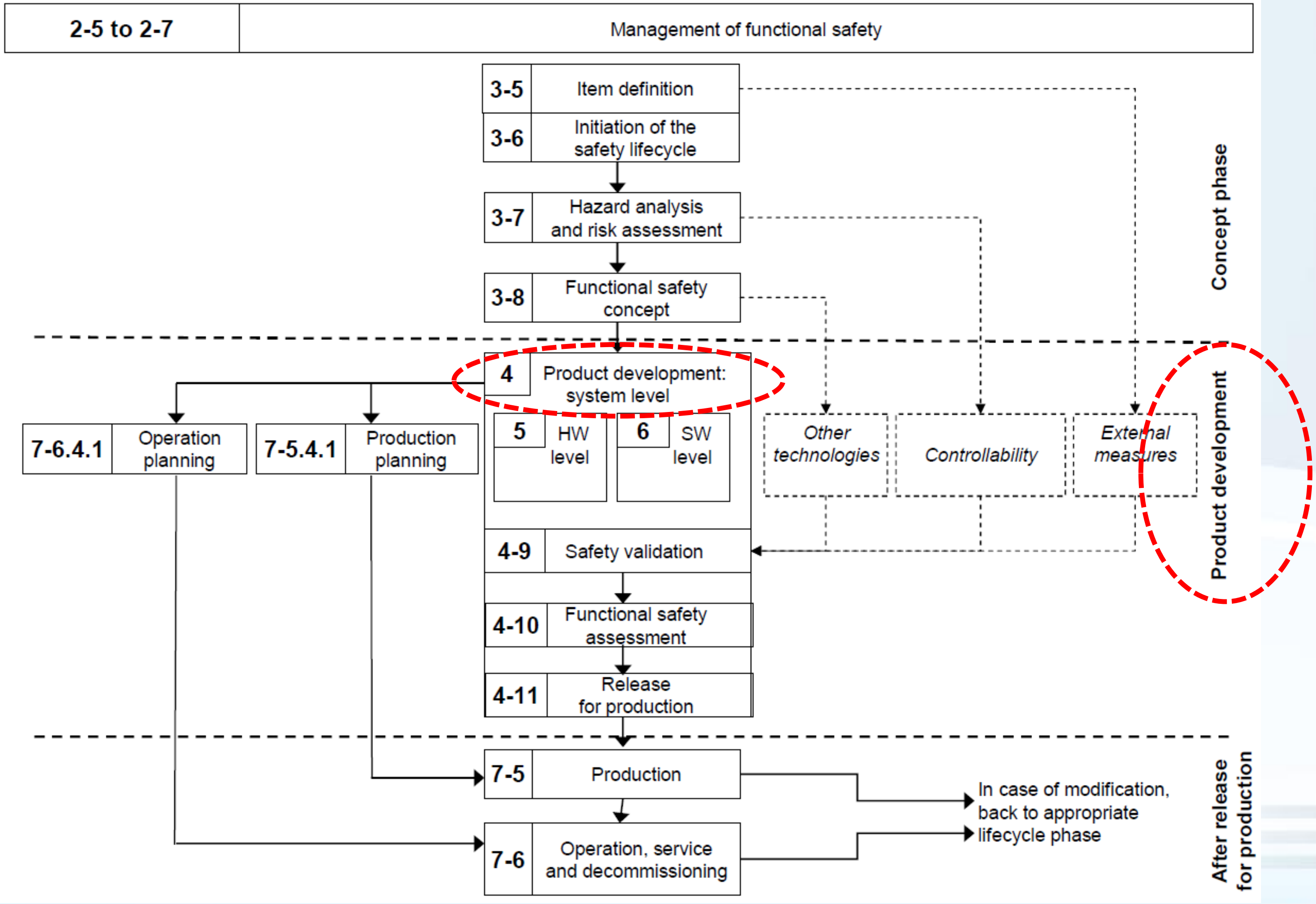
10. Guideline on ISO 26262

11. Guideline on application of ISO 26262 to semiconductors

4 Product Development at the System Level

4-5	General Topics for the Product Development at the System Level	4-8	Safety Validation
4-6	Technical Safety Concept	4-7	System and Item Integration and Testing

ISO 26262 Safety Lifecycle


2-5 to 2-7
Management of functional safety
3-5
Item definition
3-6
Initiation of the safety lifecycle
3-7
Hazard analysis and risk assessment
3-8
Functional safety concept
Concept phase
4
Product development: system level
7-6.4.1
Operation planning
7-5.4.1
Production planning
5
HW level
6
SW level
Other technologies
Controllability
External measures
Product development
4-9
Safety validation
4-10
Functional safety assessment
4-11
Release for production
7-5
Production
7-6
Operation, service and decommissioning
In case of modification, back to appropriate lifecycle phase
After release for production

Product Development at the System Level

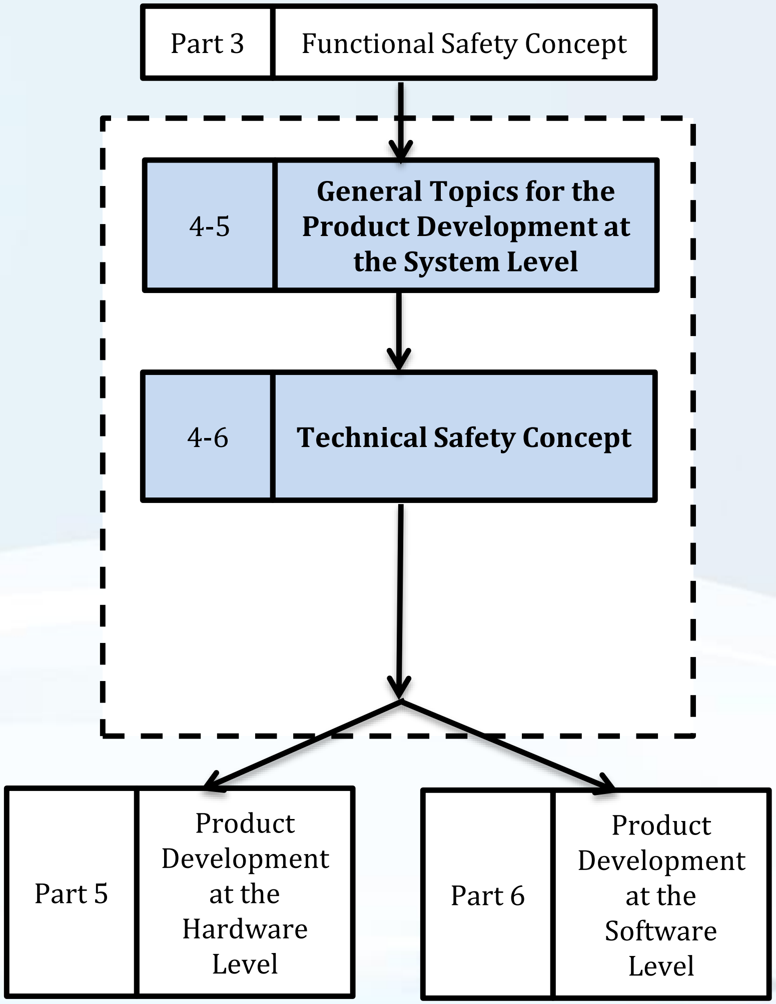
The Product Development at the System Level is divided into two parts.

- Provide rules and guidance to decomposing safety requirements into functionally redundant safety requirements to allow ASIL tailoring at the next level of detail.
- The System Validation, Safety Validation, Functional Safety Assessment and Release for Production after the Hardware and Software Development phases.

The "final product" of the first part of this phase is the Technical Safety Concept.

- This includes the Item Integrations and Testing Plan(s), Technical Safety Requirements, Technical Safety Concept, System Design Architecture Specification and Hardware-Software Interface Specification (HSI).

- An engineering cross-functional team is required.


Part 3
Functional Safety Concept
4-5
General Topics for the Product Development at the System Level
4-6
Technical Safety Concept
Part 5
Product Development at the Hardware Level
Part 6
Product Development at the Software Level

General Topics for the Product Development at the System Level

Objective

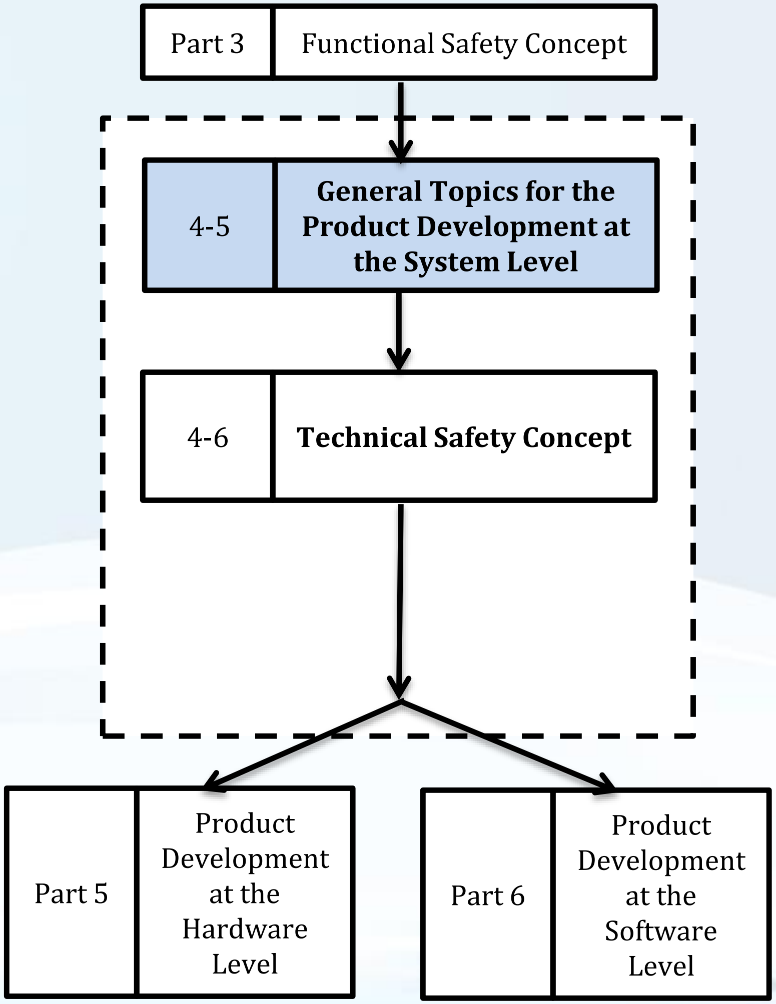
- Provide an overview of the product development at the system level.

Prerequisites

- N/A

Work Products

- N/A

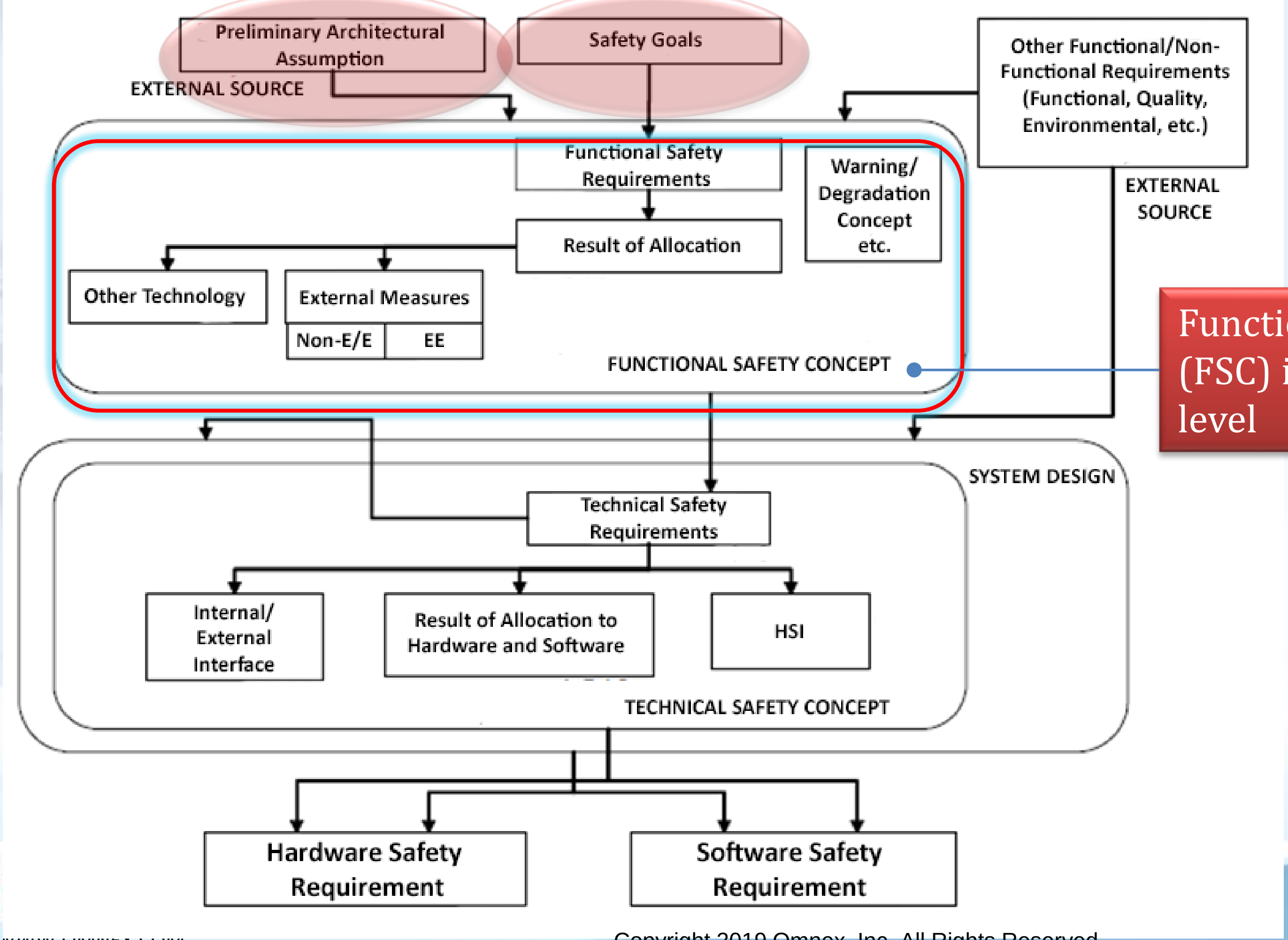

Part 3
Functional Safety Concept
4-5
General Topics for the Product Development at the System Level
4-6
Technical Safety Concept
Part 5
Product Development at the Hardware Level
Part 6
Product Development at the Software Level

Structure of Safety Requirements

- Within the development life cycle of an Item, the technical safety requirements are the technical requirements necessary to implement the functional safety concept, with the intention beginning to detail the item-level functional safety requirements into the system-level technical safety requirements.
- The system-level technical safety requirements are then allocated to the Hardware and Software for further development.

