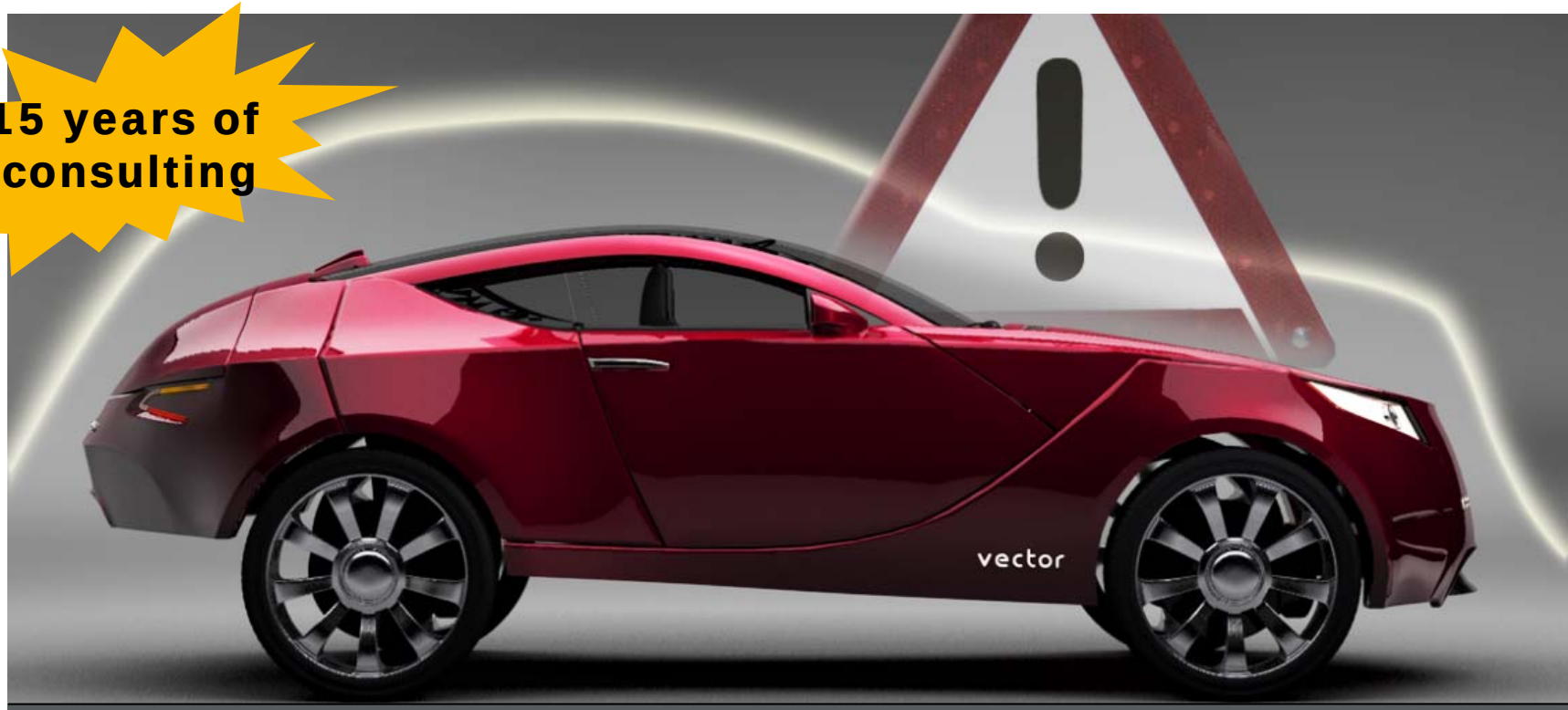
VECTOR

15 years of consulting



Functional Safety with ISO 26262

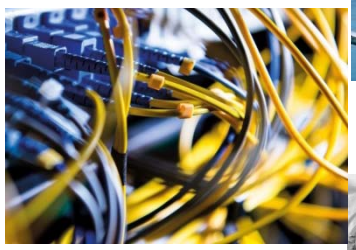
Dr. Christof Ebert, 18. October 2016

Vector Consulting Services

- … supports clients worldwide in improving their product development and IT and with interim management
- … with clients such as Accenture, Audi, BMW, Bosch, Daimler, Ford, Huawei, Hyundai, IBM, Lufthansa, Munich RE, Porsche, Siemens, Thales, Toyota and ZF
- … offers with the Vector Group a portfolio of tools, software components and services
- … is as Vector Group globally present with 1500 employees and well over 300 Mio. € sales
- **www.vector.com/consulting**

