VECTOR

Functional Safety with ISO 26262 Webinar

Dr. Arnulf Braatz, October 10th 2018

Functional Safety with ISO 26262

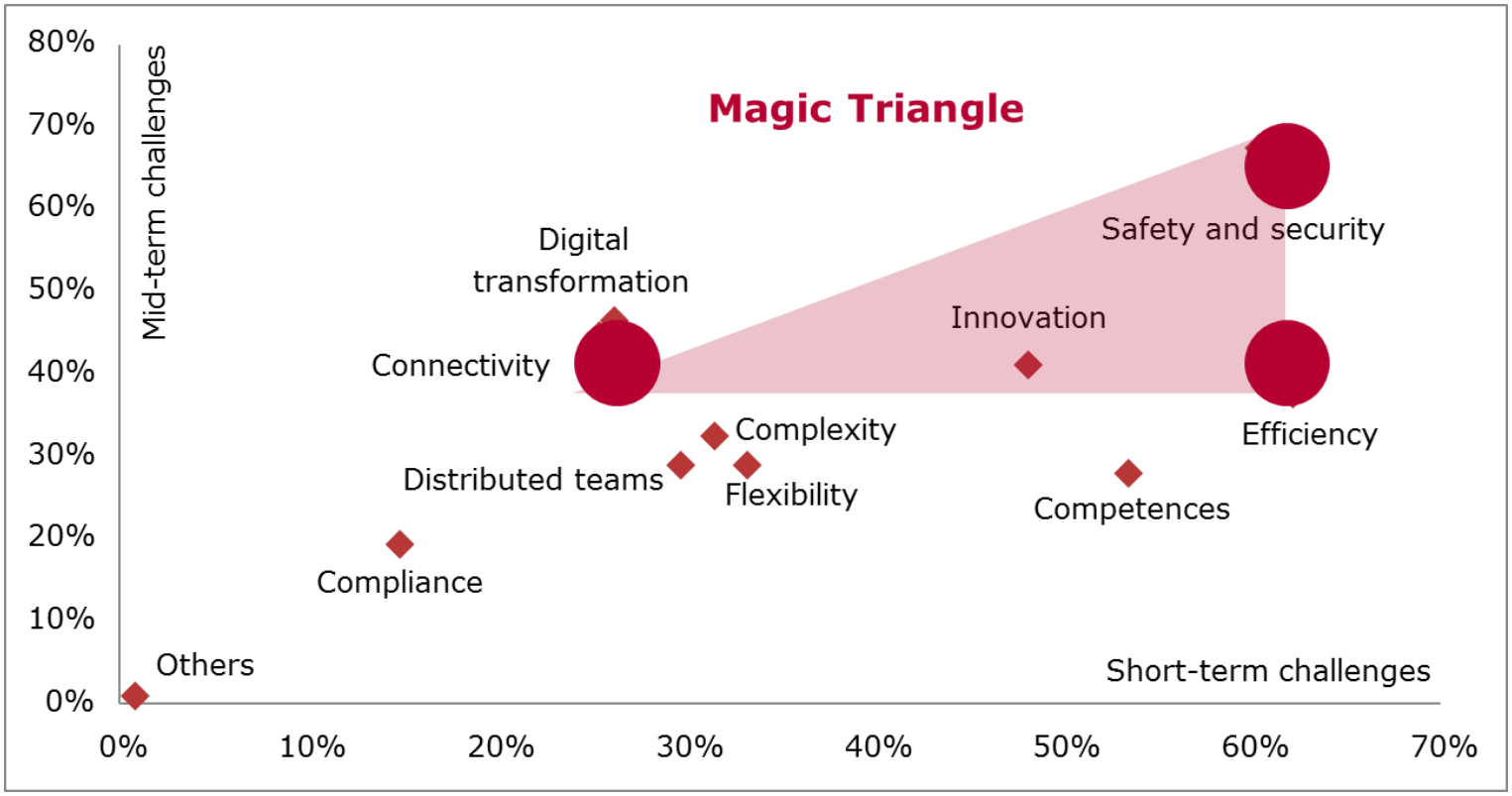
Webinar
Speaker: Dr Arnulf Braatz
Q&A: Andreas Horn

Technical Notes

- **Audio**
  There should be music to hear.
  If the audio transmission over the Internet is not working, ask for the participation in a conference call.
  Contact the "host" in the "chat" window.
- **Screen**
  Disable your screen saver.
- **Feedback & communication**
  Open and review the "chat" window to get all organizational messages of the "hosts".
  Use the "chat" window to the "host" to contact all organizational WebEx and transfer requests or disturbances.
  Use the "Q & A" window instead of the "chat" window for substantive questions about the webinar.
  Ask your questions at "All Panelists". Questions are answered online during and after the presentation.
- **Slides & Presentation**
  Within 1-2 days after the webinar, you will receive a link to the slides and additional information.
  After the webinar a link will guide you to a feedback form.
  We are looking forward to receiving your feedback to continuously improve our services.

Vector Worldwide

We Implement the Solutions to Your Current Challenges



Vector Client Survey 2018. Details: www.vector.com/trends. Horizontal axis shows short-term challenges; vertical axis shows mid-term challenges. Sum > 200% due to 5 answers per question. Strong validity with >4% response rate of 2000 recipients from different industries worldwide.

Vector provides tailored consulting solutions for Your challenges
Cost and Efficiency – Quality – Innovation

Agenda

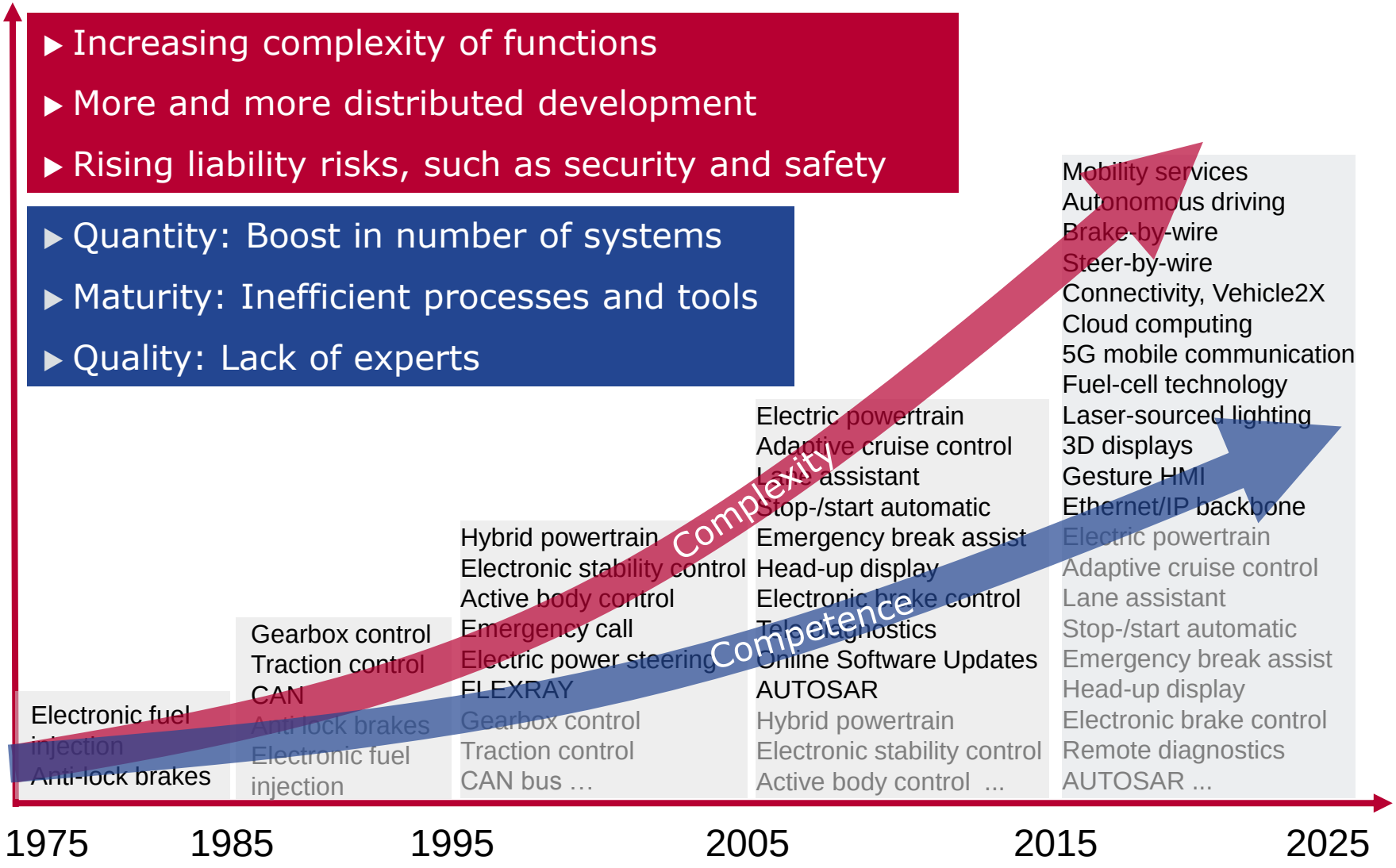
- Welcome
- Welcome and Introduction
- **Challenges and Concepts**
- Vector Safety Experiences
- Conclusions and Outlook