Flow of Safety Requirements – Key

A **functional safety concept** is derived which specifies **functional safety requirements** to **satisfy the safety goals**. These requirements define the **safety mechanisms** and the other **safety measures** that will be used for **the item**. In addition **the elements of the system architecture** are **identified** which will **support these requirements.**

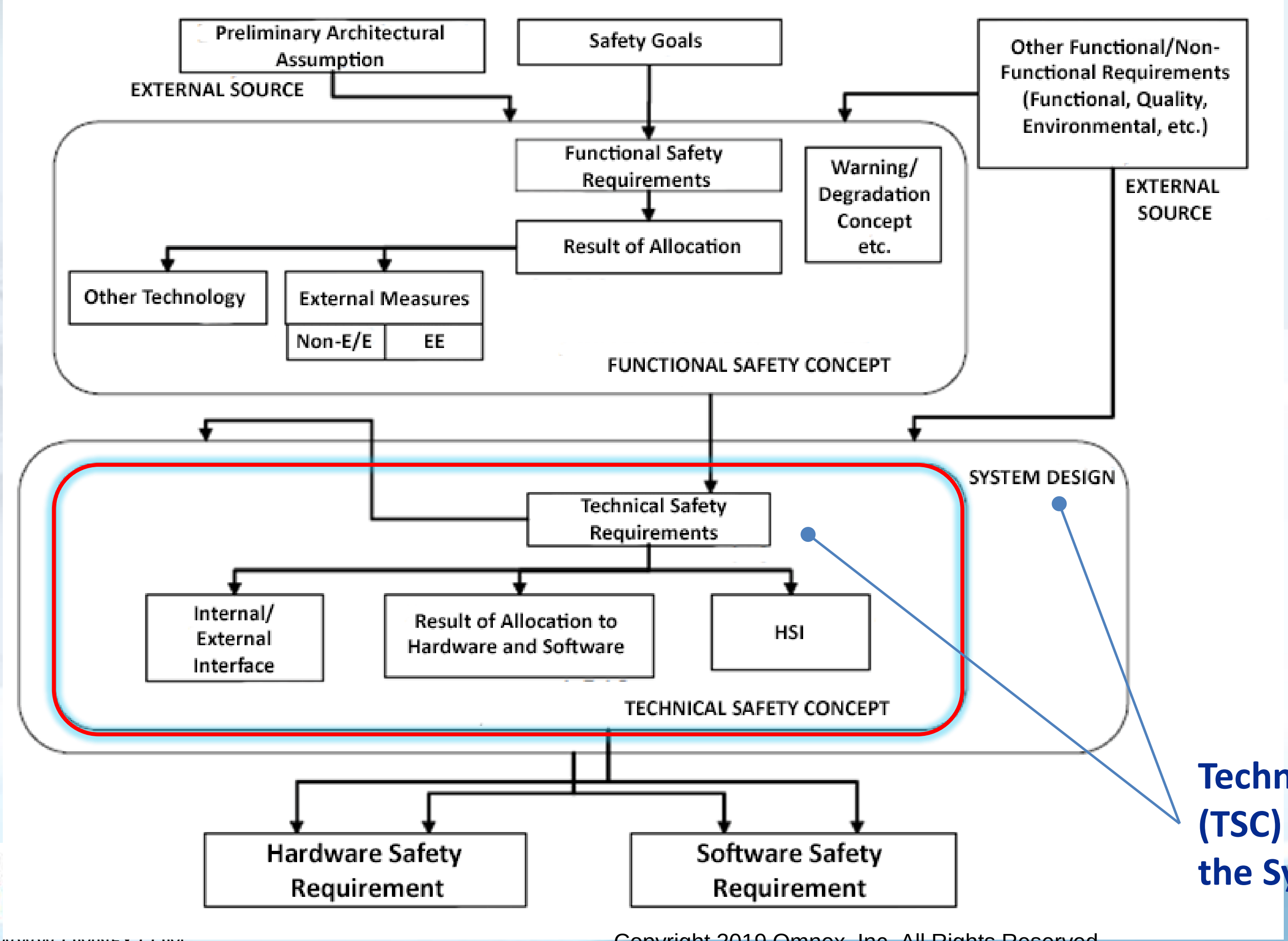

Preliminary Architectural Assumption
Safety Goals
EXTERNAL SOURCE
Other Functional/Non-Functional Requirements (Functional, Quality, Environmental, etc.)
EXTERNAL SOURCE
Functional Safety Requirements
Warning/ Degradation Concept etc.
Result of Allocation
Other Technology
External Measures
Non-E/E
EE
FUNCTIONAL SAFETY CONCEPT
SYSTEM DESIGN
Technical Safety Requirements
Internal/ External Interface
Result of Allocation to Hardware and Software
HSI
TECHNICAL SAFETY CONCEPT
Hardware Safety Requirement
Software Safety Requirement

Functional Safety Concept (FSC) is developed at vehicle level

System Design & Technical Safety Concept

A **technical safety concept** is derived which specifies how **functional safety requirements** will be **implemented**. These **technical safety requirements** will indicate the **partitioning of the elements between the hardware and the software**.

Reference ISO 26262-4, Clause 6.



Preliminary Architectural Assumption

EXTERNAL SOURCE

Safety Goals

Other Functional/Non-Functional Requirements (Functional, Quality, Environmental, etc.)

EXTERNAL SOURCE

Functional Safety Requirements

Warning/ Degradation Concept etc.

Result of Allocation

Other Technology

External Measures

Non-E/E

EE

FUNCTIONAL SAFETY CONCEPT

SYSTEM DESIGN

Technical Safety Requirements

Internal/ External Interface

Result of Allocation to Hardware and Software

HSI

TECHNICAL SAFETY CONCEPT

Hardware Safety Requirement

Software Safety Requirement

Scope for requirement responsibility

OEM

Supplier

Technical Safety Concept (TSC) is developed within the System design phase

System Design

Note the same pattern repeated hierarchically

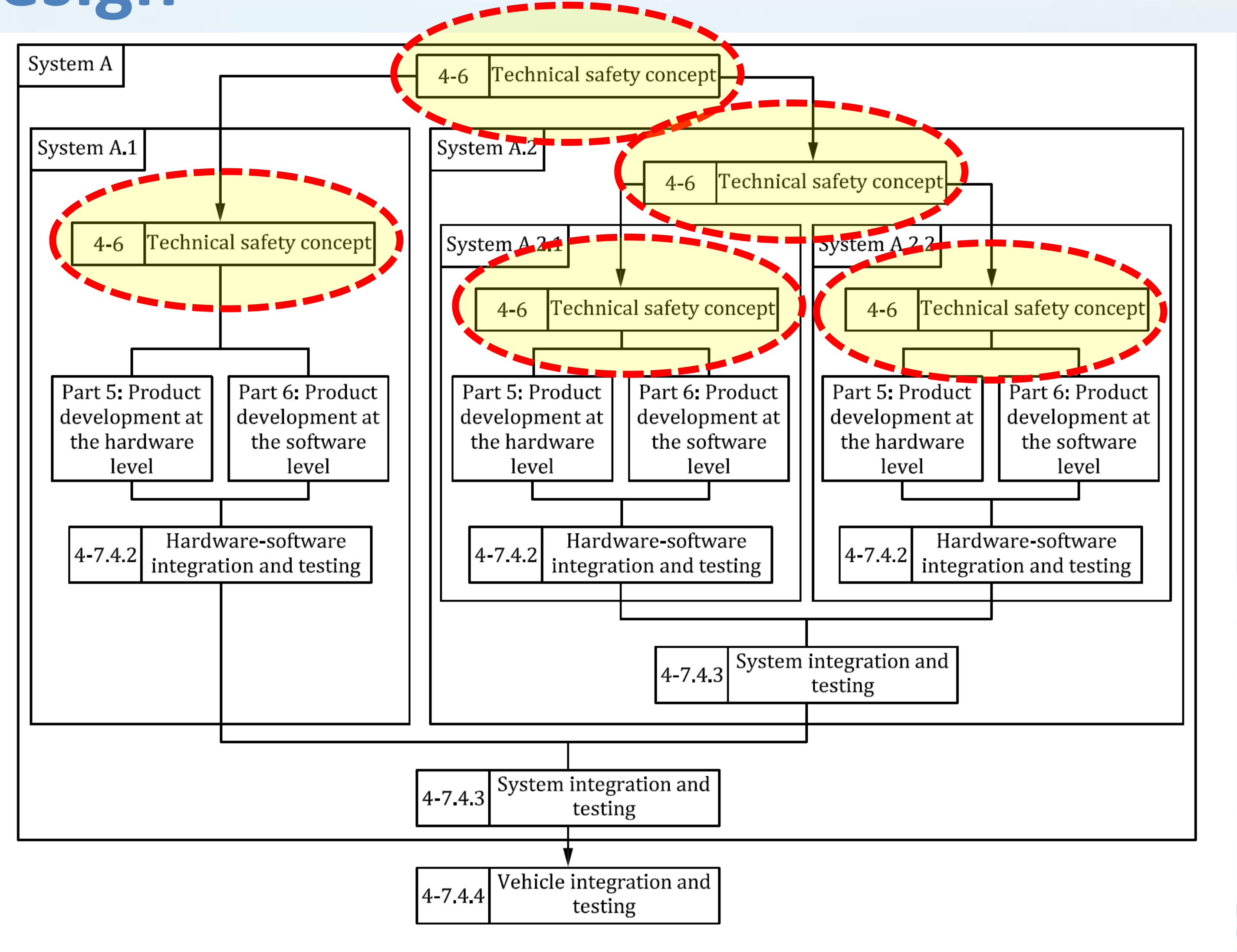
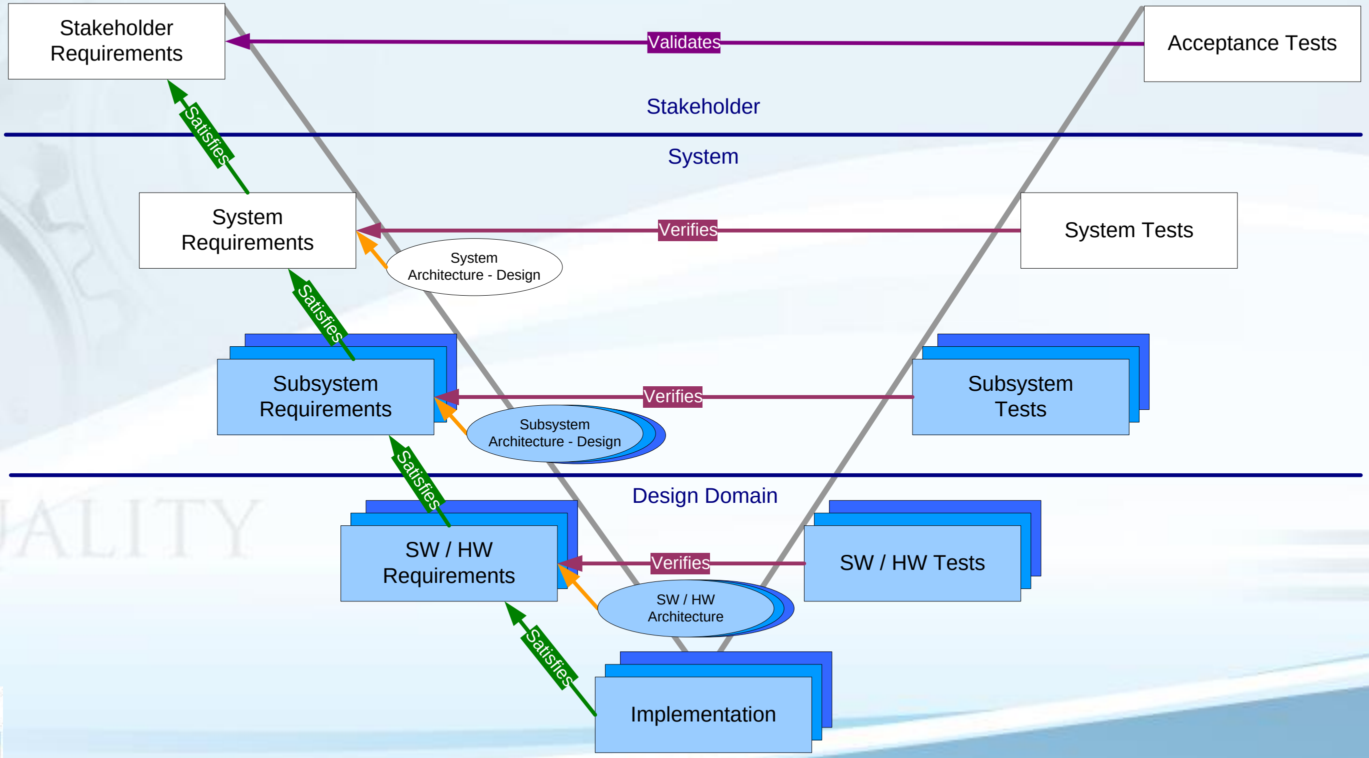

System A
4-6 Technical safety concept
System A.1
4-6 Technical safety concept
Part 5: Product development at the hardware level
Part 6: Product development at the software level
4-7.4.2 Hardware-software integration and testing
System A.2
4-6 Technical safety concept
System A.2.1
4-6 Technical safety concept
Part 5: Product development at the hardware level
Part 6: Product development at the software level
4-7.4.2 Hardware-software integration and testing
System A.2.2
4-6 Technical safety concept
Part 5: Product development at the hardware level
Part 6: Product development at the software level
4-7.4.2 Hardware-software integration and testing
4-7.4.3 System integration and testing
4-7.4.3 System integration and testing
4-7.4.4 Vehicle integration and testing

Figure 3 — Example of a product development at the system level

Structure and Categorize in System Level and Below

Trace, create traceability

- Trace bidirectional by each single requirements
- Trace from Stakeholder to System to Subsystem to design level and to implementation (SW Module) and tests
- Give every single requirement a unique identifier (ID) e.g. SYS_123



General Inclusions

- Based on the Functional Safety Concept, the preliminary architectural assumptions and the following system properties:
  a) The external interfaces, such as communication and user interfaces;
  b) The constraints, e.g. environmental condition or functional constrains; and
  c) The system configuration requirements

- If other functions or requirements are implemented by the system, then these functions or requirements shall be specified or references made to their specification
  - Example: Other requirements coming from Federal Motor Vehicle Safety Standard (FMVSS) or company platform strategies.

Technical Safety Concept

Objectives

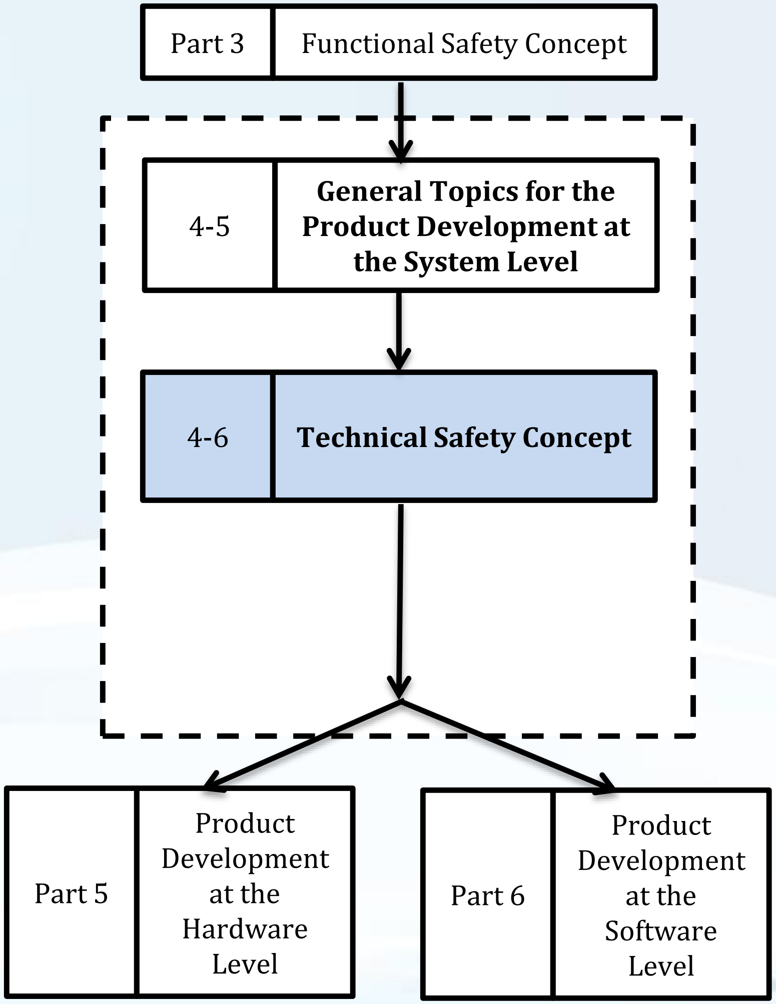
- Develop the system design and the technical safety concept that comply with the functional requirements and the technical safety requirements specification of the item.
- Verify that the system design and the technical safety concept comply with the technical safety requirements specification.