Automotive

Aerospace



IT & Finance

Industry

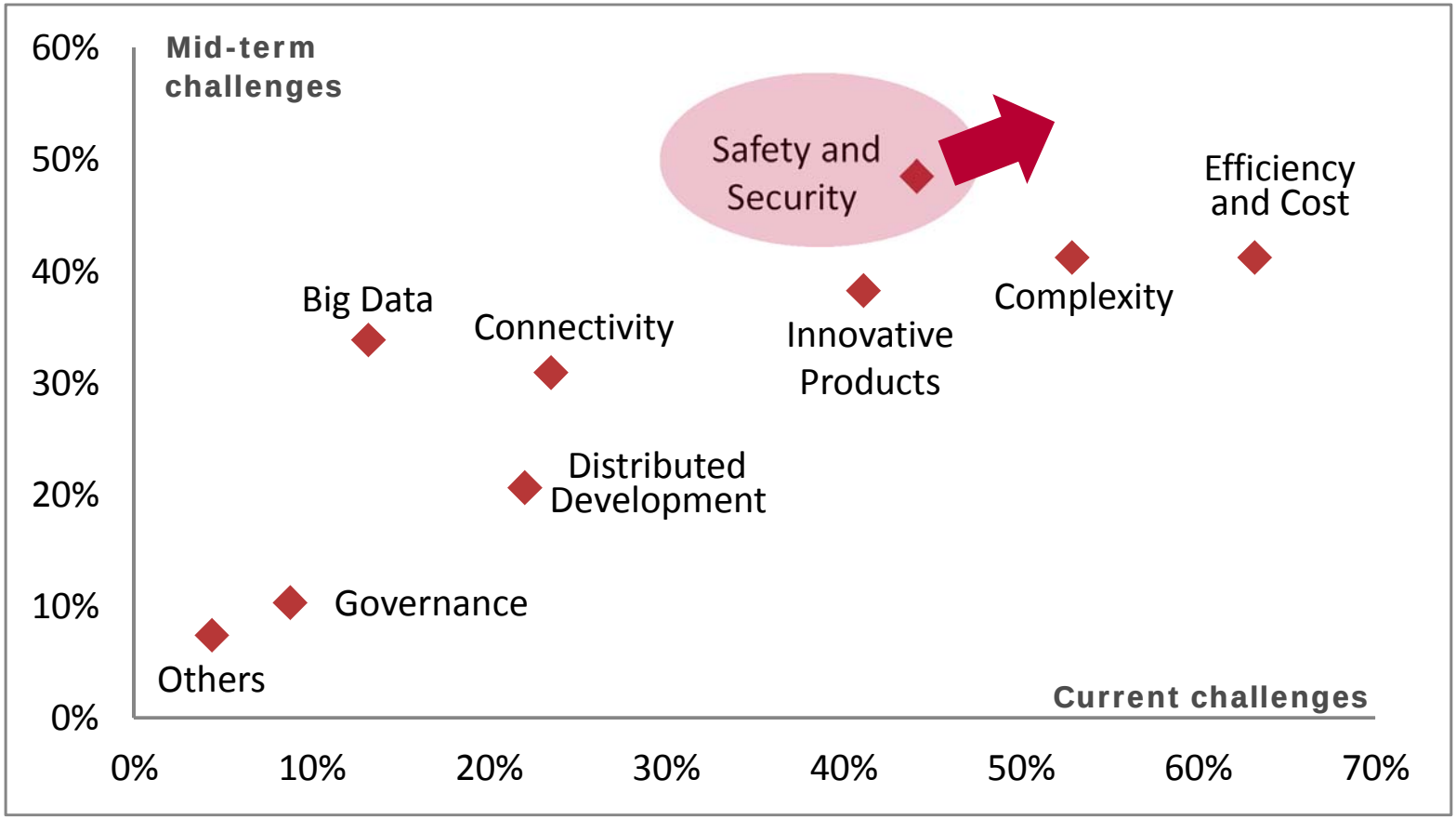
Medical

Railway

Agenda

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

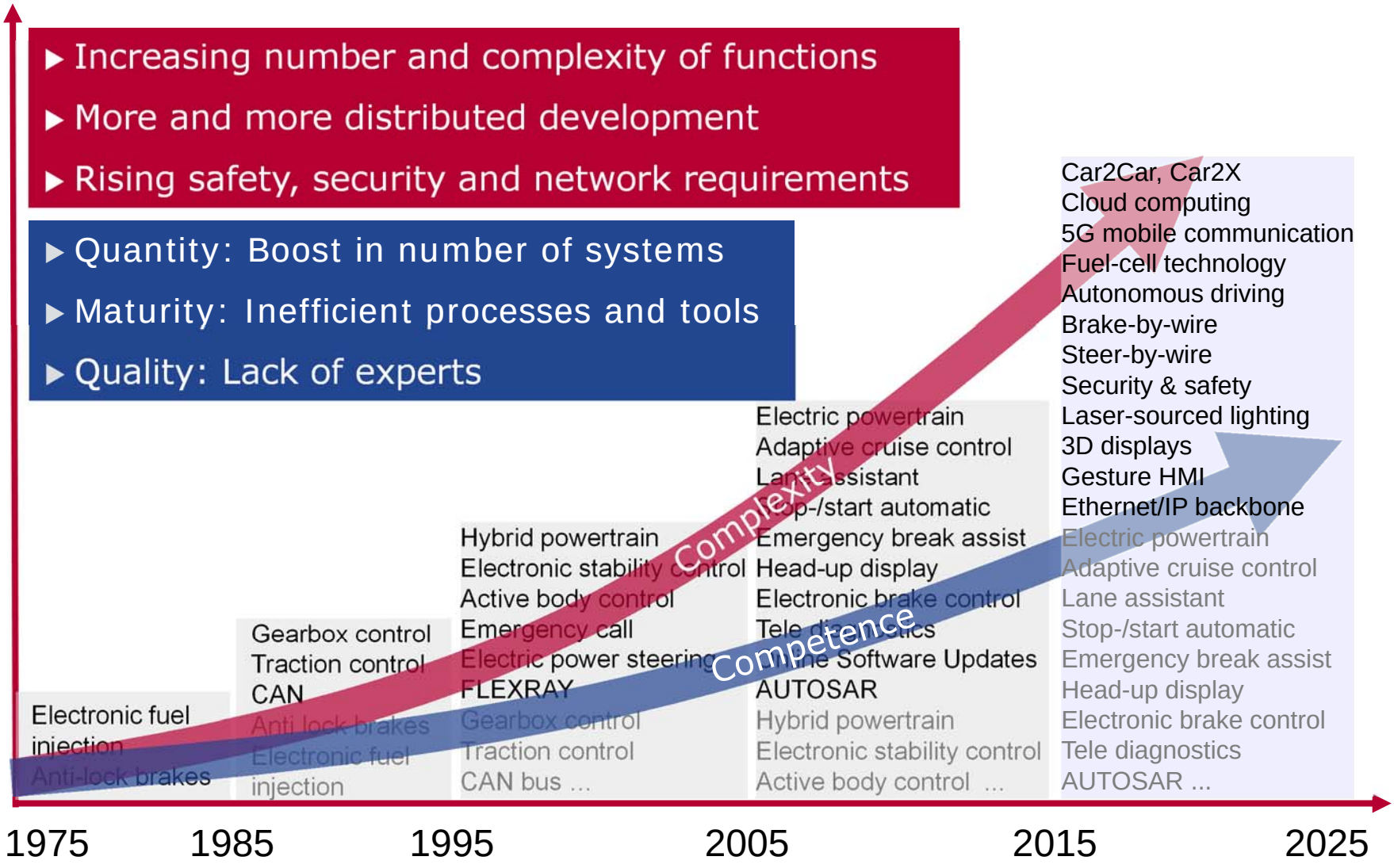
Vector Client Survey on Industry Trends



Vector Client Survey 2016. Details: www.vector.com/trends. Sum > 100% because 3 answers per question were allowed. Results from all industries overlap and are thus compiled in this report. Validity big with >4% response rate of 1700 recipients.

Safety and **security** evolved since 2015 to a major challenge.