VECTOR

Functional Safety Challenge: Complexity and Competences

- Increasing complexity of functions
- More and more distributed development
- Rising liability risks, such as security and safety

- Quantity: Boost in number of systems
- Maturity: Inefficient processes and tools
- Quality: Lack of experts



VECTOR

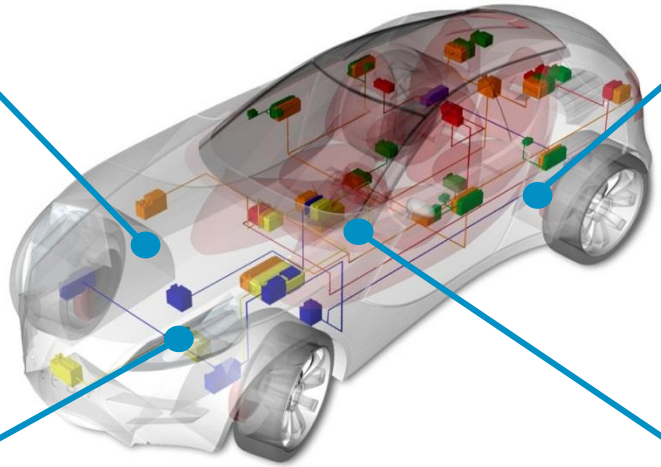
Functional Safety – Broad Exposure

ESP

Unintended, single-sided brake effect on straight lane

Electronic Park Brake

Unintended activation in motion



Collision Avoidance

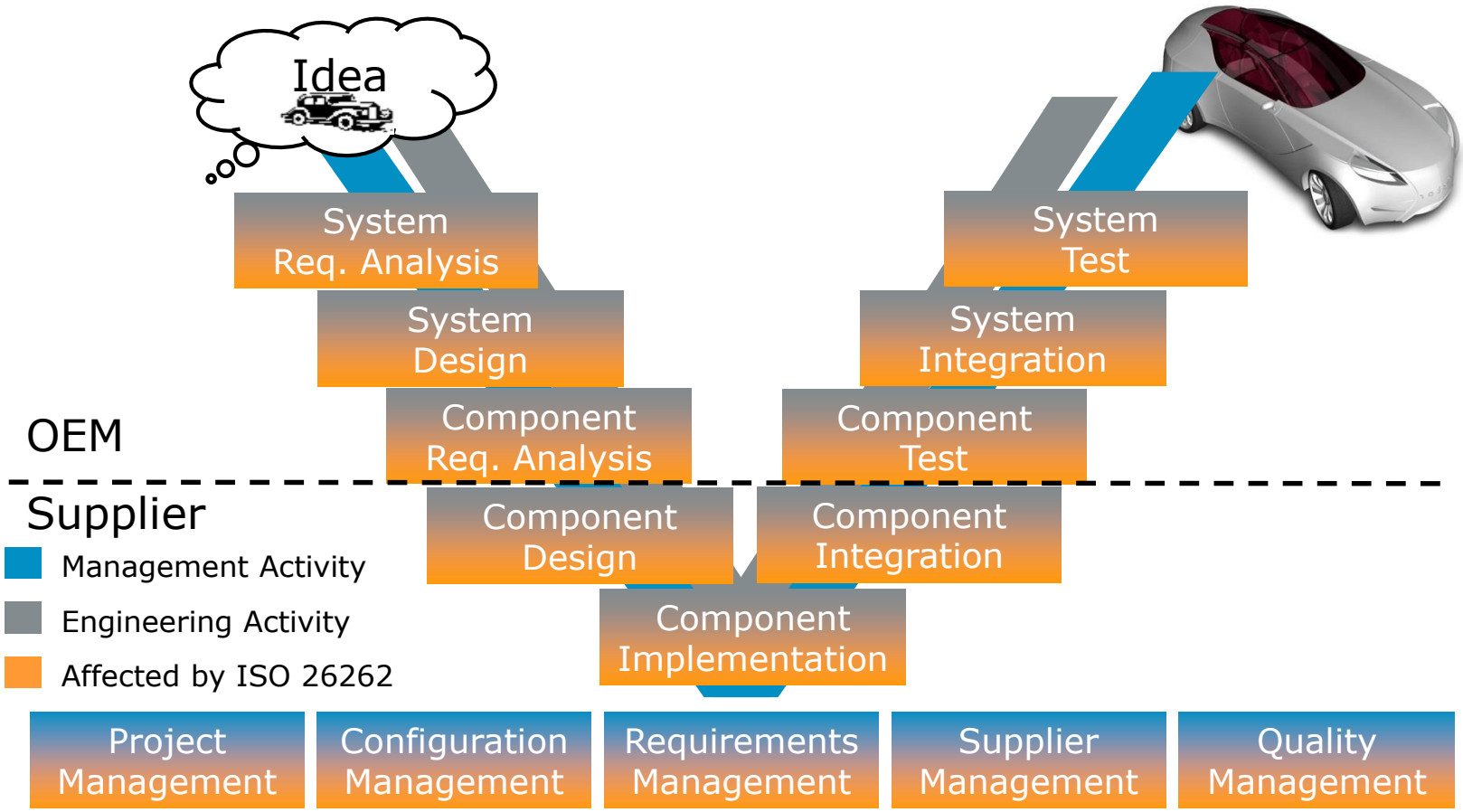
Acceleration instead of deceleration in traffic

