SAFETY STANDARDS
FOUNDATION

FUNCTIONAL SAFETY COURSE #1

Renault Group

PUBLIC

NXP
SECURE CONNECTIONS
FOR A SMARTER WORLD

Awareness of Functional Safety

- ➢ Introduction to Safety
- ➢ What is Functional Safety
- ➢ Functional Safety Standards & history
- ➢ General approach for risk management
- ➢ Systematic & Random failures, types of faults
- ➢ Risk management in the automotive
- ➢ Safety goals and safety integrity levels
- ➢ The ISO26262 standard

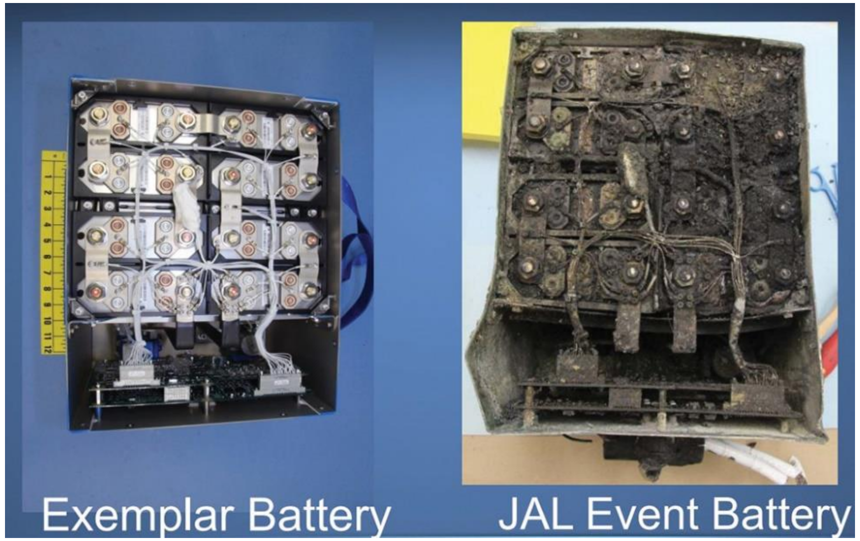
01.

INTRODUCTION TO SAFETY

Examples of accidents

Toyota Unintended Acceleration

The Ford Pinto Case



JAL B – 787

(Source: Tesla Motors Club)

Tesla Crash

Tesla’s Fatal Crash

Examples of accidents

Examples of accidents

Road Traffic Accidents: The Causes

Critical Reasons	Number	%
Driver	2,046,000	94%
Vehicles	44,000	2%
Environment	52,000	2%
Unknown	47,000	2%
Total	2,189,000	100%

Data source: NMVCCS

Driver-Related Critical Reasons	Number	%
Recognition Error	845,000	41%
Decision Error	684,000	33%
Performance Error	210,000	11%
Non-performance Error (e.g. Sleep)	145,000	7%
Other	162,000	8%
Total	2,046,000	100%

Every year!

- ~1.3 M fatalities
- >50 M people seriously injured
- >$3 trillion cost of road accidents
- >90% caused by human mistakes

We need to get the
Human Factor out of the equation!

02.

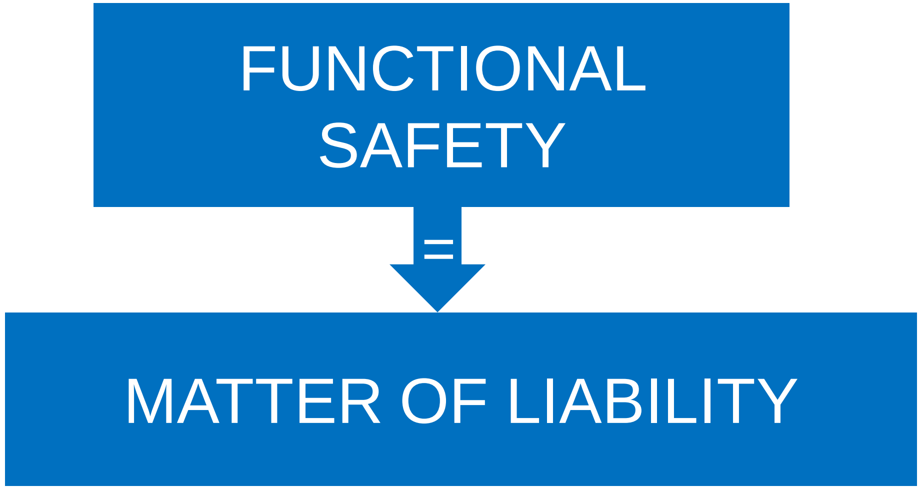
WHAT IS FUNCTIONAL SAFETY?

Awareness of Functional Safety

What is Functional Safety?

Functional safety is the absence of **unreasonable risk** due to **hazards** caused by **malfunctioning** behavior of electrical or electronic **systems**

What is Functional Safety?



FUNCTIONAL SAFETY

=

MATTER OF LIABILITY

Everyone involved in the development of a safety related project should be able to demonstrate freedom from negligence in case of product liability.

/!\ Not only the safety people involved in the project (manager, architect, assessor)

Legal Consequences

Do you have to fulfill ISO 26262 by law? NO

However, in a Court of Law after a car accident you could be asked:

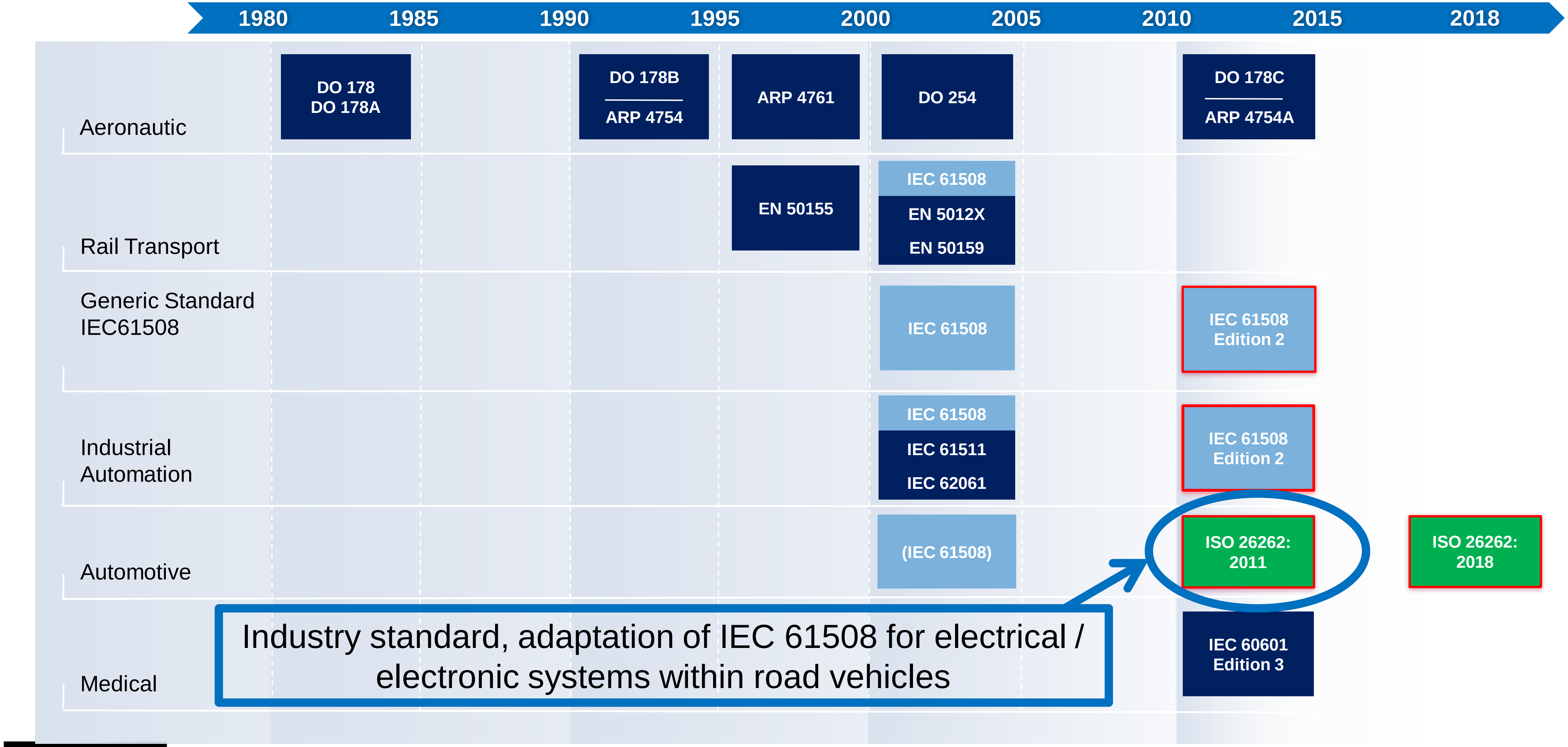
Did you follow the state of the art? Are you free from negligence?

- Functional safety standards are considered by law the minimum level of “state of the art” and have to be fulfilled
- Freedom of negligence must also be adhered to

03.

