

ISO 26262

Functional Safety Draft International Standard for Road Vehicles: Background, Status, and Overview

Barbara J. Czerny, Joseph D'Ambrosio, Rami Debouk,

General Motors Research and Development

Kelly Stashko, General Motors Powertrain



- This tutorial presents an overview of the Draft International Standard (DIS) version of the proposed ISO 26262 Functional Safety standard for road vehicles
 - It conveys the content of the standard as it is currently drafted
 - Since the release of the DIS, additional technical and editorial changes to the text have been made, but these will not be covered in the tutorial slides
- Permission was received from ISO to use content taken directly from the ISO/DIS and contained in this presentation
- The process presented in this tutorial, represents the ISO/DIS 26262 process and is not intended to reflect or discuss the processes of any specific individual manufacturer



Roadmap

- Background
- Status
- Part 1: Vocabulary and Part 10: Guideline
- Part 2: Management of Functional Safety
- Part 3: Concept Phase
- Part 4: Product Development: System Level
- Part 5: Product Development: Hardware Level
- Part 6: Product Development: Software Level
- Part 7: Production and Operation
- Part 8: Supporting Processes
- Part 9: ASIL-oriented and Safety-oriented Analyses
- Key aspects that have evolved over time
- Summary
- Q&A

Break

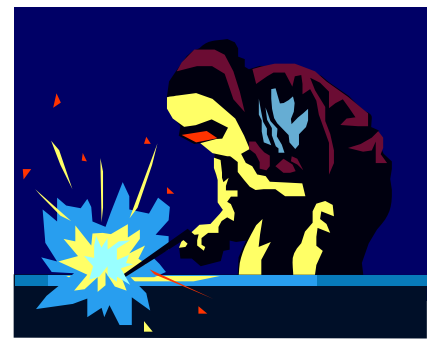
O
v
e
r
v
i
e
w



Background

Barbara J. Czerny

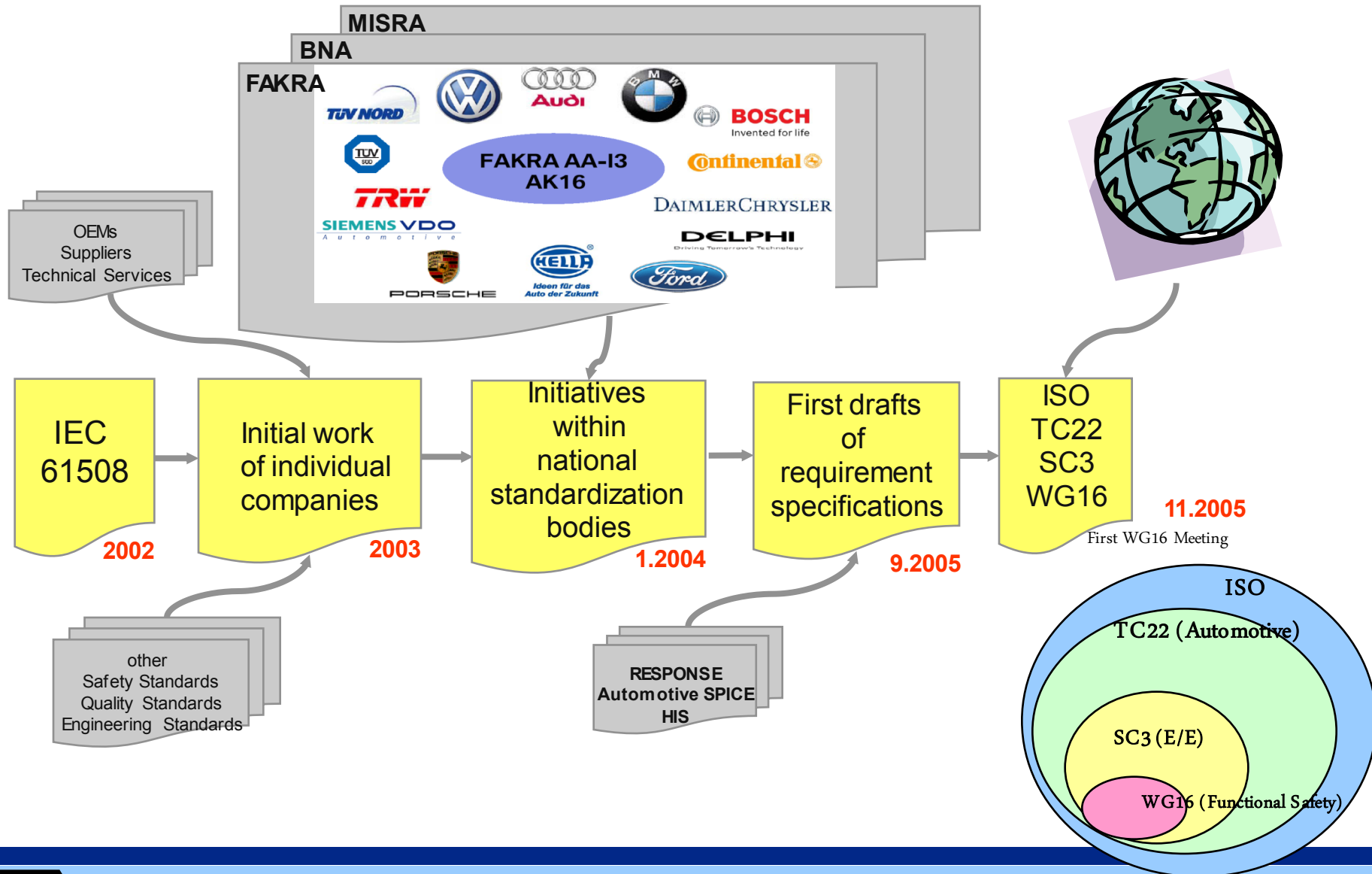




- Adaptation of IEC 61508 to comply with the specific needs of E/E systems within road vehicles
 - Specifies a functional safety life-cycle for automotive products
- Applies to all activities during the safety lifecycle of safety-related systems comprised of electrical, electronic, and software components
- Scope
 - Series production passenger cars
 - Maximum gross weight up to 3500 kg
 - Does not apply to E/E systems in special purpose vehicles
 - e.g., vehicles designed for drivers with disabilities



Origins of ISO 26262 (Automotive IEC 61508)



ISO 26262 Working Group 16

| | |
|-----------|---|
| Convenor | Ch. Jung, Independent Consultant |
| Secretary | E. Fritzsche, VDA |
| | |
| Germany | BMW, Daimler, VW, Bosch, <u>Continental</u> |
| France | <u>PSA</u> , Renault, Continental, Valeo |
| UK | Landrover, <u>MIRA</u> , Renesas |
| Sweden | Delphi, <u>Volvo Cars</u> , AB Volvo, Mecel |
| Italy | Centro Ricerche Fiat, <u>Fiat Auto</u> , TRW |
| Japan | Denso, Hitachi, Honda, <u>Nissan</u> , Toyota |
| USA | GM, IBM, <u>TRW</u> , |
| Belgium | <u>Nissan</u> , Toyota Motor Europe |

Active membership as of 10/2007



What's the Difference Between IEC 61508 and ISO 26262?

➤ IEC 61508:

1. Framework standard
2. Implied context of Process/Automation industries (where validation is done after install)
3. Safety Integrity Levels, “SIL”
 - SIL 1 – SIL 4
 - Measure of the reliability of safety functions
 - Includes a quantitative target for the probability of a dangerous failure
 - No exact mapping between SIL's and ASIL's
 - Loose mapping
 - SIL's 1, 2, 3
 - Between SIL 2 and SIL 3
4. Focus on safety functions

➤ ISO 26262:

1. IEC 61508 Automotive Sector adaptation
2. Applies to vehicles with ≥ 4 wheels (carrying passengers, goods)
3. Automotive SIL, “ASIL”
 - ASIL A-D
 - Based on the violation of a safety goal
 - Provides requirements to achieve acceptable level of risk
 - No exact mapping between SIL's and ASIL's
 - Loose mapping
 - ASIL's A, B, and D
 - ASIL C
4. Focus on safety goals
5. Adds required work products



Prescriptive (IEC 61508) vs. Goal-Oriented (ISO 26262)

➤ Tables

- Example of Part 4 Table 2 “System design verification”
- **Goal requirement:** System design shall be verified for compliance and completeness with regard to the technical safety concept. In this aim, the methods and measures in Table 2 shall be considered.

| Methods | | ASIL | | | |
|---|---|-------------|----|----|----|
| | | A | B | C | D |
| 1a | System design inspection ^a | + | ++ | ++ | ++ |
| 1b | System design walkthrough ^a | ++ | + | 0 | 0 |
| 2a | Simulation ^b | + | + | ++ | ++ |
| 2b | System prototyping and vehicle tests ^b | + | + | ++ | ++ |
| 3 | Safety analyses ^c | see Table 1 | | | |
| ^a Methods 1a and 1b serve as check of complete and correct detailing and implementation of the technical safety requirements into system design. | | | | | |
| ^b Methods 2a and 2b can be used advantageously as a fault injection technique. | | | | | |
| ^c For conducting safety analyses, see ISO 26262-9: —, Clause 8. | | | | | |

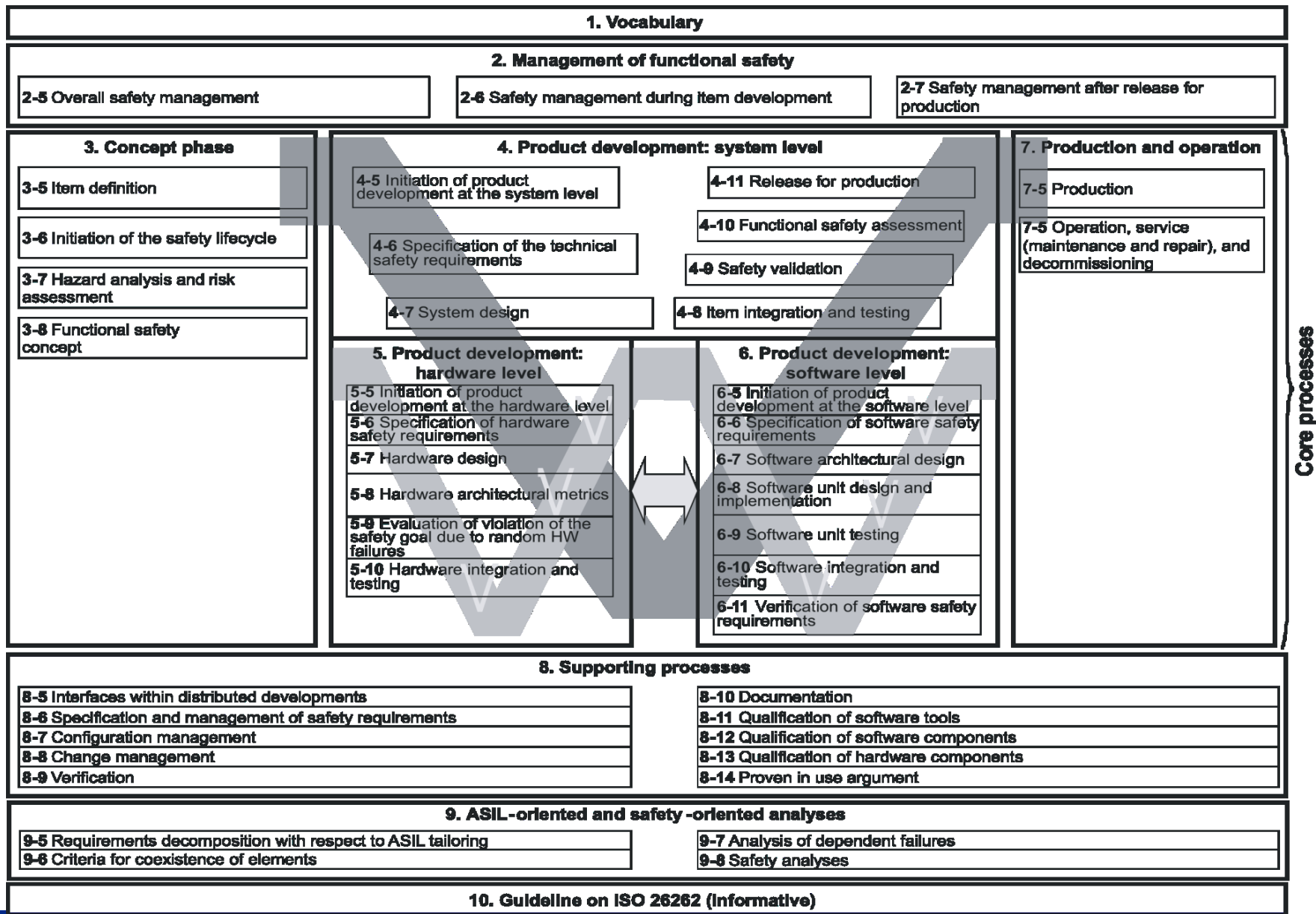
Source: ISO/DIS 26262



More Facts About ISO/DIS 26262

- Focus is on possible hazards caused by malfunctioning behavior of E/E safety-related systems
 - failures or unintended behaviours of an item with respect to its design intent
 - Includes interactions between E/E safety-related systems
- Process Framework includes the following process steps/deliverables:
 - Safety plan & safety goals
 - Safety case & documentation
 - Bidirectional traceability
 - Safety lifecycle
 - Validation, verification and independent assessment
- Corresponds to automotive product lifecycle
 - Development, validation, release for production vs. development, installation and commissioning, validation in IEC 61508
- Supports distributed development
 - e.g., division of work between OEMs/suppliers
- Hazard analysis corresponds to automotive use cases
- Includes “Controllability” in Risk Assessment

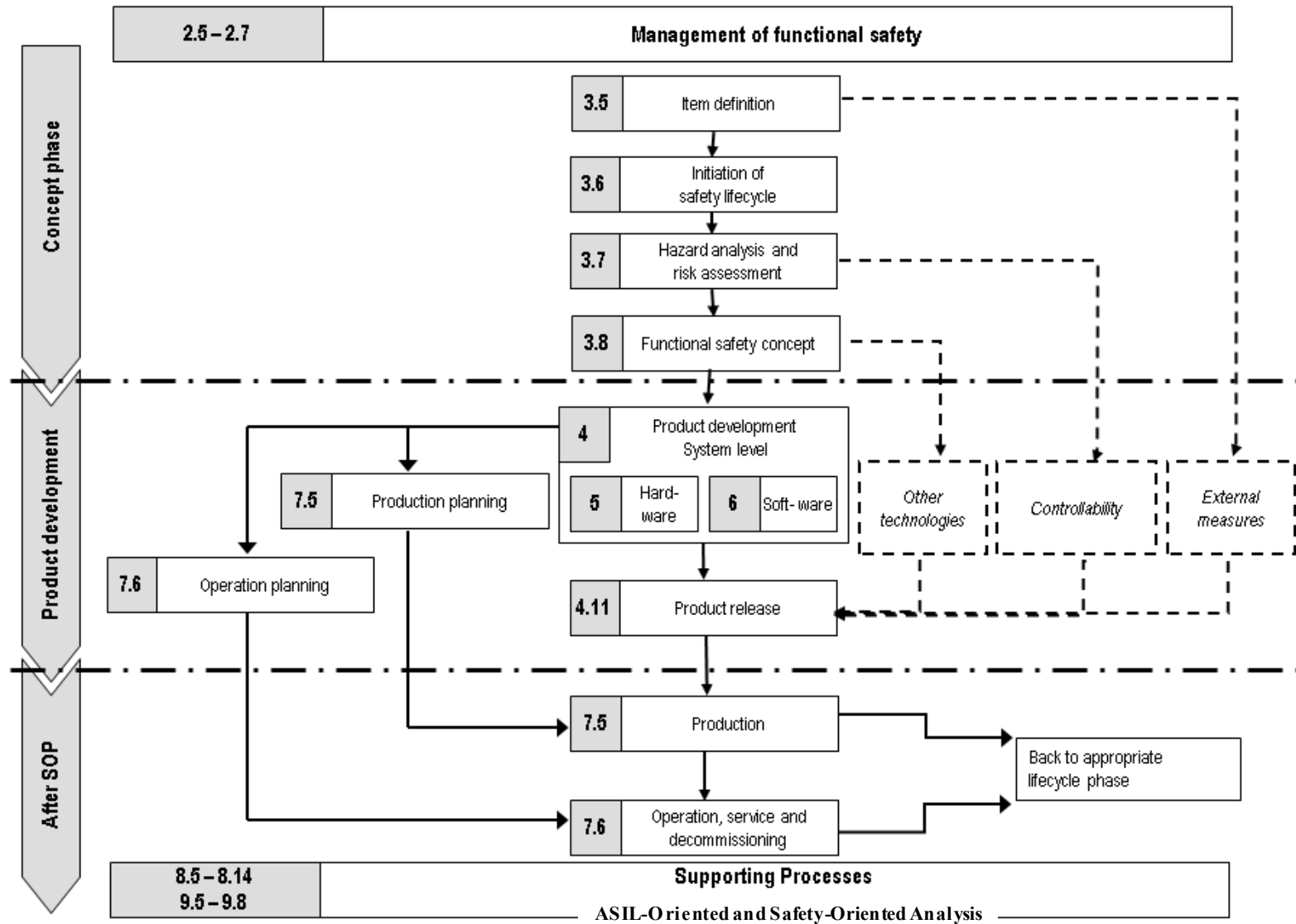




Source ISO/DIS 26262



Flow and Organization of ISO 26262



Source ISO/DIS 26262

Status of Development

- ISO Draft International Standard made available for review by all SC 3 countries July 2009
 - First time a version of the standard was made publically available
- DIS ballot held in November 2009 and ballot passed
- Preparing Final Draft International Standard (FDIS)
 - Working on resolving comments received with DIS Ballot
- FDIS version will be handed over to ISO for publication in late 2010
 - Review of FDIS will only be for editorial changes
 - Part 10 will have a second DIS ballot
- Expect publication as a full International Standard in mid-2011



Checkpoint Questions – Background and Status

1. On what standard is ISO 26262 based?
 - A. ISO/IEC 12207 – Systems Software engineering – Software life cycle processes
 - B. ISO/IEC 15504 – AutoSpice
 - C. IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems
 - D. None – ISO 26262 is completely new and developed for Automotive Safety
2. Is there a top Level probability associated with an ASIL
 - A. Yes
 - B. No
3. Name the fundamental steps/deliverables of the ISO26262 Process Framework.
 - A. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - B. Safety plan & potential hazards, Safety cases & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - C. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and external assessment
4. Is Controllability included in the Risk Assessment
 - A. Yes
 - B. No



Checkpoint Questions – Background and Status

1. On what standard is ISO 26262 based?
 - A. ISO/IEC 12207 – Systems Software engineering – Software life cycle processes
 - B. ISO/IEC 15504 – AutoSpice
 - C. IEC 61508 -- Functional safety of electrical/electronic/programmable electronic safety-related systems
 - D. None – ISO 26262 is completely new and developed for Automotive Safety
2. Is there a top Level probability associated with an ASIL
 - A. Yes
 - B. No
3. Name the fundamental steps/deliverables of the ISO26262 Process Framework.
 - A. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - B. Safety plan & potential hazards, Safety cases & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - C. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and external assessment
4. Is Controllability included in the Risk Assessment
 - A. Yes
 - B. No



Checkpoint Questions – Background and Status

1. On what standard is ISO 26262 based?
 - A. ISO/IEC 12207 – Systems Software engineering – Software life cycle processes
 - B. ISO/IEC 15504 – AutoSpice
 - C. IEC 61508 -- Functional safety of electrical/electronic/programmable electronic safety-related systems
 - D. None – ISO 26262 is completely new and developed for Automotive Safety
2. Is there a top Level probability associated with an ASIL
 - A. Yes
 - B. No
3. Name the fundamental steps/deliverables of the ISO26262 Process Framework.
 - A. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - B. Safety plan & potential hazards, Safety cases & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - C. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and external assessment
4. Is Controllability included in the Risk Assessment
 - A. Yes
 - B. No



Checkpoint Questions – Background and Status

1. On what standard is ISO 26262 based?
 - A. ISO/IEC 12207 – Systems Software engineering – Software life cycle processes
 - B. ISO/IEC 15504 – AutoSpice
 - C. **IEC 61508 -- Functional safety of electrical/electronic/programmable electronic safety-related systems**
 - D. None – ISO 26262 is completely new and developed for Automotive Safety
2. Is there a top Level probability associated with an ASIL
 - A. Yes
 - B. **No**
3. Name the fundamental steps/deliverables of the ISO26262 Process Framework.
 - A. **Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment**
 - B. Safety plan & potential hazards, Safety cases & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - C. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and external assessment
4. Is Controllability included in the Risk Assessment
 - A. Yes
 - B. No



Checkpoint Questions – Background and Status

1. On what standard is ISO 26262 based?
 - A. ISO/IEC 12207 – Systems Software engineering – Software life cycle processes
 - B. ISO/IEC 15504 – AutoSpice
 - C. **IEC 61508 -- Functional safety of electrical/electronic/programmable electronic safety-related systems**
 - D. None – ISO 26262 is completely new and developed for Automotive Safety
2. Is there a top Level probability associated with an ASIL
 - A. Yes
 - B. **No**
3. Name the fundamental steps/deliverables of the ISO26262 Process Framework.
 - A. **Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment**
 - B. Safety plan & potential hazards, Safety cases & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and independent assessment
 - C. Safety plan & safety goals, Safety case & documentation, Bidirectional traceability, Safety lifecycle, Validation, verification and external assessment
4. Is Controllability included in the Risk Assessment
 - A. **Yes**
 - B. No



Part 1: Vocabulary
&
Part 10: Guideline on ISO 26262 (Informative)

Rami Debouk



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Safety management during item development

2-7 Safety management after release for production

3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4. Product development: system level

4-5 Initiation of product development at the system level

4-11 Release for production

4-10 Functional safety assessment

4-6 Specification of the technical safety requirements

4-9 Safety validation

4-7 System design

4-8 Item integration and testing

7. Production and operation

7-5 Production

7-5 Operation, service (maintenance and repair), and decommissioning

5. Product development: hardware level

5-5 Initiation of product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Hardware architectural metrics

5-9 Evaluation of violation of the safety goal due to random HW failures

5-10 Hardware integration and testing

6. Product development: software level

6-5 Initiation of product development at the software level

6-6 Specification of software safety requirements

6-7 Software architectural design

6-8 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

6-11 Verification of software safety requirements

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 Qualification of software tools