Airbag

Delayed deployment after crash detection

Exposure of practically all E/E functions ➔ Risk of liability

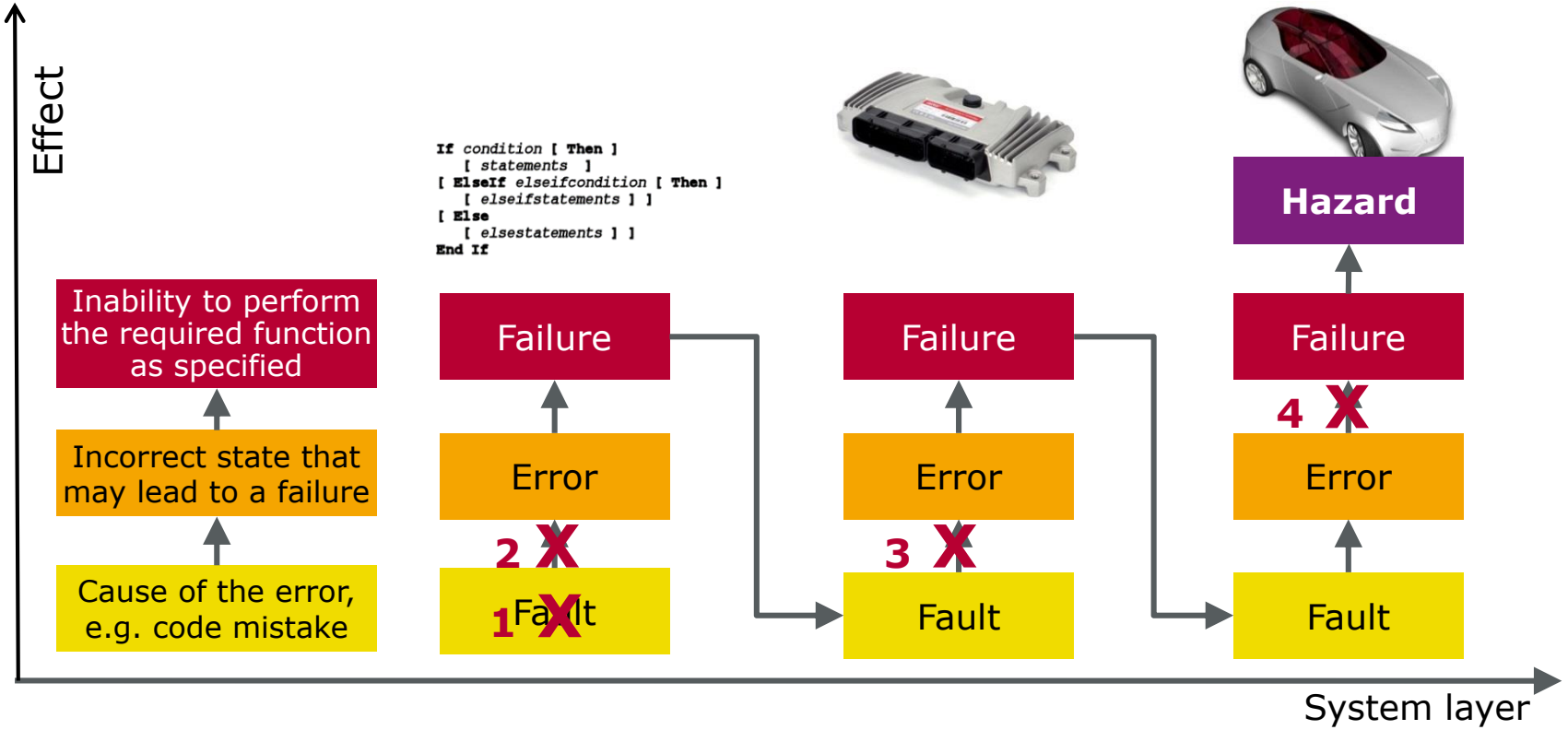
Functional Safety – Wide Impact



Wide impact on entire life-cycle ➔ Risk of gaps and inconsistencies

VECTOR

Functional Safety – Many Methods



1 Fault prevention
- Guidelines
- Processes

2 Fault detection
- Code analysis
- Review, Test

3 Fault tolerance
- Redundant design
- Memory protection

4 Robustness
- Redundant shut-off
- Fail-operational

Many methods and techniques ➔ Risk of uninformed usage

Functional Safety – Complex Standard

10 Parts

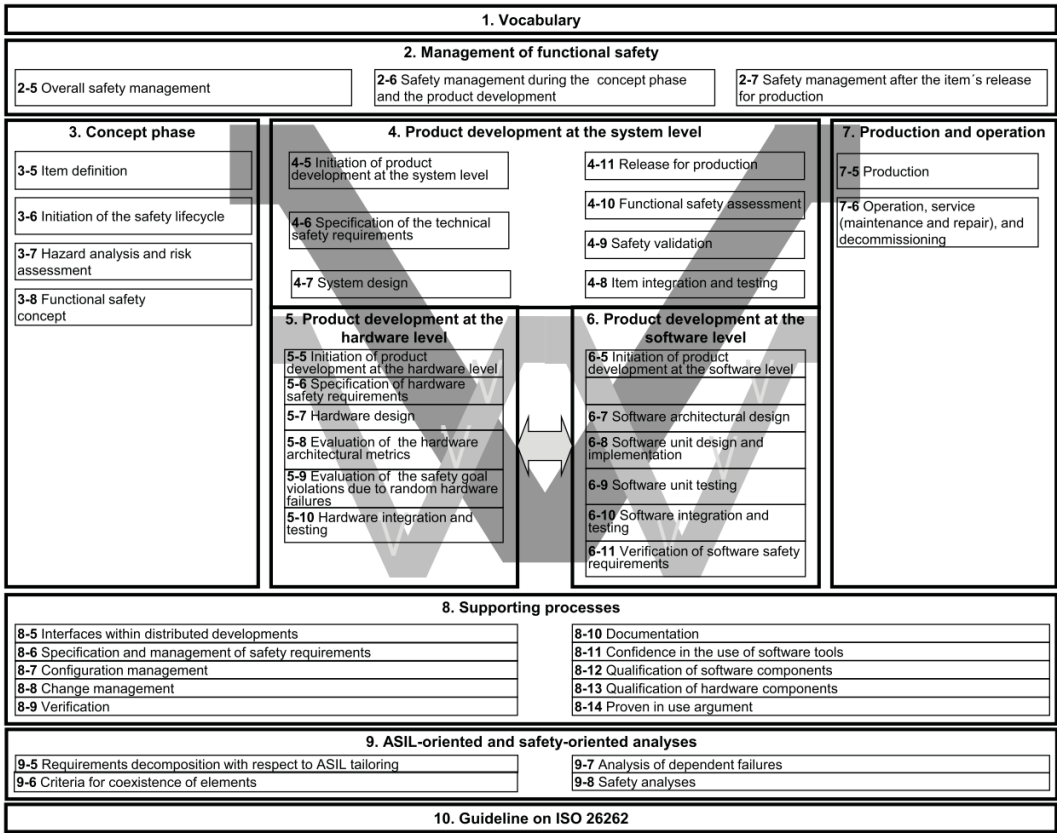
43 Chapters

100 work products

180 engineering methods

500 pages

600 requirements



Source: ISO 26262

Complex standard ➔ Risk of overheads and bureaucracy

VECTOR

Parts of ISO 26262 – 2nd Edition (Q3 of 2018) – Main Changes

ISO/PRF PAS 21448 Road vehicles -- Safety of the intended functionality

1. Vocabulary

2. Management of functional safety

3. Concept phase

4. Product development at the **system level**

5. Product development at the **hardware level**

6. Product development at the **software level**

7. Production and operation

12. Adaption of ISO 26262 for motorcycles

Currently published as:
ISO PAS 19695
Motorcycles

Currently published as:
ISO PAS 19451
-1: Application of Concepts
-2: Application of HW Qualification