FUNCTIONAL SAFETY STANDARDS & HISTORY

Functional Safety Standards : History



1980 1985 1990 1995 2000 2005 2010 2015 2018

Aeronautic: DO 178 DO 178A | DO 178B ARP 4754 | ARP 4761 | DO 254 | DO 178C ARP 4754A

Rail Transport: EN 50155 | IEC 61508 EN 5012X EN 50159

Generic Standard IEC61508: IEC 61508 | IEC 61508 Edition 2

Industrial Automation: IEC 61508 IEC 61511 IEC 62061 | IEC 61508 Edition 2

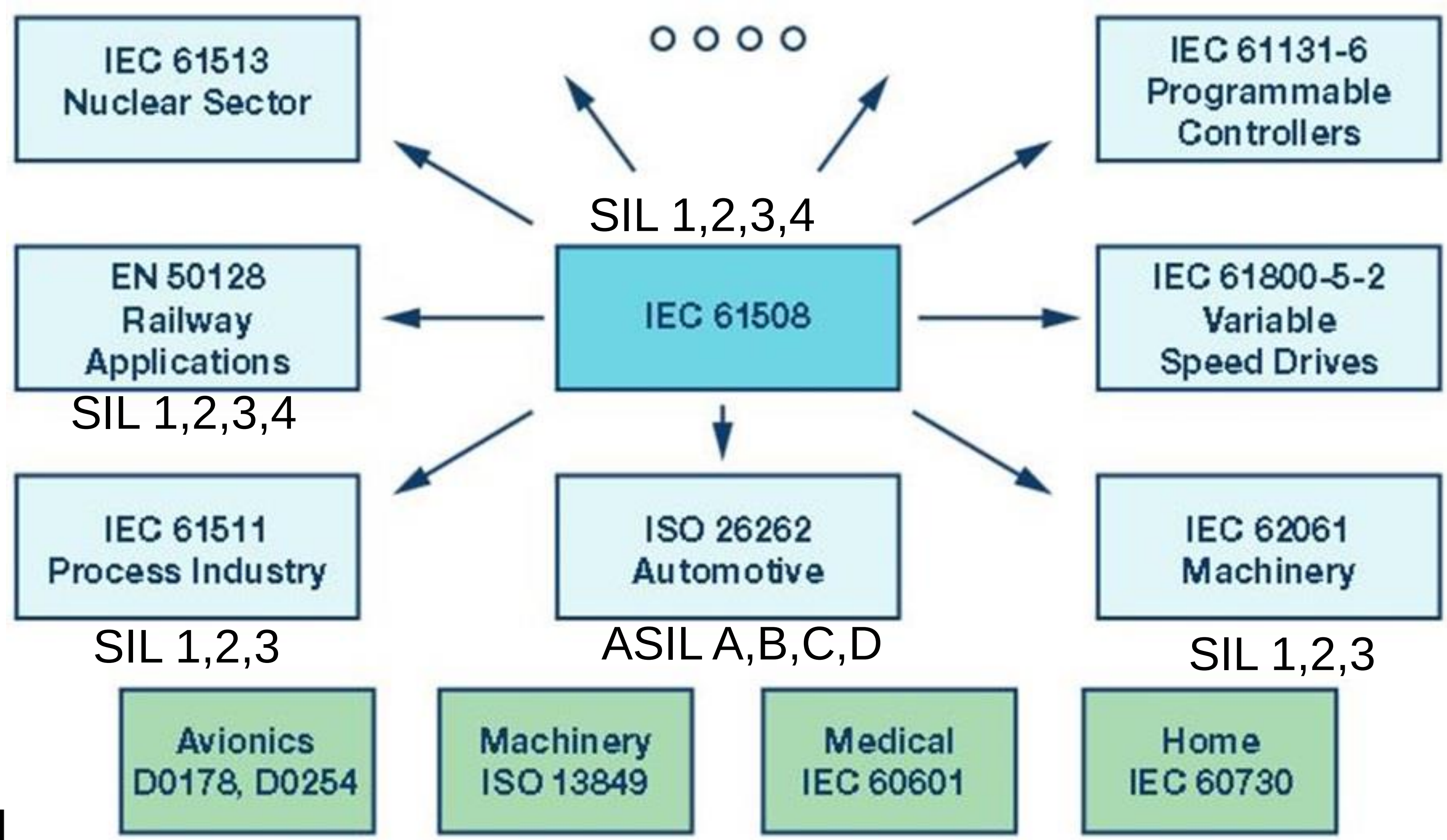
Automotive: (IEC 61508) | ISO 26262: 2011 | ISO 26262: 2018

Medical: IEC 60601 Edition 3

Industry standard, adaptation of IEC 61508 for electrical / electronic systems within road vehicles

Renault Group

Functional Safety Standard Landscape



IEC 61508

SIL 1,2,3,4

IEC 61513
Nuclear Sector

○○○○

IEC 61131-6
Programmable
Controllers

EN 50128
Railway
Applications

SIL 1,2,3,4

IEC 61800-5-2
Variable
Speed Drives

IEC 61511
Process Industry

SIL 1,2,3

ISO 26262
Automotive

ASIL A,B,C,D

IEC 62061
Machinery

SIL 1,2,3

Avionics
D0178, D0254

DAL E,D,C,B,A

Machinery
ISO 13849

EN954

Medical
IEC 60601

Home
IEC 60730

CLASS A,B,C

04.

GENERAL APPROACH FOR RISK MANAGEMENT

Functional Safety: A Bit Of Wording

Fault: abnormal condition or defect which may lead to a failure

Failure: inability of an element to perform a function

Safety Mechanism: detects failure and allow the system to react in accordance (i.e. bring the system in a safe state)

Safe State: it is the operating mode of the system, hardware, component without unreasonable level of risk

Fault tolerant time (FTTI): Is the maximum time a system may consume to detect and handle a fault, before resulting in a hazard

Functional Safety - General Approach

Hazard and Risk Analysis

Mitigation

SAFE System

Functional Safety - General Approach

Hazard and Risk Analysis

- Identify the potential malfunctions of the system (failure modes)
- Assess the effects of these malfunctions and their impact on Safety
- Identify the list of feared events
- Classify their criticality (based on standards)
- Define/Calculate the characteristics of the feared event (Safe state, FTTI)

Functional Safety - General Approach

- Define a Safety Architecture
- Identify mitigation measures
  - Detection measures
  - Control measures
- Implement the “Safety Mechanisms”

Mitigation

- Verify the implementation of the Safety mechanisms
- Verify the effectiveness of the Safety mechanisms

Functional Safety - General Approach

SAFE System

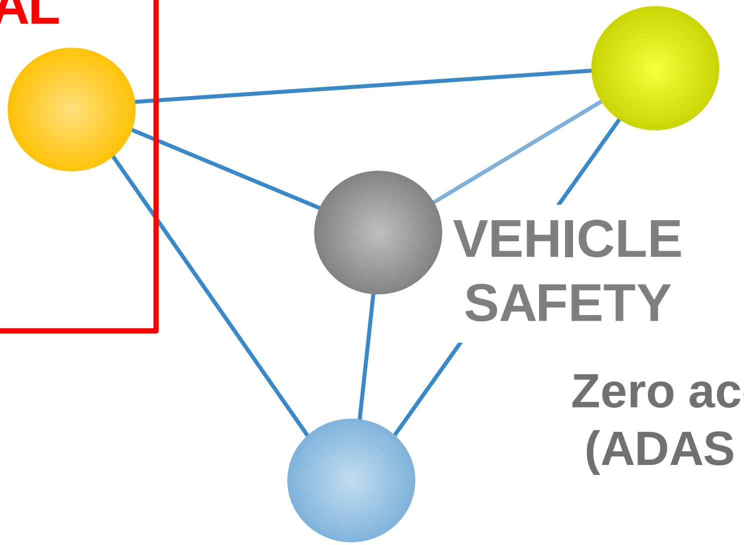
05.

RISK MANAGEMENT IN THE AUTOMOTIVE

Automotive example

Characteristics of A Safe System

Safety



FUNCTIONAL SAFETY

Zero accidents due to system failures

SECURITY

Zero accidents by system hacks

VEHICLE SAFETY

Zero accidents by human error (ADAS & SOTIF)

DEVICE RELIABILITY

Zero components failures (robust product)

SOTIF: Safety of the intended functionality

Quantify A Risk: Automotive Safety Integrity Level (ASIL) Definition

Severity

What is the level of injury ?

Exposure

How often is it likely to happen?