8-12 Qualification of software components

8-13 Qualification of hardware components

8-14 Proven in use argument

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 analyses

10. Guideline on ISO 26262 (Informative)

Core processes

Source ISO/DIS 26262

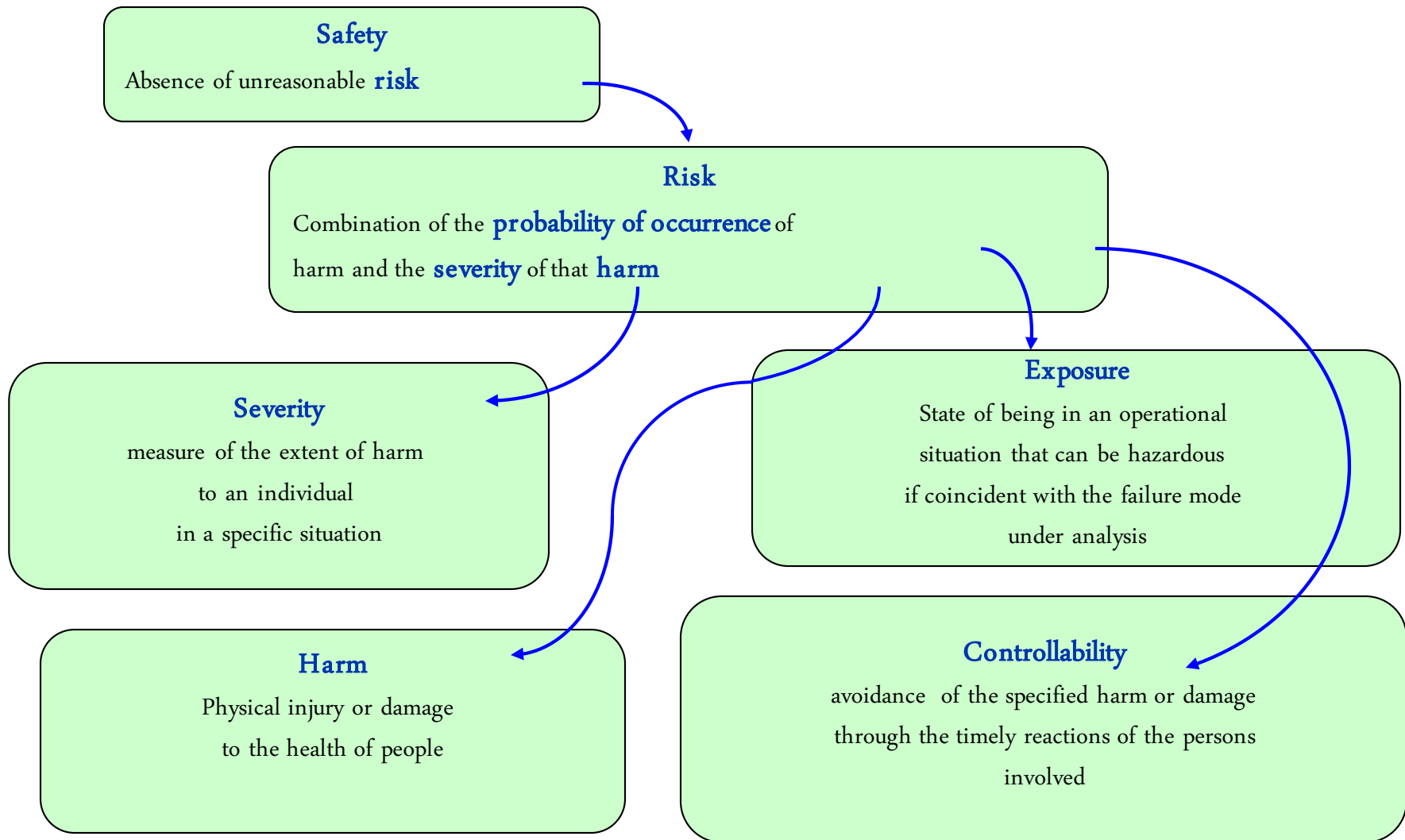
ISO 26262 Road Vehicles - Functional Safety

Draft International Standard Tutorial

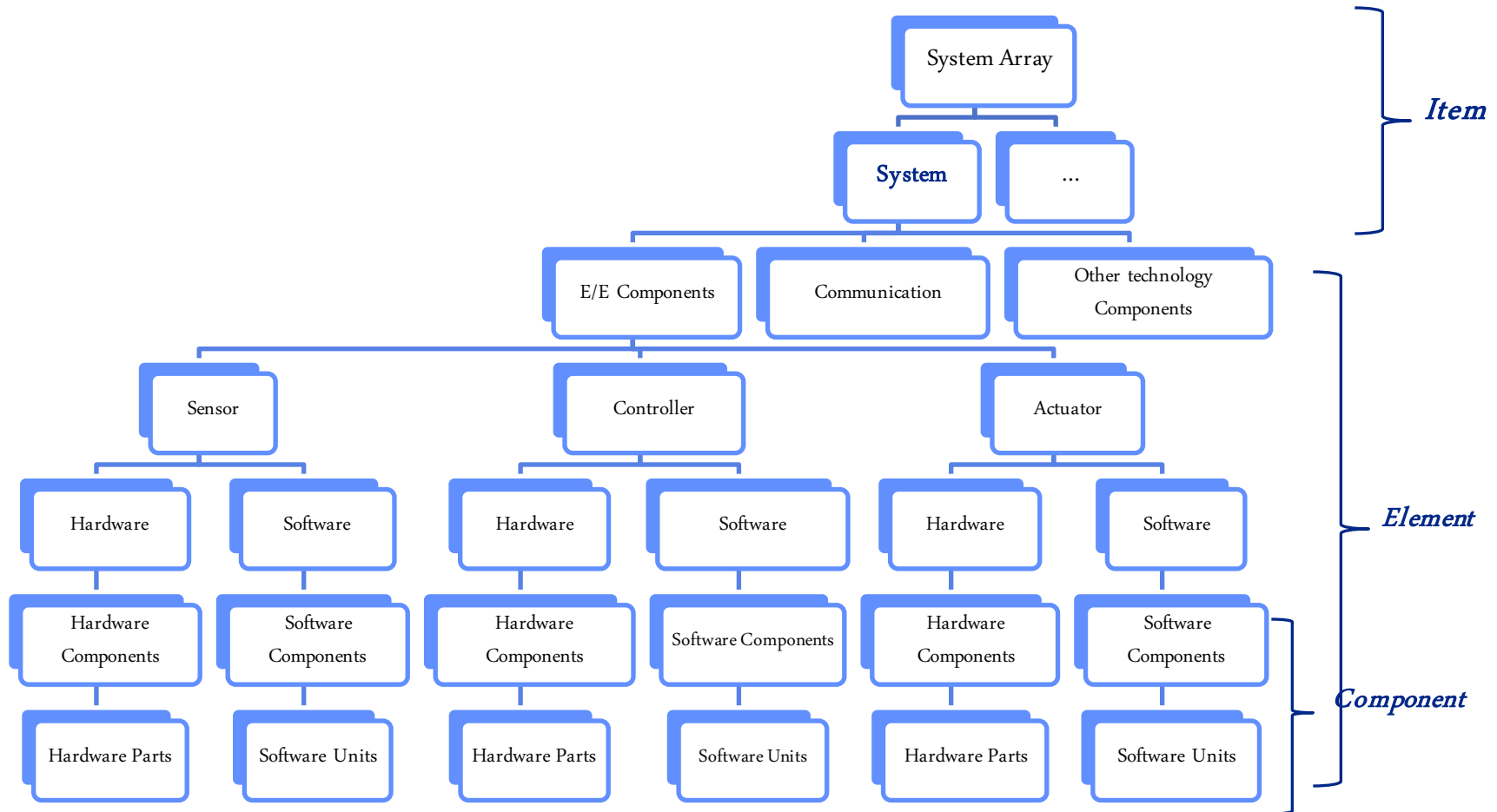
ISSC 2010 Minneapolis, Minnesota



ISO/DIS 26262 Terms



Item, system, element, & component



A software component consists of one or more software components, or software units, or both



Failure Types

- Random Hardware Failures
 - failure that may occur unpredictably during the lifetime of a hardware element and that follows a probability distribution

- Systematic Failures
 - failure of an element or item that is caused in a deterministic way during development, manufacturing, or maintenance
 - all software faults and a subset of hardware faults are systematic



ISO 26262 Terms

Safety Mechanism

Safety Mechanism

- Activity or technical solution to detect / avoid / control failures or mitigate their harmful effects
- Implemented by an E/E function or element or in other technologies
- The safety mechanism is either
 - able to switch 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



ISO 26262 Terms

Work Products

Work product

- Information or data
- The result of one or more system safety process activities
- Format appropriate to the work product's content
 - Data files, models, source code, etc.
 - May include currently existing documents
 - Several work products may be in one document



ISO 26262 Terms

Confirmation Measures

Confirmation measures

- Ensure the sufficient completion of work products and proper execution of the safety lifecycle.
- Provide for the evaluation of the system safety activities and work products as a whole
- Used to determine the adequacy of achievement of the functional safety goals



ISO 26262 Terms

Safety Case

Safety case

- Communicates a clear, comprehensive and defensible argument (supported by evidence) that a system is acceptably safe to operate in a particular context.
- Includes references to safety requirements and supporting evidence
- AND a “safety argument” that describes how the safety requirements have been interpreted, allocated, decomposed, etc., and fulfilled as shown by the supporting evidence.



Part 2: Management of Functional Safety

Rami Debouk



1. Vocabulary

2. Management of functional safety

2-5 Overall safety management

2-6 Safety management during item development

2-7 Safety management after release for production

3. Concept phase

3-5 Item definition

3-6 Initiation of the safety lifecycle

3-7 Hazard analysis and risk assessment

3-8 Functional safety concept

4. Product development: system level

4-5 Initiation of product development at the system level

4-6 Specification of the technical safety requirements

4-7 System design

4-11 Release for production

4-10 Functional safety assessment

4-9 Safety validation

4-8 Item integration and testing

5. Product development: hardware level

5-5 Initiation of product development at the hardware level

5-6 Specification of hardware safety requirements

5-7 Hardware design

5-8 Hardware architectural metrics

5-9 Evaluation of violation of the safety goal due to random HW failures

5-10 Hardware integration and testing

6. Product development: software level

6-5 Initiation of product development at the software level

6-6 Specification of software safety requirements

6-7 Software architectural design

6-8 Software unit design and implementation

6-9 Software unit testing

6-10 Software integration and testing

6-11 Verification of software safety requirements

7. Production and operation

7-5 Production

7-5 Operation, service (maintenance and repair), and decommissioning

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 Qualification of software tools

8-12 Qualification of software components

8-13 Qualification of hardware components

8-14 Proven in use argument

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 analyses

10. Guideline on ISO 26262 (Informative)

Core processes

Source ISO/DIS 26262

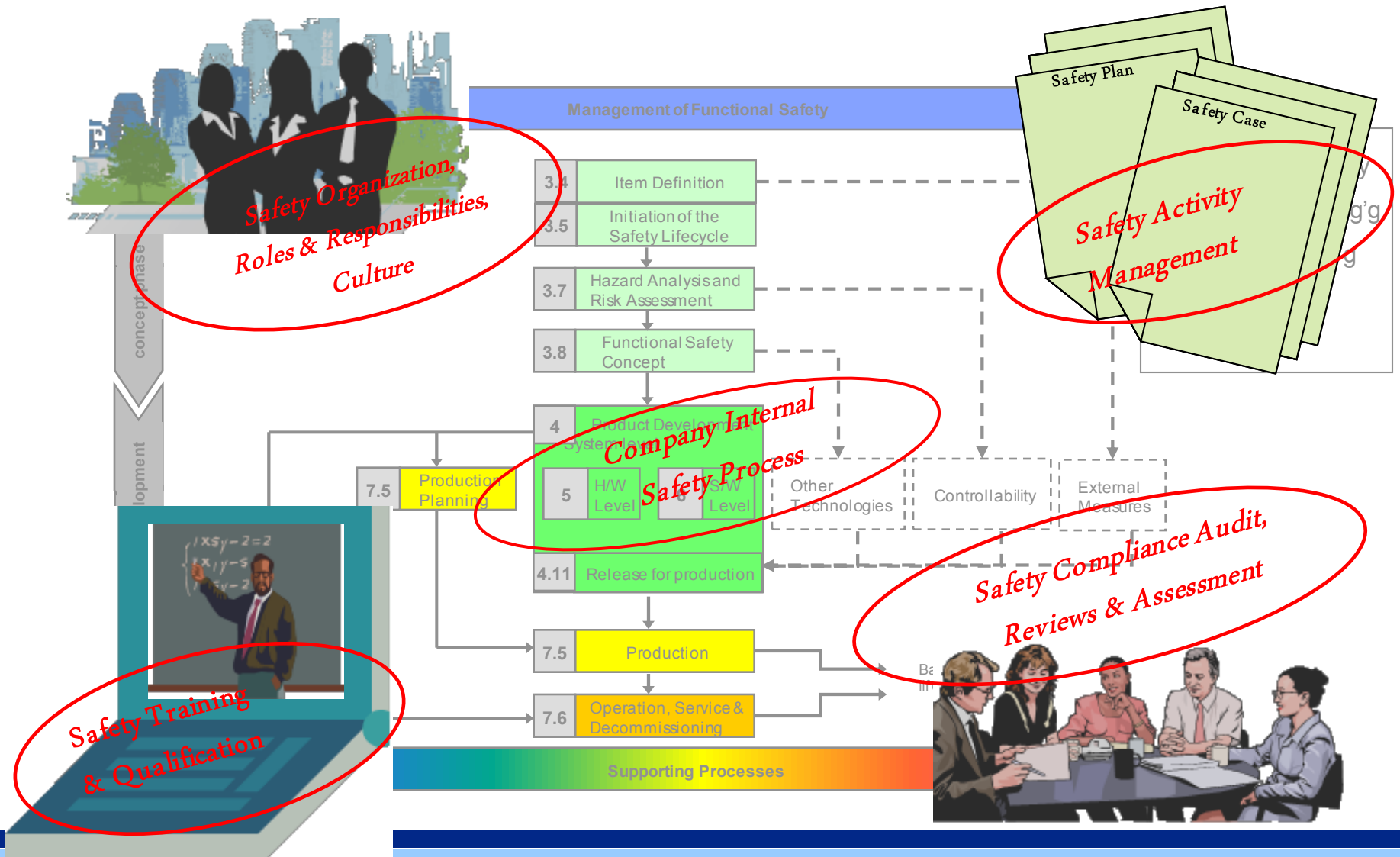
ISO 26262 Road Vehicles - Functional Safety

Draft International Standard Tutorial

ISSC 2010 Minneapolis, Minnesota



Part 2: Management of Functional Safety



Overview

Functional Safety Management requires:

- Planning, coordinating, and documenting activities related to functional safety
- Implementing management plan for all phases of the safety lifecycle, including:
 - Overall project-independent functional safety management activities
 - Safety management during development
 - Safety management after Start of Production (SOP)



Overall Project Independent Safety Management

Objectives

- Define **responsibilities** of persons, departments and organisations in charge of each phase during the overall **safety lifecycle**
- Define **management activities** during the complete **safety lifecycle**

Management plan to incorporate:

- Safety culture
- Quality management
- Continuous improvement
- Training and qualification
- Application of the lifecycle



Safety Management during Development

Objectives

- To define **responsibilities** of the persons, departments and organisations in charge of functional safety for each phase **during development**
- Includes activities to ensure functional safety of the item
- Includes activities for confirmation of functional safety measures
- Define **management activities** during the **development phases**

Management plan to incorporate:

- Allocation of safety responsibilities and duties
- All safety management activities during development
- Safety case
- Confirmation measures for assessment of functional safety



Safety Management during Development

Confirmation Measures

Confirmation review

- Purpose: Evaluate the safety activity work products for compliance with the requirements of ISO 26262
- How: Work products are evaluated for compliance after completion of select safety activities, and a subsequent review of this compliance evidence is conducted, resulting in confirmation review reports

Functional safety audit

- Purpose: Evaluate the development process applied (as defined by the product's safety plan)
- How: Phased reviews during the development process, resulting in audit reports

Functional safety assessment

- Purpose: Evaluate the achieved functional safety of the item
- How: Progressive review of processes and safety measures applied during development to achieve functional safety of the item



Confirmation Measures Requirements

- Depending on the work product and the ASIL assigned to safety goals, confirmation measures are either recommended or required

- In the case of required confirmation measures:
 - There are no requirements on the person performing the confirmation measure
 - The confirmation measure shall be performed by a person from a different team, not reporting to the same direct superior
 - The confirmation measure shall be performed, by a person from a different department or organization, i.e., independent from the relevant department, regarding management, resources, and responsibility for release for production



Safety Management after Start of Production (SOP)

Objectives

- To define **responsibilities** of persons, departments and organisations in charge of functional safety **after SOP**
- Relates to general activities necessary to ensure the required functional safety of the item

Requirements

- Organizational measures to achieve functional safety
- Management of functional safety after SOP
- Field monitoring and collection of data
- Malfunction survey
- Malfunction analysis
- Malfunction solution



Part 2 Work Products

- ☐ Company-specific standard for functional safety
- ☐ Training and qualification program
- ☐ Quality management system
- ☐ Safety plan
- ☐ Overall project plan
- ☐ Safety case
- ☐ Results of the Confirmation measures
- ☐ Confirmation plan
- ☐ Functional safety assessment plan
- ☐ Evidence of a field monitoring process



Checkpoint Questions –

Part 2: Management of Functional Safety

1. What are the requirements for Project Independent Safety Management?
 - A. Safety culture and Quality management
 - B. Continuous improvement, Training, and qualification
 - C. Application of the lifecycle
 - D. All of the above
2. Are a Safety Plan, Confirmation Plan, and a Safety Case required Work products
 - A. Yes
 - B. No



Checkpoint Questions –

Part 2: Management of Functional Safety

1. What are the requirements for Project Independent Safety Management?
 - A. Safety culture and Quality management
 - B. Continuous improvement, Training, and qualification
 - C. Application of the lifecycle
 - D. All of the above**

2. Are a Safety Plan, Confirmation Plan, and a Safety Case required Work products
 - A. Yes
 - B. No



Checkpoint Questions –

Part 2: Management of Functional Safety

1. What are the requirements for Project Independent Safety Management?
 - A. Safety culture and Quality management
 - B. Continuous improvement, Training, and qualification
 - C. Application of the lifecycle
 - D. All of the above**

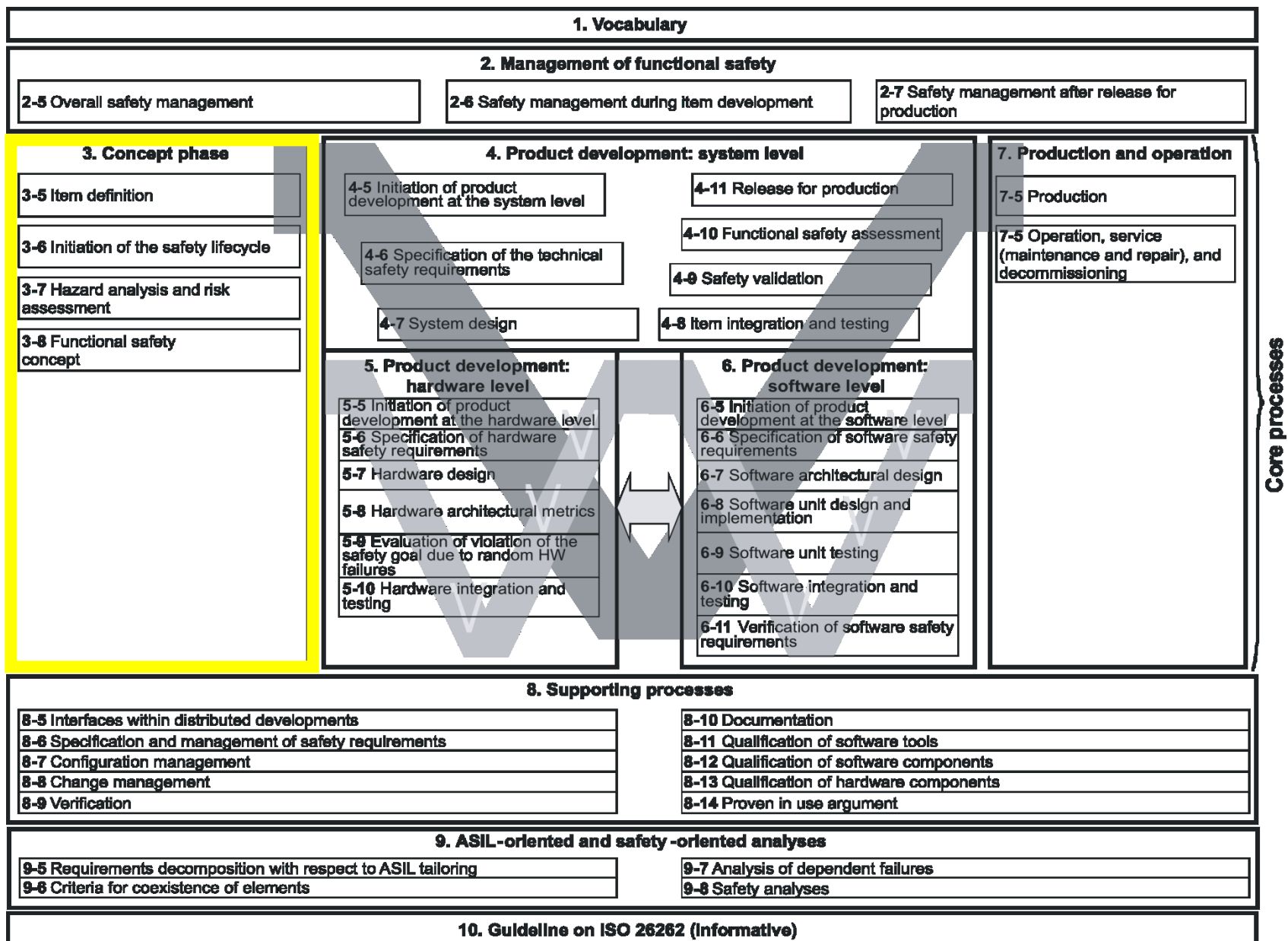
2. Are a Safety Plan, Confirmation Plan, and a Safety Case required Work products?
 - A. Yes**
 - B. No