8. Supporting processes

8-13 to 8-16

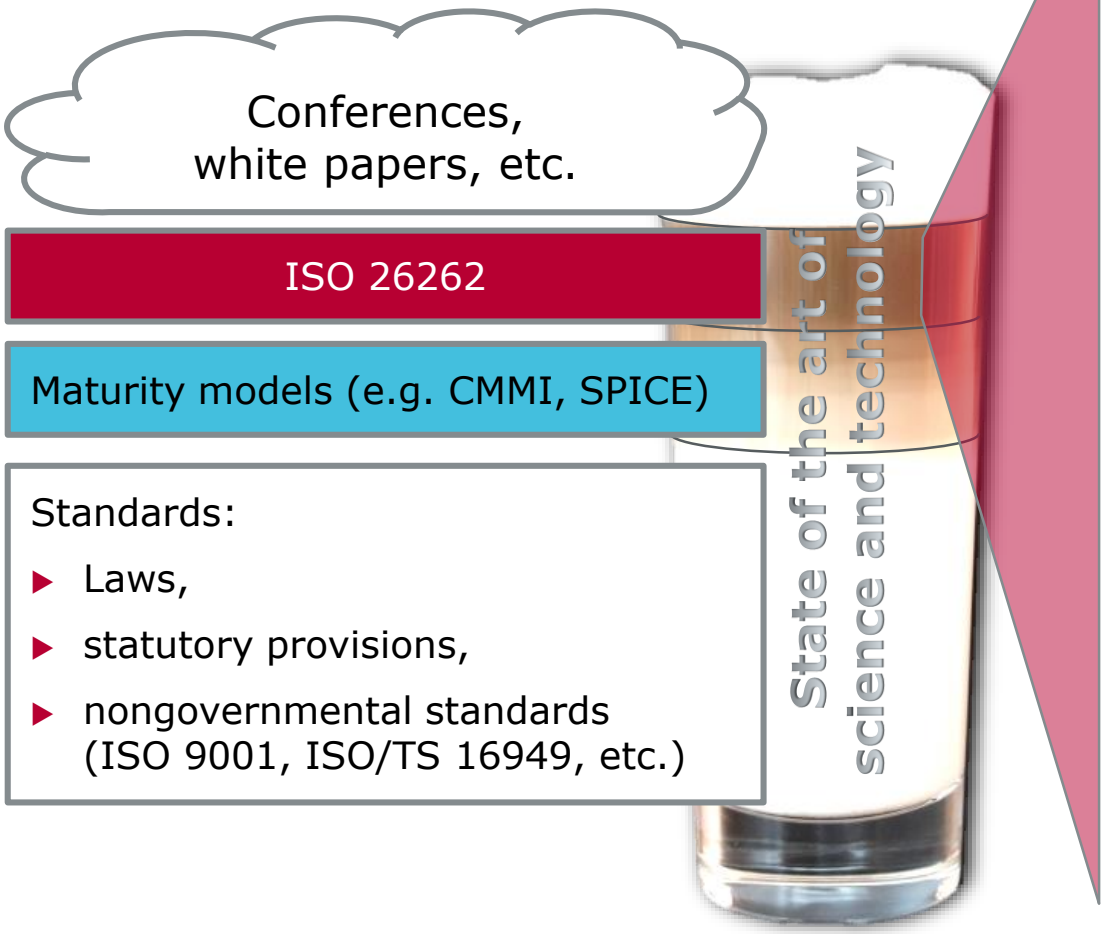
9. ASIL-oriented and safety-oriented analyses

10. Guideline on ISO 26262

11. Application of ISO 26262 to semiconductor

VECTOR

Legal Liability: State of the art of science and technology



Process

- Safety Management
- Project Management
- Risk Management
- Quality Assurance
- Requirements-Mgmt.
- Configuration-Mgmt.
- Test Management
- …

Technology

- Measures against random HW failures
- Measures against systematic failures (System, HW, SW)
- Development of safety concepts
- Implementation of safety mechanisms
- …

Methods

- FMEA,FTA
- FMEDA
- Analysis of dependent failures
- ASIL decomposition
- …

Basic Concept of ISO 26262: Risk Classification by „ASIL“

Risk = Severity x Probability

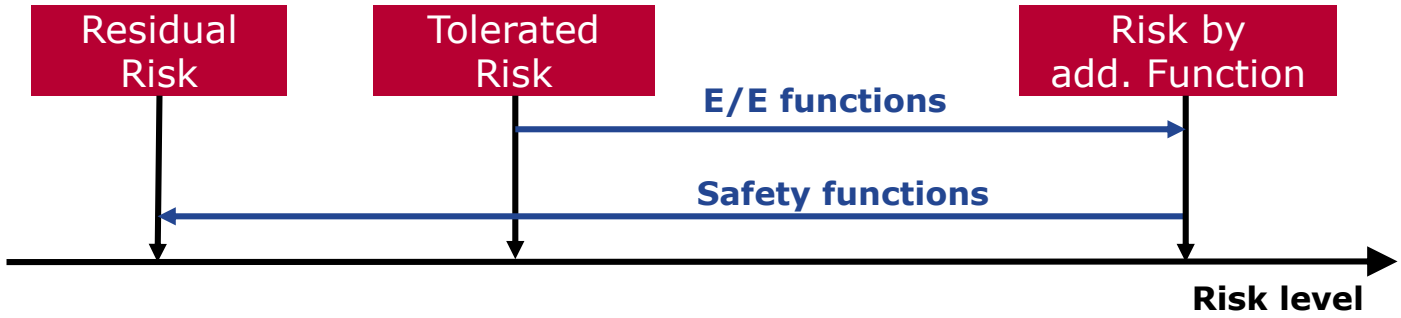
$$R = S \times P_E \times P_C \times P_I$$

ASIL

Automotive **S**afety **I**ntegrity **L**evel

(= required integrity of a function)

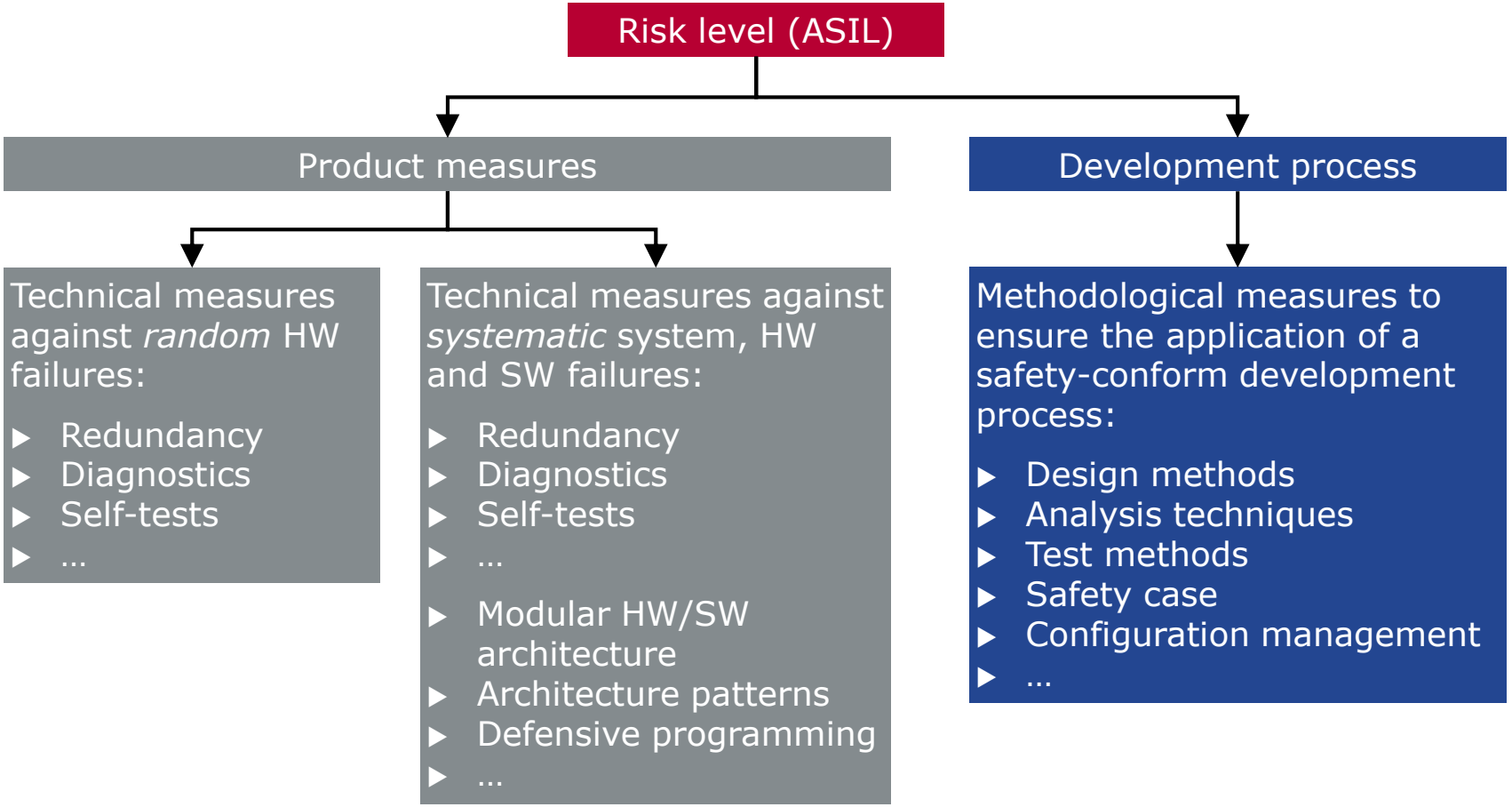
S: Severity
E: Exposure
C: Controllability
I: necessary Integrity