Prerequisites

- Functional Safety Concept
- System Architectural Design
- Requirements to the item from other safety relevant items, if applicable.

Work Products

- Technical Safety Concept
- System Design Specification
- Hardware-Software Interface Specification (HIS)
- System Verification Report (refined)
- Safety Analysis Reports


Part 3
Functional Safety Concept
4-5
General Topics for the Product Development at the System Level
4-6
Technical Safety Concept
Part 5
Product Development at the Hardware Level
Part 6
Product Development at the Software Level

Technical Safety Concept

The objectives of this clause are to:

a) Specify technical safety requirements

b) Specify safety mechanisms to be implemented

c) Specify requirements regarding the functional safety of the system and its elements during production, operation, service and decommissioning;

d) Verify that the technical safety requirements are suitable

e) Develop a system architectural design and a technical safety concept that satisfy the safety requirements and that are not in conflict with the non-safety-related requirements;

f) Analyze the system architectural design in order to prevent faults and to derive the necessary safety-related special characteristics for production and service; and

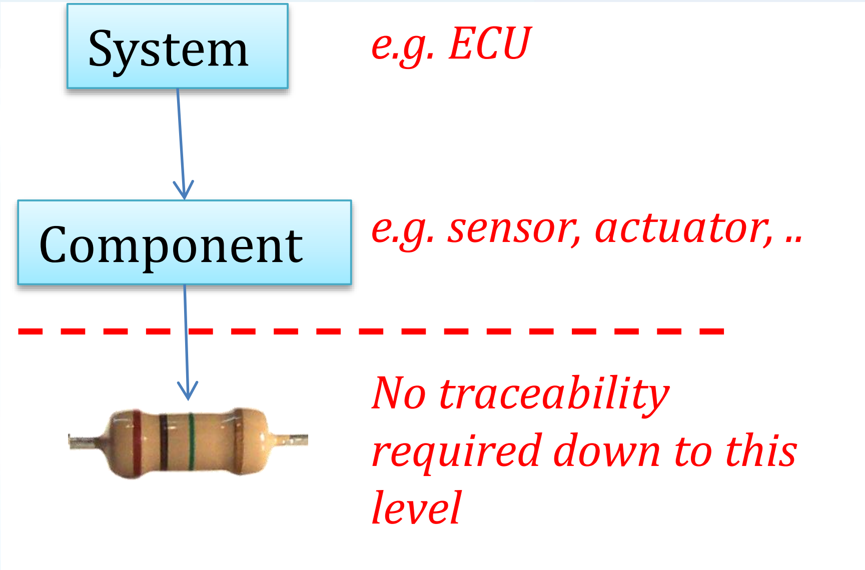
g) Verify that the system architectural design and the technical safety concept are suitable to satisfy the safety requirements according to their respective ASIL.

Required Traceability

- The traceability of safety-related requirements shall be ensured.
  - This can include adequate labeling or other identification of hardware elements to indicate that they are safety-related.

But how far must that traceability go?

- 26262 only requires that traceability go as far as hardware **components.**
  - This means that the traceability need not arrive at the level of detailed design of the hardware components (e.g., at the level of resistors, capacitors, etc.)



System

e.g. ECU

Component

e.g. sensor, actuator, ..

No traceability required down to this level

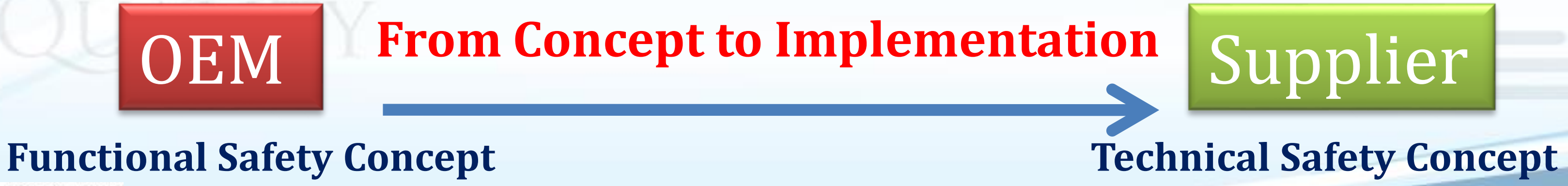
Required Traceability

From Safety Goal

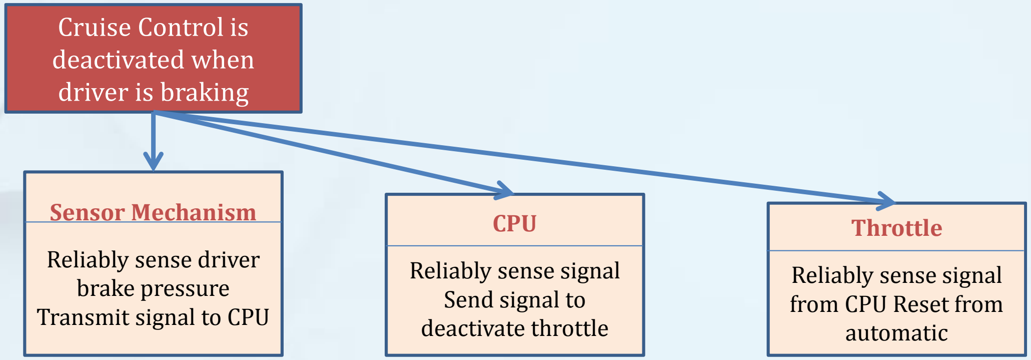
- To Functional Safety Requirements
  - Including test plan and results
- To Technical Safety Requirements
  - Including test plan and results
- To Hardware and Software Safety Requirements
  - Including test plan and results
- To Production
  - Including control plan reports

Technical Safety Requirements

- The first objective is to specify the technical safety requirements which ***refines*** the functional safety concept, considering both the **functional concept and the preliminary architectural assumptions**.
- The second objective is to verify through analysis that the technical safety requirements ***comply with the functional safety requirements.***
  - It is where the **handover from OEM to Supplier (internal or external)** usually occurs.
  - Usually, the OEM creates the functional safety concept, and the supplier implements it with the most appropriate technological solution.



Technical Requirements – Sensor Mechanism



Cruise Control is deactivated when driver is braking

Sensor Mechanism

Reliably sense driver brake pressure
Transmit signal to CPU

CPU

Reliably sense signal
Send signal to deactivate throttle

Throttle

Reliably sense signal from CPU Reset from automatic

Functional Safety Requirement

Provide redundant sensing to signal brake pedal is pressed to the CPU

Technical Safety Requirement 1

Sensor senses Pressure on brake pedal of – xx lbs /square inch or greater and transmits to CPU to signal brake is pressed

Technical Safety Requirement 2

Sensor senses Travel of pedal of xx inches is transmitted to CPU to signal brake is pressed

Technical Safety Requirements

- If other functions or requirements are implemented by the system or its elements (not related to the technical safety requirements) then these functions or requirements shall be specified or references made to their specification.
  - Example: Other requirements coming from Federal Motor Vehicle Safety Standard (FMVSS) or company platform strategies.
- The technical safety requirements shall specify safety-related dependencies between systems or item elements and between the item and other systems.
- The technical safety requirements shall specify the necessary safety mechanisms.

System Design

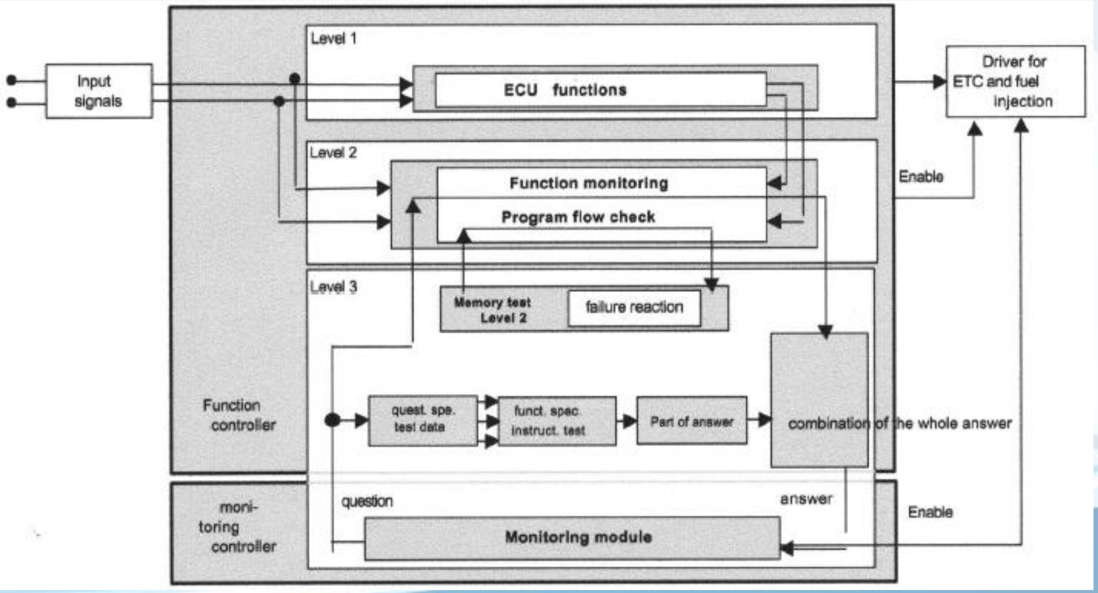
During 4-6, the Technical Safety Requirements are available, together with the Functional Safety Concept and the Preliminary Architectural Design.

- At this point, the system design based on the technical safety concept are created.
  - These describe how the requirements on the safety mechanisms are to be implemented.
  - They carry through their allocation to hardware and software.
- The system design should be **verifiable.**
- The system design should make use of **well-trusted safety** architectures.

Safety Architectures

- By simply stating “use well-trusted safety architectures” without specifying which ones to use, and by introducing the new hardware metrics, ISO 26262 makes a departure from IEC 61508.
  - IEC 61508 describes standard architectures and their error tolerances.
  - It is prescriptive – where ISO 26262 is only descriptive.
- A typical “well-trusted safety architecture” is the “E-GAS” architecture with its monitoring concept.

The E-GAS three-level safety architecture is a typical “trusted architecture”



Technical Safety Requirements

The technical safety requirements shall specify:

a) the safety-related dependencies and constraints of items, systems and their elements;

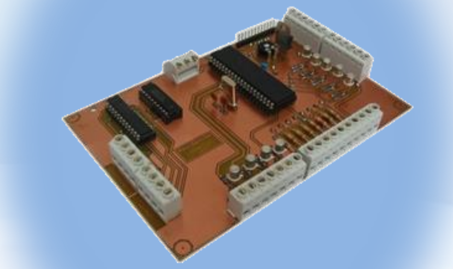
b) the external interfaces of the system, if applicable; and

c) the configurability of the system.

- If other functions or requirements are implemented by the system or its elements, then these functions or requirements shall be specified or their specification referenced.
  - Technical safety and non-safety requirements shall not contradict.
- The technical safety requirements shall specify the necessary safety mechanisms.

Safety Mechanisms

- These are technical solution implemented by E/E functions or elements or by other technologies to detect faults or control failures in order to achieve or maintain a safe state.
  - Safety mechanisms are implemented within the item to prevent faults from leading to single-point failures or to reduce residual failures and to prevent faults from being latent.
  - The safety mechanism is either able to transition to, or maintain, the item in a safe state; or able to alert the driver such that the driver is expected to control the effect of the failure as defined in the functional safety concept.
- This requirement applies to ASILs (A), (B), C, and D.



Safety mechanisms are added to the system

Safety Mechanisms

These include:

a) The measures relating to the detection, indication and control of faults in the system itself;

- For example, the self-monitoring of the system or elements to detect random hardware faults and, if appropriate, to detect systematic failures.
- For example, measures for the detection and control of failure modes of the communication channels (data interfaces, communication buses, wireless radio link).

b) The measures relating to the detection, indication and control of faults in external devices that interact with the system;

- For example, external devices include other electronic control units, power supply or communication devices.

Safety Mechanisms

These include:

c) The measures that enable the system to achieve or maintain a safe state;

- This includes prioritization and arbitration logic in the case of conflicting safety mechanisms.

d) The measures to detail and implement the warning and degradation concept; and

e) The measures which prevent faults from being latent.

These measures are usually related to tests that take place during power up (pre-drive checks), as in the case of measures a) to d), during operation, during power down (post-drive checks), and as part of maintenance.

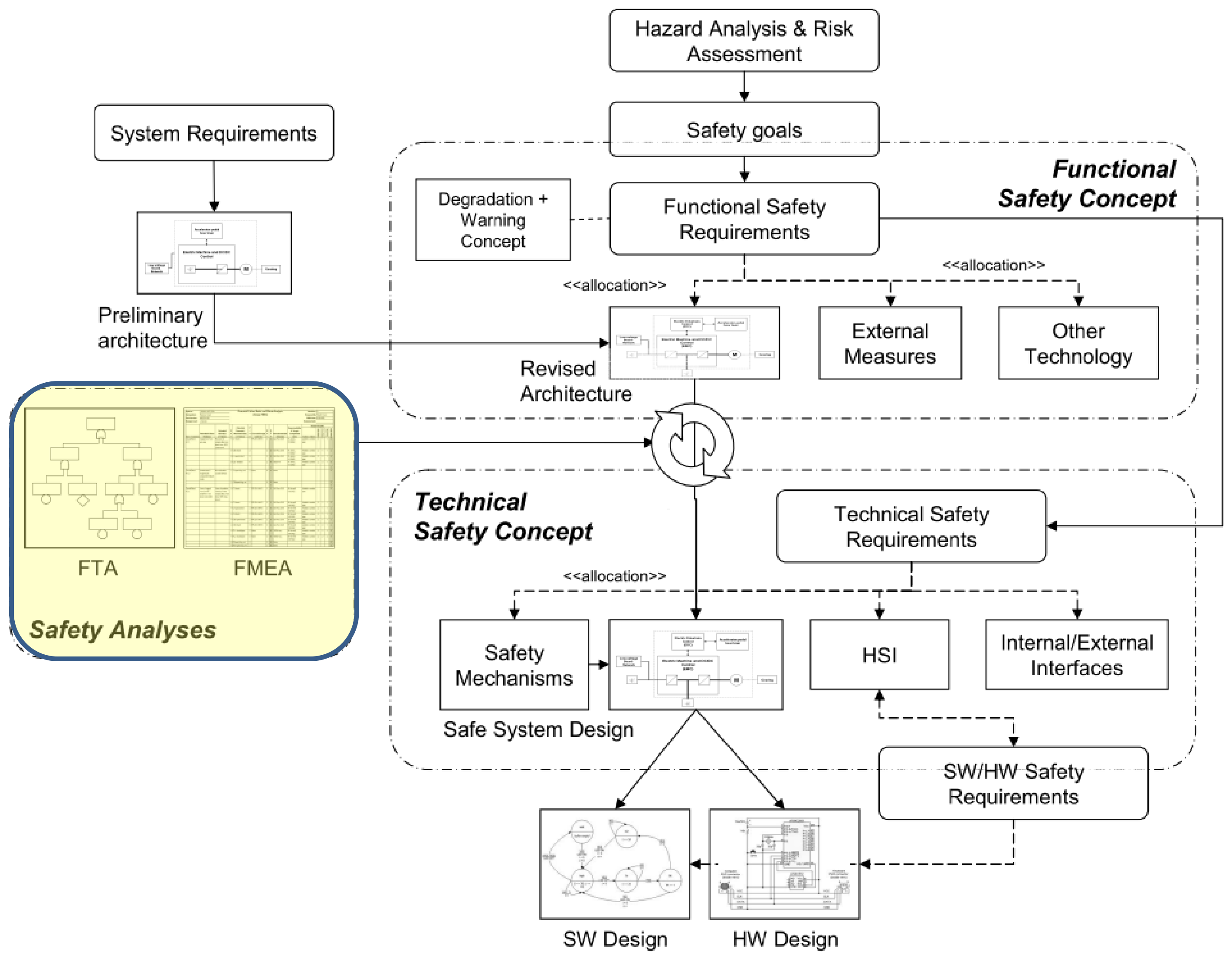
Safety Mechanism Design

- Safety mechanisms are dedicated to identify failure modes and diagnostics of **sensors and actuators.**
  - In most systems, the failure of a sensor or actuator can lead to incorrect system behavior and violation of a safety goal.
- The designer will usually have a **design choice** to make:
  - Design the sensor/actuator to be as reliable as required?
  - Or design the system to detect failures and switch to a safe state?
  - Or implement redundancy in the system to enable fault tolerance?
- Often a combination of these measures is necessary:
  - For example, it's often not possible to ensure the level of reliability needed for a sensor – it is a single-point of failure.
  - But some failure modes (e.g. metal fatigue) are hard to detect before the failure actually occurs!
- This is what the description of technical safety requirements is all about – making those hard design choices.