Controllability

Can the hazard be controlled

ASIL

An ASIL is defined for each Safety Goal

Functional Safety - Integrity Level Evaluation

E = Exposure

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

C = Controllability

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

S = Severity

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

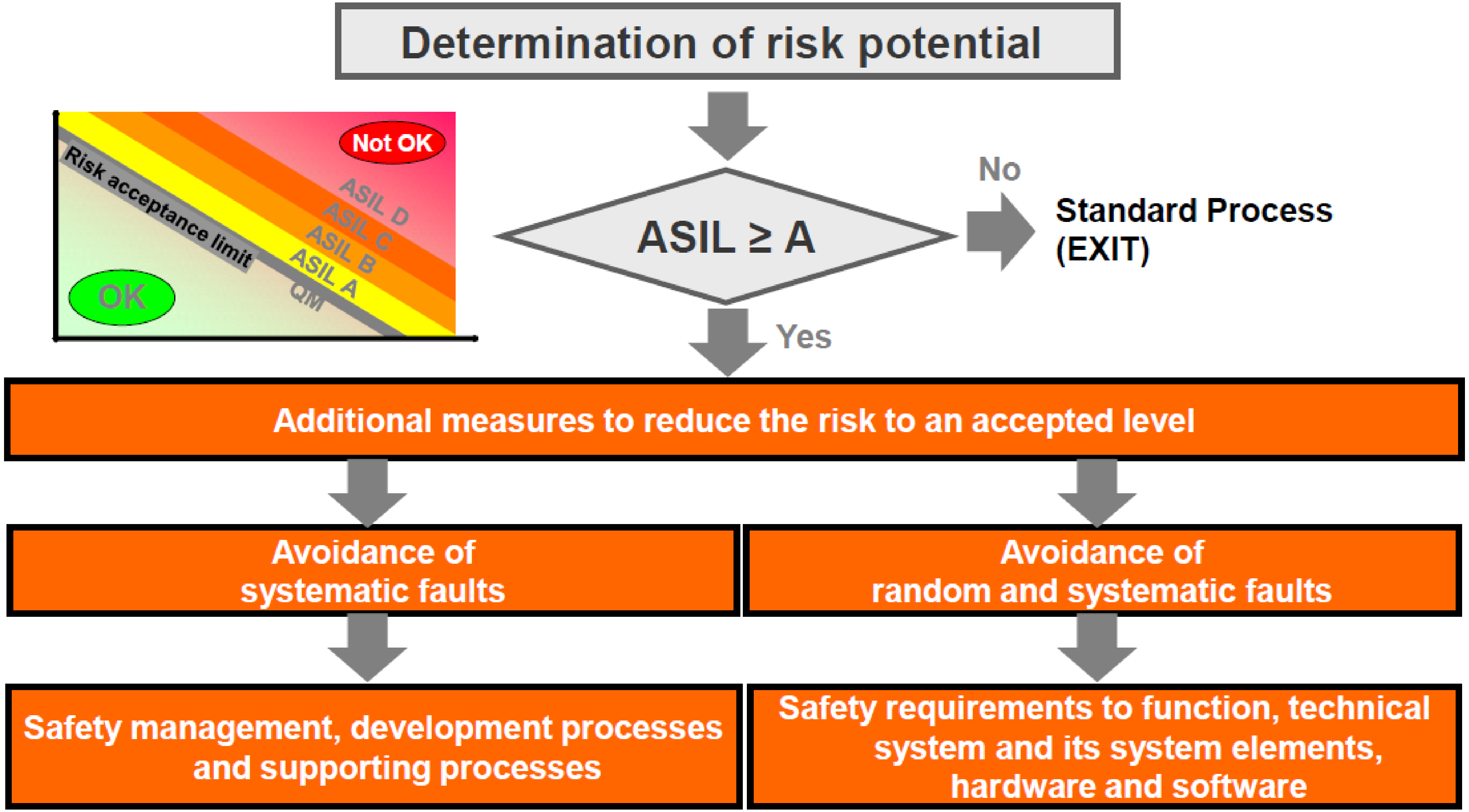
		C1 – SIMPLE	**C2** – NORMAL	**C3** – DIFFICULT
S1 LIGHT	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	QM
	E3 (medium)	QM	QM	A
	E4 (high)	QM	A	B
S2 SEVERE	E1 (very low)	QM	QM	QM
	E2 (low)	QM	QM	A
	E3 (medium)	QM	A	B
	E4 (high)	A	B	C
S3 FATAL	E1 (very low)	QM	QM	A
	E2 (low)	QM	A	B
	E3 (medium)	A	B	C
	E4 (high)	B	C	D

(QM: "quality managed" → no requirements from standard applied explicitly)

Example of System and Corresponding Safety integrity Level

Application / System	ASIL
Wiper	A
Computer Vision – mono / stereo camera	B
Radar	B
Lighting – low beam	B
Battery Management system	D
Chassis dynamic – suspension / damping	C
Gateway – ADAS controller - Fusion	D
Transmission – Dual Clutch Automatic Gearbox	D
Braking – Electro-mechanic	D
Airbag – (unwanted deployment)	D
Electric Power steering	D

Functional Safety - Risk Management



Determination of risk potential

ASIL ≥ A

No

Standard Process
(EXIT)

Yes

Additional measures to reduce the risk to an accepted level

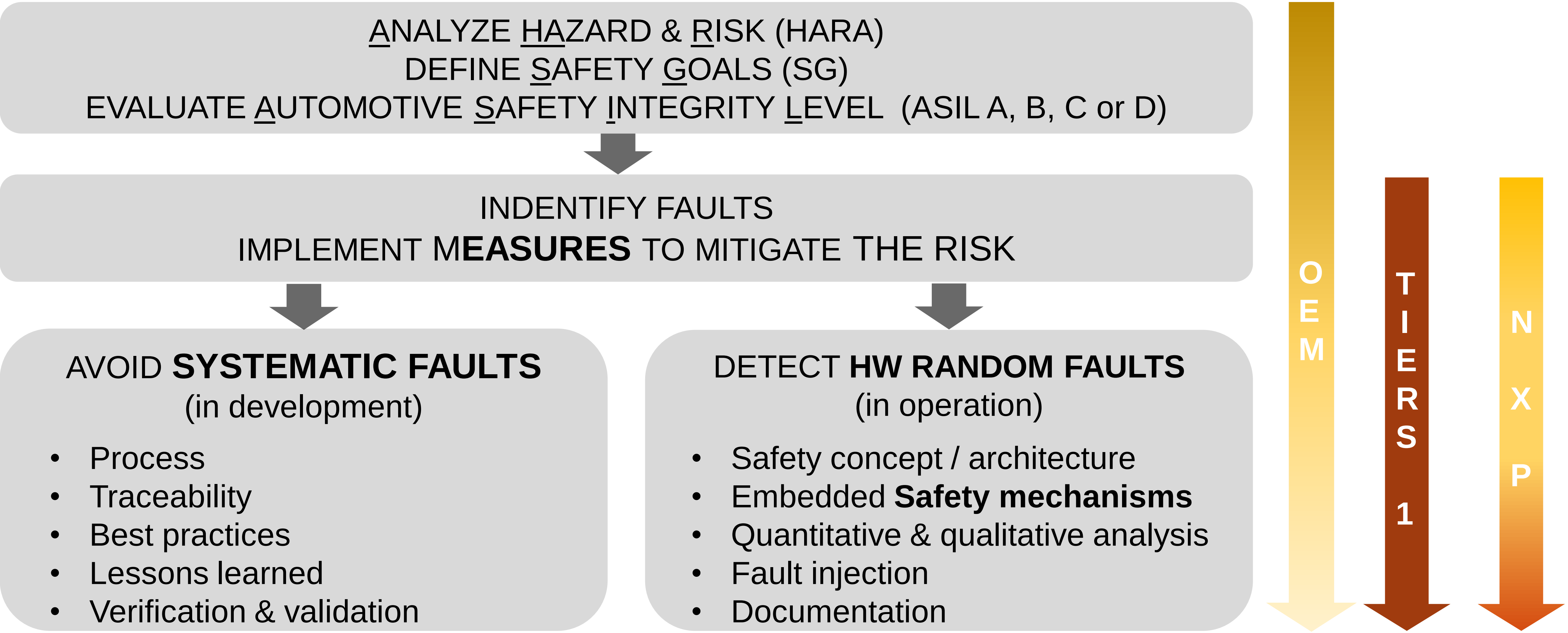
Avoidance of
systematic faults

Avoidance of
random and systematic faults

Safety management, development processes and supporting processes

Safety requirements to function, technical system and its system elements, hardware and software

Functional Safety – Risk Management



ANALYZE HAZARD & RISK (HARA)
DEFINE SAFETY GOALS (SG)
EVALUATE AUTOMOTIVE SAFETY INTEGRITY LEVEL (ASIL A, B, C or D)

INDENTIFY FAULTS
IMPLEMENT M**EASURES** TO MITIGATE THE RISK

AVOID **SYSTEMATIC FAULTS**
(in development)

- Process
- Traceability
- Best practices
- Lessons learned
- Verification & validation

DETECT **HW RANDOM FAULTS**
(in operation)

- Safety concept / architecture
- Embedded **Safety mechanisms**
- Quantitative & qualitative analysis
- Fault injection
- Documentation

06.

SYSTEMATIC & RANDOM FAILURES, TYPES OF FAULTS

Types of failures

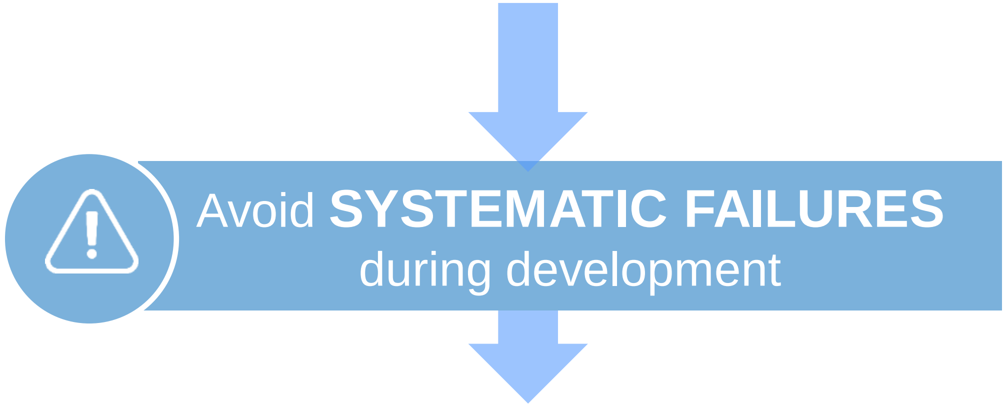
Failure: inability of an element to perform a function

Systematic failure: it can be eliminated by applying a strong process, by reviews, by verifications and by testing

Random failure: can occur unpredictably during the lifetime of a system, hardware, integrated circuit component.