Source: IEC 61508:2010

VECTOR

Approaches to Risk Reduction



ASIL = Automotive Safety Integrity Level

Goals: Avoid failures – Make unavoidable failures safe

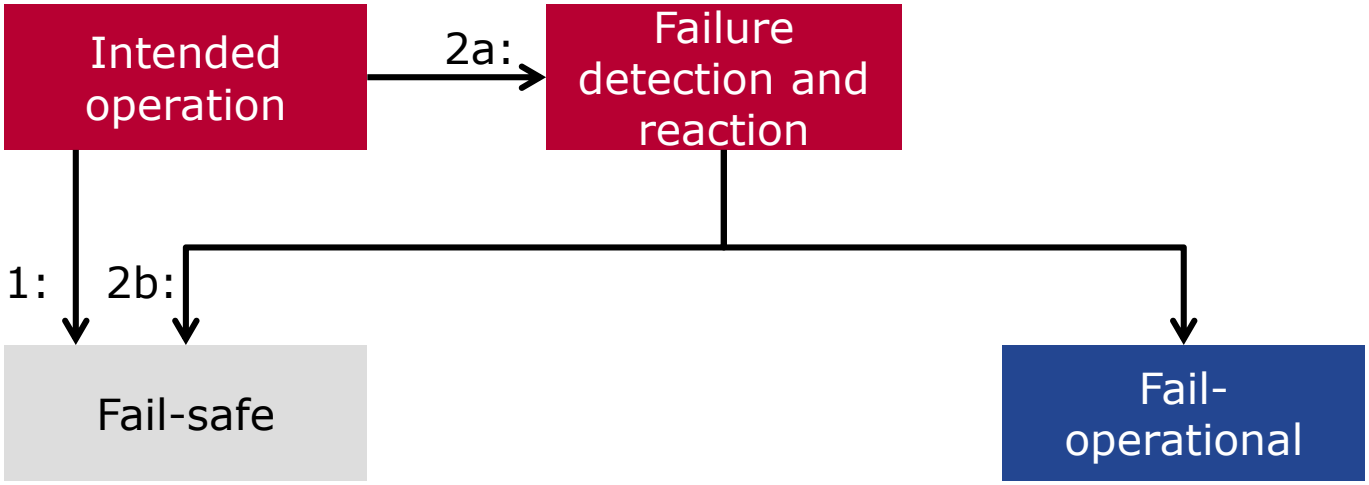
VECTOR

Development – HARA for deriving Safety Goals and ASIL

Failure Mode	Vehicle State	Road Condition	Environment Condition	E	C	S	ASIL
No Braking Effect	> 100 km/h	Wet	Highway	E3	C3	S3	C
Unexpected Braking Effect	> 50 km/h < 100 km/h	Dry	Main Road	E4	C2	S3	C
Asymmetric Braking Effect	Parking < 10 km/h	Dry	Side Road	E4	C2	S1	A

- Exposure:
  - E3: 1-10% of average operating time
  - E4: >10% of average operation time
- Controllability (Average Driver):
  - C2: Hazardous situation is usually controllable
  - C3: Hazardous situation is usually not controllable
- Severity:
  - S1: Light to moderate injuries
  - S3: Critical injuries

Fail-safe vs. Fail-operational

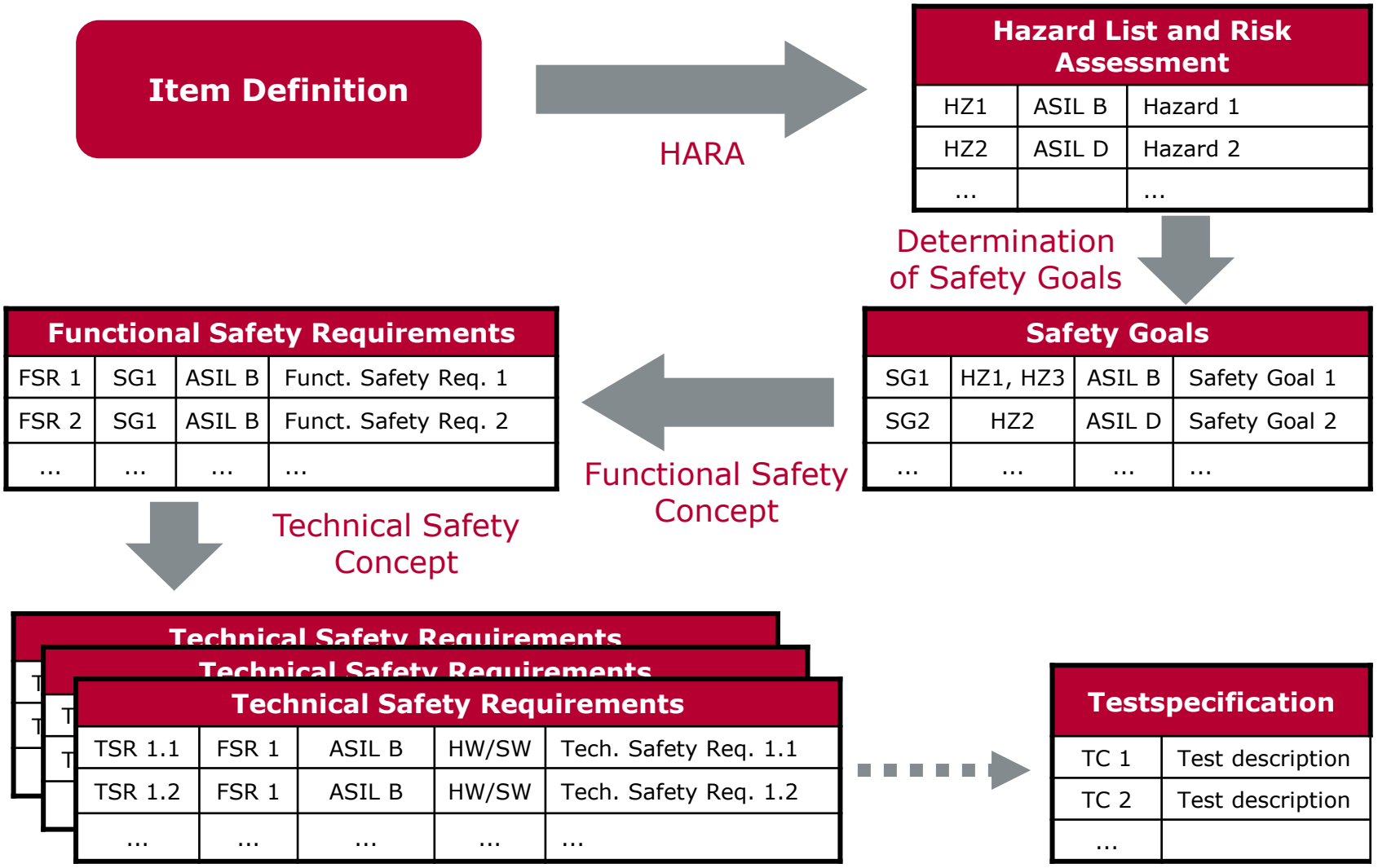


- Bring the system into the fail-safe state to avoid any hazard.
- Two approaches:
  1. Fail-safe by design (default)
  2. Failure mitigation and transition to fail-safe state
- Sufficient for most "classic" automotive systems, often with mechanical back-up

- System remains operational
- E.g. degraded - but safe - operation mode.
- Availability of elements assuring the required safety
- Diverse / redundant architecture
- Required for continuous and automated safe operation