System Architectural Design Specification and Technical Safety Concept

- The system architectural design in this sub-phase and the technical safety concept shall be based on the item definition, functional safety concept and the prior system architectural design.
- The system architectural design shall implement the technical safety requirements and the following shall be considered:
  a) the ability to verify the system architectural design;
  b) the technical capability of the intended hardware and software elements with regard to the achievement of functional safety; and
  c) the ability to execute tests during system integration.
- The internal and external interfaces of safety-related elements shall be defined such that other elements shall not have adverse safety-related effects on the safety-related elements.

System Design Analysis



Modular System Design

In order to avoid failures resulting from high complexity, the architectural design shall exhibit the following properties by use of the principles:

a) modularity;

b) adequate level of granularity; and

c) simplicity

Properties of Modular System Design	
Methods	
1	Hierarchical design
2	Precisely defined interfaces
3	Avoidance of unnecessary complexity of hardware components and software components
4	Avoidance of unnecessary complexity of interfaces
5	Maintainability during service
6	Testability during development and operation

System Design Analysis

- In order to prevent systematic errors in the system design an inductive analysis (usually FMEA) must *always* be carried out.
- For higher ASIL levels, deductive analyses must also be carried out (usually Fault Tree Analysis).
- This activity is also effectively a part of **System Design Verification.**

Table 1 – System Design Analysis – Safety Analysis

Methods		ASIL			
		A	B	C	D
1	**Deductive analysis;** includes **FTA**, reliability block diagrams	o	+	++	++
2	**Inductive analysis;** includes **FMEA**, ETA, Markov modeling	++	++	++	++

Safety-related properties include independency and freedom from interference requirements

Allocation to Hardware and Software

- The technical safety requirements shall be allocated to the system architectural design elements.
- Each system architectural design element shall inherit the highest ASIL from the technical safety requirements that it implements.
- If technical safety requirements are allocated to custom hardware elements that incorporate programmable behavior (such as ASICs, FPGA or other forms of digital hardware) an adequate development process, combining requirements from ISO 26262-5 and ISO 26262-6, shall be defined and implemented.

Guidance can be found in ISO 26262-11:2018

Hardware-Software Interface (HSI)

- The hardware diagnostic features shall be defined; and
- The diagnostic features concerning the hardware to be implemented in software shall be defined.

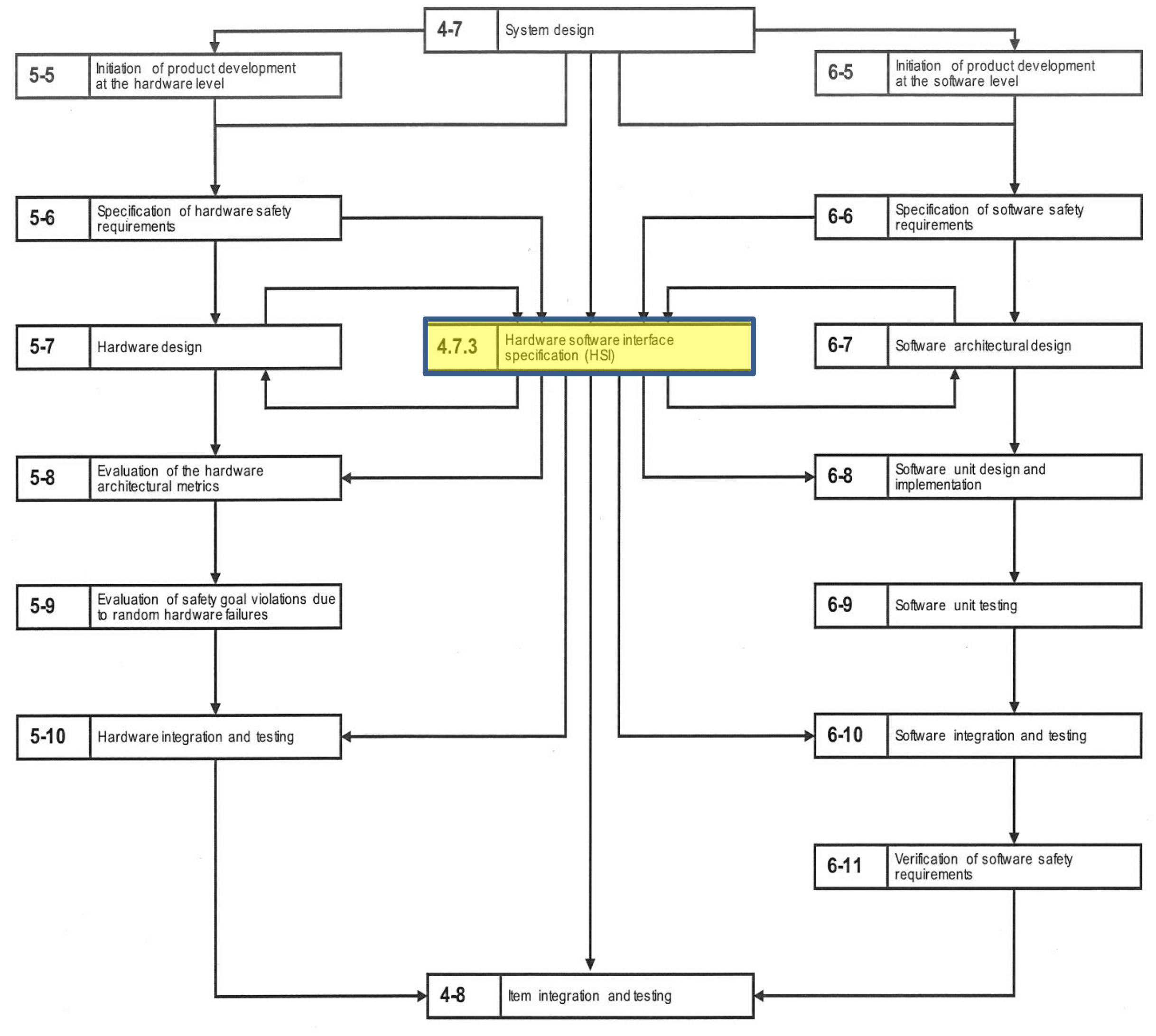
The HSI shall be specified during the system design and will be refined during hardware development and during software development.

software

hardware

Hardware-Software Interface Specification (HSI)

- The HSI document will be used for this requirement.
- HSI shall specify the hardware and software interaction and be consistent with the TSC.
- HSI shall include component's hardware devices that are controlled by software and hardware resources that support the execution of software.
- HSI acts as the linkage between the different phases of development.



4-7 System design
5-5 Initiation of product development at the hardware level
6-5 Initiation of product development at the software level
5-6 Specification of hardware safety requirements
6-6 Specification of software safety requirements
5-7 Hardware design
4.7.3 Hardware software interface specification (HSI)
6-7 Software architectural design
5-8 Evaluation of the hardware architectural metrics
6-8 Software unit design and implementation
5-9 Evaluation of safety goal violations due to random hardware failures
6-9 Software unit testing
5-10 Hardware integration and testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
4-8 Item integration and testing

Hardware-Software Interface (HSI)

The HSI specification shall specify the hardware and software interaction and be consistent with the technical safety concept.

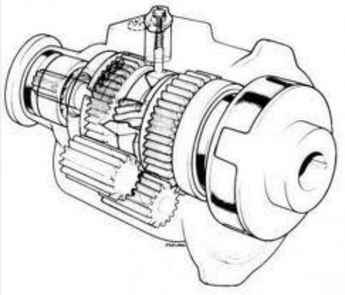
The HSI specification shall include:

- The component's hardware devices, that are controlled by software and hardware resources that support the execution of software;
- The relevant ***operating modes*** of hardware devices and the relevant ***configuration parameters***;
- The hardware features that ***ensure the independence*** between elements and that support software partitioning;
- Shared and exclusive ***use of hardware resources***, e.g. Memory mapping, allocation of registers, timers, interrupts, I/O ports;
- The ***access mechanism*** to hardware devices; e.g. Serial, parallel, slave, master/slave; and the ***timing*** constraints defined for each service involved in the technical safety concept;
- The relevant ***diagnostic*** capabilities of the hardware, and their use by the software.

Other Activities

Recalling that this part concerns the overall development of the system, the specification of the safety-related requirements concerning production, operation, maintenance, repair and decommissioning (addressed later in ISO 26262-7 on Production) are also initiated during this subpart:

- Assembly instructions
- Description of specific safety-related characteristics
- Procedures for production, diagnosis:
  - The requirements dedicated to ensure proper identification of systems or elements
  - The verification methods and measures for production
- Service requirements including diagnostic data and service notes
- Decommissioning requirements
- Procedures for field data acquisition



Service and maintenance manuals

Field data acquisition procedures

System Design Verification

To ensure conformance and completeness of the design with respect to the technical safety requirements, the system must undergo verification ***before release*** for HW and SW implementation.

Table 2– System design verification					
	Methods	**ASIL**			
		A	**B**	**C**	**D**
1a	**System design Inspection;** serve as check of complete and correct detailing and implementation of the technical safety requirements into system design.	+	++	++	++
1b	**System design walkthrough;** serve as check of complete and correct detailing and implementation of the technical safety requirements into system design.	++	+	o	o
2a	**Simulation;** can be used advantageously as a fault injection technique	+	+	++	++
2b	**System prototyping and vehicle tests;** can be used advantageously as a fault injection technique	+	+	++	++
3	**Safety analyses**	**See Table 1**			

OMNEX

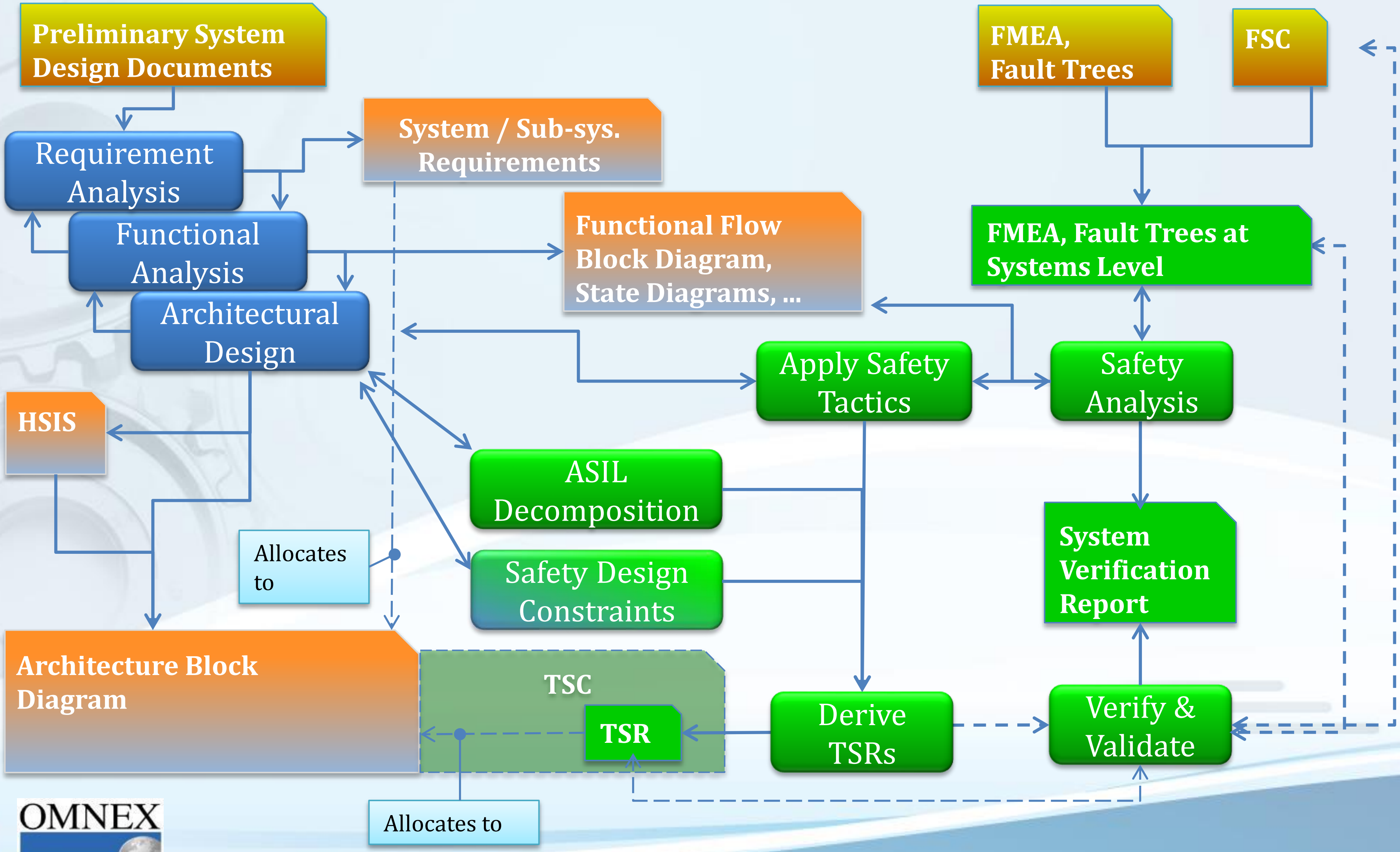
Hardware-Software Integration and Testing

The integration and validation testing of the hardware and software to be developed shall be consistent with the requirements in Part 4: Tables 3 to 8:

3. Methods for deriving test cases for integration testing;
4. The correct implementation of technical safety requirements at the hardware-software level;
5. The correct functional performance, accuracy and timing of safety mechanisms at the hardware-software level;
6. The consistent and correct implementation of external and internal interfaces at the hardware-software level;
7. The effectiveness of a safety mechanism's diagnostic coverage at the hardware-software level.
8. Level of robustness at the hardware-software level

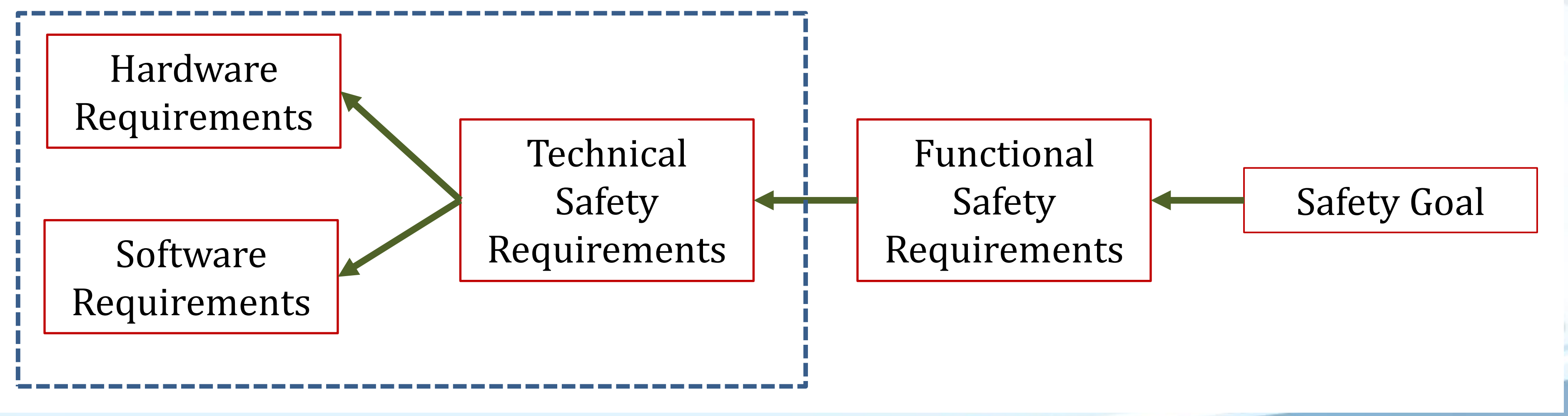
These will be implemented after Hardware and Software development ***but should be planned during the TSC***.