Systematic & Random Failures

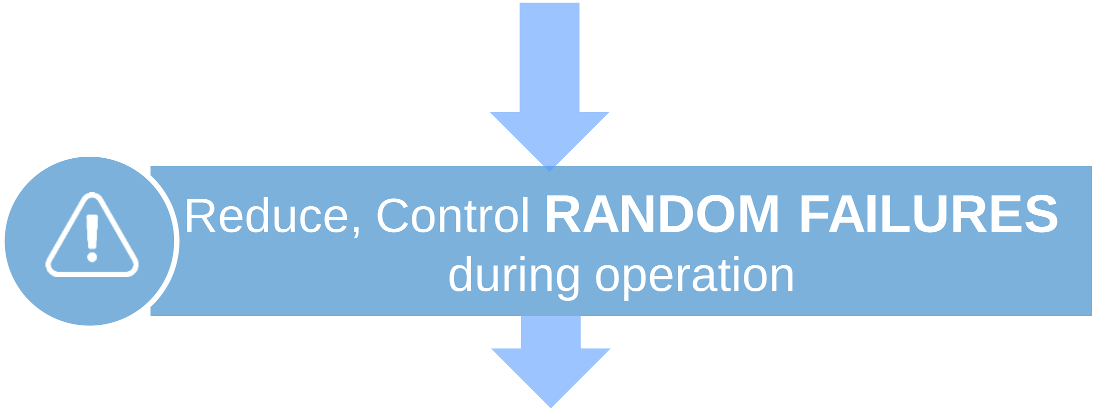
For both HW and SW



Avoid **SYSTEMATIC FAILURES** during development

- Process
- Safety management
- Best practices
- Lessons learned
- Verification & validation

Only for HW

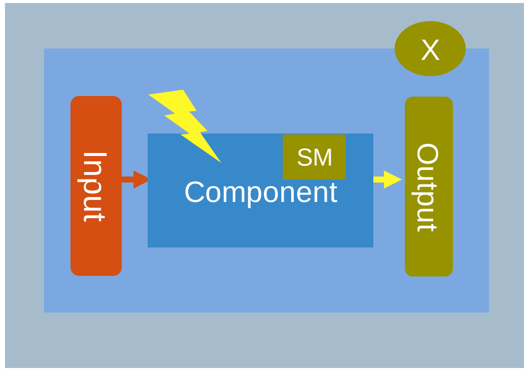


Reduce, Control **RANDOM FAILURES** during operation

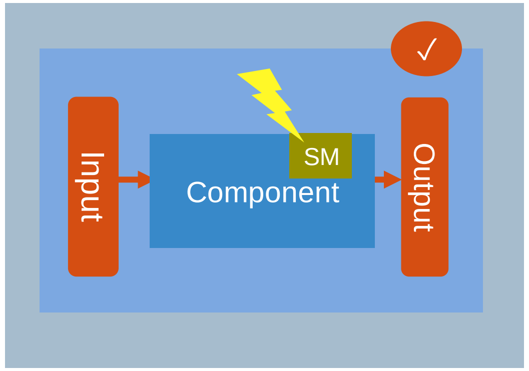
- System safe state
- Safety architecture
- Quantitative & qualitative analysis
- Documentation

Functional Safety - Types of Faults

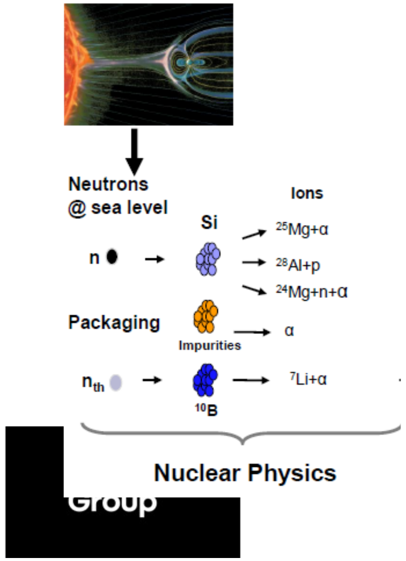
Single Point Fault



Latent Fault



Transient Fault

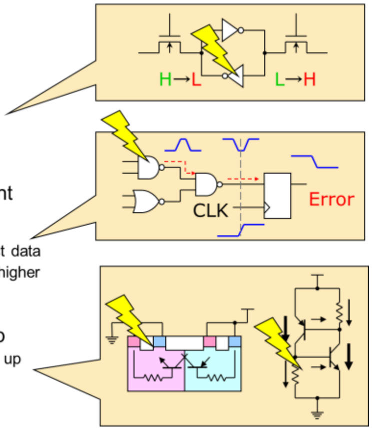


Soft Error Issue

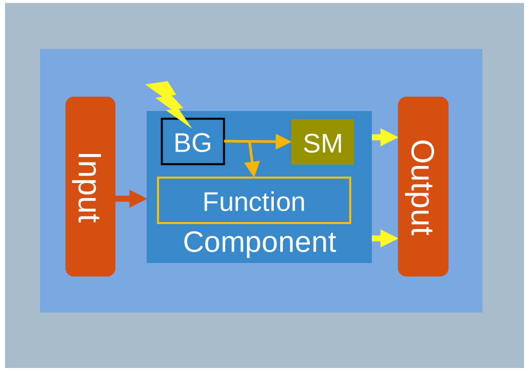
1. SEU = Single Event Upset
   - Data upset
   - DRAM
   - SRAM

2. SET = Single Event Transient
   - Temporary logic data upset
     ↓
     Error If Flip flop latch incorrect data
   - Error rate become higher as higher frequency clock

3. SEL = Single Event Latch up
   - Induced by PN isolation latch up



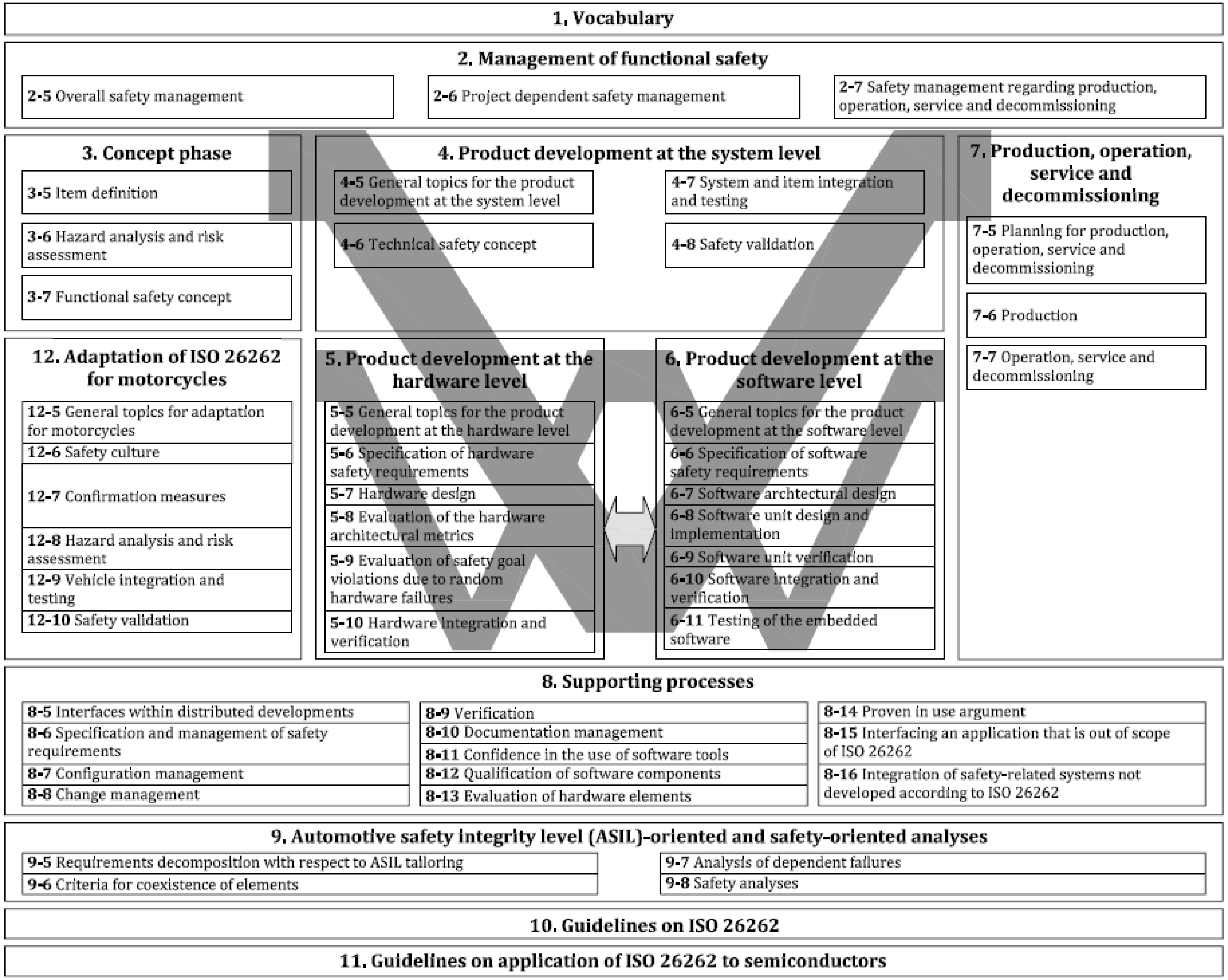
Common Cause Fault



07.