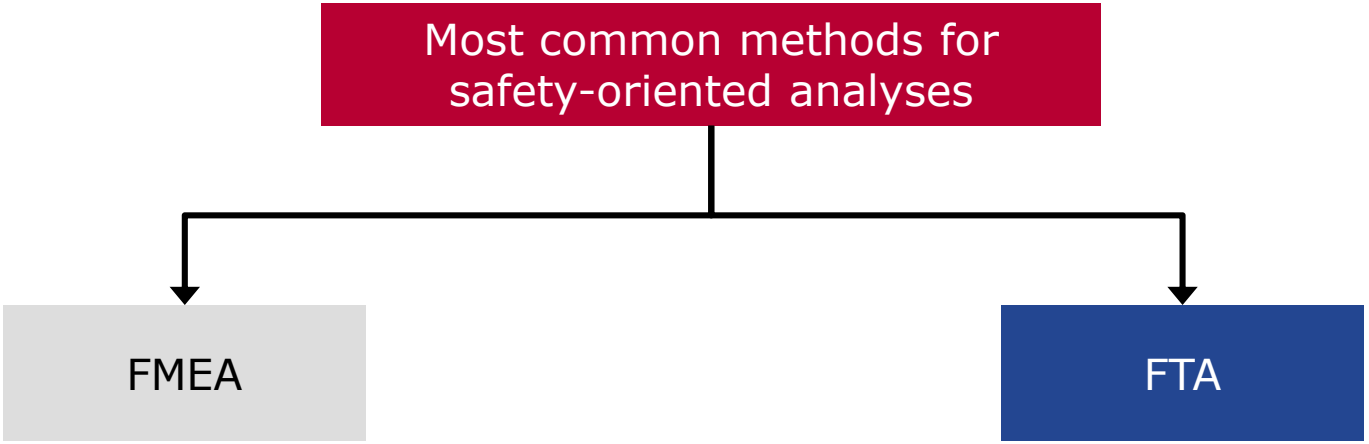
The safety related system has always to be in one safe state!

Efficient Traceability and Consistency



VECTOR

FMEA and FTA – Safety Analysis on System and HW level



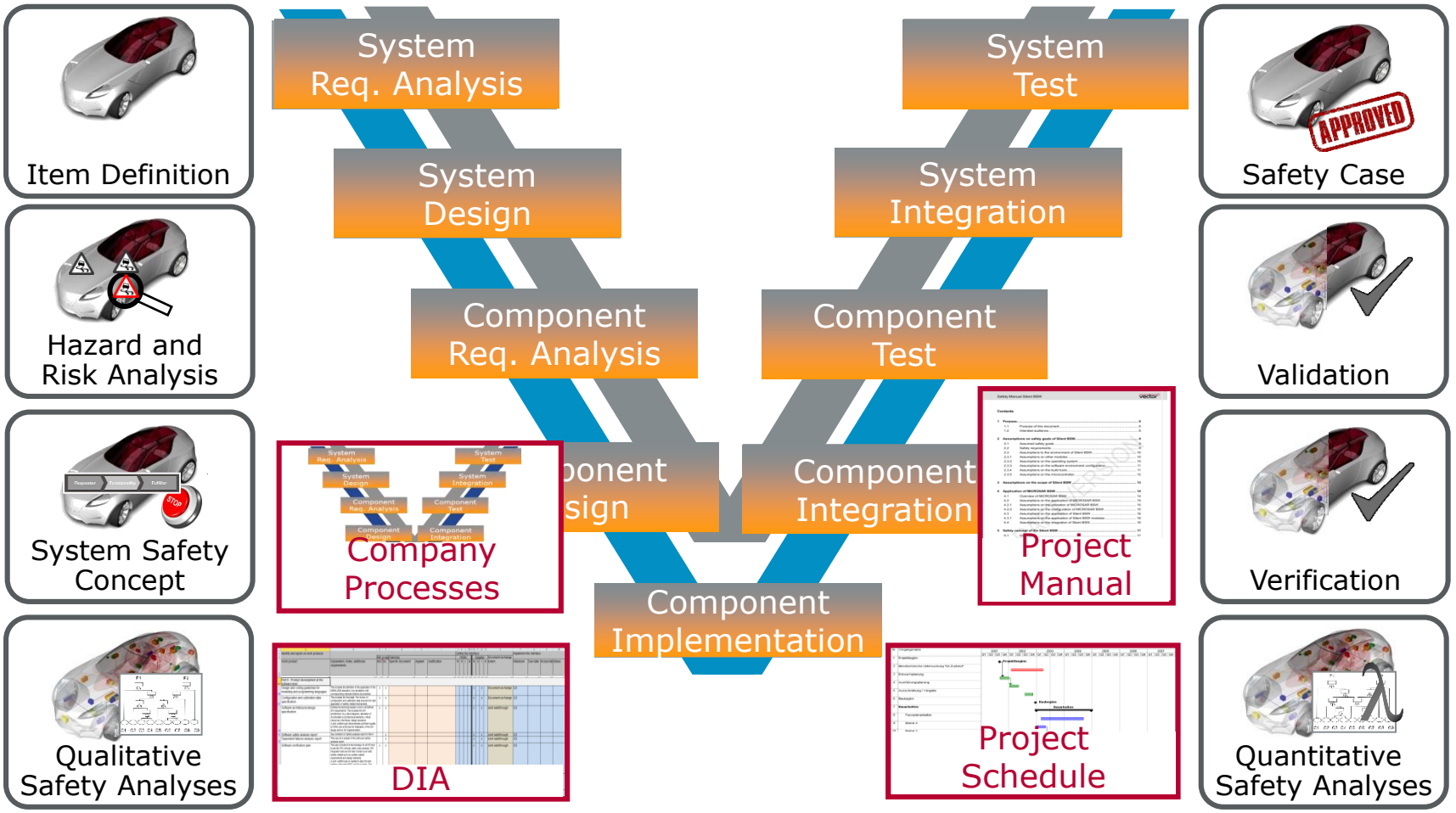
- = Failure Mode Effect Analysis
- **Inductive** analysis method
- Used to identify **root causes** of failures and **effects** of failures in the system.
- Can only be applied to an existing design or implementation.

- = Fault Tree Analysis
- **Deductive** analysis method
- Used to identify **root causes** of failures and their **correlation** in the system.
- Development of design alternatives
- Discovery of unexpected scenarios

Agenda

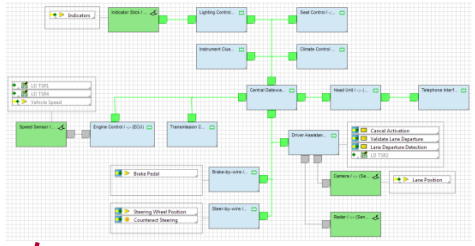
- Welcome
- Welcome and Introduction
- Challenges and Concepts
- **Vector Safety Experiences**
- Conclusions and Outlook

Vector Experiences – Support Throughout the Life-Cycle

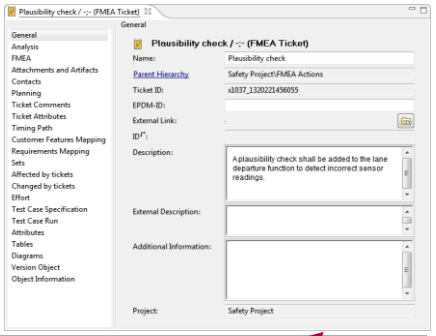


Consistently plan and systematically maintain safety artefacts

Vector Experiences – Systematic Analysis and Design



TP.2.2.4.2	*Safety goals*	
LD1-SG.1	*Defect LD Faults*	All actions taken by the lane departure system shall be vali lane departure system shall be forced into a safe, inactive system is no longer active.
LD1-SG.2	*Counteract LD Activation*	The driver shall be able to cancel the lane departure warnir angle or by applying the brakes...
LD1-SG.3	*Limit Counter Steering*	The angle of counter steering that can be applied shall be l
LD1-SG.4	*Limit Asymmetric Braking*	The amount of the assymmetric braking force that can be a than YYY N.
LD1-SG.5	*Detect Lane Departure*	A lane departure shall be detected with a certainty equivale