TSC Development — Summary


Preliminary System Design Documents
Requirement Analysis
System / Sub-sys. Requirements
Functional Analysis
Functional Flow Block Diagram, State Diagrams, ...
Architectural Design
FMEA, Fault Trees
FSC
FMEA, Fault Trees at Systems Level
Apply Safety Tactics
Safety Analysis
HSIS
ASIL Decomposition
Safety Design Constraints
Allocates to
System Verification Report
Architecture Block Diagram
TSC
TSR
Derive TSRs
Verify & Validate
Allocates to

DETAIL LEVEL DEVELOPMENT

Hardware and Software



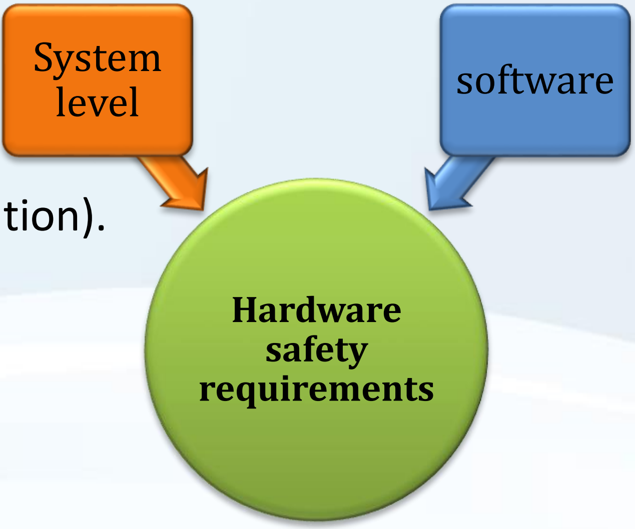
Detail Level Development

This section will be covered in greater detail throughout the rest of the week.

It is included to provide an insight into the detailed design for those stopping their journey today.

Technical Safety Concept

- Parts 5 and 6 concerns the implementation of the technical safety concept.
  - The hardware-related and software safety requirements are created.
- The hardware safety requirements may be derived from several sources, and in particular:
  - They may be derived from the system level safety requirements (including relevant environmental conditions and conditions of operation).
  - They may be derived from software safety requirements (which generally place demands on the hardware).

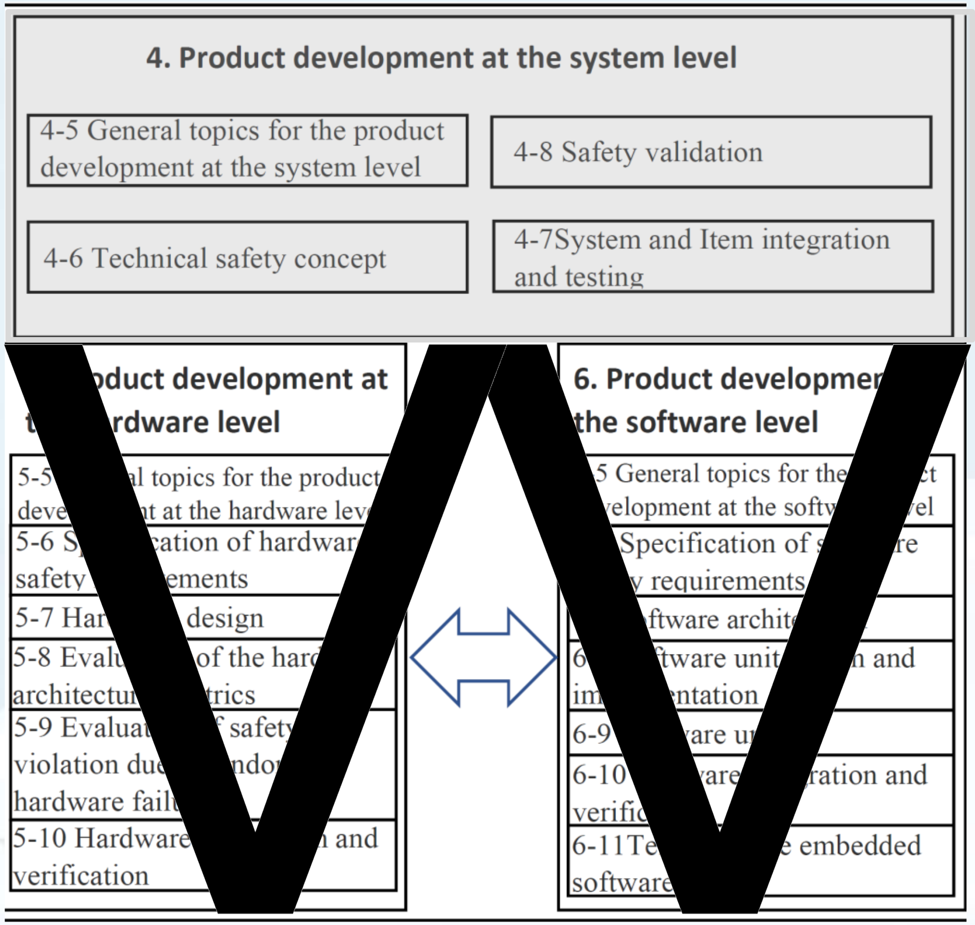


There may be several sources for hardware requirements

HW / SW Development

At this point, hardware and software development can begin

hardware



4. Product development at the system level

4-5 General topics for the product development at the system level

4-8 Safety validation

4-6 Technical safety concept

4-7System and Item integration and testing

oduct development at t rdware level

5-5 l topics for the product deve t at the hardware lev

5-6 S cation of hardwar safety ements

5-7 Har design

5-8 Evalu of the hard architectu trics

5-9 Evaluat f safety violation du ndor hardware fail

5-10 Hardware n and verification

6. Product developmen the software level

5 General topics for the t velopment at the softw vel

Specification of s re y requirements

ftware archit

6 ftware unit n and im ntation

6-9 are u

6-10 are ration and verific

6-11Te e embedded software

software

Recall that both HW and SW development have their own "V" lifecycle

OMNEX

HS/SW Teamwork

- Hardware – Software interface requirements have a major reference in the standard.
- When refining the hardware and software safety requirements and developing the architecture, usually new ideas emerge for better safety solutions.
- In particular, modifying the way that hardware and software cooperate to provide safety related functions.
  - Sometimes it involves more software functionality.
  - Sometimes it involves more hardware functionality.
- It always involves close cooperation and communication between hardware and software development.
  - Iteration between both activities.

ASIL-Dependent Tables

Hardware

- Requirements Verification
- Safety Analyses
- Design Verification
- Integration Test Cases
- Safety Mechanisms
- Integration Tests
- Random Failure Target Values
- Diagnostic Coverage Targets – Residual Faults

ASIL-Dependent Tables

Software

- Requirements Verification
- Modeling and Coding
- Architecture: Design Notations
- Architecture: Design Principles
- Architecture: Error Detection
- Architecture: Error Handling
- Architecture: Design Verification

ASIL-Dependent Tables

Software

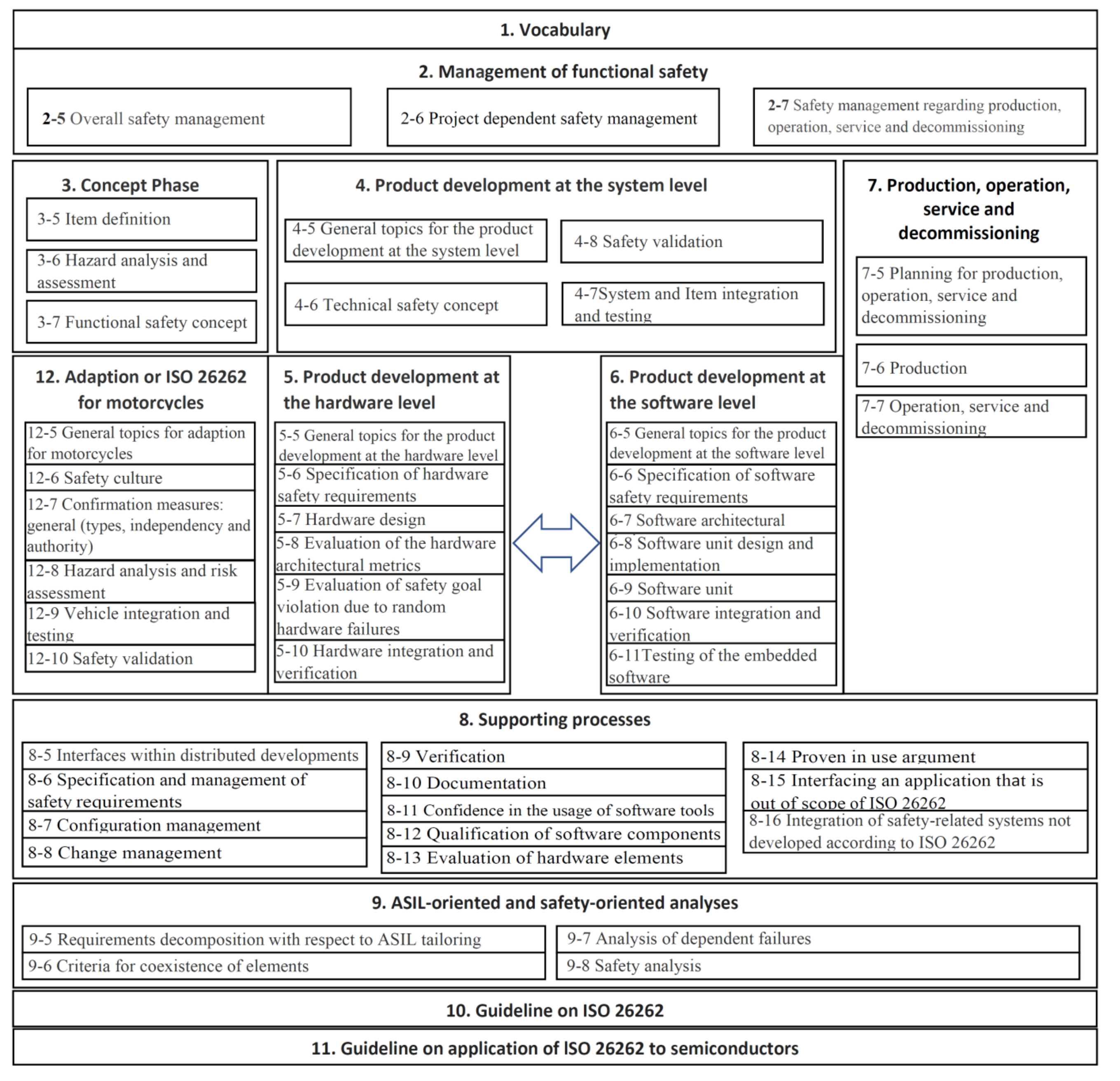
- Unit Design Notations
- Unit Design Principles
- Unit Design Verification
- Unit Testing
- Deriving Test Cases
- Structural Coverage Metrics

ASIL-Dependent Tables

Software

- Integration Testing
- Test Cases for Integration Test
- Architecture: Structural Coverage
- Test Environments
- Unintended Data Changes

ISO 26262:2018 – 12 Parts



1. Vocabulary

2. Management of functional safety
- 2-5 Overall safety management
- 2-6 Project dependent safety management
- 2-7 Safety management regarding production, operation, service and decommissioning

3. Concept Phase
- 3-5 Item definition
- 3-6 Hazard analysis and assessment
- 3-7 Functional safety concept

4. Product development at the system level
- 4-5 General topics for the product development at the system level
- 4-8 Safety validation
- 4-6 Technical safety concept
- 4-7System and Item integration and testing

7. Production, operation, service and decommissioning
- 7-5 Planning for production, operation, service and decommissioning
- 7-6 Production
- 7-7 Operation, service and decommissioning

12. Adaption or ISO 26262 for motorcycles
- 12-5 General topics for adaption for motorcycles
- 12-6 Safety culture
- 12-7 Confirmation measures: general (types, independency and authority)
- 12-8 Hazard analysis and risk assessment
- 12-9 Vehicle integration and testing
- 12-10 Safety validation

5. Product development at the hardware level
- 5-5 General topics for the product development at the hardware level
- 5-6 Specification of hardware safety requirements
- 5-7 Hardware design
- 5-8 Evaluation of the hardware architectural metrics
- 5-9 Evaluation of safety goal violation due to random hardware failures
- 5-10 Hardware integration and verification

6. Product development at the software level
- 6-5 General topics for the product development at the software level
- 6-6 Specification of software safety requirements
- 6-7 Software architectural
- 6-8 Software unit design and implementation
- 6-9 Software unit
- 6-10 Software integration and verification
- 6-11Testing of the embedded software

8. Supporting processes
- 8-5 Interfaces within distributed developments
- 8-6 Specification and management of safety requirements
- 8-7 Configuration management
- 8-8 Change management
- 8-9 Verification
- 8-10 Documentation
- 8-11 Confidence in the usage of software tools
- 8-12 Qualification of software components
- 8-13 Evaluation of hardware elements
- 8-14 Proven in use argument
- 8-15 Interfacing an application that is out of scope of ISO 26262
- 8-16 Integration of safety-related systems not developed according to ISO 26262

9. ASIL-oriented and safety-oriented analyses
- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of elements
- 9-7 Analysis of dependent failures
- 9-8 Safety analysis

10. Guideline on ISO 26262

11. Guideline on application of ISO 26262 to semiconductors

THE NEED FOR FUNCTIONAL SAFETY AND “GETTING STARTED”

Why ISO 26262?

- Marketing Advantage?

- Customer Requirement?

- Reduce Large Risks with More Robust Safety Related Processes?

- Opportunity to Strengthen Software and Hardware Processes?

Cost of ISO 26262?

- Additional tests?
- Additional Reviews?
- Additional Hardware and Software?

The attitude taken by the implementation team and top management will provide a strategic advantage to the implementation.
Generally, no difference between ASIL A and B – the increase takes place between ASIL B and C. The cost for this difference needs to be calculated
The cost to conduct two Bs vs. one C or D should be calculated, i.e., ASIL decomposition.

General Attitude – ISO 26262 is good. Opportunity to put in good practices for software and hardware. Some of these practices should be implemented across the board, not just for safety characteristics. General method to conduct flow down of significant and critical characteristics.