ISO 26262 STANDARD

Functional Safety ISO 26262 - 2018 Overview



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 1: Vocabulary

Part 2: Management of Functional Safety

Part 3: Concept Phase

Part 4: Product development at system level

Part 5: Product development at HW level

Part 6: Product development at SW level

Part 7: Production, operation, service and decommissioning

Part 8: Supporting processes

Part 9: Automotive Safety Integrity Level (ASIL) oriented and safety oriented analyses

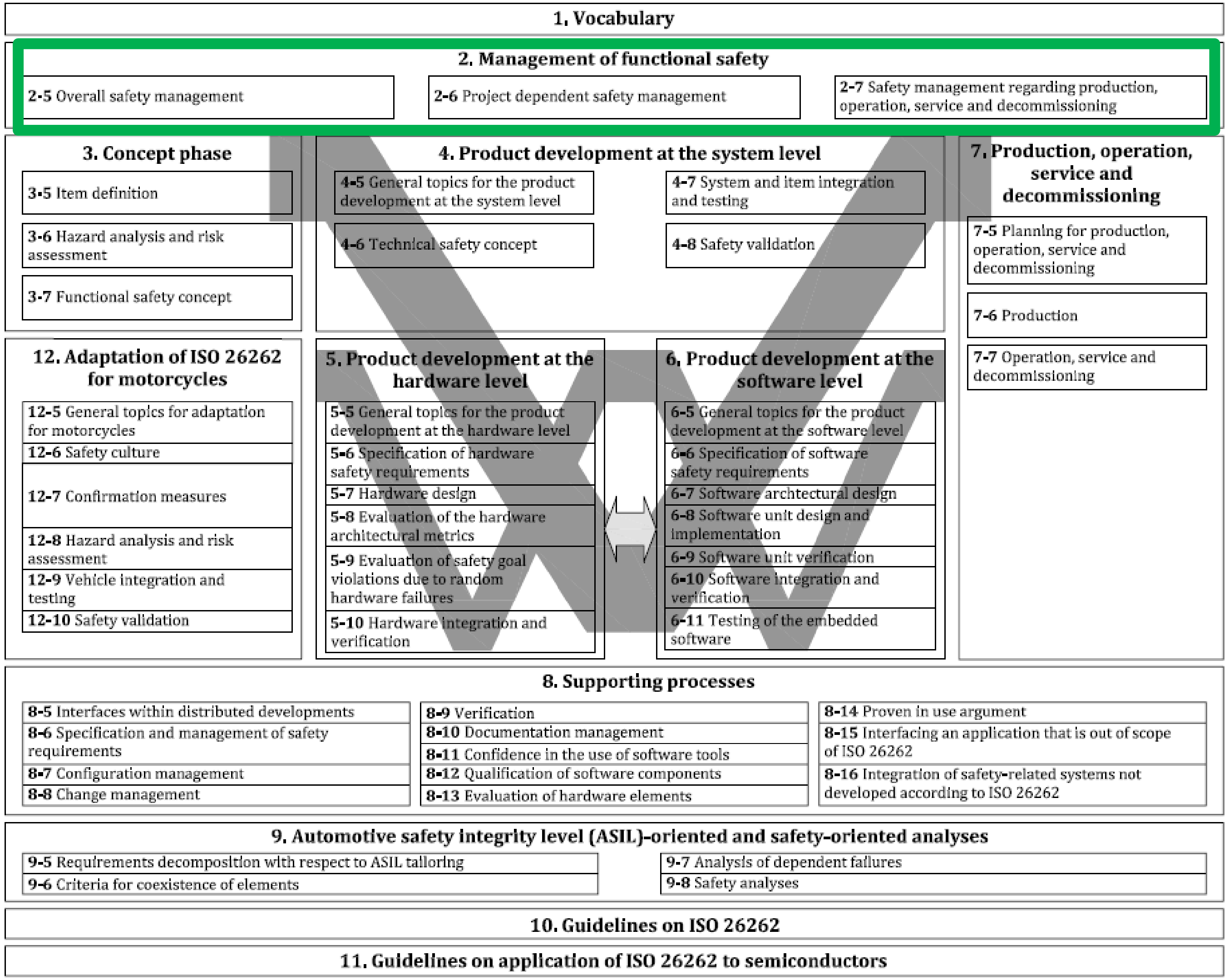
Part 10: Guideline on ISO 26262

Part 11: Guideline on application of ISO26262 to semiconductors

Part 12: Adaptation of ISO26262 for motorcycles

Part 2: Safety Management

- Safety Lifecycle
- Safety Culture
- Competence Management
- Quality Management
- Tailoring



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 archtectural design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

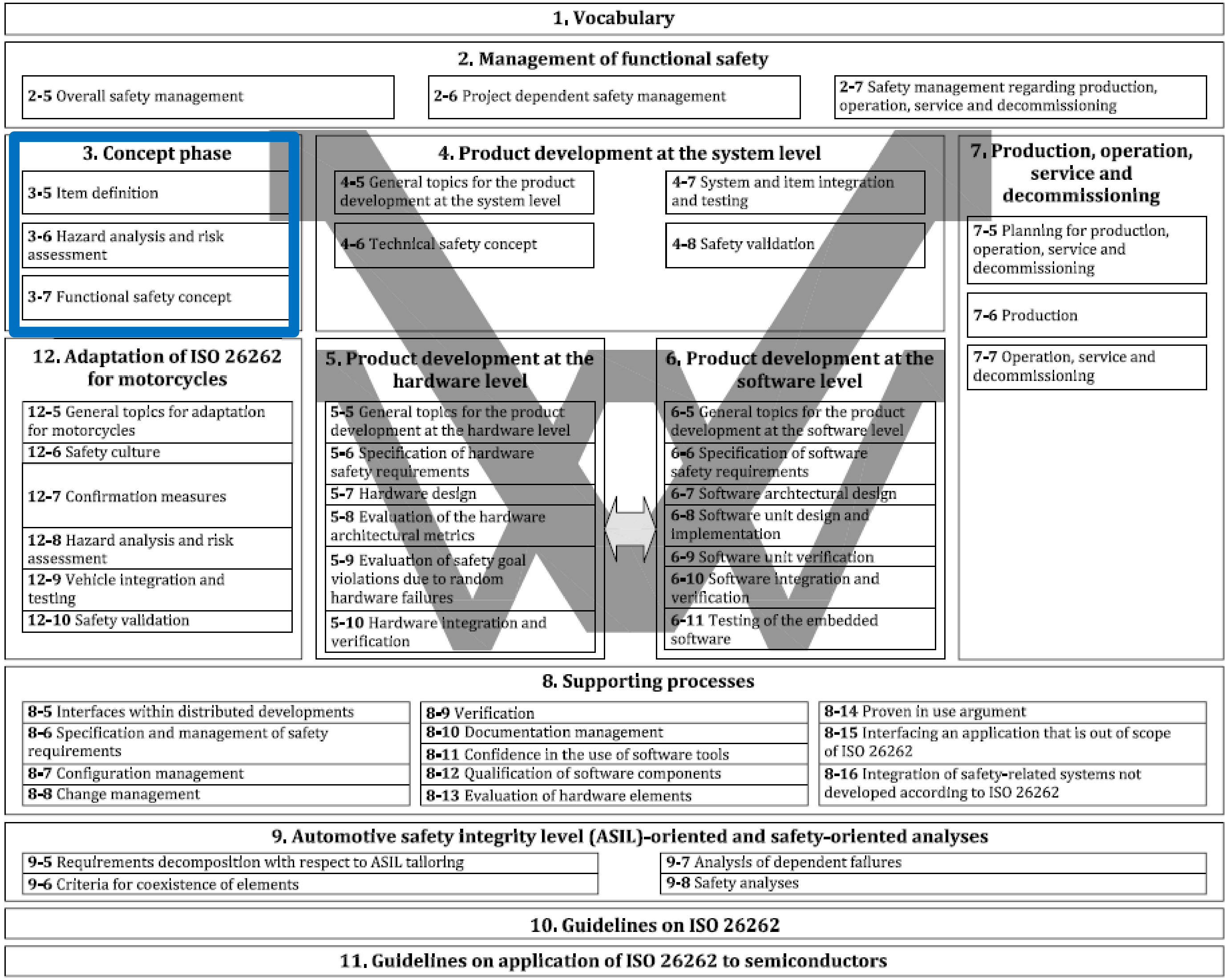
10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 3: Concept Phase

Car OEM / Tier1

- Item definition
- HARA
- FSC



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 archtectural design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