*Lane Departure::Lane Departure FMEA

No.	FMEA Part	Design Intent	Failure Mode	Failure Effects	SEV	Class	Cause	OCC	Prevention Measures	Detection Measures	DET	RPN	Rec. Actions	Responsible	Target Date
1	Speed Sensor	Deliver speed data The speed sensor is used to deliver data used to determine the activation conditions of the lane departure warning.	Stuck at The sensor continuously delivers the same speed reading.	Falsely activated The lane departure system is activated when it shouldn't be.	9	YC	Hardware failure Stuck at fault due to hardware failure internal to the sensor.	5	The speed sensor is currently qualified to ASIL A	None defined as yet.	10	450	Plausibility check A plausibility check shall be added to the lane departure function to detect incorrect sensor readings.	Metzker	Nov 30, 2011
2			Shortcut to ground Shortcut to ground	No activation Lane departure is not activated	6	YS	Internal hardware fa... Stuck at fault to hardware	5	The speed sensor is currenlty qualified to ASIL A	None defined as yet.	10	300	Plausibility check A plausibility check shall be	Metzker	Nov 30, 2011
				actual ... speed.											
5	Camera	Provide lane position d...	No data The camera delivers no picture at all	Departure not dete... A departure from the lane cannot be detected.	7	YS	Camera obscured For example due to dirt or water on the windscreen.	5	Camera is placed behind the windscreen in an area that is regularly cleaned by the wash/wiper system.	The DSP software used to calculate lane position determines picture quality. If insufficient an error is signalled.	2	70			

Support by Vector Consulting Services and PREEvision tool:

- Single source for item definition, based on features, requirements, operating scenarios, dependencies
- Model-based design of functional and technical safety concept, including ASIL decomposition and requirements based tests

Vector Experiences – Including the Customer and Supplier

- Often insufficient information shared between OEM and Tier-1 supplier and Tier-1 and Tier-2 suppliers concerning safety-critical functions and related hazards
- Risk that system and component design is not optimized to balance safety and costs
- Our experience shows that companies which tried more intense supplier-collaboration, continue to do so for all critical interfaces

Perform joint workshops on requirements & design and apply DIA

Vector Experiences – Development Interface Agreement (DIA)

List of relevant artefacts

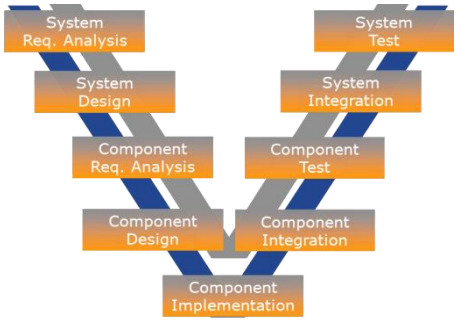
Minimum scope: ~ 60 artefacts

Project specific tailoring, application and tracking

	A	D	E	F	G	H	I	J	K	L	M	O	P	Q	R	S	T	U	V	W
1	Identify and agree on work products							Define the interface									Implement the interface			
2			Min scope		Tailoring			OEM				Supplier				Document exchange				
3	Work product	Explanation, Notes, additional requirements	NSC	SC	Specific document	Applied	Justification	R	S	I	A	R	S	I	A	Extent	Milestone	Due date	Actual date	Status
65	Part 6 - Product development at the software level																			
66	Design and coding guidelines for modelling and programming languages	This includes the definition of the application of the MISRA:2004 standard. Any deviations with corresponding rationale shall be documented.	x	x								x		x		Document exchange	G3			
67	Configuration and calibration data specification	This includes the final data. The review of configuration and calibration data ensures the right application of safety related mechanisms.	x	x								x		x		Document exchange	G3			
70	Software architectural design specification	Defines the technical solution which will fulfill all SW requirements. This includes the SW architecture (e.g. block diagram), allocation of functionality to architectural elements, critical resources, interfaces, design decisions A joint walkthrough demonstrates sufficient quality to HKMC and enforces the finalization of the SW design before SW implementation.	x	x								x		x		Joint walkthrough	G3			
71	Software safety analysis report	See comment on Safety analysis report in Part 4		x								x		x		Joint walkthrough	G3			
72	Dependent failures analysis report	This may be a subset of the software safety analysis report		x								x		x		Joint walkthrough	G3			
76	Software verification plan	This plan includes the test strategy for all SW test levels like SW unit test, static code analysis, SW integration test and SW test. It shall cover both safety-related and non-safety-related requirements and design elements. A joint walkthrough is needed to align the test strategy between HKMC and the supplier. This walkthrough may be combined with the walkthrough of the validation plan in part 4.	x	x								x		x		Joint walkthrough	G3			
77	Software verification specification	This document specifies all test cases for verifying the SW. An insight is needed on demand, e.g. when defects occur during customer tests or in order to check the test coverage.	x	x								x		x		Insight on demand	G3			
78	Software verification report	This includes evidence on MISRA application and metrics on C0 and C1 test coverage.	x	x								x		x		Document exchange	G5			

Use the DIA for comprehensive definition of the customer/supplier interfaces. Extend the usage to not safety related artefacts

Vector Experiences – Performing Audits and Assessments



Safety Audit

- Purpose: Evaluate implementation of the processes required for functional safety
- Perform periodic audits in projects
- Combine with SPICE assessments
- Perform short supplier audits before nomination, and comprehensive audits in B sample stage

Safety Assessment

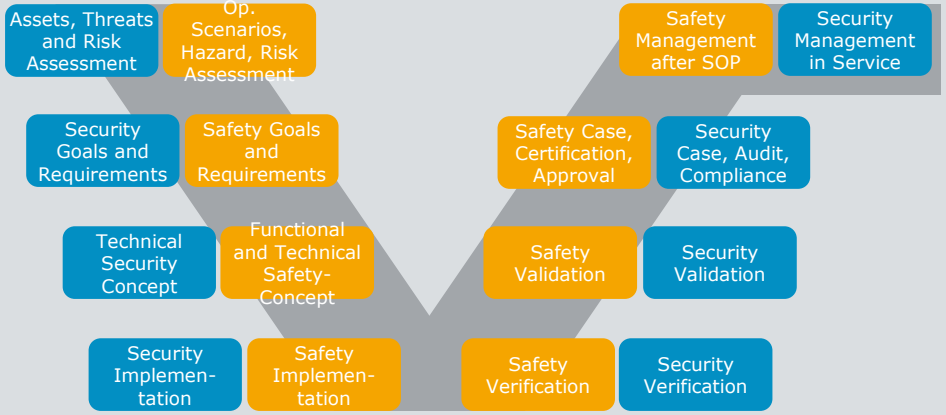
- Purpose: Evaluate achieved functional safety within the defined item for product and process
- Continuously compile the safety case as basis for the assessment
- If the OEM requests assessment by a third party, involve the third party early

Demand audit and assessment results from suppliers, consider the independency requirements for auditors and assessors

Vector Experiences – Security Directly Impacts Safety

Functional Safety (IEC 61508, ISO 26262)

- Hazard analysis and risk assessment
- Functions and risk mitigation
- Safety engineering



Security not explicitly addressed

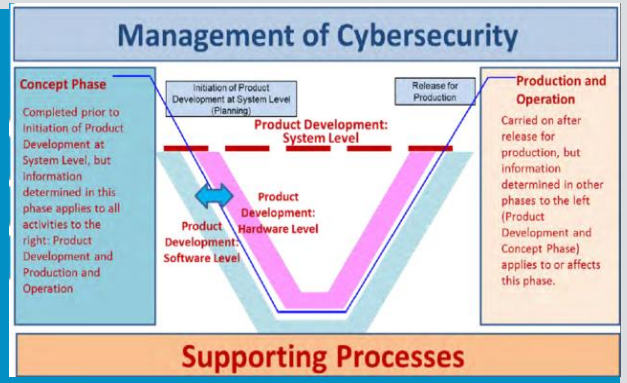
+ Security

(ISO 15408, J3061, ISO/SAE AWI 21434)