Part 3: Concept Phase

Rami Debouk





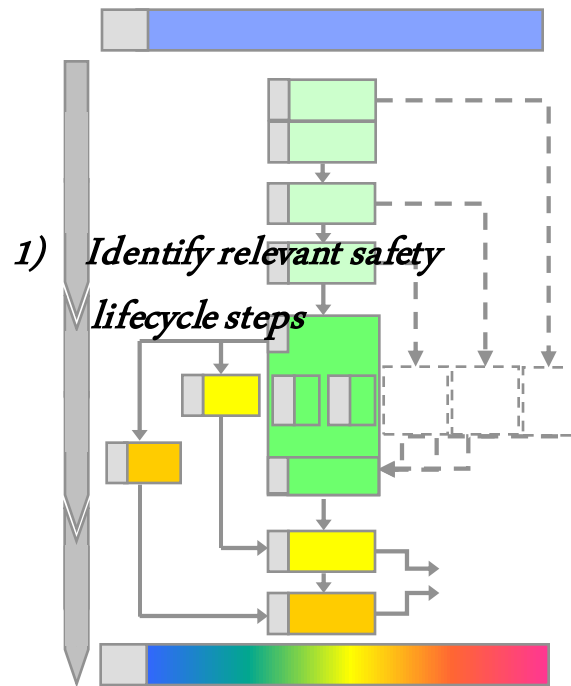
Core processes



Source ISO/DIS 26262

Functional Safety during Concept Phase

For a given Product “Item”:

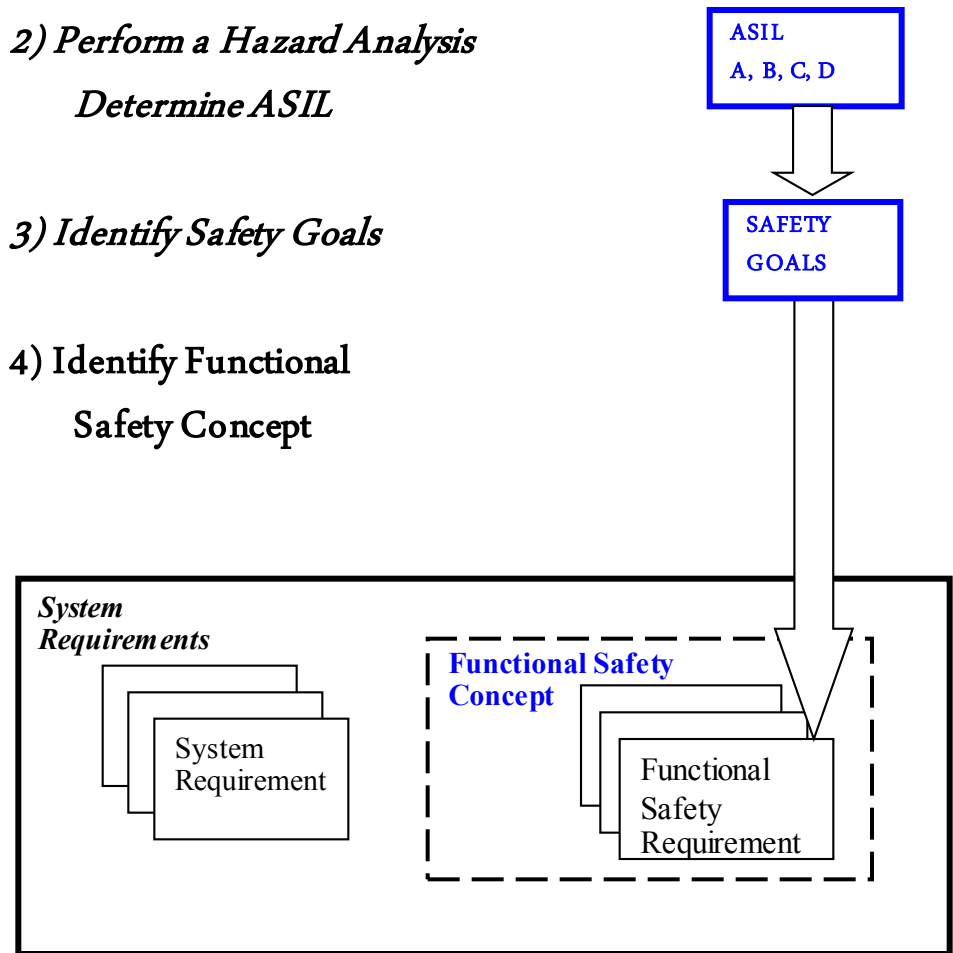


2) *Perform a Hazard Analysis*

Determine ASIL

3) *Identify Safety Goals*

4) *Identify Functional Safety Concept*



Identify relevant safety lifecycle steps

Safety Lifecycle for given item is adapted based on:



“New development”



Consider all safety lifecycle steps relevant



“Modification” of an existing component/system



Tailor safety lifecycle following an impact analysis of the modifications



Impact analysis considers the “proven in use argument” if original component/system was not developed based on ISO 26262



Perform a Hazard Analysis

Determine ASIL

Situation Analysis & Hazard Identification

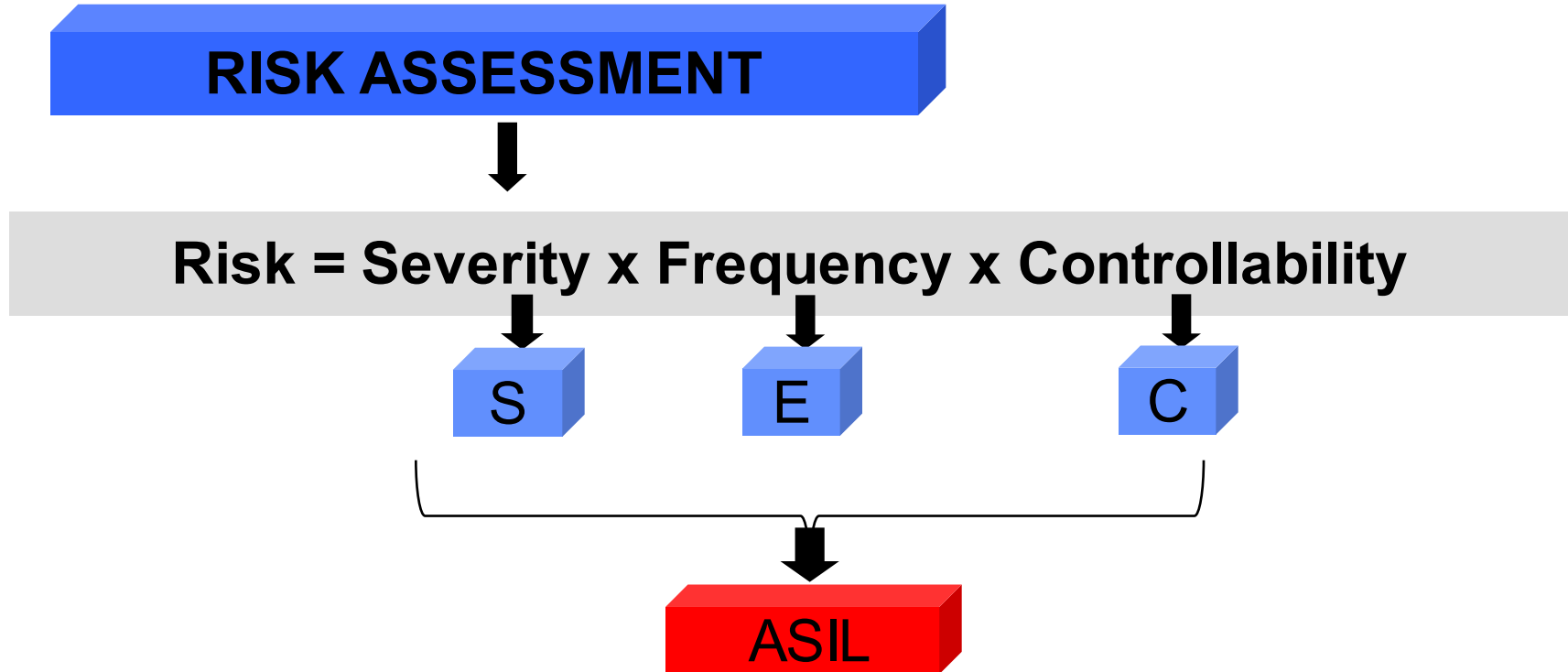
“Identify potential unintended behaviors of the item that could lead to a hazardous event.”

- Vehicle Usage
- Environmental Conditions
- Foreseeable driver use and misuse
- Interaction between vehicle systems



Perform a Hazard Analysis

Determine ASIL



ASIL: Automotive Safety Integrity Level



Perform a Hazard Analysis

Determine ASIL

- For each identified hazardous scenario, evaluate ...

Severity

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

Exposure

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

Controllability

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

Source ISO/DIS 26262



Perform a Hazard Analysis,

Determine ASIL



Use Severity, Exposure, Controllability to set ASIL

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

Source ISO/DIS 26262

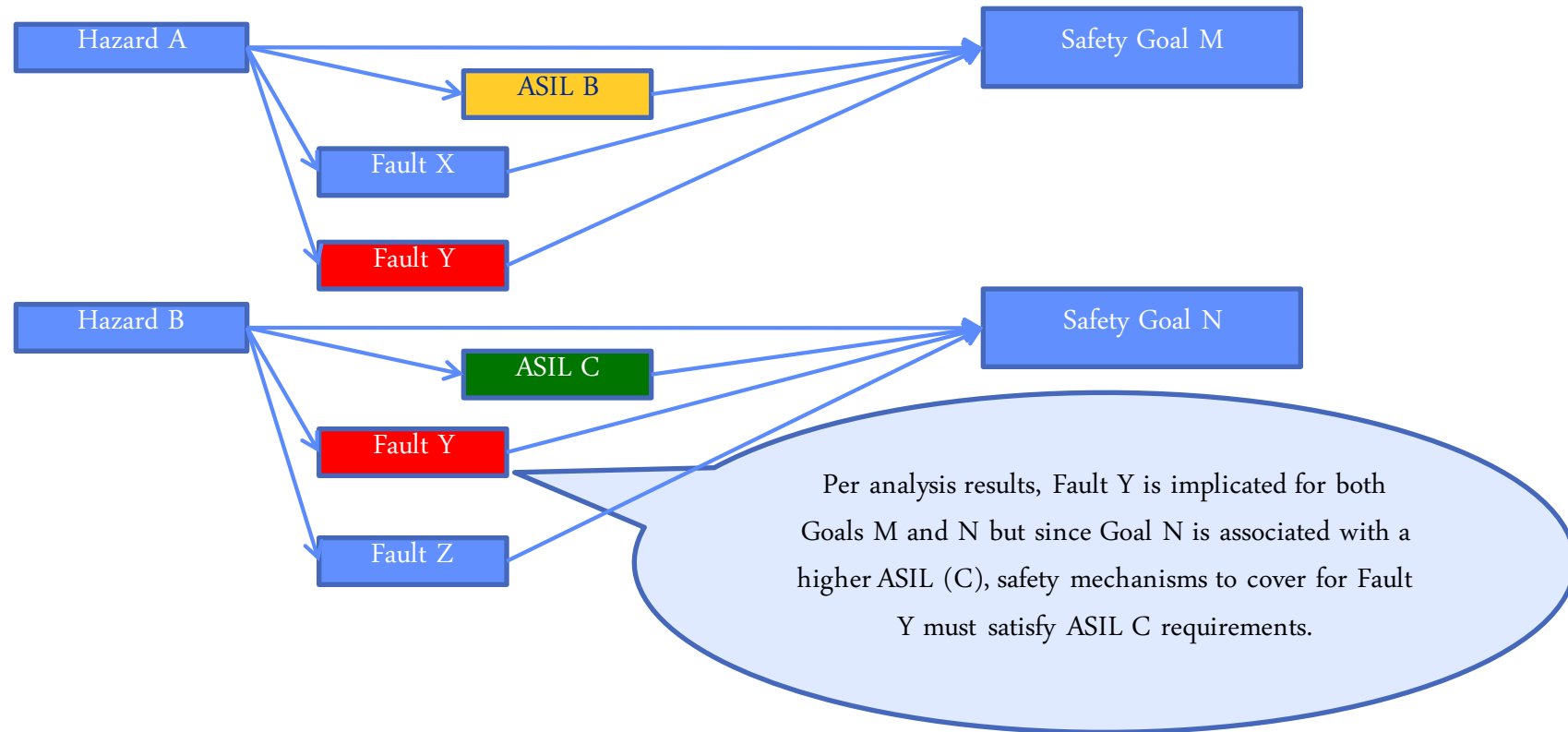


Identify Safety Goals

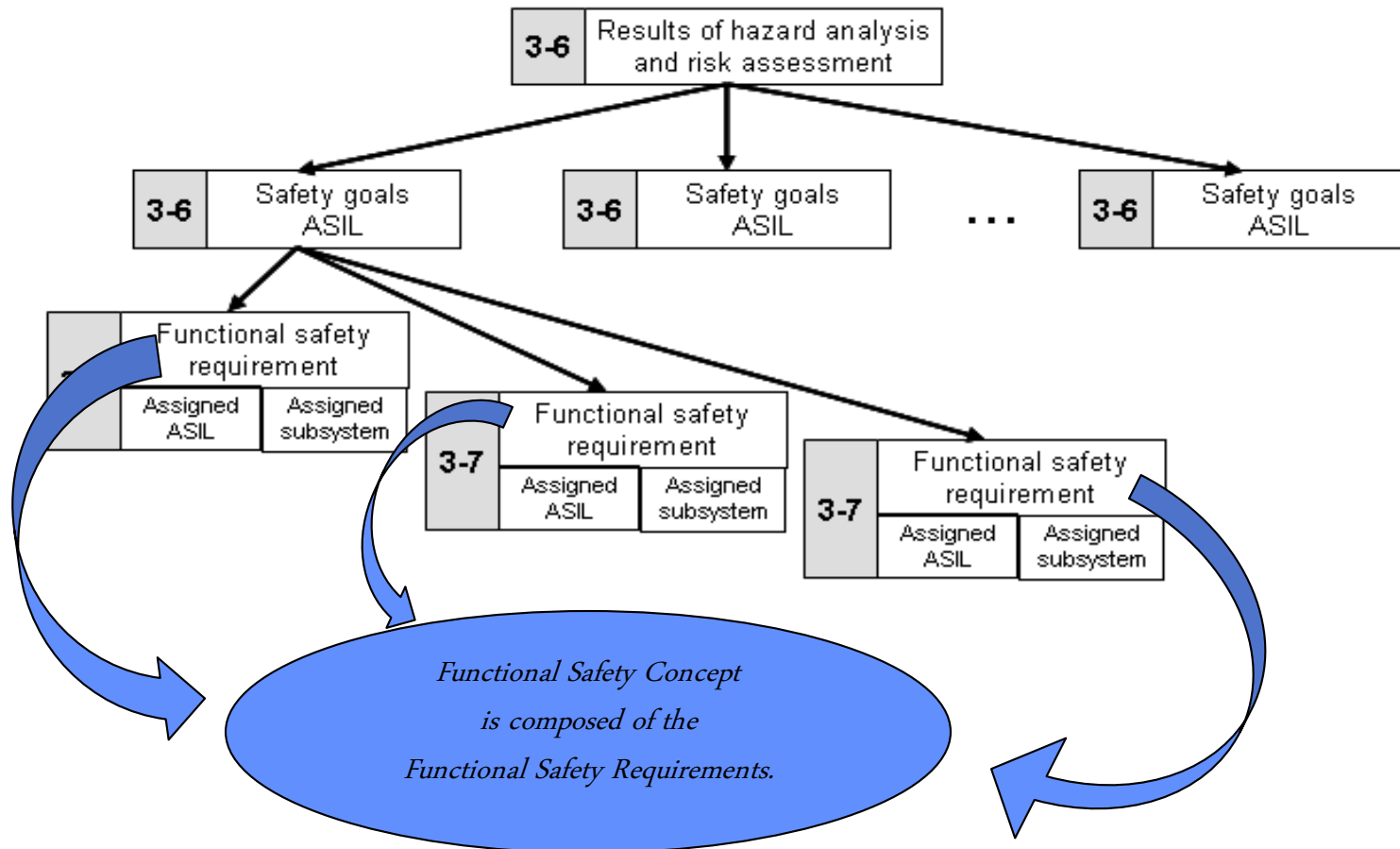
- Safety Goals are top-level safety requirement as a result of the hazard analysis and risk assessment
- A safety goal is to be determined for each hazardous event evaluated in the hazard analysis
- ASIL determined for the hazardous event is to be assigned to the corresponding safety goal.
- Potential hazard may have more than one safety goal
- If similar safety goals are determined, they can be combined into one safety goal that will be assigned the highest ASIL of the similar goals



Identify Safety Goals - Combination



Identify Functional Safety Concept



Source ISO/DIS 26262



Part 3 Work Products

- ☐ Item definition
- ☐ Impact Analysis
- ☐ Hazard analysis and risk assessment
- ☐ Safety goals
- ☐ Review of hazard analysis, risk assessment and the safety goals
- ☐ Functional safety concept
- ☐ Review of the functional safety requirements



Checkpoint Questions - Part 3: Concept Phase

1. What determines the activities needed for a modification of a previous product?
 - A. ASIL
 - B. Item Definition
 - C. Impact Analysis
 - D. Hazard and Risk Analysis
2. What 3 factors determine an ASIL?
 - A. Severity, Occurrence, and Detection.
 - B. Risk, Controllability and Severity.
 - C. Severity, Controllability, and Exposure
3. What are the 4 ASILs
 - A. A, B, C, D
 - B. 1,2,3,4
 - C. Critical, Severe, serious, and moderate



Checkpoint Questions - Part 3: Concept Phase

1. What determines the activities needed for a modification of a previous product?
 - A. ASIL
 - B. Item Definition
 - C. **Impact Analysis**
 - D. Hazard and Risk Analysis
2. What 3 factors determine an ASIL?
 - A. Severity, Occurrence, and Detection.
 - B. Risk, Controllability and Severity.
 - C. Severity, Controllability, and Exposure
3. What are the 4 ASILs
 - A. A, B, C, D
 - B. 1,2,3,4
 - C. Critical, Severe, serious, and moderate



Checkpoint Questions - Part 3: Concept Phase

1. What determines the activities needed for a modification of a previous product?
 - A. ASIL
 - B. Item Definition
 - C. **Impact Analysis**
 - D. Hazard and Risk Analysis
2. What 3 factors determine an ASIL?
 - A. Severity, Occurrence, and Detection.
 - B. Risk, Controllability and Severity.
 - C. **Severity, Controllability, and Exposure**
3. What are the 4 ASILs
 - A. A, B, C, D
 - B. 1,2,3,4
 - C. Critical, Severe, serious, and moderate



Checkpoint Questions - Part 3: Concept Phase

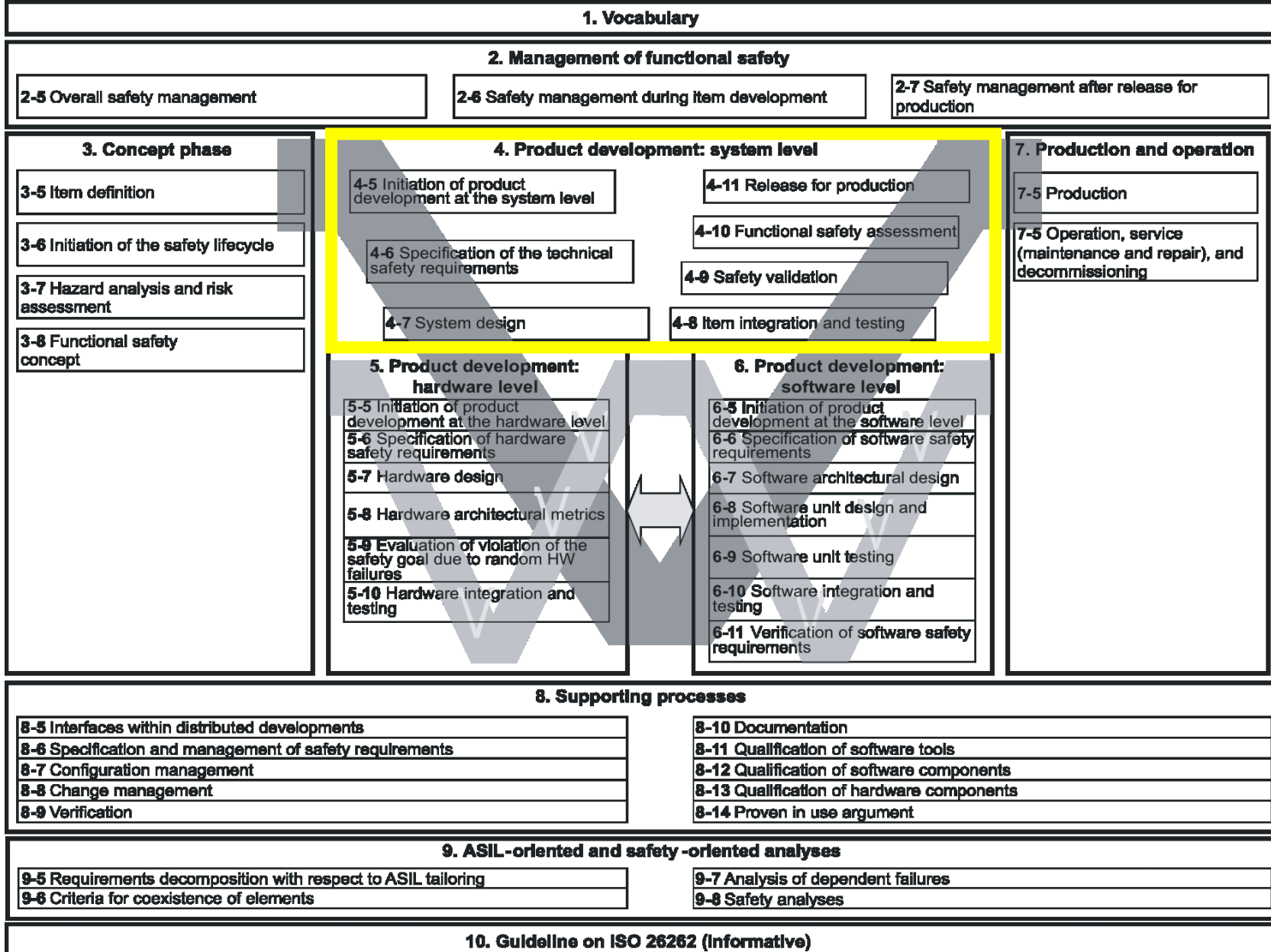
1. What determines the activities needed for a modification of a previous product?
 - A. ASIL
 - B. Item Definition
 - C. **Impact Analysis**
 - D. Hazard and Risk Analysis
2. What 3 factors determine an ASIL?
 - A. Severity, Occurrence, and Detection.
 - B. Risk, Controllability and Severity.
 - C. **Severity, Controllability, and Exposure**
3. What are the 4 ASILs
 - A. **A, B, C, D**
 - B. 1,2,3,4
 - C. Critical, Severe, serious, and moderate