Use of Functional Safety

- Functional safety is being used for Electric Cars and Autonomous Cars
- Electronics Content in cars is growing
- Large OEMs have announced move to E Cars and Autonomous cars
- Countries have announced legislation to outlaw gasoline cars
- Use of autonomous braking in cars via agreement with US DOT
- The increase in hardware and software has induced a significant risk for the customer and warranty cost for the manufacturer

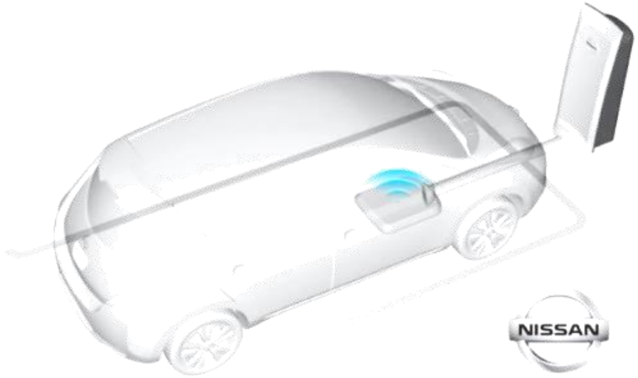
E Car Market and Competition

Audi targets 10 billion euros in cost cuts to fund electric-car push - *Andreas Cremer, Reuters, July 30th 2017*
"…The bulk of the 10 billion cost savings would come from cutting research and development costs, the sources said."

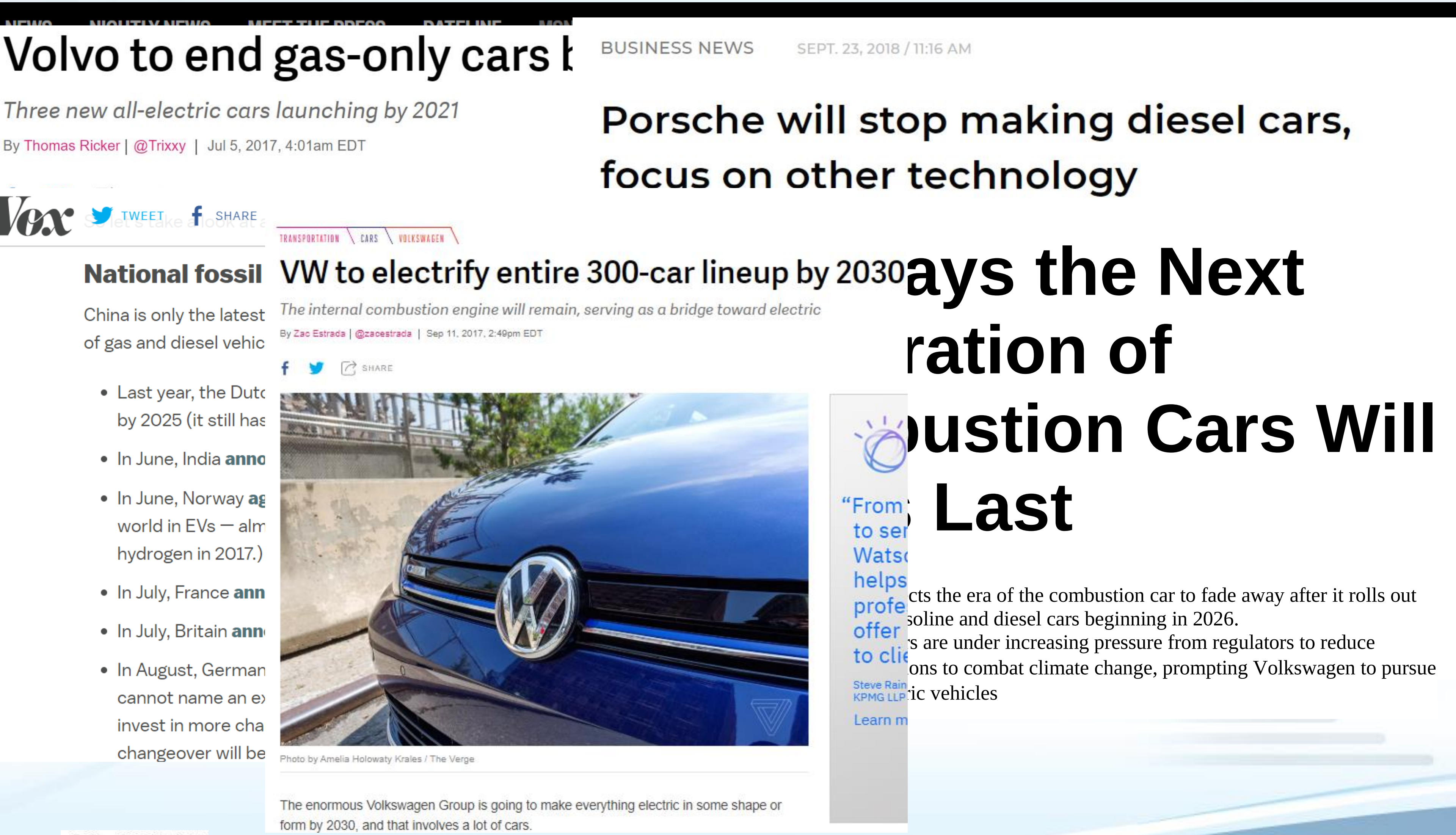
Wireless charging of moving electric vehicles overcomes major hurdle in new Stanford research – Stanford news, June 14th 2017

The race to e-mobility – *Dave Keating, DW, August 4th 2017*
"Paris & London announced plans to make their city centers combustion-engine-free by 2040…India to go all electric by 2030…"

Toyota and Mazda join forces on electric vehicles. Is this the end of the road for gas cars? – *Sintia Radu, Washington Post, August 4th 2017*
"Toyota Motor Corp and Mazda Motor Corp on Friday announced they would join forces to develop electric vehicle technologies and build a $1.6 billion assembly plant in the U.S…"



NEWS



Volvo to end gas-only cars b

Three new all-electric cars launching by 2021

By Thomas Ricker | @Trixxy | Jul 5, 2017, 4:01am EDT

BUSINESS NEWS SEPT. 23, 2018 / 11:16 AM

Porsche will stop making diesel cars, focus on other technology

So let's take a look at a

National fossil

China is only the latest of gas and diesel vehic

- Last year, the Dutc by 2025 (it still has
- In June, India anno
- In June, Norway ag world in EVs — alm hydrogen in 2017.)
- In July, France ann
- In July, Britain ann
- In August, German cannot name an ex invest in more cha changeover will be

VW to electrify entire 300-car lineup by 2030

The internal combustion engine will remain, serving as a bridge toward electric

By Zac Estrada | @zacestrada | Sep 11, 2017, 2:49pm EDT

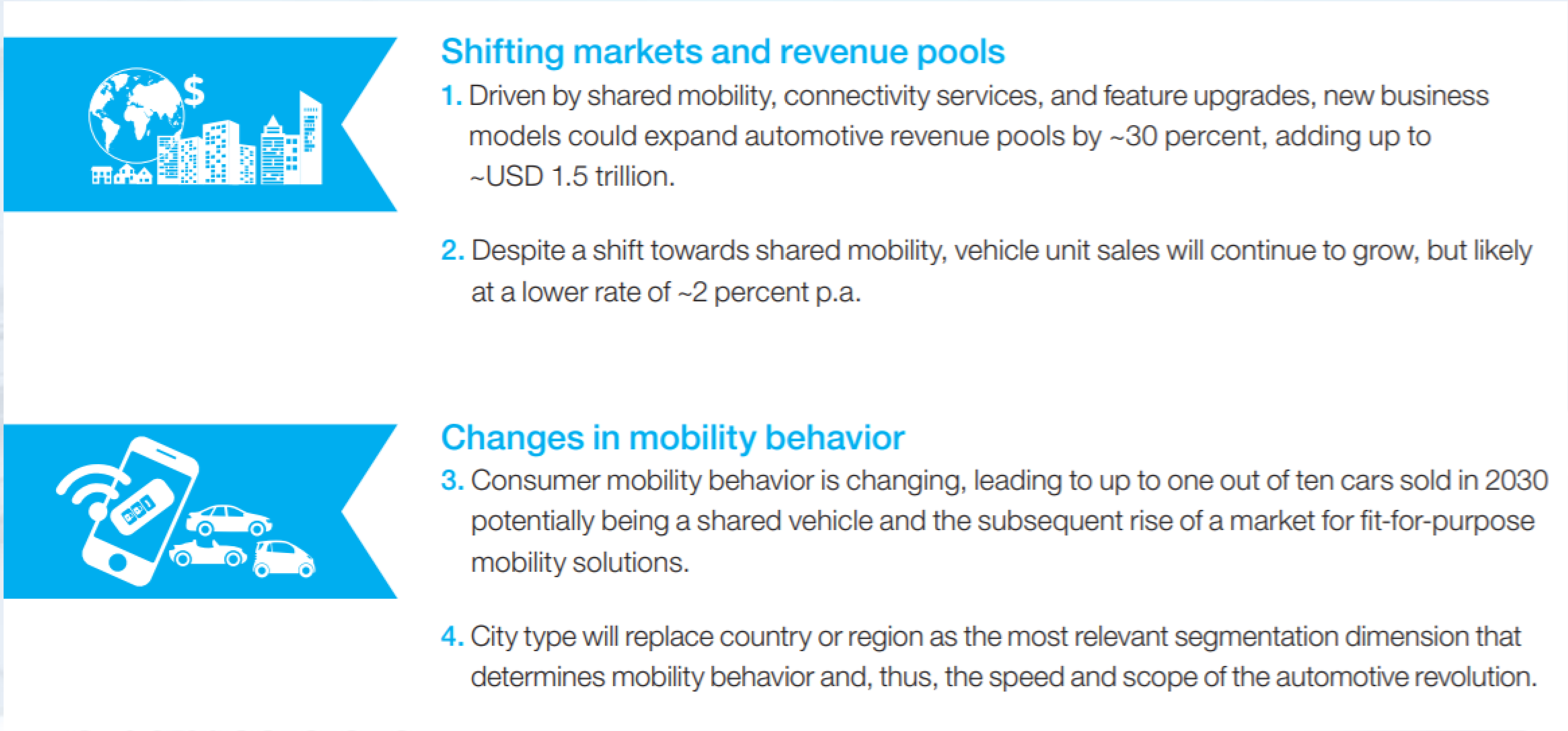
Photo by Amelia Holowaty Krales / The Verge

The enormous Volkswagen Group is going to make everything electric in some shape or form by 2030, and that involves a lot of cars.

ays the Next ration of ustion Cars Will Last

cts the era of the combustion car to fade away after it rolls out soline and diesel cars beginning in 2026.
s are under increasing pressure from regulators to reduce ons to combat climate change, prompting Volkswagen to pursue ic vehicles

Automotive Revolution Summary



Shifting markets and revenue pools

1. Driven by shared mobility, connectivity services, and feature upgrades, new business models could expand automotive revenue pools by ~30 percent, adding up to ~USD 1.5 trillion.

2. Despite a shift towards shared mobility, vehicle unit sales will continue to grow, but likely at a lower rate of ~2 percent p.a.

Changes in mobility behavior

3. Consumer mobility behavior is changing, leading to up to one out of ten cars sold in 2030 potentially being a shared vehicle and the subsequent rise of a market for fit-for-purpose mobility solutions.

4. City type will replace country or region as the most relevant segmentation dimension that determines mobility behavior and, thus, the speed and scope of the automotive revolution.

Automotive Revolution Summary

Diffusion of advanced technology

5. Once technological and regulatory issues have been resolved, up to 15 percent of new cars sold in 2030 could be fully autonomous.

6. Electrified vehicles are becoming viable and competitive; however, the speed of their adoption will vary strongly at the local level.

New competition and cooperation

7. Within a more complex and diversified mobility industry landscape, incumbent players will be forced to simultaneously compete on multiple fronts and cooperate with competitors.

8. New market entrants are expected to initially target only specific, economically attractive segments and activities along the value chain before potentially exploring further fields.

Improving Safety in Transportation

U.S. DOT and IIHS announce historic commitment of 20 automakers to make automatic emergency braking standard on new vehicles - *IIHS, March 17, 2016*

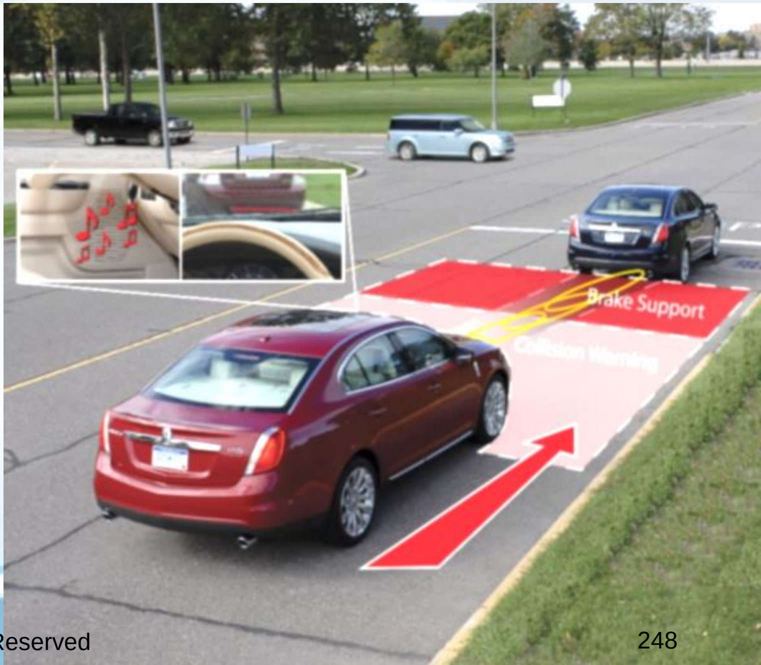
McLEAN, Va. – "…historic commitment by 20 automakers representing more than 99 percent of the U.S. auto market to make automatic emergency braking a standard feature on virtually all new cars no later than NHTSA's 2022 reporting year, which begins Sept 1, 2022…"

Lexus and Toyota Will Make Automated Braking Standard on Nearly Every Model and Trim Level by End of 2017 – *Toyota corporate pressroom, March 21, 2016*

"..Making Lexus Safety System +™ and Toyota Safety Sense™ standard equipment on almost every model by the end of 2017 will make AEB technology widely available four years ahead of the 2022 industry target…"

Backup cameras to be required in all new vehicles, starting in 2018 – *LA Times*

"…rear visibility technology" would need to be standard equipment in all vehicles under 10,000 pounds. The move aims to reduce the average of 210 deaths and 15,000 injuries caused every year by back-up accidents. Many of the accidents involve children or seniors…"