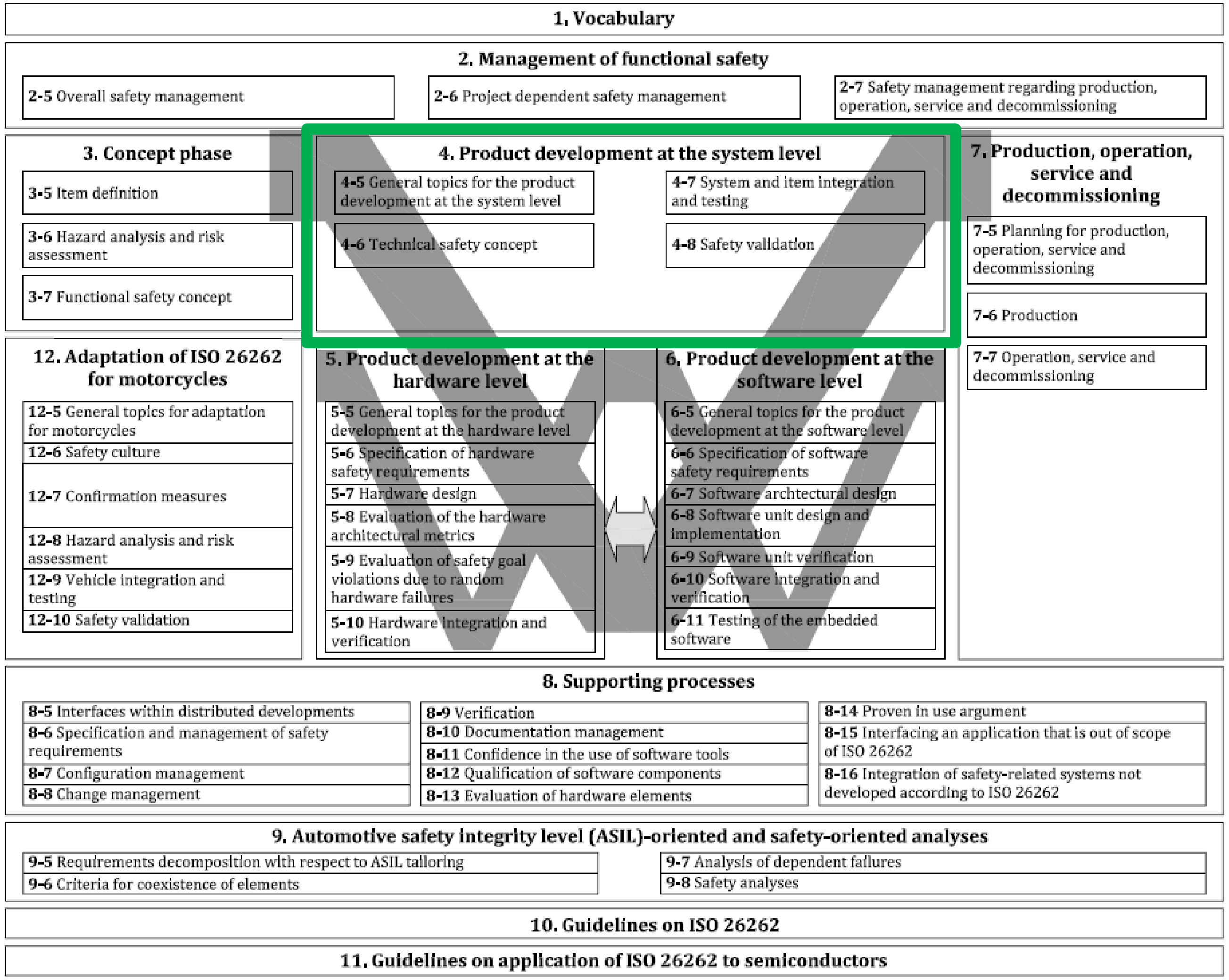
10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 4: Product Development at the System Level

Car OEM / Tier1

- Technical Safety Requirements
- System Architectural Design
- Technical Safety Concept



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 risk 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
4-7 System and item integration and testing
4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles
12-5 General topics for adaptation for motorcycles
12-6 Safety culture
12-7 Confirmation measures
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 violations 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 archtectural design
6-8 Software unit design and implementation
6-9 Software unit verification
6-10 Software integration and verification
6-11 Testing 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 management
8-11 Confidence in the use 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. 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

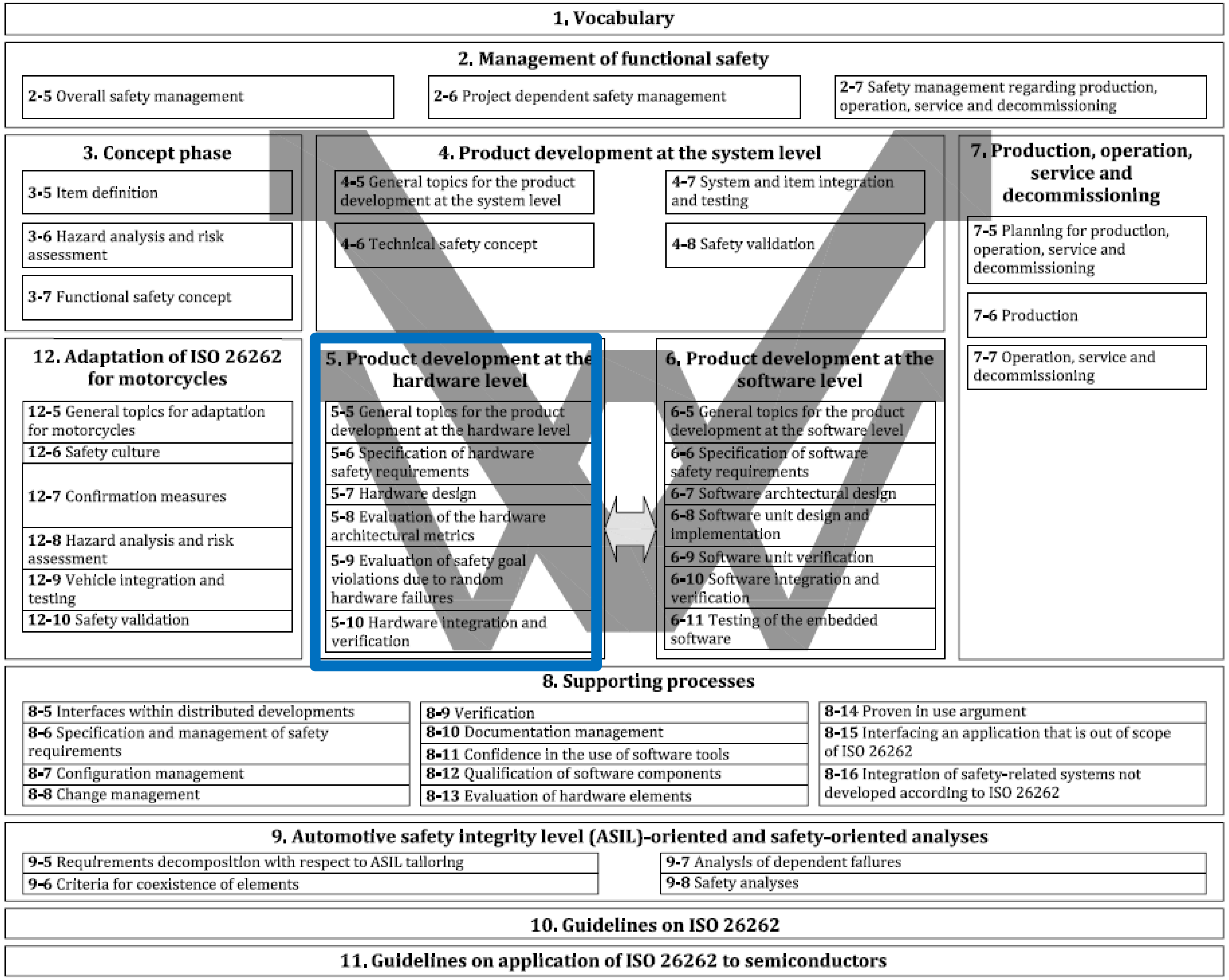
10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 5: Product development at the hardware level

NXP

- HW Safety Requirements
- HW Architecture Design
- HW Metrics
- HW Verification



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

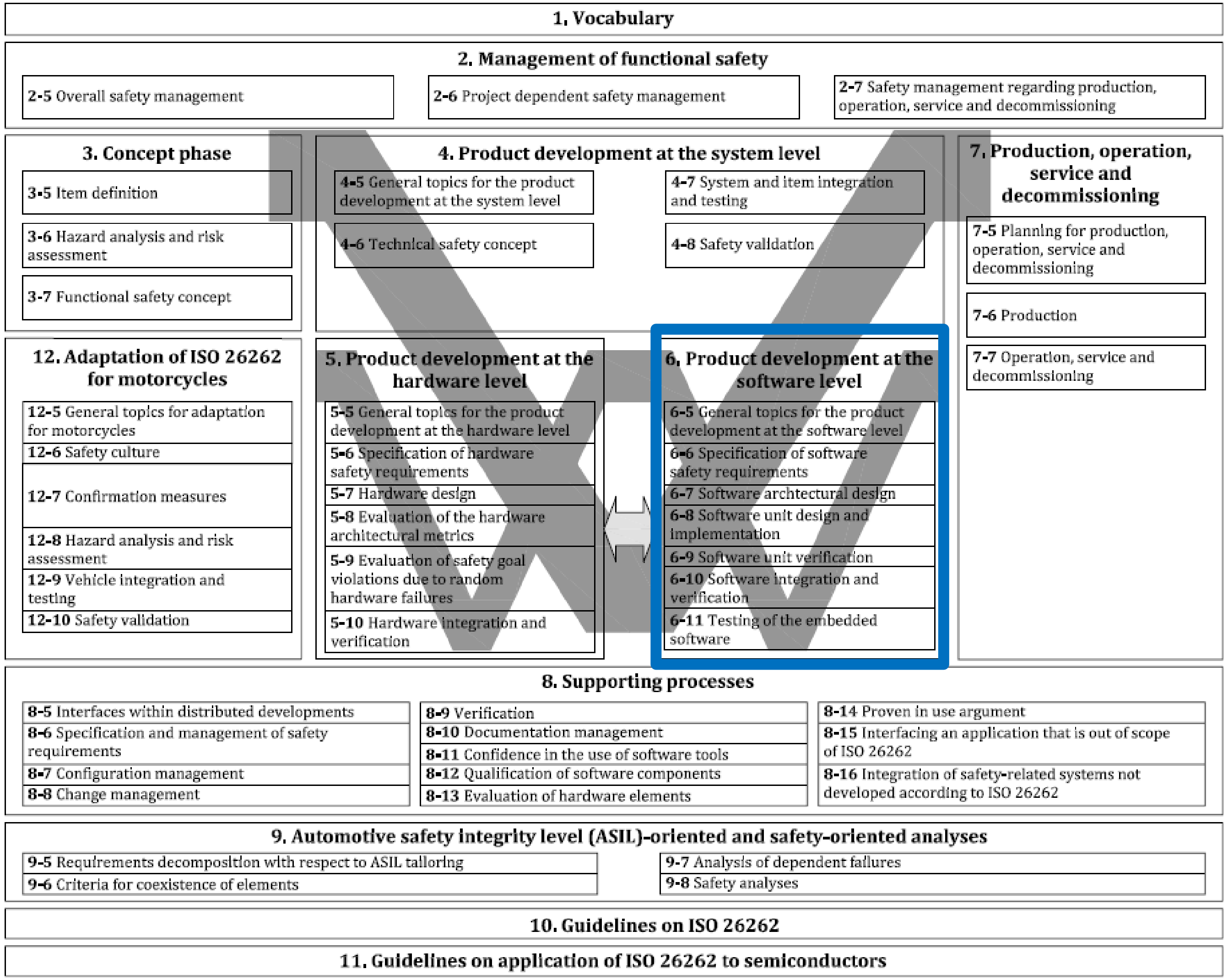
10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