Part 4: Product Development: System Level

Barbara J. Czerny





Core processes



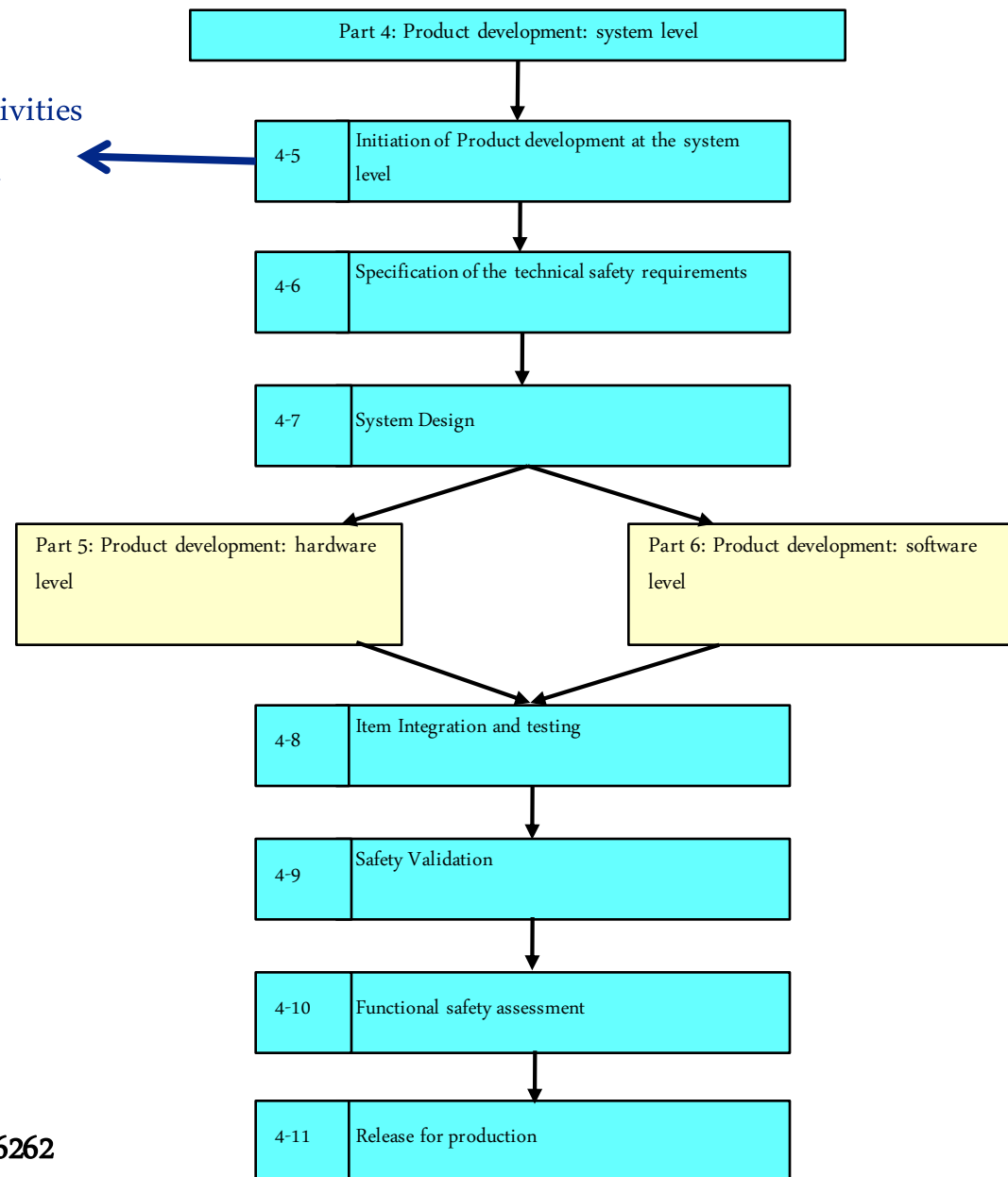
Overview

- Identify and plan the functional safety activities for each sub-phase of system development

- Includes supporting processes activities
- Includes methods to be used
- Tailoring of the lifecycle

Safety Plan

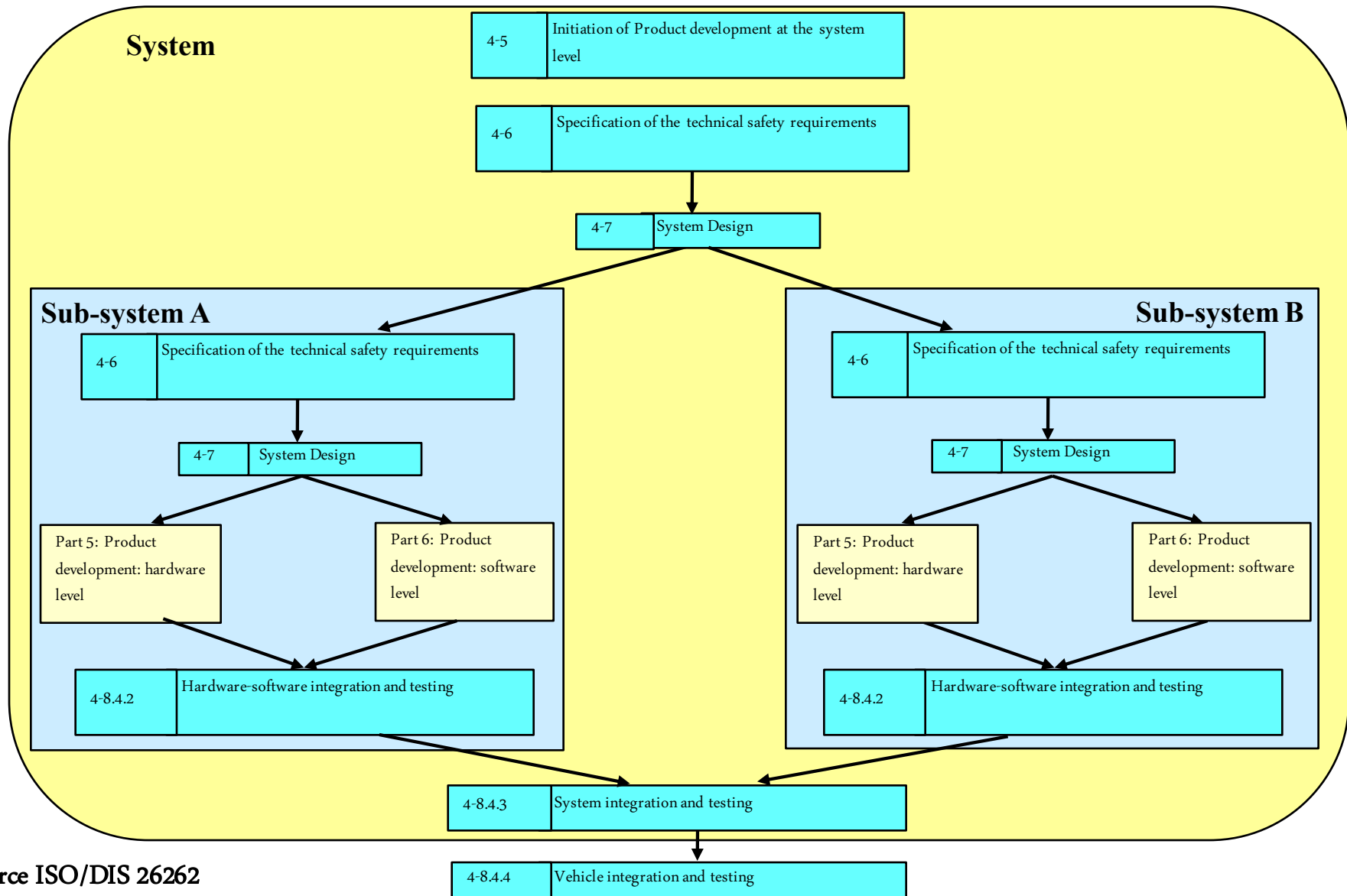
- Applies to both systems and subsystems



Source ISO/DIS 26262



Example Product Development at the System Level



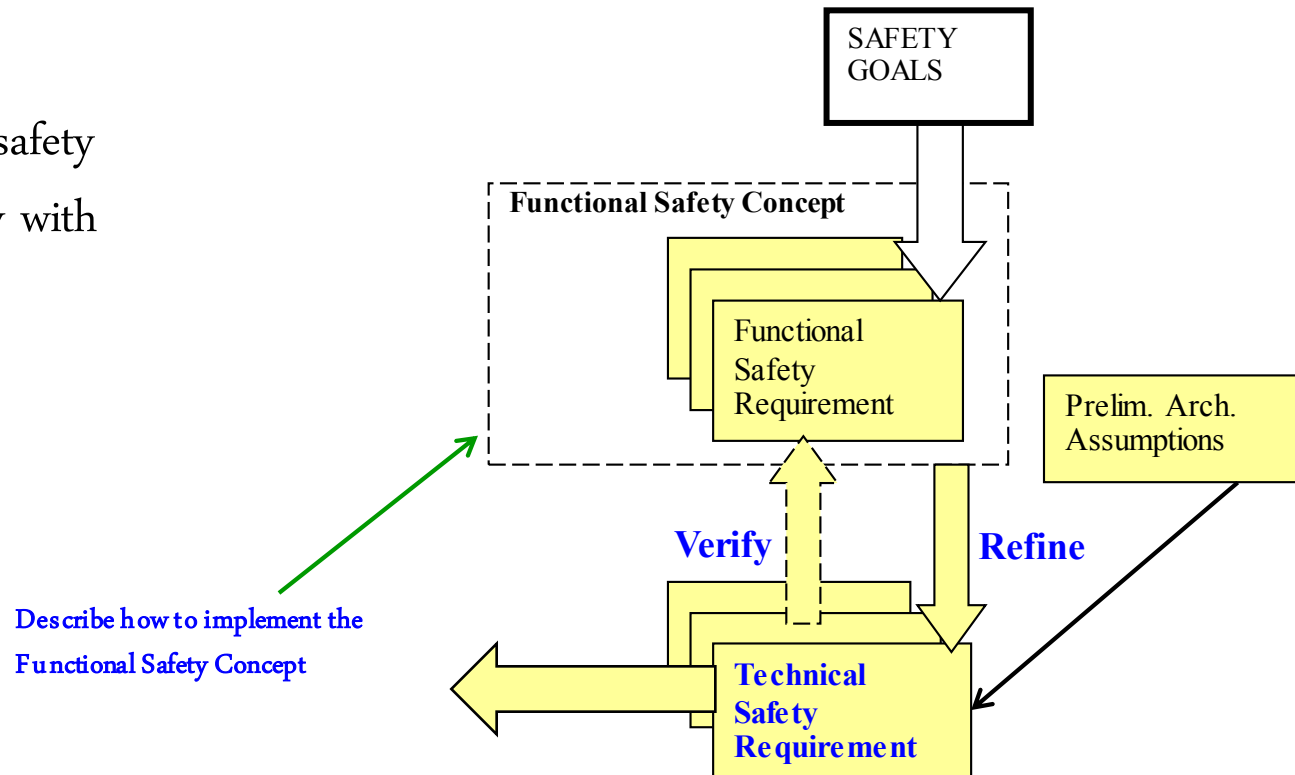
Source ISO/DIS 26262



Specification of the Technical Safety Requirements

➤ Objectives

- Develop the technical safety requirements
 - Refinement of the functional safety requirements considering the preliminary architectural assumptions
- Verify the technical safety requirements comply with the functional safety requirements



Specification of the Technical Safety Requirements Cont'd.

- Specification includes
 - Safety-related functional and safety-related non-functional dependencies
 - Between systems or elements of the item and between the item and other systems
 - System/element response to stimuli
 - Safety mechanisms
 - Related to detection, indication and control of faults, that enable the system to achieve and maintain a safe state, ...
 - Safety-related requirements for production, operation, maintenance and decommissioning
- Define system properties
 - External interfaces, constraints, system configuration requirements
- Specify other functional and non-functional requirements



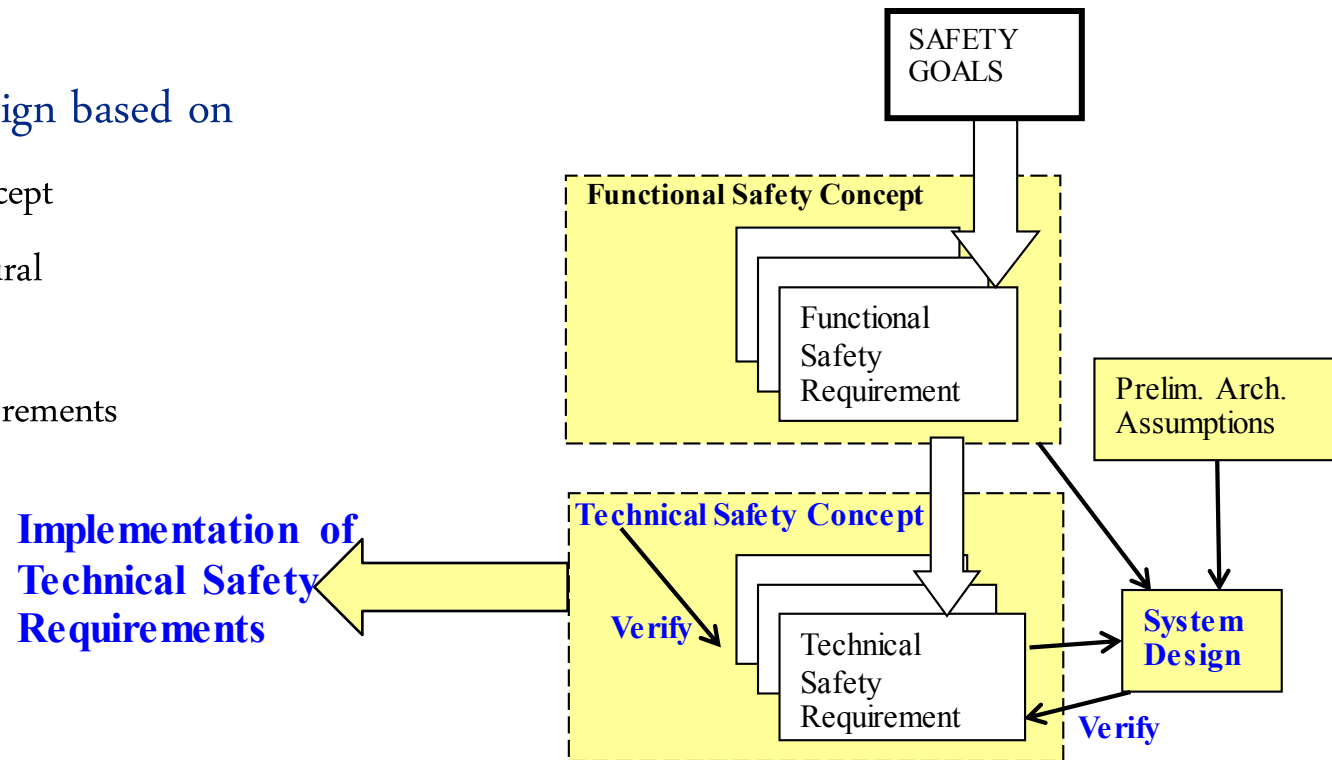
System Design and Technical Safety Concept

➤ Objectives

- Develop the system design and the technical safety concept
- Verify that the system design and technical safety concept comply with the technical safety requirements specification

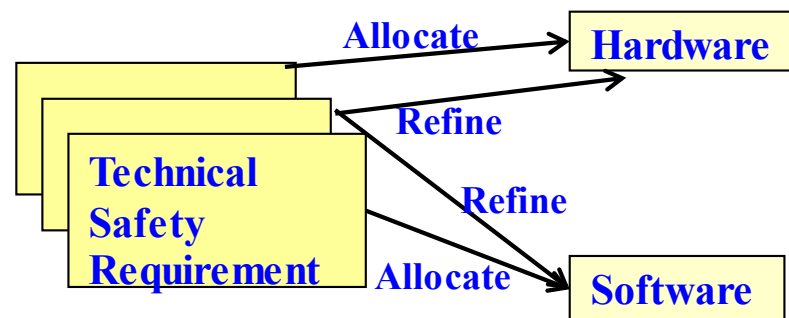
➤ Specify the system design based on

- Functional safety concept
- Preliminary architectural assumptions
- Technical safety requirements specification



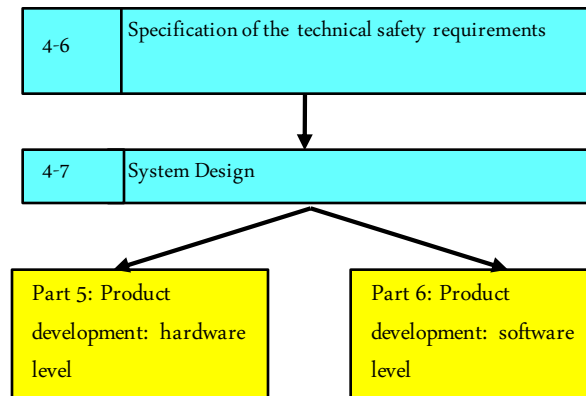
System Design and Technical Safety Concept Cont'd

- Requirements for avoiding systematic failures
 - e.g., deductive and inductive analysis to identify causes and effects of systematic failures, use well-trusted design principles, apply properties to modular design, etc.
- Overall requirements for the control of random hardware failures during operation
 - e.g., specify measures for detection and control, set target values for metrics in part 5 for final evaluation at the item level, etc.
- Allocate each technical safety requirement to hardware, software, or both



System Design and Technical Safety Concept Cont'd.

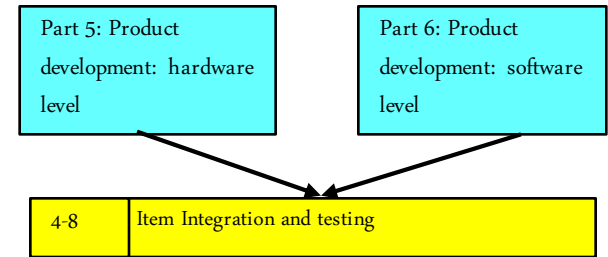
- Specify the hardware –software interface (HSI)
- Specify requirements for production, operation, service, and decommissioning
 - e.g., measures to support field monitoring, specification of diagnostic features to allow fault identification by service personnel, etc.
- Continue development at the hardware and software levels



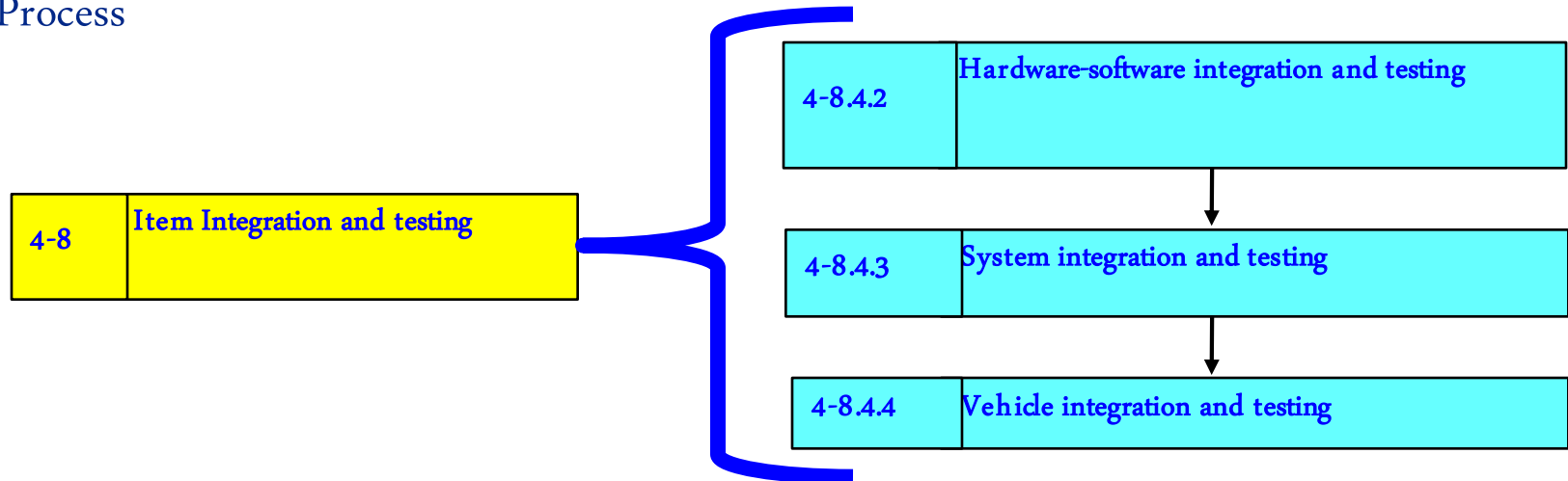
Item Integration and Testing

Objectives

- Integrate the elements of an item
 - If applicable, systems or elements of other technologies and external measures or systems
 - Test the integrated item for compliance with each safety requirement
- Verify that the system design is correctly implemented by the entire item



Process



Safety Validation



Objectives

- Evidence of compliance with the functional safety goals
- Evidence that the safety concepts are appropriate for the functional safety of the item
- Evidence that the safety goals are correct, complete, and fully achieved at the vehicle level



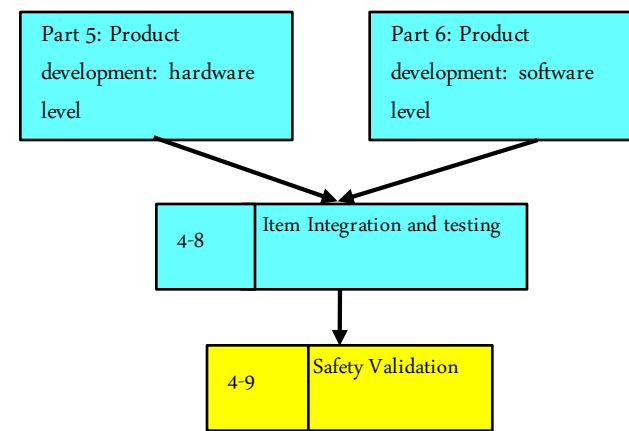
Validation of safety goals is applied to the item integrated at the vehicle level

- Includes: E/E system, software (if applicable), hardware, elements of other technologies, external measures



Validation plan includes

- Validation test procedures for each safety goal with pass/fail criteria
- Scope of the application
 - e.g., configuration, environmental conditions, driving situations, etc.