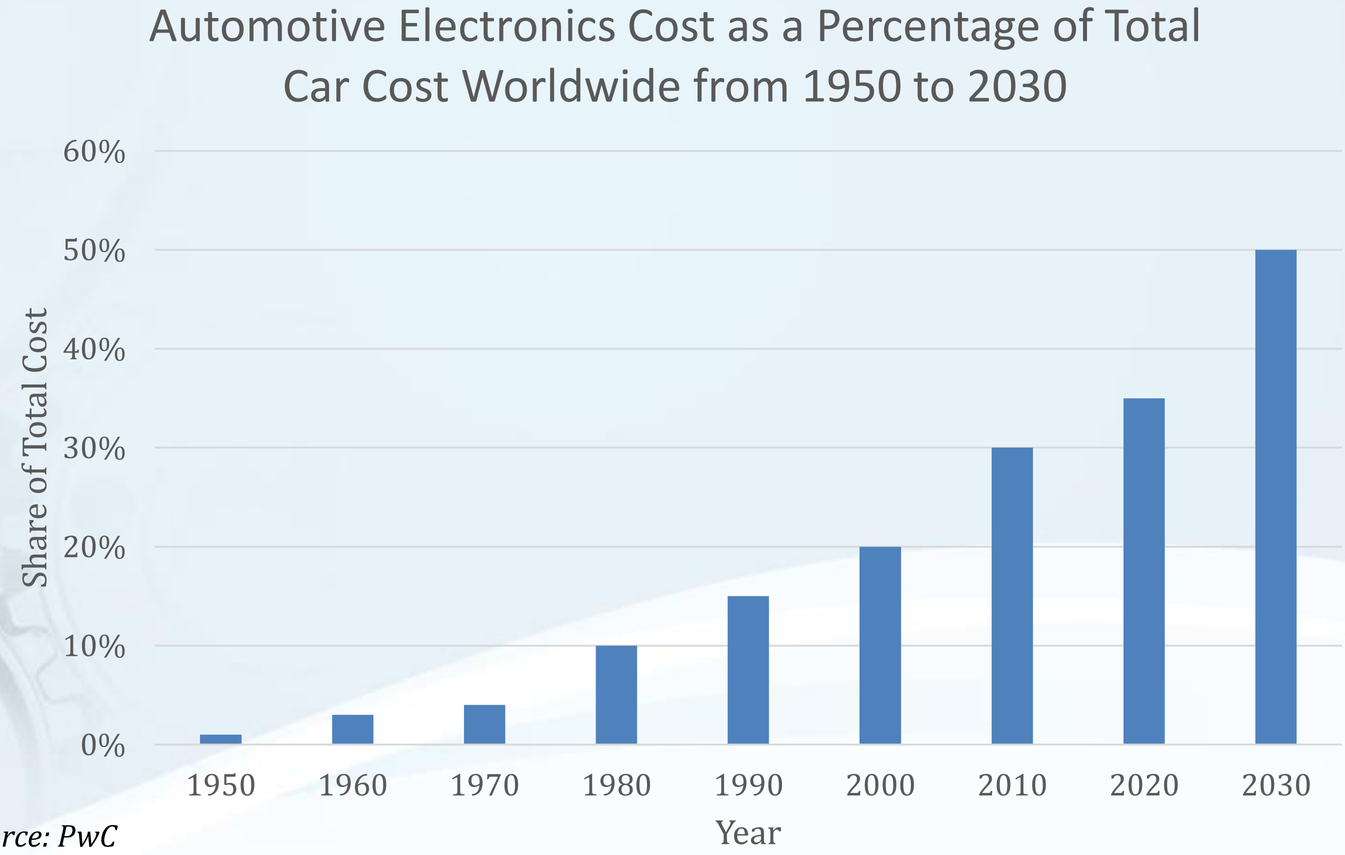
The Need for Functional Safety for E/E Systems

Vehicle's E/E systems are complex and are growing rapidly

Platform Golf IV (1998)	Platform Golf V (2003)	Platform Golf VI (2010)
17 ECUs 2 CANs 147 CAN-Messages 434 CAN signals	Central Gateway 35 ECUs 5 CANs, 3 LINs 307 CAN-Messages 2669 CAN signals	Central Gateway 49 ECUs 5 CANs, 7 LINs 704 CAN-Messages 6516 CAN signals

Source: Lisa Whalen, *Making Products and Systems Functionally Safe*, 2012 CTi Conference on ISO 26262, Troy, MI

Data On Electronic Content Increasing In Cars



Source: PwC

" …technology—including maintenance reminders and other safety alerts—hasn't reduced the number of drivers stranded on the roadside. Breakdowns are actually happening more than ever. One-in-five service calls for newer vehicles required towing to a repair facility in 2015, the study said. That's because newer vehicles are so complex, they're difficult to fix without the help of a mechanic"

– AAA Insurance

Hardware And Software Are Introducing New Faults In Cars

Software Now To Blame For 15 Percent Of Car Recalls

- *Bengt Halvorson, The Car Connection, June 2, 2016*

The number of software-related issues,…Automotive Warranty & Recall Report 2016, software-related recalls have gone from less than 5 percent of recalls in 2011 to 15 percent by the end of 2015….there have been 189 distinct software recalls issued over five years—covering more than 13 million vehicles…141 of these presented a higher risk of crashing."

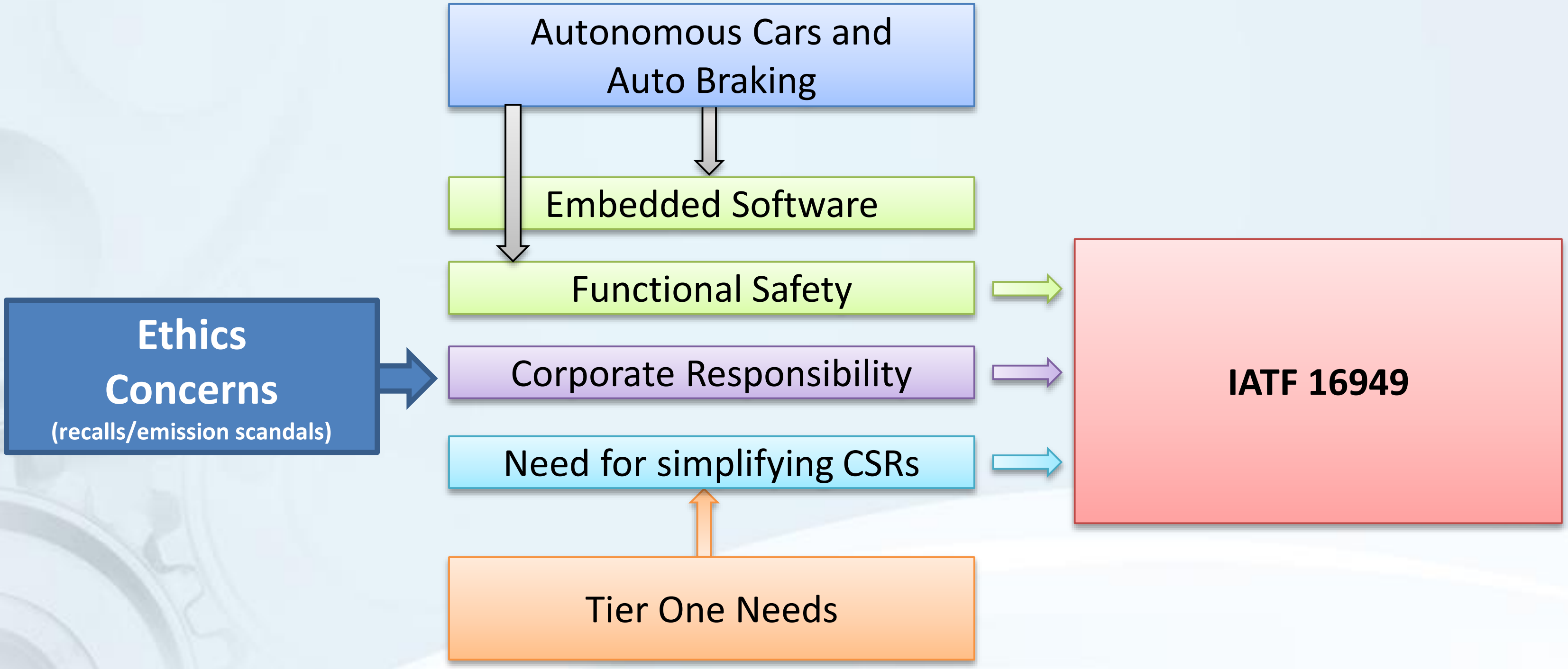
Automotive Safety Moves Into Semiconductors

– *James Morra, Electronic Design, 21st July 2017*

"…The [Automakers] industry has drafted the ISO26262 standard to make an industry rooted in mechanical engineering more safety conscious. The chip industry is adjusting, partly to avoid liability for self-driving car malfunctions and partly to hedge against costly recalls…"

The new electronics, hardware and software introduce new faults, some that are multi point. Functional Safety addresses these in software and hardware.

Drivers of IATF 16949 Changes



Autonomous Cars and Auto Braking

Embedded Software

Functional Safety

Ethics Concerns (recalls/emission scandals)

Corporate Responsibility

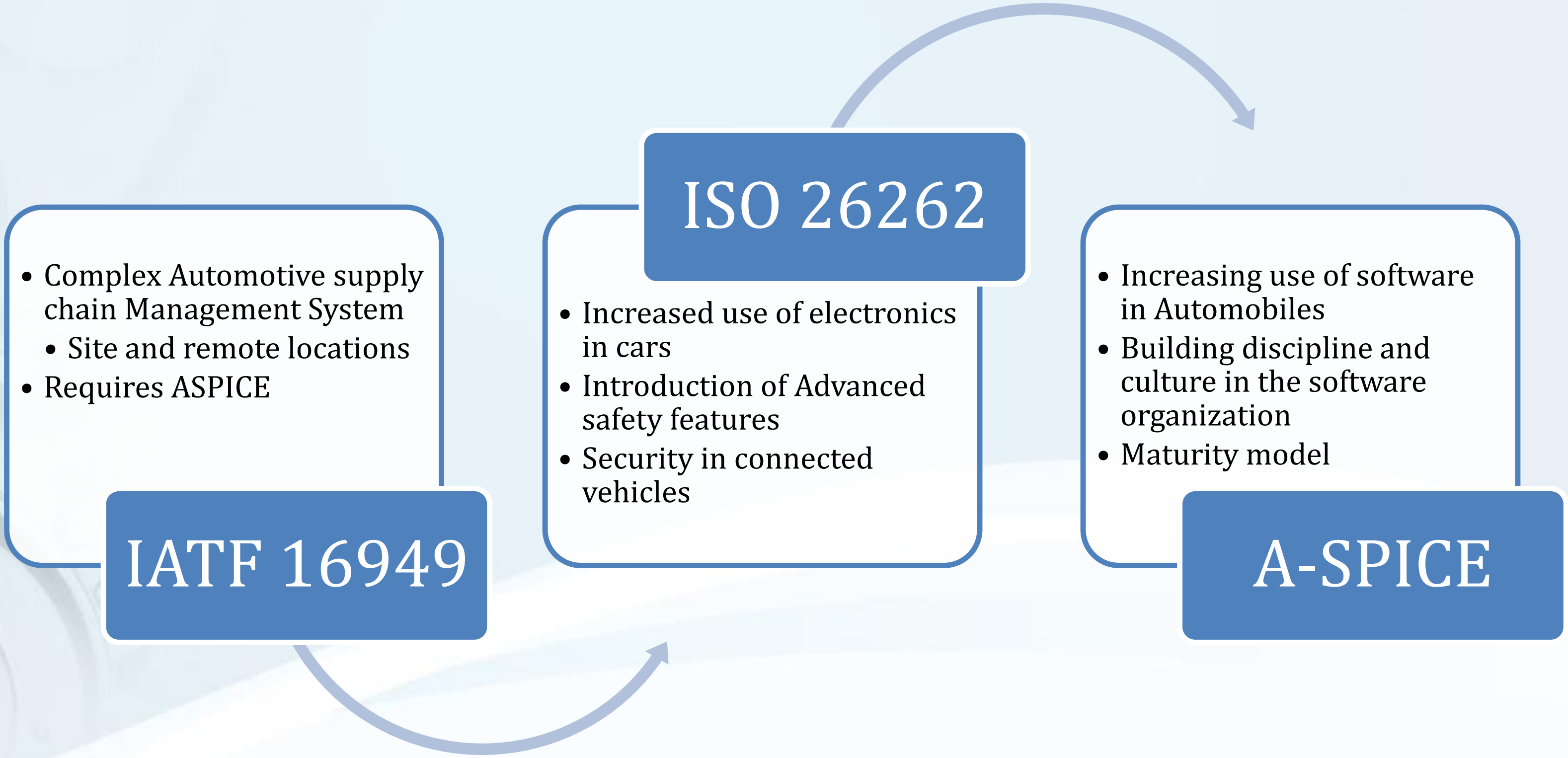
Need for simplifying CSRs

Tier One Needs

IATF 16949

Another theme in the standard involves the requirement for statutory and regulatory compliance addressed throughout the standard

IATF 16949, ISO 26262 and ASPICE



IATF 16949

- Complex Automotive supply chain Management System
  - Site and remote locations
- Requires ASPICE

ISO 26262

- Increased use of electronics in cars
- Introduction of Advanced safety features
- Security in connected vehicles

A-SPICE

- Increasing use of software in Automobiles
- Building discipline and culture in the software organization
- Maturity model

Many more standards related to Autonomous and E Cars for Cybersecurity, SOTIF, Autosar and related standards will impact the Automotive Industry as it shifts focus from Gasoline to E and Autonomous cars

Next Steps: Develop Implementation Plan

Month	1	2	3	4	5	6
Discovery Analysis	X					
Form Implementation Team	X					
Conduct Training for Implementation Team, Product Development Team, and Key Staff	X					
Safety Manual		X				
Process Documentation		X	X	X		
Develop Functional Safety Concept		X	X	X		
Develop Technical Safety Concept		X	X	X	X	
Develop Safety Analysis: FMEA/FTA		X	X	X	X	
Develop and implement V&V testing		X	X	X	X	
Develop Level II Engineers and Functional Safety Manager				**X**		

Note: This list is not exhaustive ….

Thank You!

Questions?

info@omnex.com
734.761.4940

Glossary

ISO 26262 – Part 1

Vocabulary

Part 1 provides definitions for the use of terms in the context of the ISO 26262 Standard

The definitions for these terms can be different than the use of the same term at various companies – be clear on terms and definitions used internally and those in standards, understand differences

Vocabulary

3.1 Architecture
Representation of the structure of the ***item*** **(3.84)** or ***element*** **(3.41)** that allows identification of building blocks, their boundaries and interfaces, and includes the allocation of requirements to these building blocks.

3.3 ASIL Decomposition
Apportioning of ***redundant safety*** **(3.132)** requirements to ***elements*** **(3.41)**, with sufficient ***independence*** **(3.78)**, conducing to the same ***safety goal*** **(3.139)**, with the objective of reducing the ***ASIL*** **(3.6)** of the redundant ***safety*** **(3.132)** requirements that are allocated to the corresponding ***elements*** **(3.41)**.

3.6 Automotive Safety Integrity Level – ASIL
One of four levels to specify the ***item's*** **(3.84)** or ***element's*** **(3.41)** necessary ISO 26262 requirements and ***safety measures*** **(3.141)** to apply for avoiding an ***unreasonable risk*** **(3.176)**, with D representing the most stringent and A the least stringent level.

Vocabulary

3.9 Base Vehicle
Original Equipment Manufacturer (OEM) ***T&B vehicle configuration*** **(3.175)** prior to installation **of *body builder equipment*** **(3.12)**.
Note: A base vehicle consists of all driving relevant ***systems*** **(3.163)**: engine, driveline, chassis, steering, brakes, cabin, driver information, on which ***body builder equipment*** **(3.12)** may be installed.

3.11 Body Builder (BB)
Organization that adds ***trucks*** **(3.174)**, ***buses*** **(3.14)**, ***trailers*** **(3.171)** and ***semi-trailers*** **(3.151)** (T&B) bodies, cargo carriers, or equipment to a ***base vehicle*** **(3.9)**.

3.14 Bus
Motor vehicle which, because its design and appointments, is intended for carrying persons and luggage, and which has more than nine seating places, including the driving seat.

Vocabulary

3.17 Cascading Failure

Failure **(3.50)** of an ***element*** **(3.41)** of an ***item*** **(3.84)** resulting from a root cause [inside or outside of the ***element*** **(3.41)**] and then causing a ***failure*** **(3.50)** of another ***element*** **(3.41)** or ***elements*** **(3.41)** of the same or different ***item*** **(3.84).**

Note 1: Cascading failures are ***dependent failures*** **(3.29)** that could be one of the possible root causes of a ***common cause failure*** **(3.18)**.

3.18 Common Cause Failure (CCF)

Failure **(3.50)** of two or more ***elements*** **(3.41)** of an ***item*** **(3.84)** resulting directly from a single specific event or root cause which is either internal or external to all of these ***elements*** **(3.41)**.

Note 1 to entry: Common cause failures are ***dependent failures*** **(3.29)** that are not ***cascading failures*** **(3.17)**.

3.19 Common Mode Failure CMF

Case of ***CCF*** **(3.18)** in which multiple ***elements*** **(3.41)** fail in the same manner.