NXP

Part 6: Product development at the software level

- SW Safety Requirements
- SW Architecture Design
- SW Verification



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

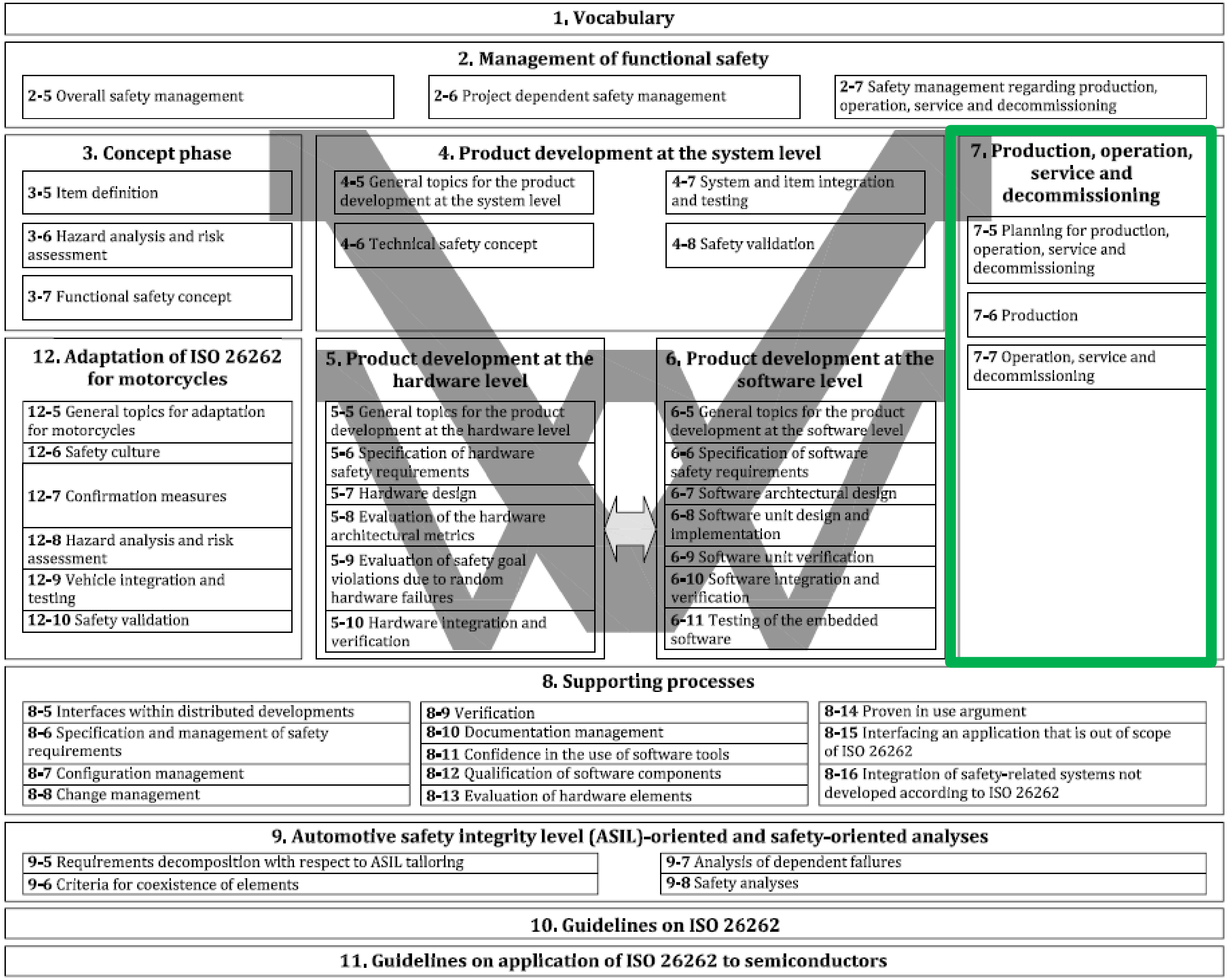
10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 7: Production, operation, service and decommissioning

- Change management

- Field monitoring



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 archtectural design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

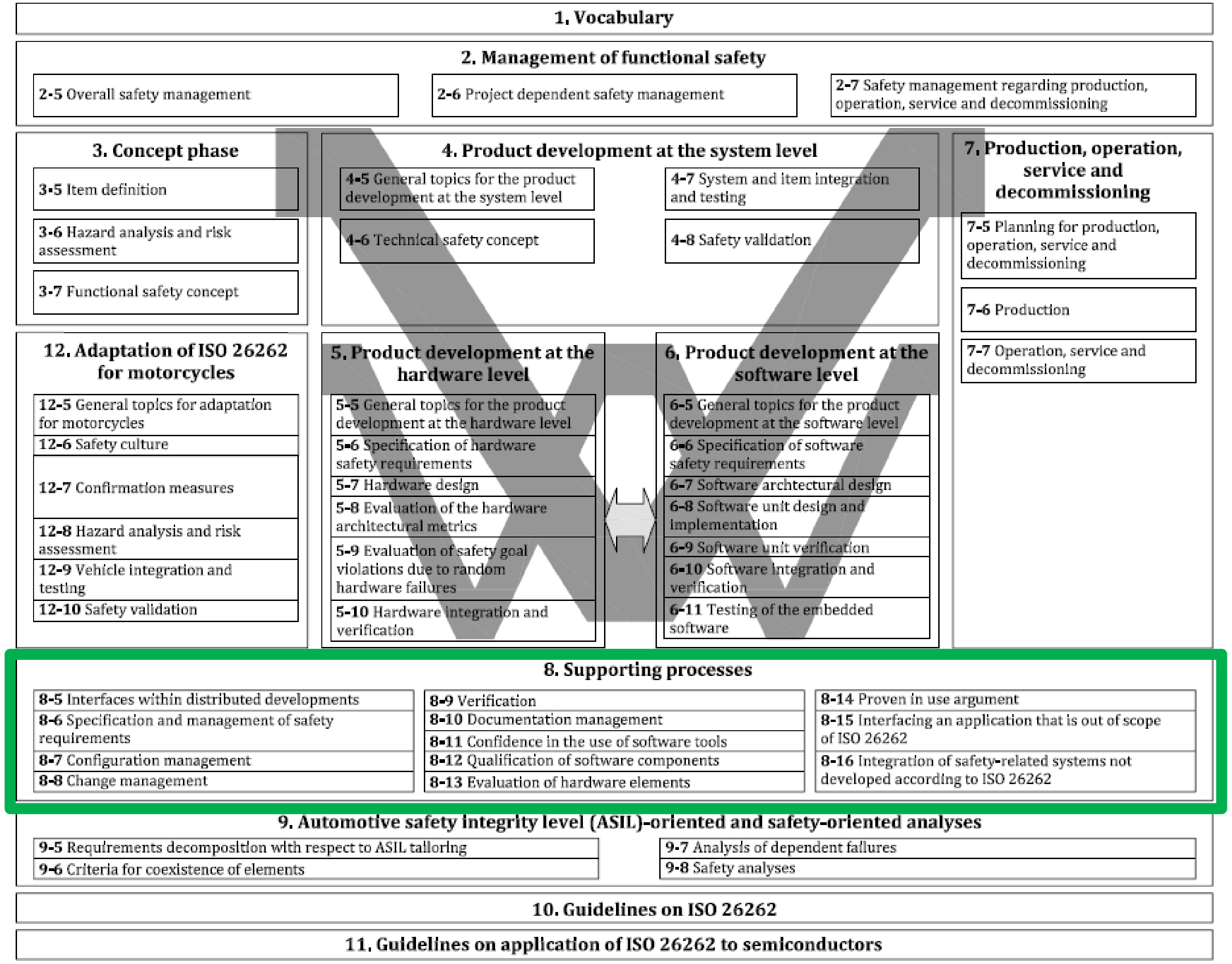
9-8 Safety analyses

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 8: Supporting Processes

- Requirements Management
- Change/Config/Doc Management
- Distributed Development
- SW Tools
- Verification & Validation



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 risk 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
- 4-7 System and item integration and testing
- 4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles
- 12-5 General topics for adaptation for motorcycles
- 12-6 Safety culture
- 12-7 Confirmation measures
- 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 violations 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 archtectural design
- 6-8 Software unit design and implementation
- 6-9 Software unit verification
- 6-10 Software integration and verification
- 6-11 Testing 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 management
- 8-11 Confidence in the use 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