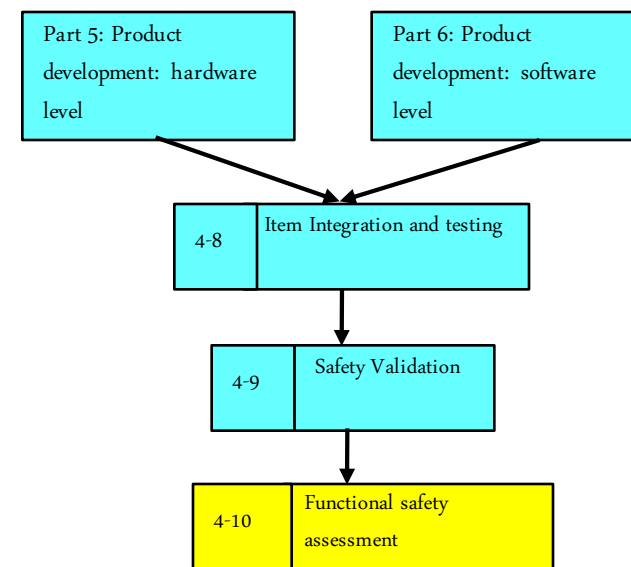
Functional Safety Assessment

➤ Objective

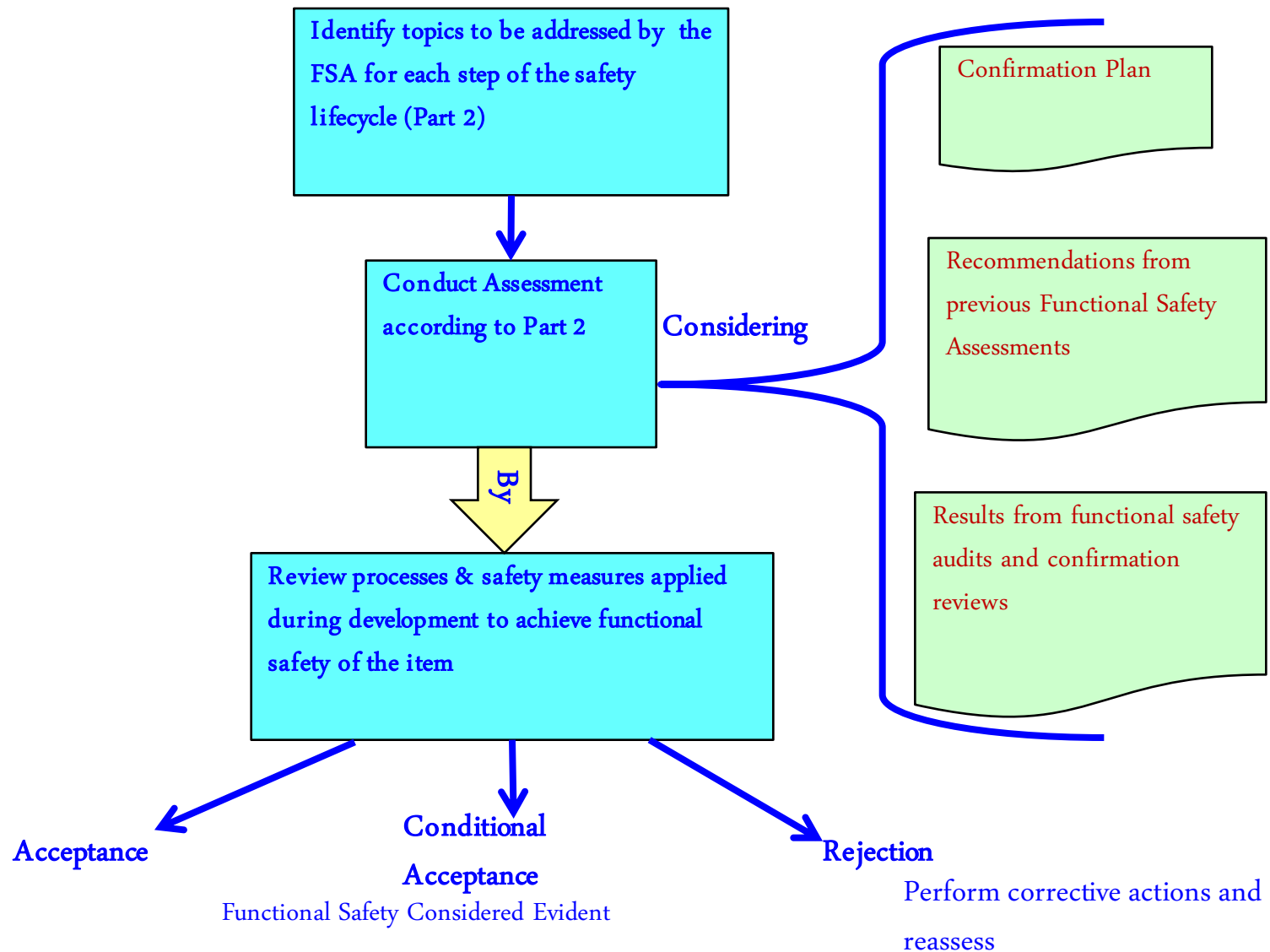
- Assess the functional safety achieved by the item

➤ Initiated by the entity with responsibility for functional safety

- e.g., the vehicle manufacturer



Functional Safety Assessment Cont'd.



Release for Production



Objective

- Specify the criteria for the release for production at the completion of item development



Confirmation that the item complies with the requirements for functional safety at the vehicle level

- Ready for series-production and operation



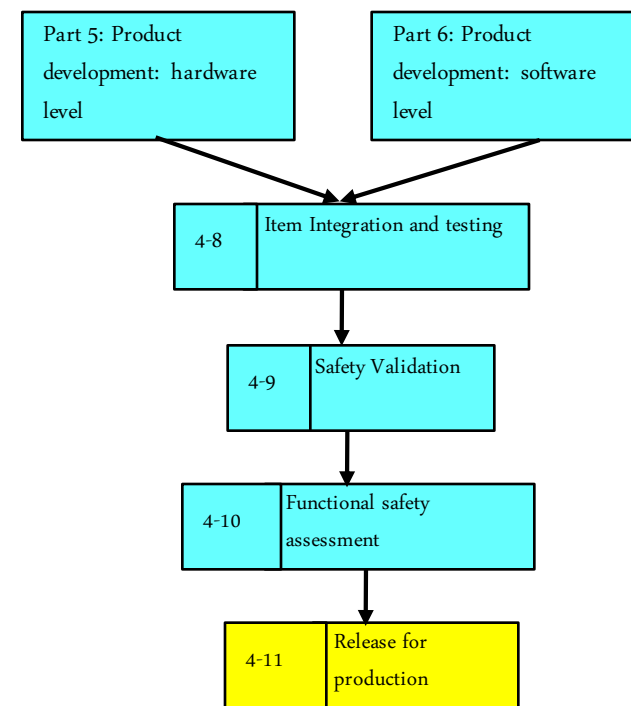
Only approved if the required work products are available and provide confidence of functional safety

- Functional safety assessment report, safety case



Requires appropriate documentation of functional safety for release for production

- Name and signature of person in charge of release, Version of released item, etc.



Part 4 Work Products

- ☐ Overall project plan (refined)
- ☐ Safety plan (refined)
- ☐ Validation plan
- ☐ Functional safety assessment plan
- ☐ Technical safety requirements specification
- ☐ System level verification report
- ☐ Technical safety concept
- ☐ System design specification
- ☐ Item integration and testing plan
- ☐ Requirements for production, operation, service, and decommissioning
- ☐ HW/SW interface specification (HSI)
- ☐ Integration testing specification
- ☐ Integration testing report
- ☐ Validation report
- ☐ Functional safety assessment report
- ☐ Release for production report



1. Where are the safety mechanisms specified and where are they allocated to hardware and software?
 - A. Item Definition and Hazard Analysis and Risk Assessment
 - B. Hazard Analysis and Risk Assessment
 - C. Functional Safety Concept and Functional Safety Requirements
 - D. Technical Safety Requirements and System Design
2. Which of the following is true concerning Safety Validation?
 - A. Item tested as integrated at vehicle level
 - B. Test procedures for each safety goal (pass/fail)
 - C. Within scope of driving situations, environmental conditions, configuration, etc.
 - D. All of the above



1. Where are the safety mechanisms specified and where are they allocated to hardware and software?
 - A. Item Definition and Hazard Analysis and Risk Assessment
 - B. Hazard Analysis and Risk Assessment
 - C. Functional Safety Concept and Functional Safety Requirements
 - D. Technical Safety Requirements and System Design**
2. Which of the following is true concerning Safety Validation?
 - A. Item tested as integrated at vehicle level
 - B. Test procedures for each safety goal (pass/fail)
 - C. Within scope of driving situations, environmental conditions, configuration, etc.
 - D. All of the above



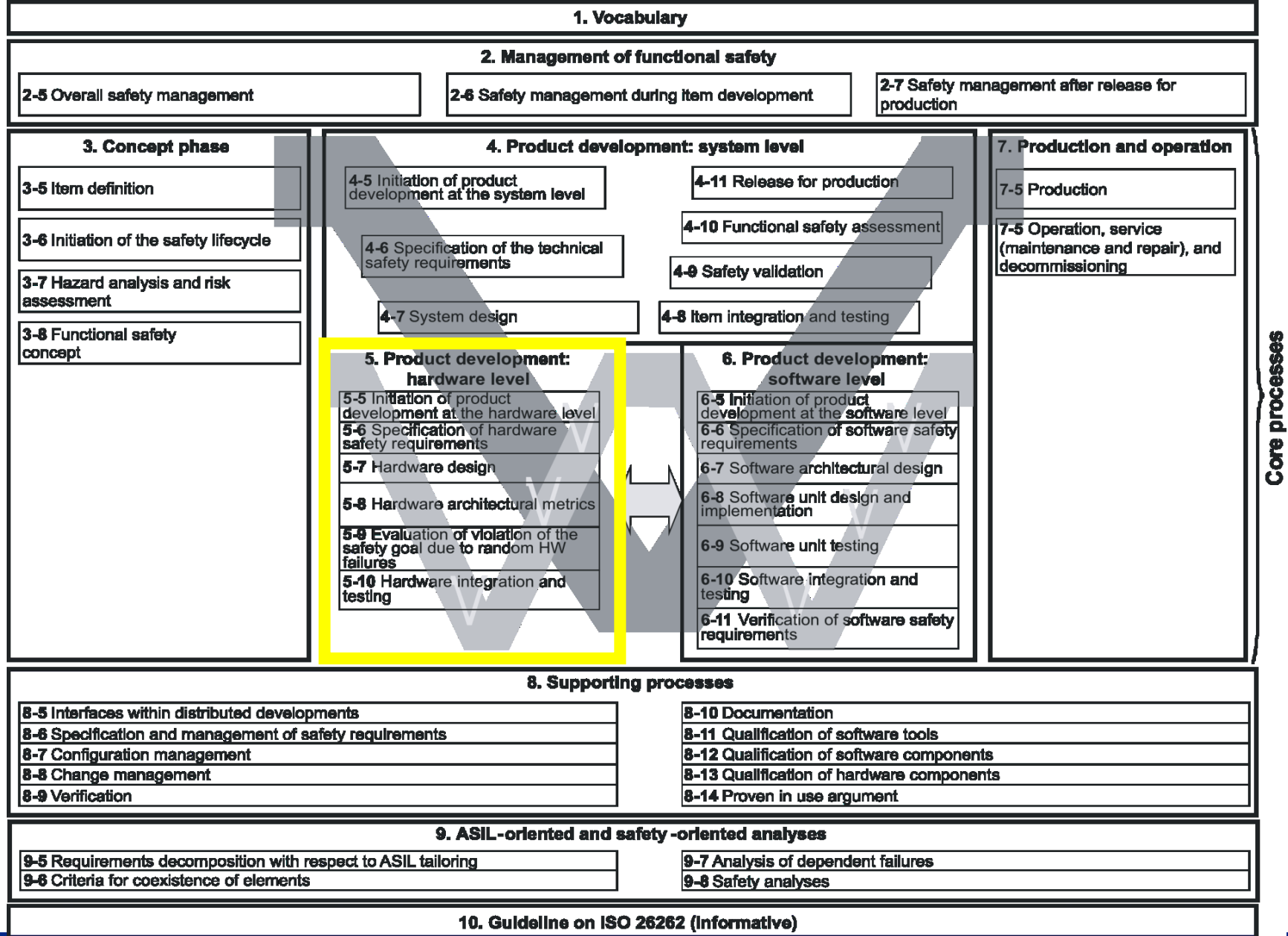
1. Where are the safety mechanisms specified and where are they allocated to hardware and software?
 - A. Item Definition and Hazard Analysis and Risk Assessment
 - B. Hazard Analysis and Risk Assessment
 - C. Functional Safety Concept and Functional Safety Requirements
 - D. Technical Safety Requirements and System Design**
2. Which of the following is true concerning Safety Validation?
 - A. Item tested as integrated at vehicle level
 - B. Test procedures for each safety goal (pass/fail)
 - C. Within scope of driving situations, environmental conditions, configuration, etc.
 - D. All of the above**



Part 5: Product Development: Hardware Level

Rami Debouk

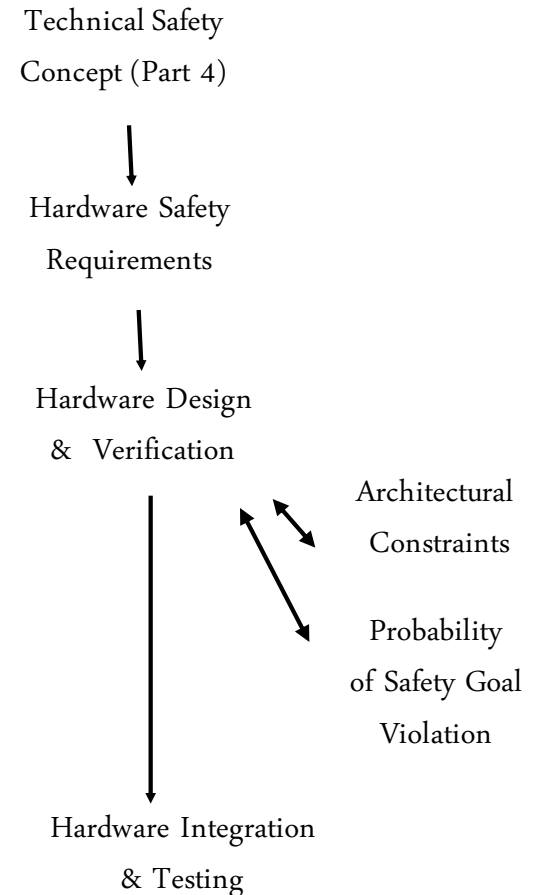




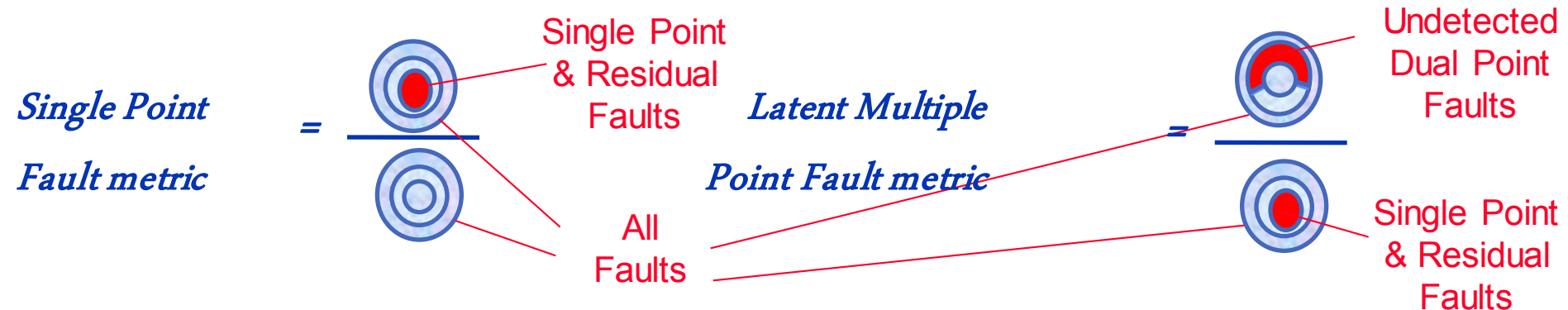
Source ISO/DIS 26262

Overview

- *Identify relevant safety lifecycle steps for item hardware engineering*
- *Identify Hardware safety requirements*
- *Design hardware, protecting for safety concerns*
- *Assess architectural constraints*
- *Evaluate probability of violation of a safety goal*
- *Hardware safety integration and test*



Establish Target Safety Goal Metrics



- Single Point Fault: fault leads directly to the violation of the safety goal
- Residual Fault: portion of a fault, not covered by a safety mechanism, that by itself leads to the violation of a safety goal
- Dual/Multiple Point Fault: combination of two/multiple independent faults that leads directly to the violation of a safety goal
- Latent Fault: multiple point fault whose presence is not detected by a safety mechanism nor perceived by the driver
- Safe Faults: fault whose occurrence will not significantly increase the probability of violation of a safety goal

| ASIL | Single Point Fault Metric | Latent Multiple Point Fault Metric |
|------|---------------------------|------------------------------------|
| B | > 90% | > 60% |
| C | >97% | >80% |
| D | >99% | >90% |



Evaluating violation of Safety Goal target metrics due to random hardware failures

“...to provide criteria to demonstrate that the risk of safety goal violation due to random hardware failures of the item is sufficiently low.”

Method 1: Probabilistic Method for Random Hardware Failure

Quantitative analysis to evaluate probability of violation of safety goal.

- *Latent fault metric targets*
- *Metrics are compared to target goals to demonstrate achievement of safety goal*

Method 2: Residual Risk Assessment Method

Evaluation of residual risks due to random hardware failures of the item, to show that the residual risk is sufficiently low.



Method 1:

Probabilistic Method for Random Hardware Failure

Compute probability of violation of each safety goal due to random hardware failures and then compare it to a target value

Quantitative target values for maximum probability of violation of each safety goal due to random hardware failures are defined from sources such as:

1. Quantitative analysis on similar well-trusted designs, using well known failure rate databases.
2. Derived from field data of similar well-trusted designs
3. Derived from Table G-1

| ASIL Level | Random hardware failure target values |
|------------|---|
| <i>D</i> | <i>$< 10^{-8}$ per hour</i> |
| <i>C</i> | <i>$< 10^{-7}$ per hour</i> |
| <i>B</i> | <i>$< 10^{-7}$ per hour</i> |
| <i>A</i> | <i>$< 10^{-6}$ per hour</i> |

Source ISO/DIS 26262



Method 1:

Probabilistic Method for Random Hardware Failure

Quantitative Analysis considers:

- a) Single point faults, residual faults, dual point faults
- b) Item architecture
- c) Estimated hardware part failure rates (all modes) for single point faults
- d) Estimated hardware part failure rates for dual point faults
- e) Diagnostic coverage (Tables B.1-B.12 may be used)
- f) Exposure duration (in case of multiple point faults)
- g) Remaining dependent faults due to random hardware faults



Method 2 – Residual Risk Evaluation Method

Individually evaluate each single point fault, residual fault and dual point failure of the hardware parts which violate the considered safety goal.