Vocabulary

3.23 Confirmation Measure
***Confirmation review* (3.24)**, ***audit* (3.5)** or ***assessment* (3.4)** concerning ***functional safety* (3.67)**.

3.24 Confirmation Review
Confirmation that a ***work product* (3.185)** provides sufficient and convincing evidence of their contribution to the achievement of ***functional safety* (3.67)** considering the corresponding objectives and requirements of ISO 26262.

3.29 Dependent Failures
***Failures* (3.50)** that are not statistically independent, i.e. the probability of the combined occurrence of the ***failures* (3.50)** is not equal to the product of the probabilities of occurrence of all considered independent ***failures* (3.50)**.

3.32 Development Interface Agreement (DIA)
agreement between customer and supplier in which the responsibilities for activities to be performed, evidence to be reviewed, or ***work products* (3.185)** to be exchanged by each party related to the development of ***items* (3.84)** or ***elements* (3.41)** are specified.

Vocabulary

3.36 Distributed Development
Development of **an *item* (3.84)** or ***element* (3.41)** with development responsibility divided between the customer and supplier(s) for the entire ***item* (3.84)** or ***element* (3.41)**.

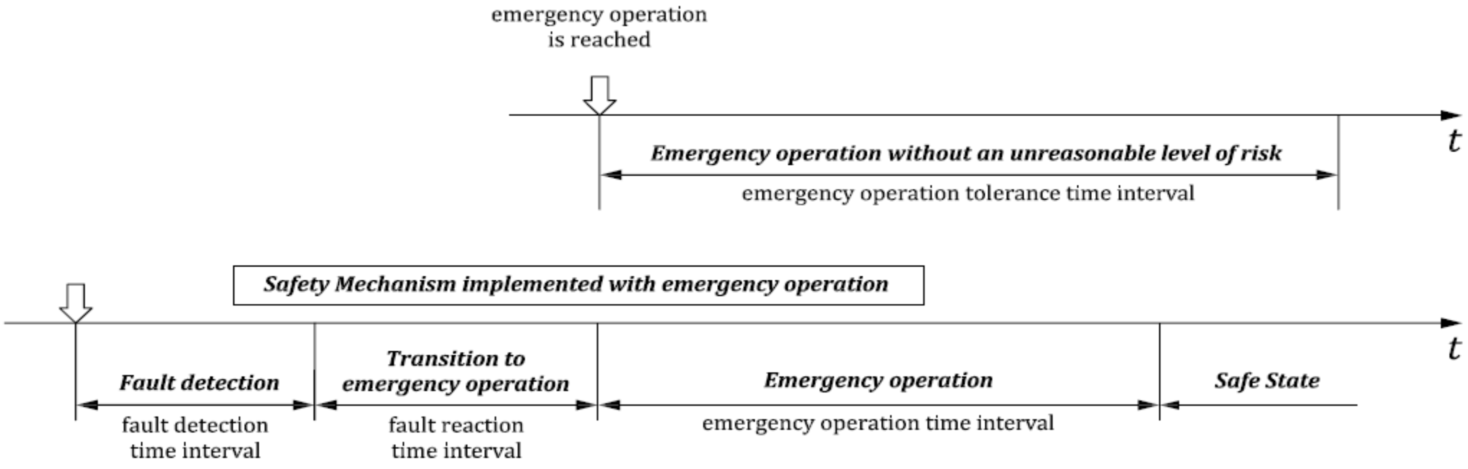
3.38 Dual-point Failure
***Failure* (3.50)** resulting from the combination of two independent hardware ***faults* (3.54)** that leads directly to the violation of a ***safety goal* (3.139)**.

3.41 Element
***System* (3.163)**, ***components* (3.21)** (hardware or software), ***hardware parts* (3.71)**, or ***software units* (3.159)**.

3.43 Emergency Operation
***Operating mode* (3.102)** of an ***item* (3.84)**, for providing ***safety* (3.132)** after the reaction to a ***fault* (3.54)** until the transition to a ***safe state* (3.131)** is achieved.

Vocabulary

3.45 Emergency Operation Tolerance Time Interval (EOTTI)
Specified time-span during which ***emergency operation* (3.43)** can be maintained without an unreasonable level of ***risk* (3.128)**.



emergency operation is reached
t
Emergency operation without an unreasonable level of risk
emergency operation tolerance time interval
Safety Mechanism implemented with emergency operation
t
Fault detection
fault detection time interval
Transition to emergency operation
fault reaction time interval
Emergency operation
emergency operation time interval
Safe State

Figure 4 — Emergency operation tolerance time interval

3.47 Expert Rider
Role filled by persons capable of evaluating ***controllability* (3.25)** classifications based on operation of actual ***motorcycles* (3.93)**.

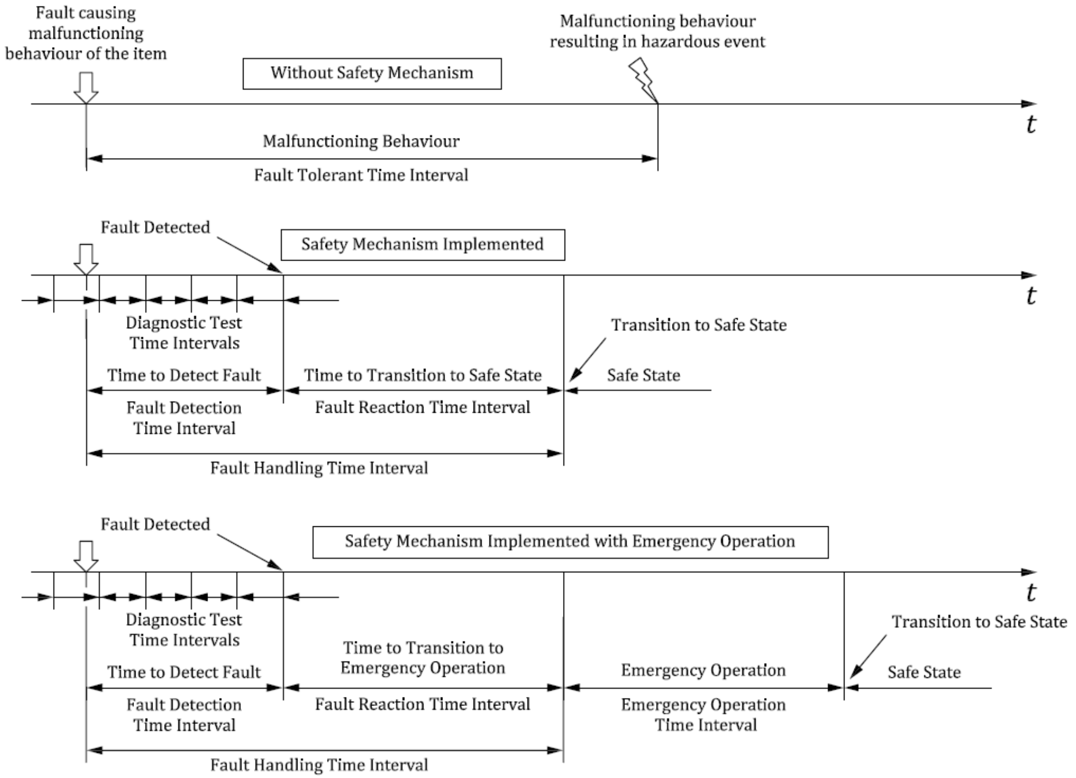
Vocabulary

3.54 Fault

Abnormal condition that can cause an ***element*** **(3.4**1) or an ***item*** **(3.84)** to fail.

3.59 Fault Reaction Time Interval (FRTI)

Time-span from the detection of a ***fault*** **(3.54)** to reaching a ***safe state*** **(3.131)** or to reaching ***emergency operation*** **(3.43)**.


Fault causing malfunctioning behaviour of the item
Without Safety Mechanism
Malfunctioning behaviour resulting in hazardous event
t
Malfunctioning Behaviour
Fault Tolerant Time Interval
Fault Detected
Safety Mechanism Implemented
t
Diagnostic Test Time Intervals
Transition to Safe State
Time to Detect Fault
Time to Transition to Safe State
Safe State
Fault Detection Time Interval
Fault Reaction Time Interval
Fault Handling Time Interval
Fault Detected
Safety Mechanism Implemented with Emergency Operation
t
Diagnostic Test Time Intervals
Transition to Safe State
Time to Transition to Emergency Operation
Time to Detect Fault
Emergency Operation
Safe State
Fault Detection Time Interval
Fault Reaction Time Interval
Emergency Operation Time Interval
Fault Handling Time Interval

Vocabulary

3.67 Functional Safety

Absence of ***unreasonable risk*** **(3.176)** due to ***hazards*** **(3.75)** caused by ***malfunctioning behavior*** **(3.88)** of ***E/E systems*** **(3.40)**.

Attributes of a Functionally Safe System

- Any random failures, systematic failures and common cause failures DO NOT lead to a malfunction of the safety-relevant system
- The injury or fatality of people is prevented

3.74 Harm

Physical injury or damage to the health of persons.

3.75 Hazard

Potential source of ***harm*** **(3.74)** caused by ***malfunctioning behavior*** **(3.88)** of the ***item*** **(3.84)**.

Vocabulary

3.76 Hazard Analysis and Risk Assessment (HARA)
Method to identify and categorize ***hazardous events*** **(3.77)** of ***items*** **(3.84)** and to specify ***safety goals*** **(3.139)** and ***ASILs*** **(3.6)** related to the prevention or mitigation of the associated ***hazards*** **(3.75)** in order to avoid ***unreasonable risk*** **(3.176)**.

3.77 Hazardous Event
Combination of a ***hazard*** **(3.75)** and an ***operational situation*** **(3.104)**.

3.85 Latent Fault
Multiple-point fault **(3.97)** whose presence is not detected by a ***safety mechanism*** **(3.142)** nor perceived by the driver within **the *multiple-point fault detection time interval*** **(3.98)**.

3.92 Modified Condition/Decision Coverage (MC/DC)
Percentage of all single condition outcomes that independently affect a decision outcome that have been exercised in the control flow.

Vocabulary

3.93 Motorcycle
Two-wheeled motor-driven vehicle, or three-wheeled motor-driven vehicle whose unladen weight does not exceed 800 kg, excluding mopeds as defined in ISO 3833.

3.94 Motorcycle Safety Integrity Level (MSIL)
One of four levels that specify the ***item's*** **(3.84)** or ***element's*** **(3.41)** necessary ISO 26262 ***risk*** **(3.128)** reduction requirements and convert to ***ASIL*** **(3.6)** for ***safety measures*** **(3.141)** to apply for avoiding unreasonable ***residual risk*** **(3.126)** for ***items*** **(3.84)** and ***elements*** **(3.41)** used specifically in ***motorcycle*** **(3.93)** applications, with D representing the most stringent and A the least stringent level

3.96 Multiple-point Failure
Failure **(3.50)**, resulting from the combination of several independent hardware ***faults*** **(3.54)**, which leads directly to the violation of a ***safety goal*** **(3.139)**.

Vocabulary

3.115 Proven in Use Argument
Evidence that, based on analysis of ***field data* (3.62)** resulting from use of a ***candidate* (3.16)**, the probability of any ***failure* (3.50)** of this candidate that could impair a ***safety goal* (3.139)** of an ***item* (3.84)**, meets the requirements for the applicable ***ASIL* (3.6)**.

3.118 Random Hardware Failure
***Failure* (3.50)** that can occur unpredictably during the lifetime of a hardware ***element* (3.41)** and that follows a probability distribution.

3.125 Residual Fault
Portion of a ***random hardware fault* (3.119)** that by itself leads to the violation of a ***safety goal* (3.139)**, occurring in a hardware ***element* (3.41)**, where that portion of the ***random hardware fault* (3.119)** is not controlled by a ***safety mechanism* (3.142)**.

3.126 Residual Risk

***Risk* (3.128)** remaining after the deployment of ***safety measures* (3.141)**.

Vocabulary

3.128 Risk
Combination of the probability of occurrence of ***harm*** **(3.74)** and the ***severity*** **(3.154)** of that ***harm*** **(3.74)**.

3.130 Safe Fault
Fault **(3.54)** whose occurrence will not significantly increase the probability of violation of a ***safety goal*** **(3.139)**.

3.131 Safe State
Operating mode **(3.102)**, in case of a ***failure*** **(3.51)**, of **an** ***item*** **(3.84)** without an unreasonable level of ***risk*** **(3.128)**.

3.132 Safety

Absence of ***unreasonable risk*** **(3.176)**.

Vocabulary

3.133 Safety Activity
Activity performed in one or more ***phases* (3.110)** or ***sub-phases* (3.161)** of the ***safety* (3.132)** ***lifecycle* (3.86)**.

3.136 Safety Case
Argument that ***functional safety* (3.67)** is achieved for ***items* (3.84)**, or ***elements* (3.41)**, and satisfied by evidence compiled from ***work products* (3.185)** of activities during development.

3.139 Safety Goal
Top-level ***safety* (3.132)** requirement as a result of the ***hazard analysis and risk assessment* (3.76)** at the vehicle level.

3.141 Safety Measure
Activity or technical solution to avoid or control ***systematic failures* (3.164)** and to detect or control ***random hardware failures* (3.118)**, or mitigate their harmful effects.

OMNEX

Vocabulary

3.142 Safety Mechanism

Technical solution implemented by E/E functions or ***elements*** **(3.41)**, or by ***other technologies*** **(3.105)**, to detect and mitigate or tolerate ***faults*** **(3.54)** or control or avoid ***failures*** **(3.50)** in order to maintain ***intended functionality*** **(3.83)** or achieve or maintain a ***safe state*** **(3.131)**.

3.145 Safety-related Function

Function that has the potential to contribute to the violation of or achievement of a ***safety goal*** **(3.139)**.

3.147 Safety-related Special Characteristic

Characteristic of an ***item*** **(3.84)** or **an *element*** **(3.41)**, or their production process, for which reasonably foreseeable deviation could impact, contribute to, or cause any potential reduction of ***functional safety*** **(3.67)**.

3.148 Safety Validation

Assurance, based on examination and tests, that the ***safety goals*** **(3.139)** are adequate and have been achieved with a sufficient level of integrity.

Vocabulary

3.151 Semi-trailer
***Trailer* (3.171)** which is designed to be towed by means of a kingpin coupled to a ***tractor* (3.170)** that imposes a substantial vertical load on the towing vehicle.

3.152 Series Production Road Vehicle
Road vehicle which is intended to be used for public roads and is not a prototype.

3.155 Single-point Failure
***Failure* (3.50)** that results from a ***single-point fault* (3.156)**.

3.156 Single-point Fault
Hardware ***fault* (3.54)** in an ***element* (3.4.1)** leads directly to the violation of a ***safety goal* (3.139**) and no ***fault* (3.5.4**) in that ***element* (3.4.1)** is covered by any ***safety mechanism* (3.142)**.

Vocabulary

3.163 System

Set of ***components*** **(3.21)** or subsystems that relates at least a sensor, a controller and an actuator with one another.

NOTE : The related sensor or actuator can external to the system.

3.164 Systematic Failure

Failure **(3.50)** related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.

3.170 Tractor

Truck **(3.174)** that is designed to tow a ***semi-trailer*** **(3.151)**.

Vocabulary

3.171 Trailer

Road vehicle which is designed to be towed such that no substantial part of the total weight is supported by the towing vehicle.

3.174 Truck

Motor vehicle designed to transport goods, or equipment on-board the chassis.

3.175 T&B Vehicle Configuration

Technical characteristics of a T&B ***base vehicle*** **(3.9)** and ***body builder equipment*** **(3.12)** that do not change during operation.

3.180 Verification

Determination whether or not an examined object meets its specified requirements.

3.184 Well-trusted

Previously used without known ***safety anomalies*** **(3.134)** in a comparable application.