- Threat and risk analysis
- Abuse, misuse, confuse cases
- Security engineering

Security and Safety are interacting and demand holistic systems engineering

For fast start security engineering should be connected to safety framework



Agenda

- Welcome
- Welcome and Introduction
- Challenges and Concepts
- Vector Safety Experiences
- **Conclusions and Outlook**

VECTOR

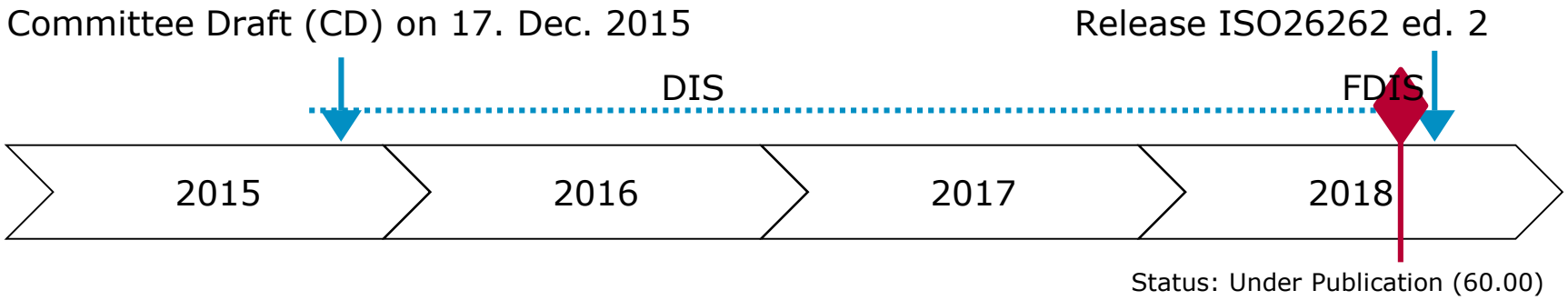
ISO26262 Experience

- **Increasing functional safety capabilities**
  - Majority of OEM´s include ISO26262 compliance in their contracts
  - Independent audits and assessments are performed
  - Methods for qualitative and quantitative analysis are available
  - ASIL D capable MCU´s are available
- **But…**
  - Many suppliers do not have full ISO26262 compliance because they develop based on legacy systems
  - Suppliers and OEMs need to further improve field observation and abilities to efficiently maintain a safety case
  - New suppliers, e.g. for electric powertrain or ADAS, struggle with ramping up a safety process
  - Security risks increasingly hamper functional safety
  - Functional safety processes in many cases create overheads – which could be done at much lower cost

Functional safety can be efficiently achieved on the basis of mature development processes together with a competent partner.

VECTOR

ISO26262 Will Further Evolve



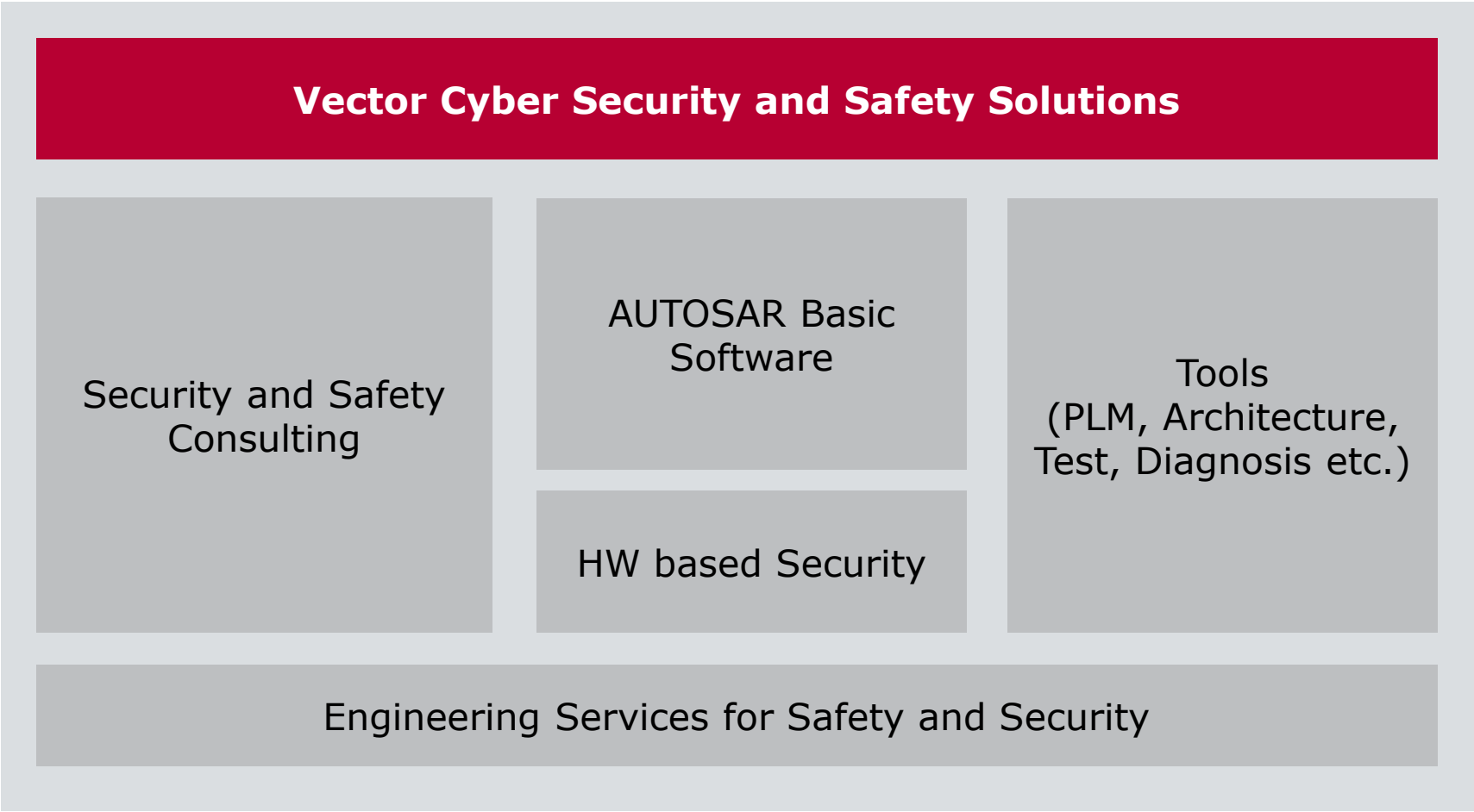
Evolution – Some Topics

1. Extension of scope by 50% to over 700 pages in 12 parts
2. Application to commercial vehicles and motor cycles (ISO PAS 19695)
3. Fully new section on semiconductors (ISO PAS 19451)
4. Improved Safety Analysis Methods for software
5. More detailed requirements for semiconductors, security (SAE-J3061)
6. Support for safety case for ADAS, fail-operational, diversified redundancy
7. “Objective” Assessment and Audit process improvement

Vector with its partners contributes to the evolution of ISO 26262

VECTOR

Vector: Comprehensive Portfolio for Security and Safety



www.vector.com/safety **www.vector.com/security** **www.vector.com/consulting**

Vector Safety Solutions

Trainings and media

- Training "Functional Safety with ISO 26262"
  Stuttgart, continuously
  www.vector.com/training-safety
- In-house trainings tailored to your needs available worldwide
- Free white papers… www.vector.com/media-safety

- **9th Vector Congress – In Sync with Tomorrow's Mobility (20-21 November 2018)**
  https://www.vector.com/int/en/events/global-de-en/2018/9-vector-congress/

- **Free Webinar: Automotive Cyber Security—Challenges and Practical Guidance (7 November 2018)**

Thanks for your attention.
Contact us for support.

Passion. Partner. Value.

Vector Consulting Services

www.vector.com/consulting
consulting-info@vector.com
Phone: +49 711 80670-0