Defines Failure Rate Classes based on random hardware failure targets :

Failure Rate Class 1 $< 10^{-10}$

Failure Rate Class 2 $< 10^{-9}$

Failure Rate Class 3 $< 10^{-8}$



Method 2 – Evaluation Method – Single Point Faults

A single point fault occurring in a hardware part shall be considered as acceptable, if the corresponding hardware part failure rate is:

| ASIL of Safety Goal | Failure Rate Class |
|---------------------|--|
| D | Class 1 (10^{-10}) + dedicated measures to ensure Class 1 |
| C | Class 2 (10^{-9}) + dedicated measures to ensure Class 2 OR Class 1 (10^{-10}) |
| B | Class 2 (10^{-9}) OR Class 1 (10^{-10}) |



Hardware Integration & Testing

- To ensure, by testing, the compliance of the integrated hardware elements with the hardware safety requirements

Table 9 — Hardware integration tests

| Methods | | ASIL | | | |
|---------|--|------|----|----|----|
| | | A | B | C | D |
| 1 | Functional testing under environmental conditions ^a | ++ | ++ | ++ | ++ |
| 2a | Expanded functional testing ^b | 0 | + | + | ++ |
| 2b | Statistical testing ^c | 0 | 0 | + | ++ |
| 2c | Worst case testing ^d | 0 | 0 | 0 | + |
| 2d | Over limit testing ^e | + | + | + | + |
| 3a | Mechanical testing | ++ | ++ | ++ | ++ |
| 3b | Environmental testing ^f | ++ | ++ | ++ | ++ |
| 3c | Accelerated life test ^g | + | + | ++ | ++ |
| 3d | Mechanical Endurance test ^h | ++ | ++ | ++ | ++ |
| 4 | EMI test ⁱ | ++ | ++ | ++ | ++ |
| 5 | Chemical testing ^j | ++ | ++ | ++ | ++ |

Source ISO/DIS 26262



Part 5 Work Products

- ☐ Overall project plan (refined)
- ☐ Safety plan (refined)
- ☐ Hardware safety requirements specification (including test and qualification criteria)
- ☐ Hardware architectural metrics requirements
- ☐ Random hardware failure requirements
- ☐ Hardware-software interface specification (refined)
- ☐ Hardware safety requirements verification report
- ☐ Hardware design specification
- ☐ Hardware safety analysis report
- ☐ Hardware design verification report
- ☐ Requirements for production and operation
- ☐ Assessment of the effectiveness of the system architecture to cope with the hardware random failures
- ☐ Review report of assessment of the effectiveness of the system architecture to cope with the hardware random failures
- ☐ Evaluation of random hardware failures
- ☐ Specification of dedicated measures
- ☐ Review report of evaluation of violation of the safety goal due to random HW failures
- ☐ Hardware integration and verification report



Checkpoint Questions - Part 5: Product Development Hardware Level

1. What is the Single Point Fault Metric requirement for ASIL D?
 - A. >99%
 - B. >97%
 - C. >90%
 - D. None of the above

2. What is the Latent Fault Metric requirement for ASIL C?
 - A. >90%
 - B. >80%
 - C. >60%
 - D. None of the above



Checkpoint Questions - Part 5: Product Development Hardware Level

1. What is the Single Point Fault Metric requirement for ASIL D?
A. >99%
B. >97%
C. >90%
D. None of the above

2. What is the Latent Fault Metric requirement for ASIL D?
A. >90%
B. >80%
C. >60%
D. None of the above



Checkpoint Questions - Part 5: Product Development Hardware Level

1. What is the Single Point Fault Metric requirement for ASIL D?
 - A. >99%
 - B. >97%
 - C. >90%
 - D. None of the above

2. What is the Latent Fault Metric requirement for ASIL D?
 - A. >90%
 - B. >80%
 - C. >60%
 - D. None of the above



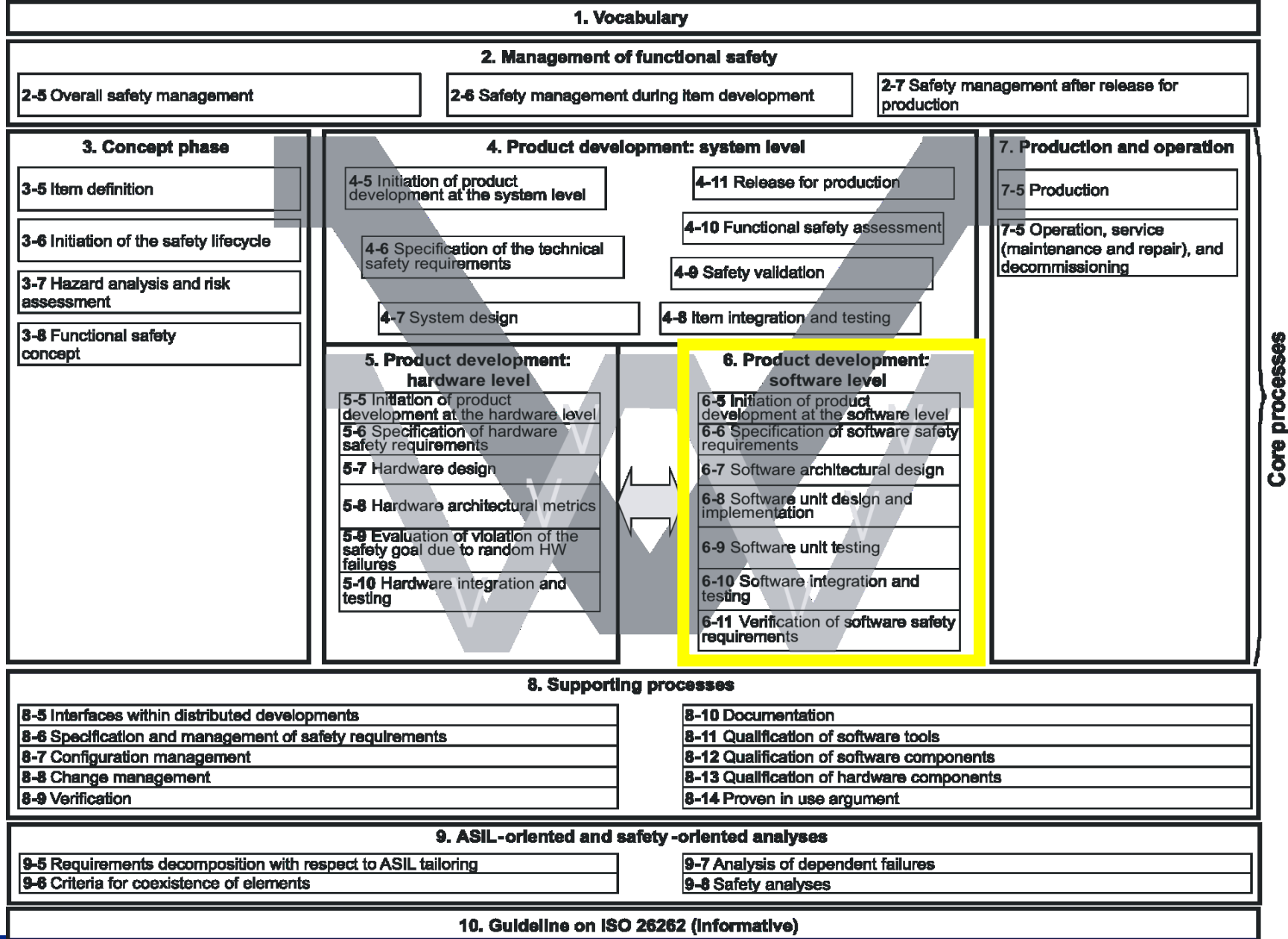
Break



Part 6: Product Development: Software Level

Barbara J. Czerny





Source ISO/DIS 26262

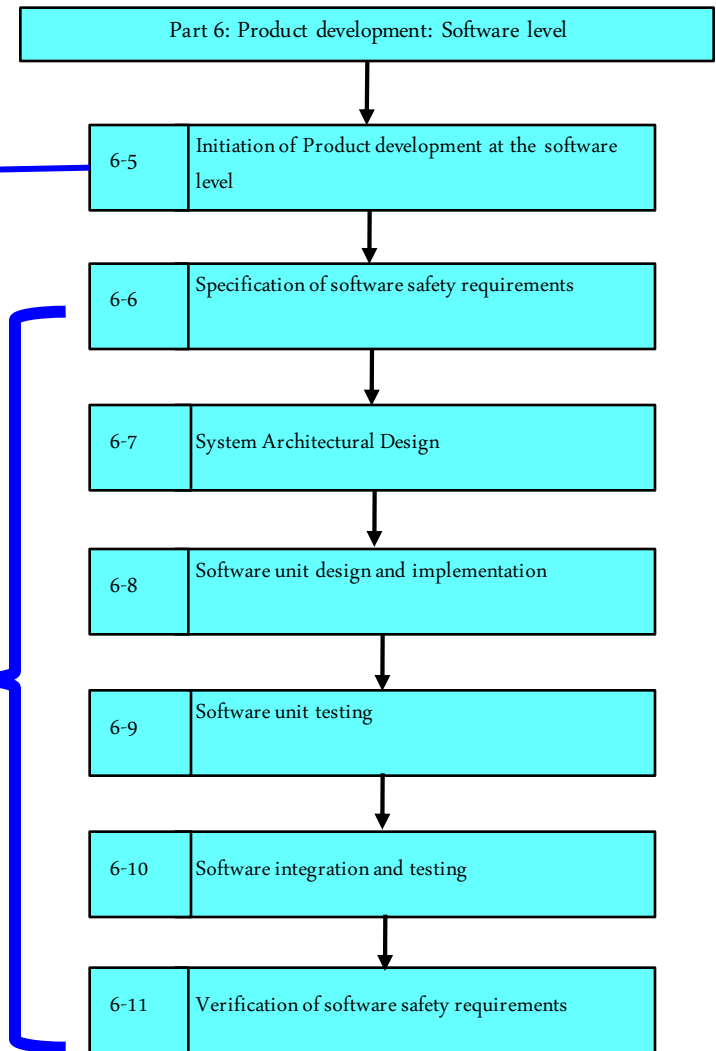
Part 6 Overview

➤ Planning

- Software development activities wrt functional safety
- Supporting processes
- Methods to achieve requirements of assigned ASIL
- Guidelines and tools
- Coordination with product development at hardware level

➤ Lists requirements to be satisfied for each phase of the software development lifecycle

- Dependent on ASIL



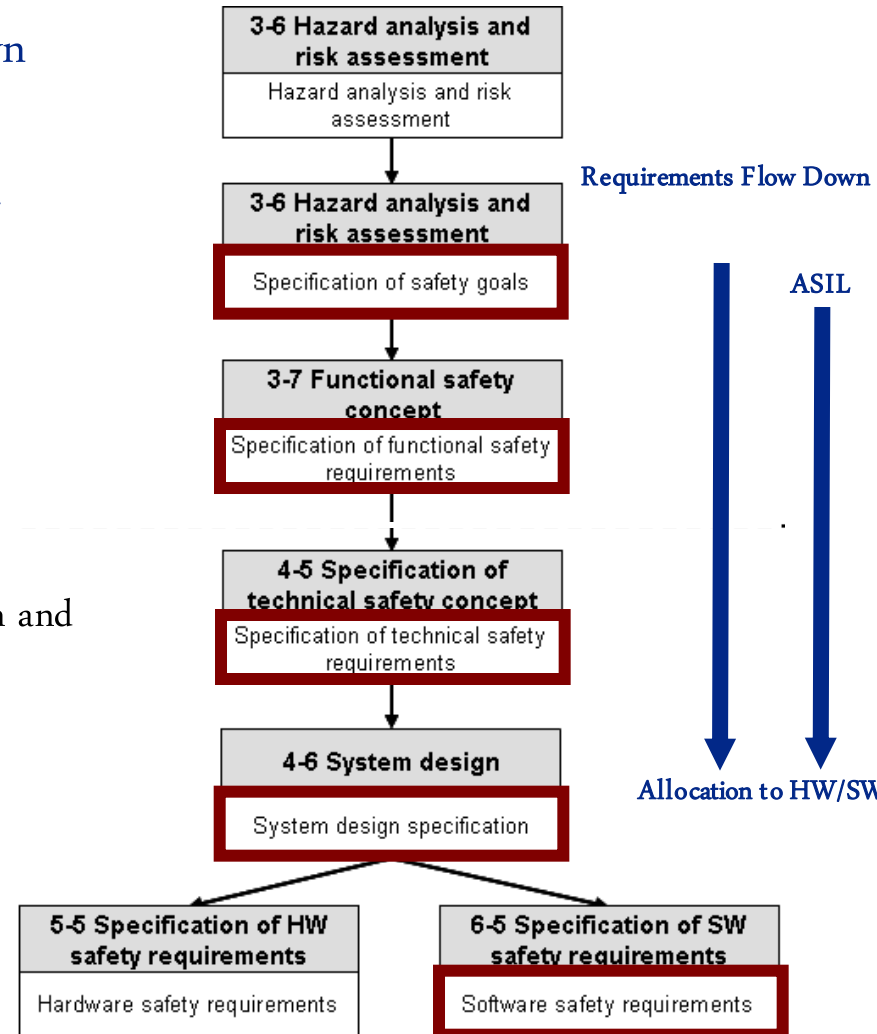
Source ISO/DIS 26262



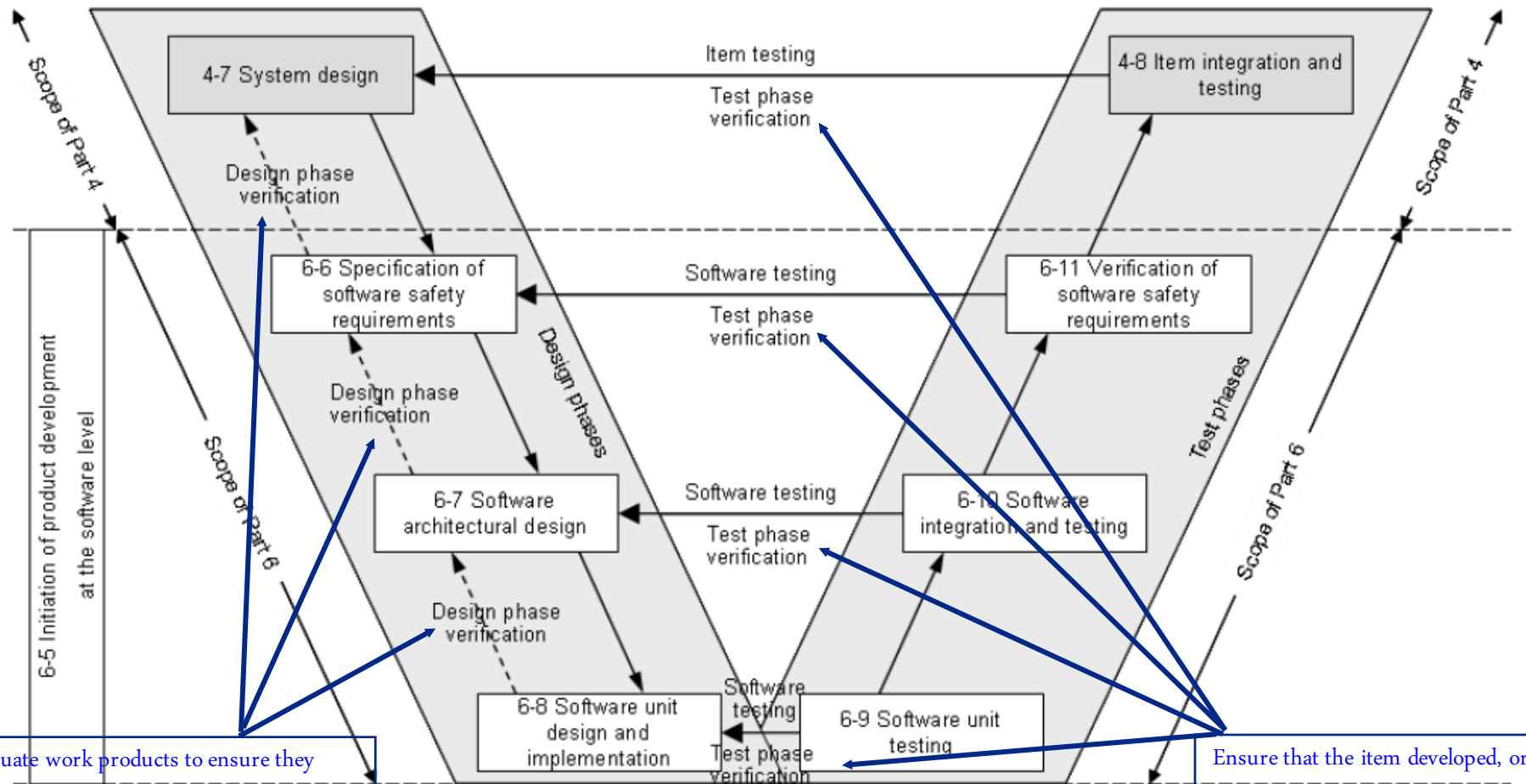
Part 6 Overview Cont'd.

- ASIL of software safety requirements flows down
- Requires qualification of software tools used for software development (Part 8 Clause 11)
- Identifies criteria to be addressed in design and coding guidelines
 - e.g., use of language subsets, support for abstraction and modularity, strong typing, ...

Source ISO/DIS 26262



Tailoring of the lifecycle at the software level based on:



Reference Phase Model for the Software Development

Source ISO/DIS 26262



Specification of Software Safety Requirements

➤ Objectives

- Specify the SW safety requirements from the technical safety requirements (including their ASIL) and the system design specification
- Detail the hardware-software interface requirements
- Verify that the SW safety requirements are consistent with the technical safety requirements and the system design specification

System Design

6-5 Spec. of SW Safety Reqs.

Compliant with technical safety requirements and system design, and consistent with relevant hardware safety requirements

6-6 Spec. of SW Safety Reqs.

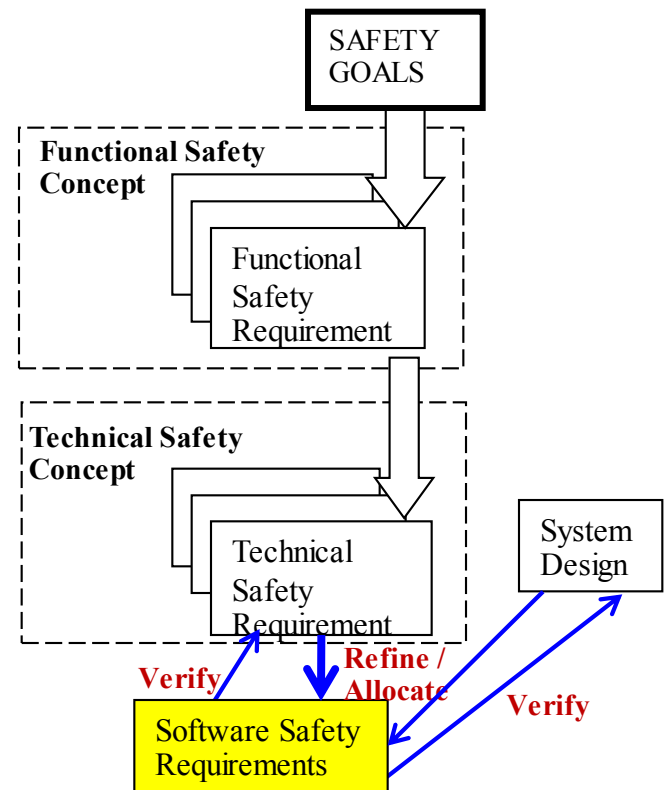
6-7 SW Arch. Design

6-8 SW Unit Des. & Imp.

6-11 Verif. of SW Safety Reqs

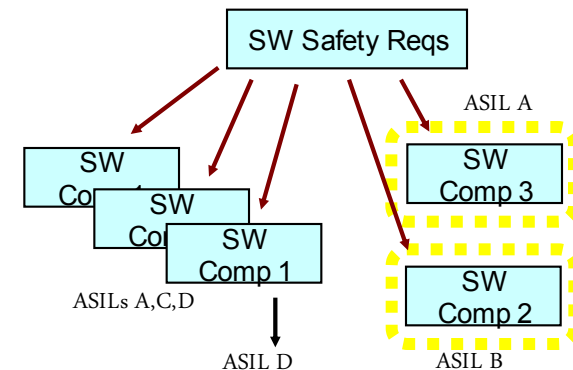
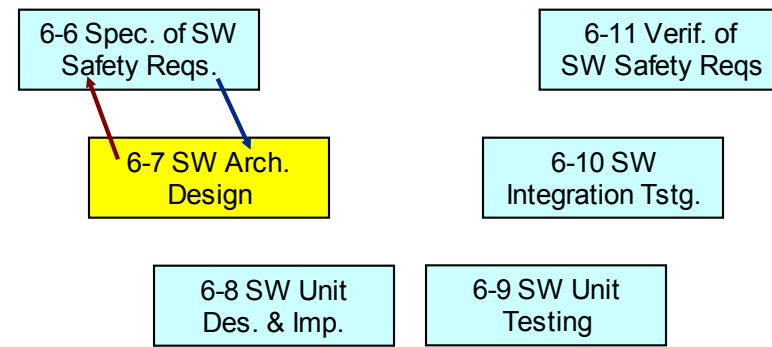
6-10 SW Integration Tstg.

6-9 SW Unit Testing



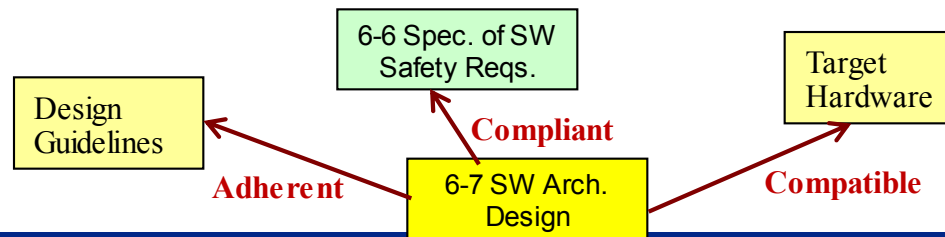
Software Architectural Design

- Objectives
 - Develop a SW architectural design that
 - Realizes the software safety requirements
 - Verify the SW architectural design
- Gives requirements for notations for SW architectural design
 - Goal – appropriate levels of abstraction
- Includes design principles to apply to achieve modularity, encapsulation, minimum complexity
 - e.g., hierarchical structure, restricted size of SW components/interfaces ...
- Allocates SW safety requirements to the SW components
 - SW components of different ASILs
 - Treat as belonging to the highest ASIL
 - Exception: adequate freedom from interference between SW components



Software Architectural Design Cont'd.

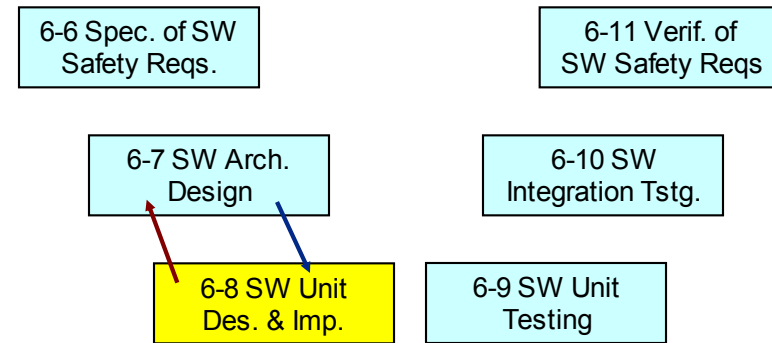
- Safety analysis (Part 9-8) applied to the software architecture to
 - Help identify and confirm safety-related characteristics
 - Support specification of the safety mechanisms
- Requirements for addressing error detection
 - e.g., plausibility checks, detection of data errors, control flow monitoring, ...
- Requirements for addressing error handling
 - e.g., static recovery mechanisms, graceful degradation, correcting codes for data, ...
- Specifies verification requirements
 - Includes control flow analysis, data flow analysis, inspections, etc.