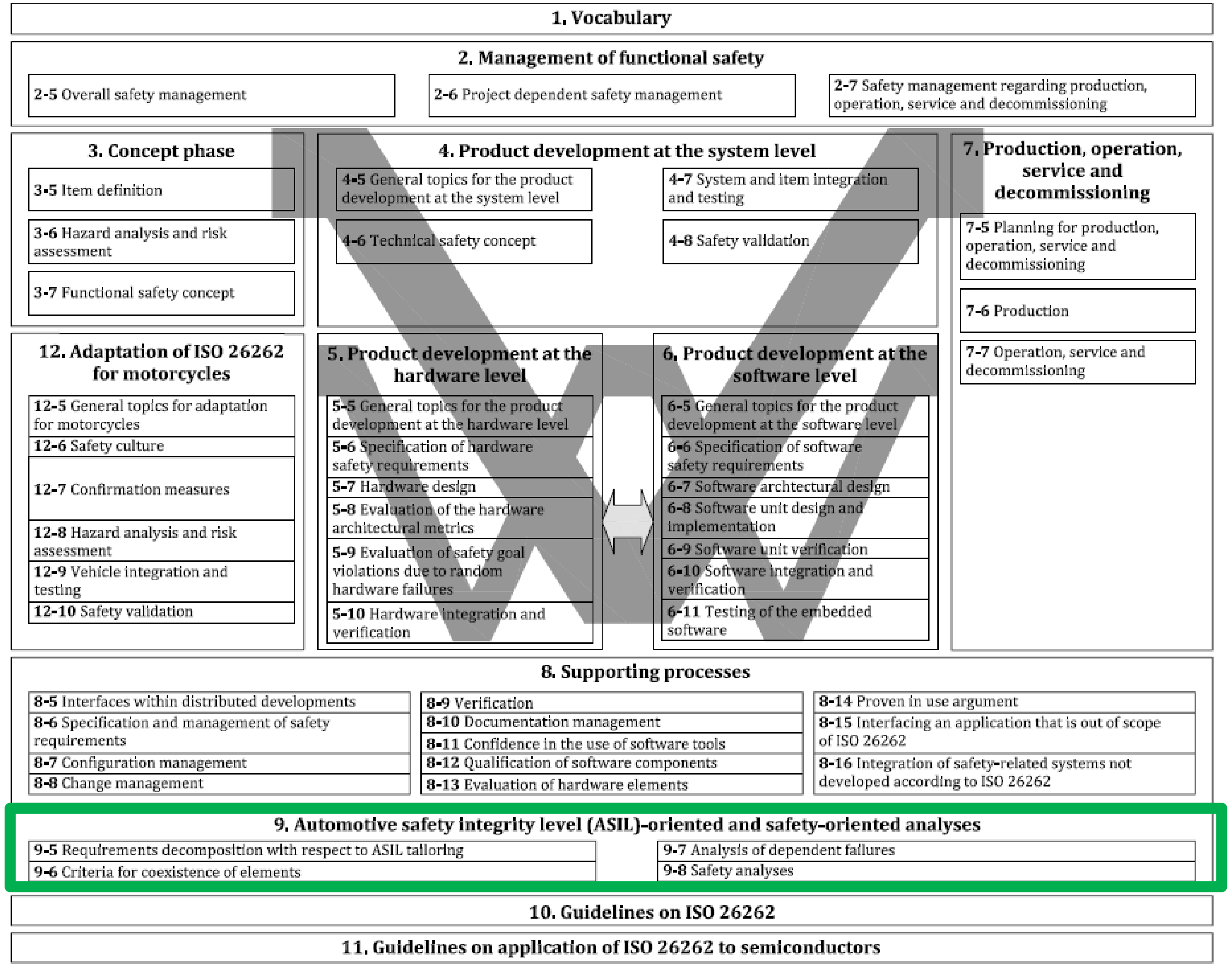
9. Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses
- 9-5 Requirements decomposition with respect to ASIL tailoring
- 9-6 Criteria for coexistence of elements
- 9-7 Analysis of dependent failures
- 9-8 Safety analyses

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 9: Automotive safety integrity level (ASIL) – oriented and safety oriented analysis

- FMEA, FMEDA, FTA, DFA
- ASIL decomposition



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 risk 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

4-7 System and item integration and testing

4-8 Safety validation

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. Adaptation of ISO 26262 for motorcycles

12-5 General topics for adaptation for motorcycles

12-6 Safety culture

12-7 Confirmation measures

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 violations 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 archtectural design

6-8 Software unit design and implementation

6-9 Software unit verification

6-10 Software integration and verification

6-11 Testing 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 management

8-11 Confidence in the use 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. 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

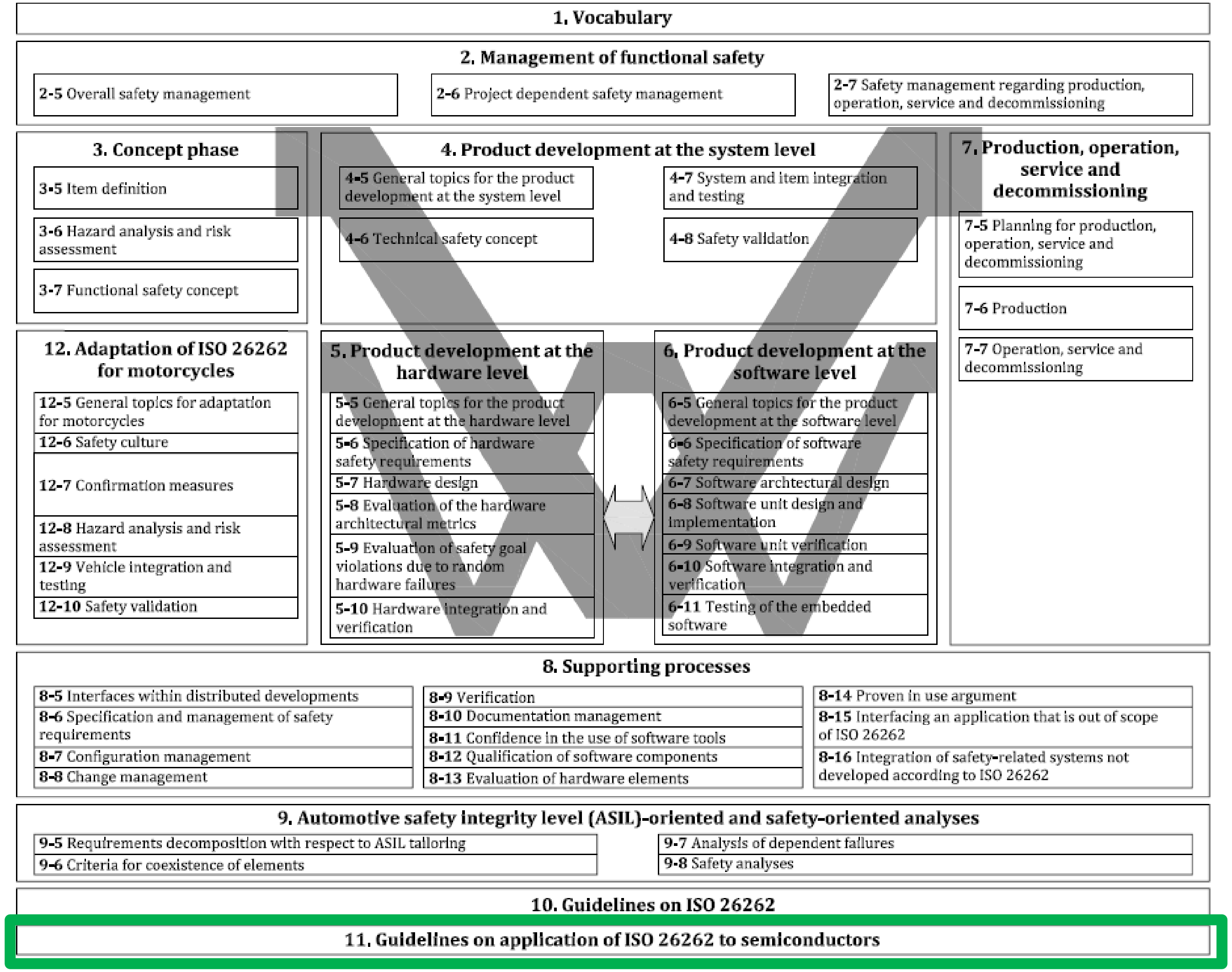
9-7 Analysis of dependent failures

9-8 Safety analyses

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Part 11: Guidelines on application of ISO26262 to semiconductors



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 risk 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
- **4-7** System and item integration and testing
- **4-8** Safety validation

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. Adaptation of ISO 26262 for motorcycles

- **12-5** General topics for adaptation for motorcycles
- **12-6** Safety culture
- **12-7** Confirmation measures
- **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 violations 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 design
- **6-8** Software unit design and implementation
- **6-9** Software unit verification
- **6-10** Software integration and verification
- **6-11** Testing 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 management
- **8-11** Confidence in the use 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. 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

10. Guidelines on ISO 26262

11. Guidelines on application of ISO 26262 to semiconductors

Conclusion

- Functional safety is part of the overall Safety
- Functional safety is about RISK assessment, prevention, protection
- Car OEMs set risk of HAZARD and SAFETY GOALS at System Level
- There are market driven reasons that mean that functional safety is a requirement for the future of EVERY safety related automotive development
- ISO 26262 process and ASIL definition provide the FRAMEWORK and EVIDENCES to demonstrate that safety objectives are met

SECURE CONNECTIONS
FOR A SMARTER WORLD