Software Unit Design and Implementation

➤ Objectives

- Specify the software units in accordance with the software architectural design and the associated software safety requirements
- Implement the software units as specified
- Verify the design of the software units and their implementation

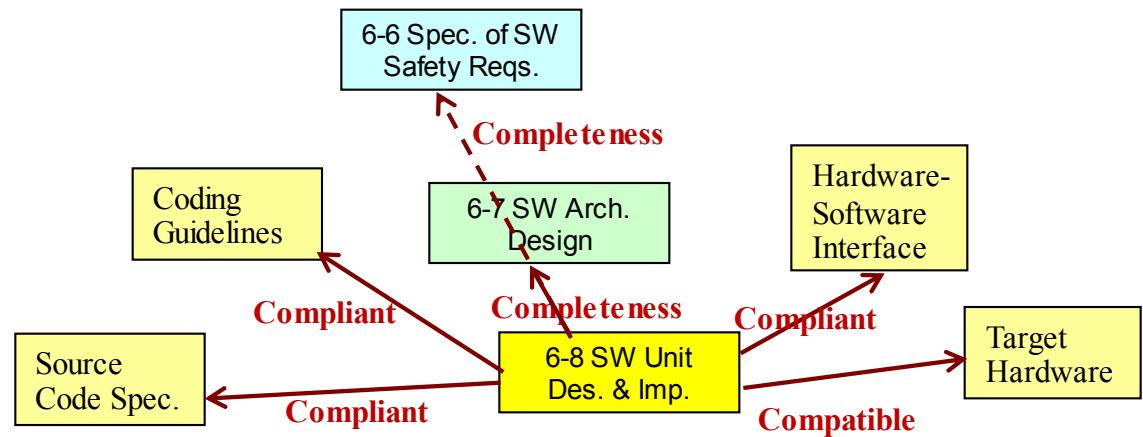


➤ Notation requirements based on ASIL

- To allow subsequent development activities to be performed correctly and effectively
- Specifies design principles to apply to achieve robustness, testability, simplicity, ...
 - e.g., one entry and one exit point in subprograms and functions, limited use of pointers, ...



- Specifies verification requirements
 - Control flow analysis, data flow analysis, static code analysis, walkthrough's, inspections, ...



Software Unit Testing

➤ Objective

- Demonstrate that the software units satisfy their specification and do not contain undesired functionality

➤ Addresses

- SW unit test planning
- Selection of test methods
 - Interface test, resource usage test, ...
- Methods for deriving test cases to demonstrate appropriate specification of test cases
 - Analysis of requirements, boundary value analysis, ...
- Test environment requirements
 - As close as possible to the target environment
- Evaluation criteria
 - Compliance with expected results, & pass or fail criteria

➤ Demonstrates

- Compliance with the SW unit design specification and the HW/SW interface
- Correct implementation of the functionality
- Absence of unintended functionality
- robustness

6-6 Spec. of SW
Safety Reqs.

6-11 Verif. of
SW Safety Reqs

6-7 SW Arch.
Design

6-10 SW
Integration Tstg.

6-8 SW Unit
Des. & Imp.

6-9 SW Unit
Testing

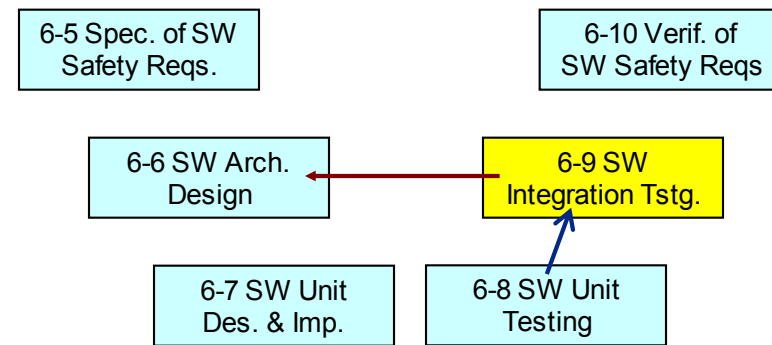


➤ Objectives

- Integrate the software components
- Demonstrate that the software architectural design is correctly realized by the embedded software

➤ Addresses

- Planning
- Selection of test methods to demonstrate that the SW components and embedded SW achieve
 - Compliance with the architectural design and the HW/SW interface
 - Correct implementation of the functionality
 - Robustness
 - Sufficiency of the resources to support the functionality
 - Example test methods - Fault injection, resource usage tests, ...
- Methods for deriving test cases
 - Analysis of requirements, boundary value analysis, ...
- Requirements on the test environment



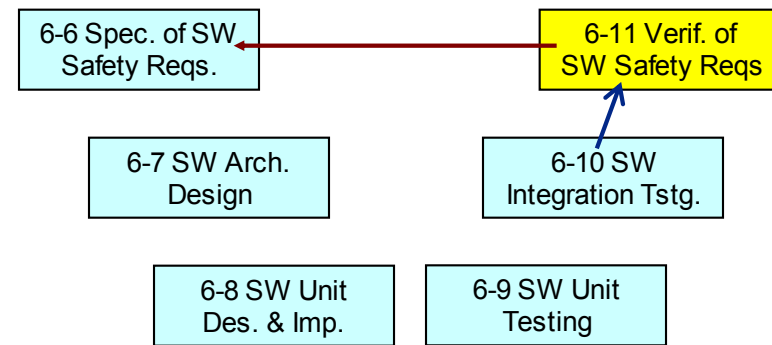
Verification of Software Safety Requirements

➤ Objective

- Demonstrate that the embedded software fulfills the software safety requirements in the target environment

➤ Addresses

- Planning
- Selection of test environments
 - Hardware-in-the-loop, vehicles, ...
- Execution on the target hardware
- Evaluation criteria
 - Compliance with expected results, coverage of the software safety requirements, pass/fail criteria



Part 6 Work Products

- ☐ Safety plan (refined)
- ☐ Software verification plan
- ☐ Design and coding guidelines for modelling and programming languages
- ☐ Software tool application guidelines
- ☐ Software safety requirements specification
- ☐ Hardware-software interface specification (refined)
- ☐ Software verification plan (refined)
- ☐ Software verification report
- ☐ Software architectural design specification
- ☐ Safety analysis report
- ☐ Dependent failures analysis report
- ☐ Software unit design specification
- ☐ Software unit implementation
- ☐ Software verification specification (refined)
- ☐ Embedded software



Checkpoint Questions - Part 6: Product Development Software Level

1. Do software requirements inherit an ASIL?
 - A. Yes
 - B. No
2. Do Software components always inherit the highest ASIL?
 - A. Yes
 - B. No
3. Where is the verification of software safety requirements executed?
 - A. On the target system
 - B. In the system model
 - C. In the software to software integration phase
 - D. None of the above



Checkpoint Questions - Part 6: Product Development Software Level

1. Do software requirements inherit an ASIL?
A. Yes
B. No
2. Do Software components always inherit the highest ASIL?
A. Yes
B. No
3. Where is the verification of software safety requirements executed?
A. On the target system
B. In the system model
C. In the software to software integration phase
D. None of the above



Checkpoint Questions - Part 6: Product Development Software Level

1. Do software requirements inherit an ASIL?
A. Yes
B. No
2. Do Software components always inherit the highest ASIL?
A. Yes
B. No
3. Where is the verification of software safety requirements executed?
A. On the target system
B. In the system model
C. In the software to software integration phase
D. None of the above



Checkpoint Questions - Part 6: Product Development Software Level

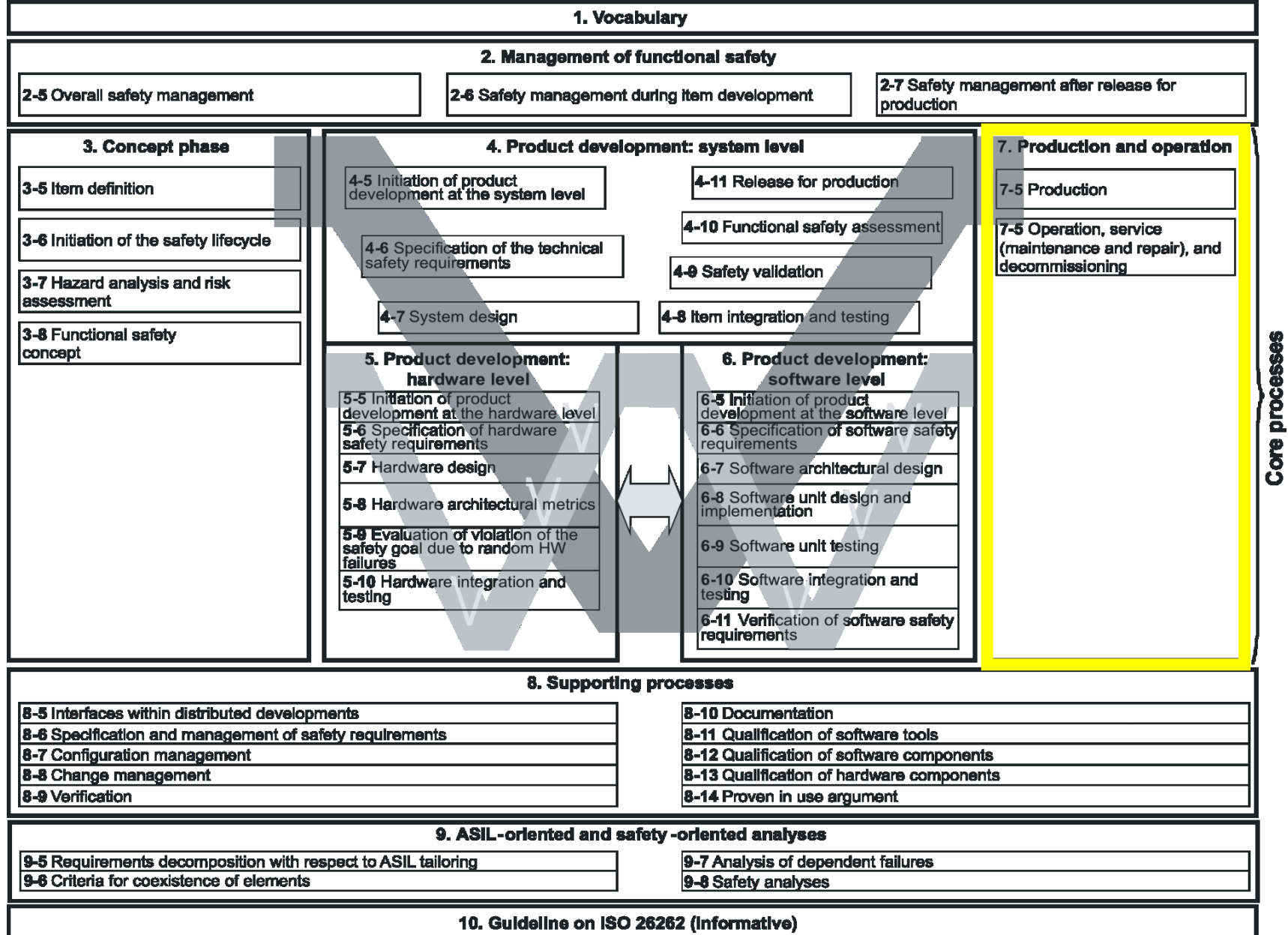
1. Do software requirements inherit an ASIL?
A. Yes
B. No
2. Do Software components always inherit the highest ASIL?
A. Yes
B. No
3. Where is the verification of software safety requirements executed?
A. On the target system
B. In the system model
C. In the software to software integration phase
D. None of the above



Part 7: Production and Operation

Barbara J. Czerny





Core processes

Source ISO/DIS 26262



Production and Operation

- Specifies requirements on production, operation, service, and decommissioning
- Production objectives
 - Develop a production plan for safety-related products
 - Ensure that the required functional safety is achieved during the production process
- Planning
 - Includes planning for safety-related special characteristics
 - e.g., temp. range for specific processes, material characteristics, configuration ...
 - Considers requirements for production, conditions for storage, transport, and handling of hardware elements, approved configurations, ...
 - Describes, as applicable production process flow and instructions, production tools and means, ...
- Requirements for production
 - Implementation of the planned production process, Analysis of process failures and monitoring of corrective measures, ...



Production and Operation Cont'd.

- Operation, service (maintenance and repair), and decommissioning objectives
 - Define the scope of customer information, and maintenance and repair instructions regarding the safety-related products in order to maintain the required functional safety during operation of the vehicle
 - Provide the requirements concerning activities addressing safety issues before disassembly

- Planning
 - Considers requirements for operation, the warning and degradation concept, measures for field data collection and analysis, ...
 - Maintenance plan describes methods required for maintenance including steps, intervals, means of maintenance, and tools

- User manual requirements
 - Relevant functions and operating modes, how to use them in the intended way, required maintenance activities, warnings regarding known hazards resulting from interactions with third party products, ...



Production and Operation Cont'd.

➤ Operation

- Field monitoring process for functional safety events related to the item needs to be implemented as planned

➤ Requirements for decommissioning activities need to be developed

- Measures to be taken before disassembling the vehicle
 - Emphasis on deactivating the systems or elements that would lead to violation of a safety goal if activated during disassembly or decommissioning



Part 7 Work Products

- ☐ Production plan (refined)
- ☐ Production Control plan (refined)
- ☐ Documentation of performed control measures
- ☐ If applicable, requirements on producibility at system, hardware or software development level
- ☐ Assessment report for capability of the production process
- ☐ Maintenance plan (refined)
- ☐ Repair instructions
- ☐ User manual
- ☐ Instructions regarding field observations
- ☐ Instructions for decommissioning
- ☐ If applicable, requirements concerning operation, maintenance and decommissioning at system, hardware or software development level



Checkpoint Questions –

Part 7: Production and Operation

1. What requirements are specified in the clause on Production and Operation?
 - A. Production
 - B. Operation
 - C. Service and decommissioning
 - D. All of the above



Checkpoint Questions –

Part 7: Production and Operation

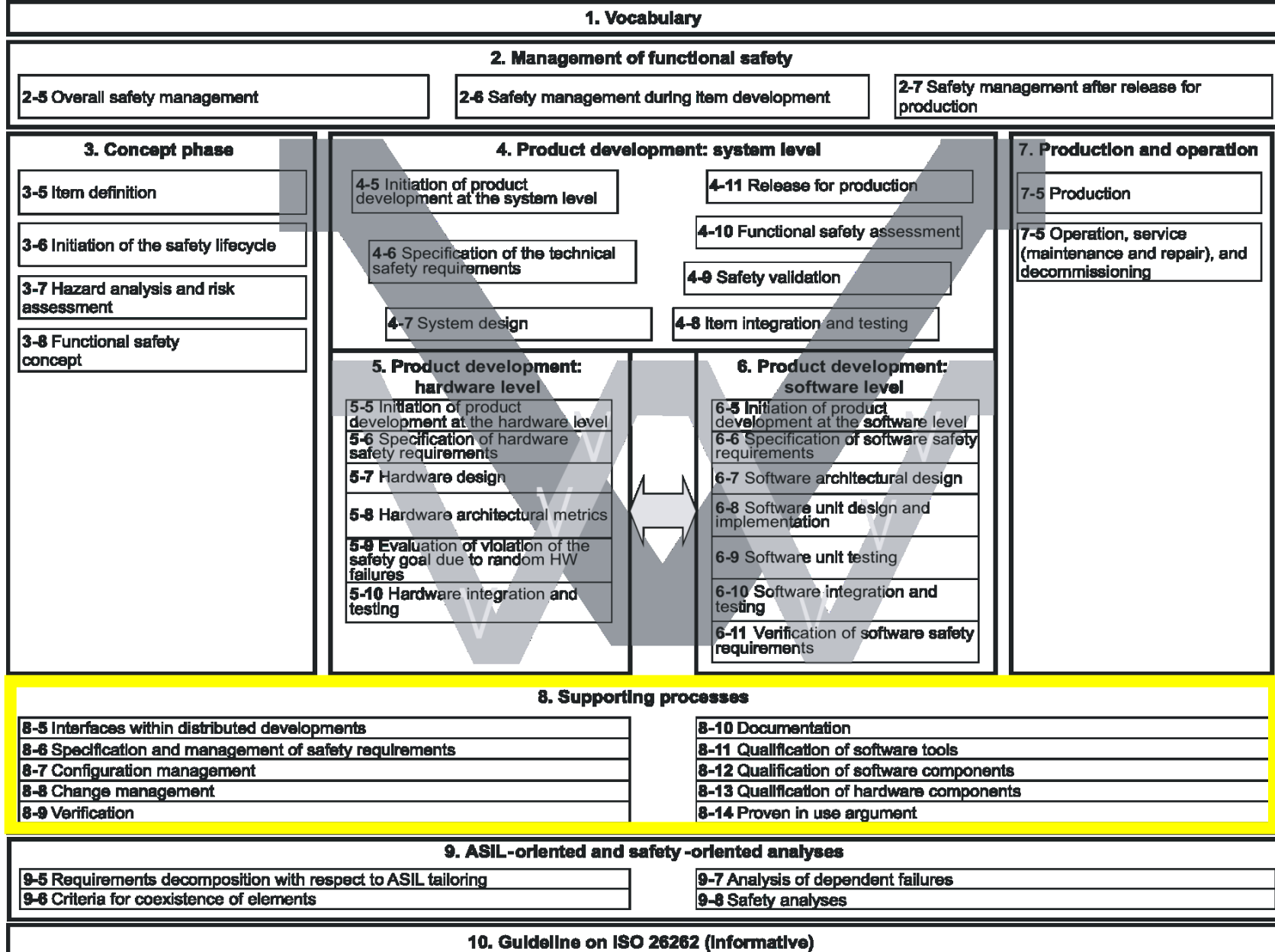
1. What requirements are specified in the clause on Production and Operation?
 - A. Production
 - B. Operation
 - C. Service and decommissioning
 - D. All of the above**



Part 8: Supporting Processes

Barbara J. Czerny





Core processes



Source ISO/DIS 26262

Requirements for Supporting Processes

- Objective
 - Consolidate common requirements to maintain consistency

- Supporting Processes
 - Interfaces within distributed developments
 - Specification and management of safety requirements
 - Configuration management
 - Change management
 - Verification
 - Documentation
 - Qualification of software tools
 - Qualification of software components
 - Qualification of hardware components
 - Proven in use argument



Clause 5: Interfaces Within Distributed Developments

➤ Objective

- Describe procedures and allocate responsibilities within distributed developments (e.g., vehicle manufacturer and supplier) for items and elements

➤ Supplier selection criteria

- Evaluate the supplier's capability to develop and produce items of comparable complexity and ASIL according to ISO 26262
 - Supplier's quality management system, experience, capability in developing products of comparable complexity and ASIL, ...



Clause 5: Interfaces Within Distributed Developments Cont'd.

- Development Interface Agreement (DIA) specifying:
 - Safety managers at the customer's and supplier's
 - Joint tailoring of the safety lifecycle, with identification of activities and processes to be performed by the customer and by the supplier;
 - The information required; work products to be exchanged; persons responsible
 - Communication of target values (derived from system level targets) specified to fulfil the targets for single point faults metric and latent faults metric, and evaluation of violation of the safety goal due to random hardware failures
- Coordination of supporting processes and tools
 - Including interfaces assuring compatibility between the customer and the supplier
- Adequate customer access to supplier work products to allow completion of safety case
- Information related to execution of DIA, including Safety Assessment at the supplier's facility, and post-production support



Clause 5: Interfaces within distributed environments

Work Products

- ☐ Supplier selection report
- ☐ Development Interface Agreement
- ☐ Supplier's project plan
- ☐ Supplier's safety plan
- ☐ Safety Assessment Report
- ☐ Supply agreement



Clauses 6 through 10: Existing engineering processes

- Include requirements for existing engineering processes
 - Accommodate the functional system safety activities defined in other parts of the standard

- Engineering process capabilities addressed include:
 - Clause 6: Specification and Management of safety requirements
 - Clause 7: Configuration Management
 - Clause 8: Change management
 - Clause 9: Verification
 - Clause 10: Documentation



Clause 6 – Specification and Management of Safety Requirements

➤ Objectives

- Ensure correct specification of safety requirements with respect to attributes and characteristics
- Support consistent management of safety requirements throughout the safety lifecycle

➤ Clause includes requirements for

- Notations for the specification of safety requirements
- Attributes and characteristics of safety requirements
 - Unambiguous and comprehensible, atomic, internally consistent ...
- Properties for the collection of safety requirements
 - Hierarchical, complete, externally consistent, maintainable, ...
- Management of safety requirements
 - Traceability, configuration management, verification

➤ Work Product – Safety Plan (refined)



Clause 7 – Configuration Management

- Objective
 - Ensure unique identification and reproducibility of work products at any time
 - Ensure traceability of relationships and differences between earlier and current versions
- Clause includes requirements for
 - Compliance with the requirements of ISO TS 16949, 4.2.3 and ISO 12207, 6.2
 - Work products listed in ISO 26262 are subject to configuration management
 - Tools subject to configuration management
 - Software tools and software development environments
 - Test tools and test environments
- Work product – configuration management plan



Clause 8 – Change Management

- Objective
 - The analysis and management of changes to safety-related work products occurring throughout the safety lifecycle
- Involves
 - Systematically planning, controlling, monitoring, implementing, and documenting changes, while maintaining consistency of all work products
- Clause includes requirements for
 - Planning and initiating change management
 - Change requests
 - Unambiguously identified, author, reason for change, exact description, ...
 - Impact analysis of the change requests
 - Type of change, affected work products, impact on functional safety ...
 - Deciding on a change request
 - Carrying out and documenting the change



Clause 8 – Change Management – Work Products

- Change management plan
- Change request
- Impact analysis
- Change request plan
- Change report



Clause 9– Verification

- Objective
 - Ensure that all work products
 - are correct, complete, and consistent
 - meet the requirements of ISO 26262
- Clause includes requirements for
 - Planning of verification
 - Specification of verification
 - Selection and specification of verification methods, specification of test cases, ...
 - Execution of verification
 - Verification shall be executed as planned and specified
 - Evaluation of verification
 - Requirements on the evaluation of the verification results
- Work products – verification plan, specification of verification, verification report



Clause 10 – Documentation

➤ Objectives

- Develop a documentation management strategy so that every phase of the entire safety lifecycle can be executed effectively and can be reproduced

➤ Clause includes requirements for

- Availability of documentation
- Content of documentation
 - e.g., precise and concise, structured in a straightforward manner, easy to understand, maintainable, etc.

➤ Work Products – document management plan, documentation requirements



Clause 11 – Qualification of Software Tools

➤ Objective


- Provide evidence of SW tool suitability for use in developing a safety-related item or element
 - Confidence in correct execution of activities and tasks required by ISO 26262

➤ Clause includes

- Planning of qualification of a software tool
- Classification of a software tool
 - Tool impact
 - Possible violation of safety requirement if tool is malfunctioning or producing erroneous output (TI0 – no possibility, TI1 – possibility)
 - Tool detection
 - Possibility of preventing or detecting that the software tool is malfunctioning or producing erroneous output (TD1 – TD4)
 - Tool confidence level
 - Based on tool impact and tool detection determinations (TCL1 – TCL4)



Clause 11 — Qualification of software tools

- Methods for qualifying software tools
 - For TCL2, TCL3, and TCL4
 - Increased confidence from use
 - Evaluation of the development process
 - Validation of the software tool
 - Development in compliance with a safety standard
 - Description of each method for qualification
 - Verification requirements of the qualification of software tools
 - Work Products — software tool classification analysis, software tool qualification plan, software tool documentation, software tool qualification report
- 
- Dependent on Tool
Confidence Level
and ASIL



Clause 12 – Qualification of Software Components

- Objectives
 - To enable the re-use of existing software components as part of items, systems, or elements developed in compliance with ISO 26262 without completely re-engineering the software components
 - To show their suitability for re-use

- Required information to treat a software component as qualified
 - Specification of the software component
 - Evidence that the software component complies with its requirements
 - Evidence that the software component is suitable for its intended use

- Requirements on the verification of the qualification of a software component

- Work Products – software component documentation, software component qualification report



Clause 13 – Qualification of Hardware Components

➤ Objectives

- To show the suitability of intermediate level hardware 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
- Provide relevant information regarding
 - Failure modes and their distribution
 - Diagnostic capability with regard to the safety concept for the item



- Qualification using analysis and/or testing
 - Ensure that the functional performance of components is adequate for the purposes of the safety concept
 - Identify failure modes and models by using appropriate tests or analyses
 - Ensure sufficient robustness and evaluate limitations of component use
- Requirements on qualification by analysis and testing
- Requirements on qualification report
 - Pass/fail with respect to the operating envelope
 - Verification of the qualification report
- Work Products
 - Qualification plan
 - Hardware component testing plan, if applicable
 - Qualification report



➤ Objective

- Provide guidance for proven in use argument
 - Alternate means of compliance with ISO 26262 requirements
 - May be used in case of reuse of existing items or elements when field data is available
- Proven in use credit does not eliminate need for integration safety lifecycle activities
- Considers:
 - Service period for the item/element
 - Changes to the candidate for a future application



➤ Requirements on analysis of field data

- Configuration management and change control applied to candidate
- Target values for proven in use
 - Observable incident rate must not exceed targets for the ASIL of the candidate
 - Observable incident is a failure that is reported to the manufacturer and caused by the candidate with the potential to lead to the violation of a safety goal
- Field problems need to be recorded and retrievable

Table 7 – Targets for minimum service period for candidate

| ASIL | Minimum service period without observable incident (hours) |
|------|--|
| D | $1.2 \cdot 10^9$ |
| C | $1.2 \cdot 10^8$ |
| B | $1.2 \cdot 10^8$ |
| A | $1.2 \cdot 10^7$ |

Source ISO/DIS 26262

➤ Work Products

- Proven in use credit
- Definition of candidate for proven in use argument
- Proven in use analysis reports



Checkpoint Questions - Part 8: Supporting Processes

1. What specifies the interfaces between a manufacturer and supplier in a distributed development?
 - A. The system specification
 - B. The purchase order
 - C. The Development Interface Agreement (DIA)
2. What tools are subject to configuration management?
 - A. Software tools and software development environments
 - B. Test tools and test environments
 - C. All of the above
3. What is the objective of verification?
 - A. Ensure that all work products are correct, complete, and consistent
 - B. Ensure that all work products meet ISO 26262 requirements
 - C. All of the above
4. What is required for a Proven in Use Argument?
 - A. Definition of the candidate for proven in use argument
 - B. Analysis of changes to the candidate
 - C. Analysis of field data
 - D. All of the above



Checkpoint Questions - Part 8: Supporting Processes

1. What specifies the interfaces between a manufacturer and supplier in a distributed development?
 - A. The system specification
 - B. The purchase order
 - C. **The Development Interface Agreement (DIA)**
2. What tools are subject to configuration management?
 - A. Software tools and software development environments
 - B. Test tools and test environments
 - C. All of the above
3. What is the objective of verification?
 - A. Ensure that all work products are correct, complete, and consistent
 - B. Ensure that all work products meet ISO 26262 requirements
 - C. All of the above
4. What is required for a Proven in Use Argument?
 - A. Definition of the candidate for proven in use argument
 - B. Analysis of changes to the candidate
 - C. Analysis of field data
 - D. All of the above



Checkpoint Questions - Part 8: Supporting Processes

1. What specifies the interfaces between a manufacturer and supplier in a distributed development?
 - A. The system specification
 - B. The purchase order
 - C. **The Development Interface Agreement (DIA)**
2. What tools are subject to configuration management?
 - A. Software tools and software development environments
 - B. Test tools and test environments
 - C. **All of the above**
3. What is the objective of verification?
 - A. Ensure that all work products are correct, complete, and consistent
 - B. Ensure that all work products meet ISO 26262 requirements
 - C. All of the above
4. What is required for a Proven in Use Argument?
 - A. Definition of the candidate for proven in use argument
 - B. Analysis of changes to the candidate
 - C. Analysis of field data
 - D. All of the above



Checkpoint Questions - Part 8: Supporting Processes

1. What specifies the interfaces between a manufacturer and supplier in a distributed development?
 - A. The system specification
 - B. The purchase order
 - C. **The Development Interface Agreement (DIA)**
2. What tools are subject to configuration management?
 - A. Software tools and software development environments
 - B. Test tools and test environments
 - C. **All of the above**
3. What is the objective of verification?
 - A. Ensure that all work products are correct, complete, and consistent
 - B. Ensure that all work products meet ISO 26262 requirements
 - C. **All of the above**
4. What is required for a Proven in Use Argument?
 - A. Definition of the candidate for proven in use argument
 - B. Analysis of changes to the candidate
 - C. Analysis of field data
 - D. All of the above



Checkpoint Questions - Part 8: Supporting Processes

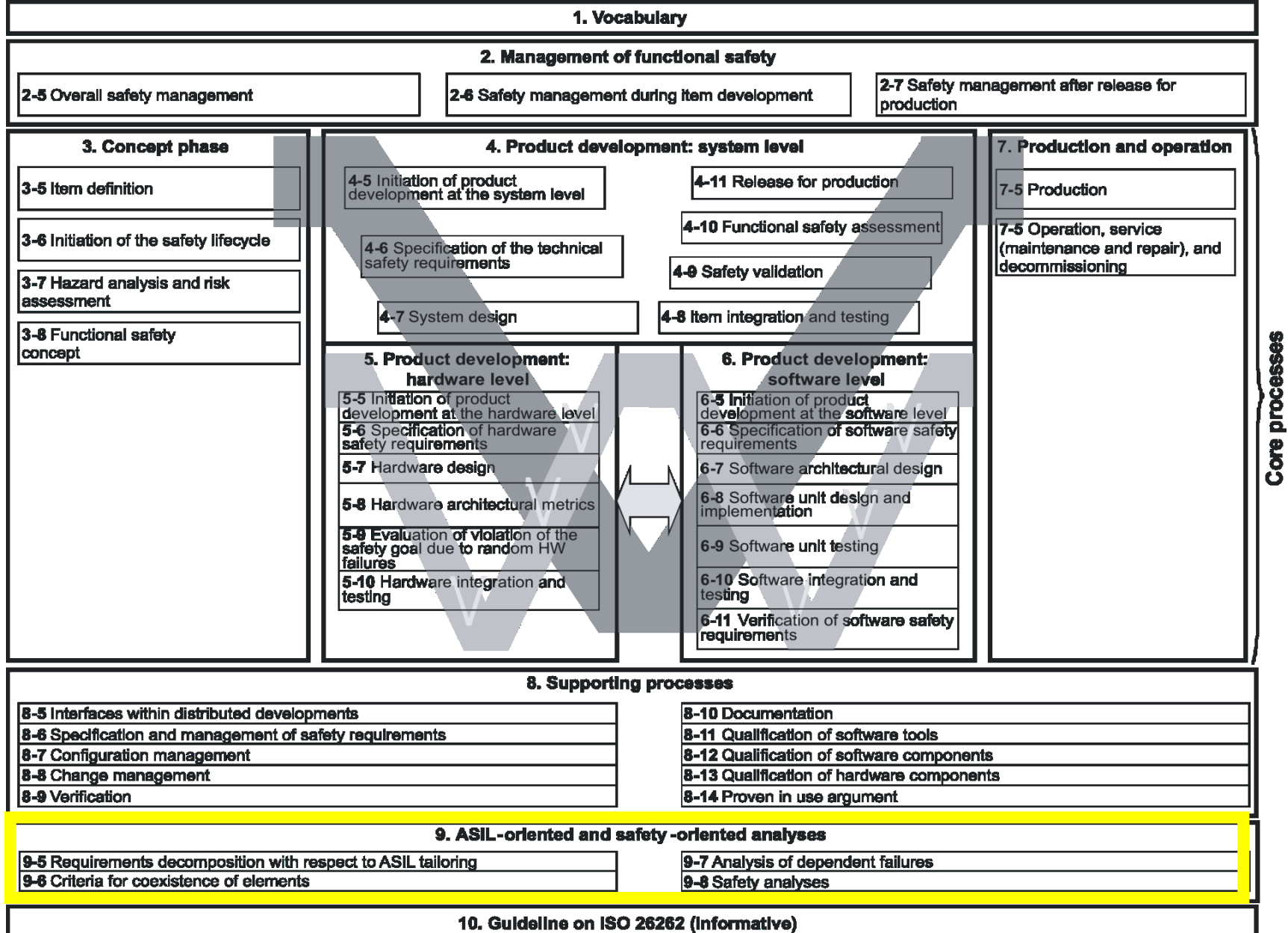
1. What specifies the interfaces between a manufacturer and supplier in a distributed development?
 - A. The system specification
 - B. The purchase order
 - C. **The Development Interface Agreement (DIA)**
2. What tools are subject to configuration management?
 - A. Software tools and software development environments
 - B. Test tools and test environments
 - C. **All of the above**
3. What is the objective of verification?
 - A. Ensure that all work products are correct, complete, and consistent
 - B. Ensure that all work products meet ISO 26262 requirements
 - C. **All of the above**
4. What is required for a Proven in Use Argument?
 - A. Definition of the candidate for proven in use argument
 - B. Analysis of changes to the candidate
 - C. Analysis of field data
 - D. **All of the above**



Part 9: ASIL-oriented and Safety-oriented Analyses

Rami Debouk





Source ISO/DIS 26262



ASIL-oriented and safety-oriented analyses

- Requirements decomposition with respect to ASIL tailoring
- Criteria for coexistence of elements
- Analysis of Dependent Failures
- Safety Analyses



Requirements decomposition with respect to ASIL tailoring

Objectives

- Decomposing safety requirements into redundant safety requirements (not necessarily identical) to allow ASIL tailoring at the next level of detail
 - In this decomposition, the relevant safety goal is only violated if both elements fail simultaneously

Some Requirements

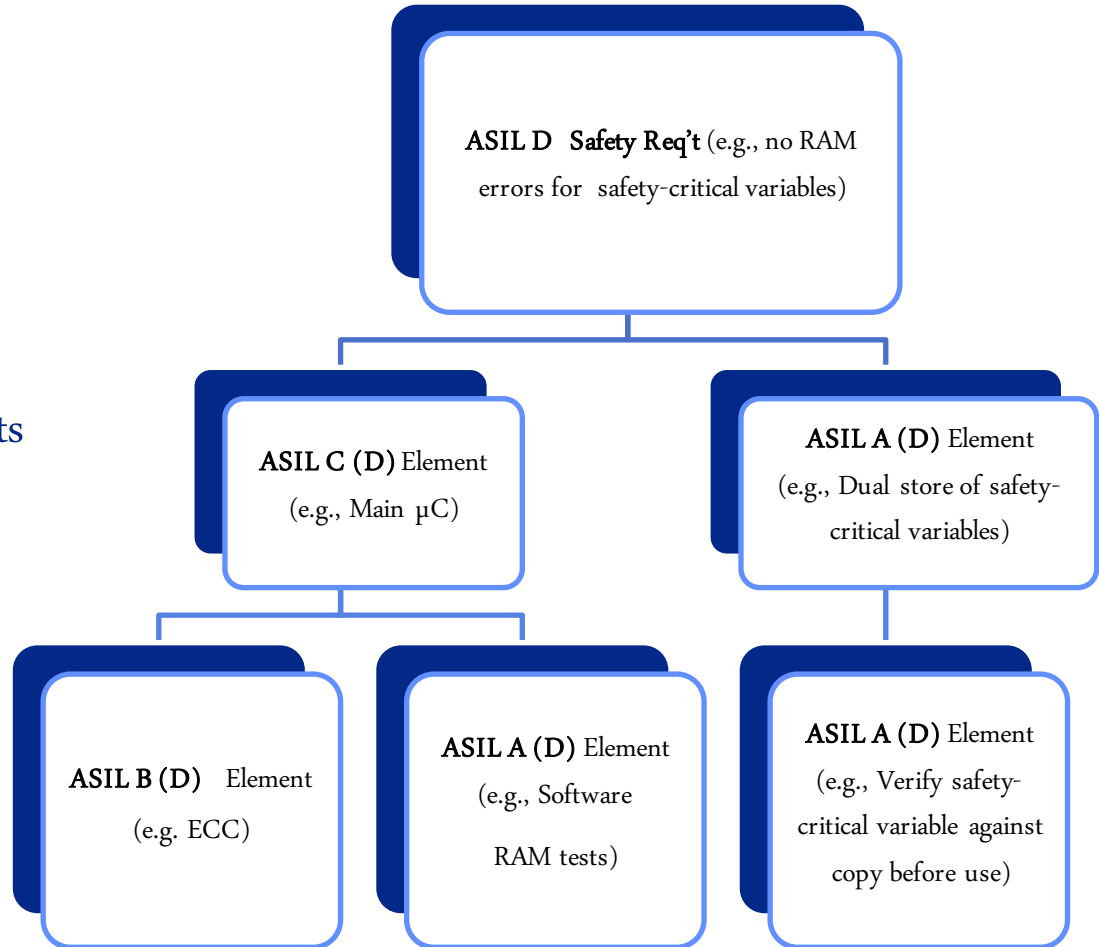
- ASIL decomposition is performed considering each allocated safety requirement of the element
- Initial safety requirements are implemented by sufficiently independent elements and redundant safety requirements are derived for each of these elements



Requirements decomposition with respect to ASIL tailoring

Part 9 Work Products

- Updated architectural information
- Update of ASIL as attribute of safety requirements and elements



Criteria for coexistence of elements

Objectives

Provide criteria for coexistence within the same element of

- safety-related sub-elements with non-safety-related ones
- safety-related sub-elements assigned different ASILs

Can be beneficial to avoid raising the ASIL of sub-elements



Criteria for coexistence of elements

Requirements

- A non-safety-related sub-element coexisting in the same element with safety-related sub-element(s) shall only be treated as a QM sub-element, if it has no functional dependency with any of the safety requirements allocated to the element and it does not interfere with any other safety-related sub-elements of the element
- In the case of coexistence in the same element of safety-related sub-elements with different ASILs, a sub-element shall only be treated as a lower ASIL sub-element if it is shown that it does not interfere with any other sub-element assigned a higher ASIL, for each of the safety requirements allocated to the element



Analysis of Dependent Failures

Objective

- Identify any single event or single cause that could bypass or invalidate the independence or freedom from interference between elements of an item required to comply with its safety goals

Requirements

- Identification of potential for dependent failures from safety analyses
- Evaluation for dependent failures in order to determine if a reasonably foreseeable cause exists which will cause the dependent failures to occur and violate a safety goal
- Resolution of dependent failures in change requests to mitigate the root cause in the sub-phases of the safety lifecycle for which analysis of dependent failure is applied



Analysis of Dependent Failures

Part 9 Work Products

- Results of analyses of dependent failures
- Change requests for confirmed dependent failures



Safety Analyses

Objectives

- To examine the influence of faults and failures on items or elements regarding their architecture, functions and behaviour
- Provide information on conditions and causes that could lead to violation of a safety goal or safety requirement
- Contribute to the identification of new functional or non-functional hazards not previously considered during hazard analysis and risk assessment



Safety Analyses

Requirements

- Carried out according to the ASIL assigned to the item or element
- Performed according to national, international or other appropriate standards or guidelines
- Provide measures and apply them to faults or failures that could potentially violate the safety goals or safety requirements
- Implement the above measures as part of the product development
- The results of the safety analyses is used to determine the need for additional safety-related test cases
- The results of the safety analyses are documented and reviewed



Checkpoint Questions - Part 9: ASIL-oriented and Safety-oriented Analyses

1. ASIL Decomposition is about decomposing safety requirements into identical redundant requirements
 - A. True
 - B. False
2. Why perform dependent failure analysis?
 - A. To reduce the ASIL requirement of a component
 - B. To identify any single event or single cause that could bypass or invalidate the independence required to satisfy the safety goals of a system.
 - C. To analyze field data
 - D. All of the above



Checkpoint Questions - Part 9: ASIL-oriented and Safety-oriented Analyses

1. ASIL Decomposition is about decomposing safety requirements into identical redundant requirements
 - A. True
 - B. False**
2. Why perform dependent failure analysis?
 - A. To reduce the ASIL requirement of a component
 - B. To identify any single event or single cause that could bypass or invalidate the independence required to satisfy the safety goals of a system.
 - C. To analyze field data
 - D. All of the above



Checkpoint Questions - Part 9: ASIL-oriented and Safety-oriented Analyses

1. ASIL Decomposition is about decomposing safety requirements into identical redundant requirements
 - A. True
 - B. False**
2. Why perform dependent failure analysis?
 - A. To reduce the ASIL requirement of a component
 - B. To identify any single event or single cause that could bypass or invalidate the independence required to satisfy the safety goals of a system.**
 - C. To analyze field data
 - D. All of the above



Key Aspects that Have Evolved Over Time During ISO/DIS 26262 Development

- What is meant by malfunctioning behavior?
 - Includes more than just failures of an item
 - Also includes unintended behaviours of an item with respect to its design intent and interactions between E/E safety-related systems
- Requirement for manufacturers to ensure proper decommissioning of systems
 - Changed to a “should”
 - Not possible in all cases for manufacturers to ensure this
- From prescriptive to goal-based
 - Methods listed in tables are now related to satisfying a specific goal
 - Change required a restructuring and reinterpretation of tables and introduction of a goals clause related to methods in the tables



Summary

- Background of ISO 26262
 - What is it?
 - What are the origins of ISO 26262?
 - Differences between IEC 61508 and ISO 26262
- Status of ISO 26262
- Overview of each part of the standard
 - Objectives, requirements, and work products
- Overview of key aspects that have evolved over time



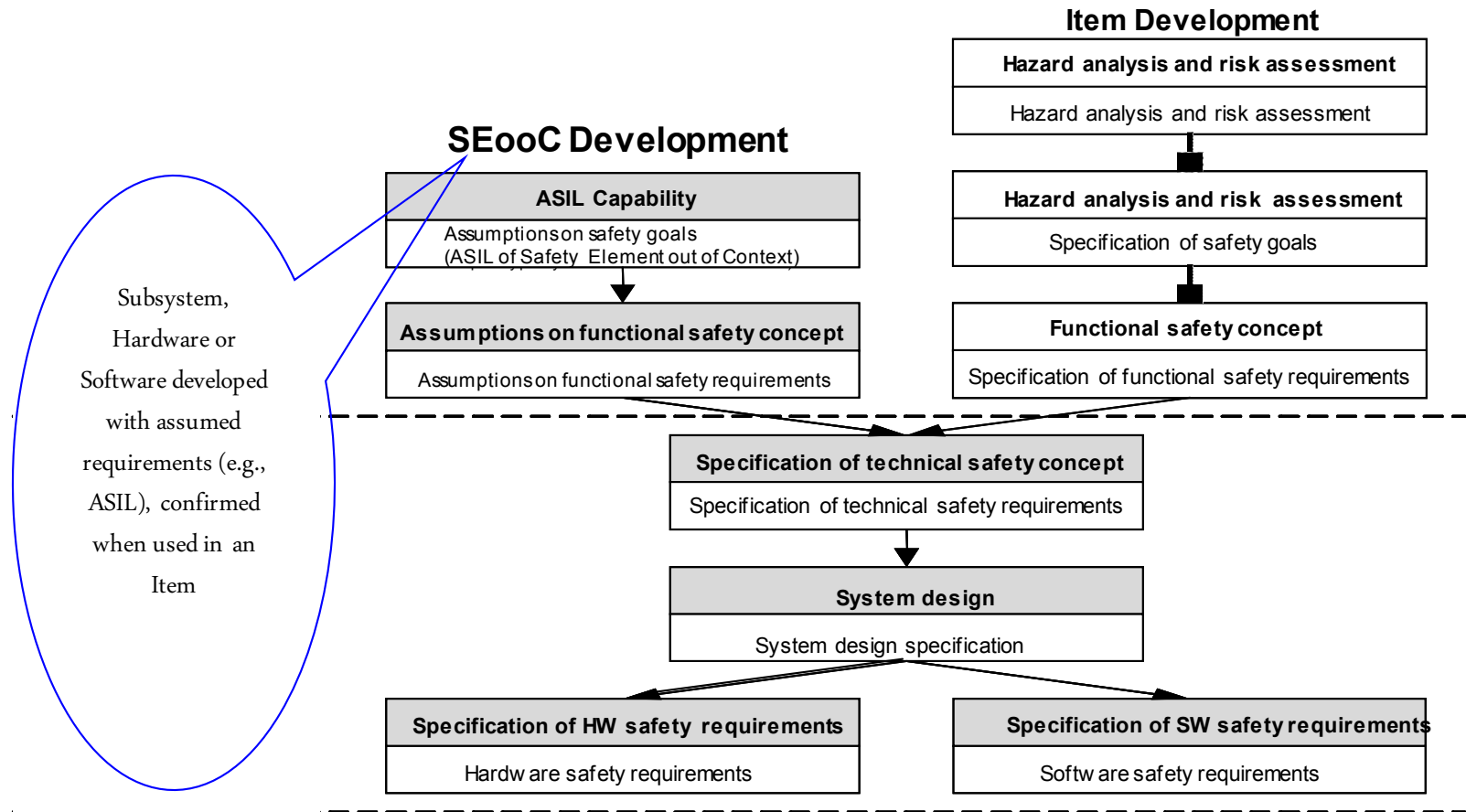
Q & A



BACKGROUND



Safety Element out of Context (SEooC)



Source ISO/DIS 26262