Functional Safety Challenge: Complexity and Competences



VECTOR

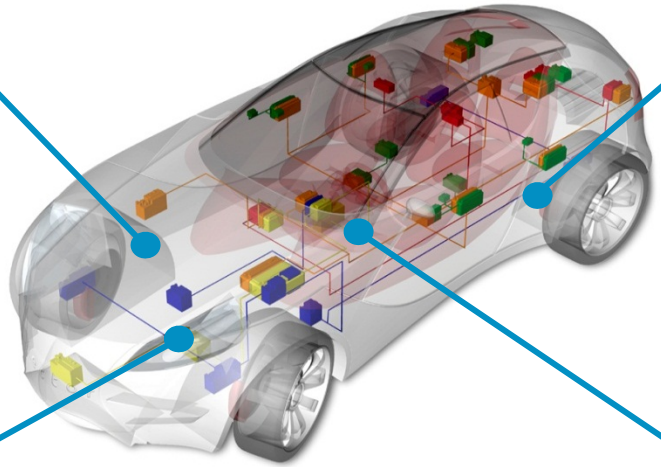
Functional Safety – Broad Exposure

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 – Major Risk and Cost Driver

Problems with switch:
Brake lights either don't light up or light up continuously

Korean OEM

Problems with acceleration:
Car unintentionally accelerates thus causing personal damage

Japanese OEM

Problem with automatic gear control:
Gear is unintentionally switched to neutral

American OEM

Problems with airbag control:
Airbags and seat belt pre-tensioner are not or too late activated

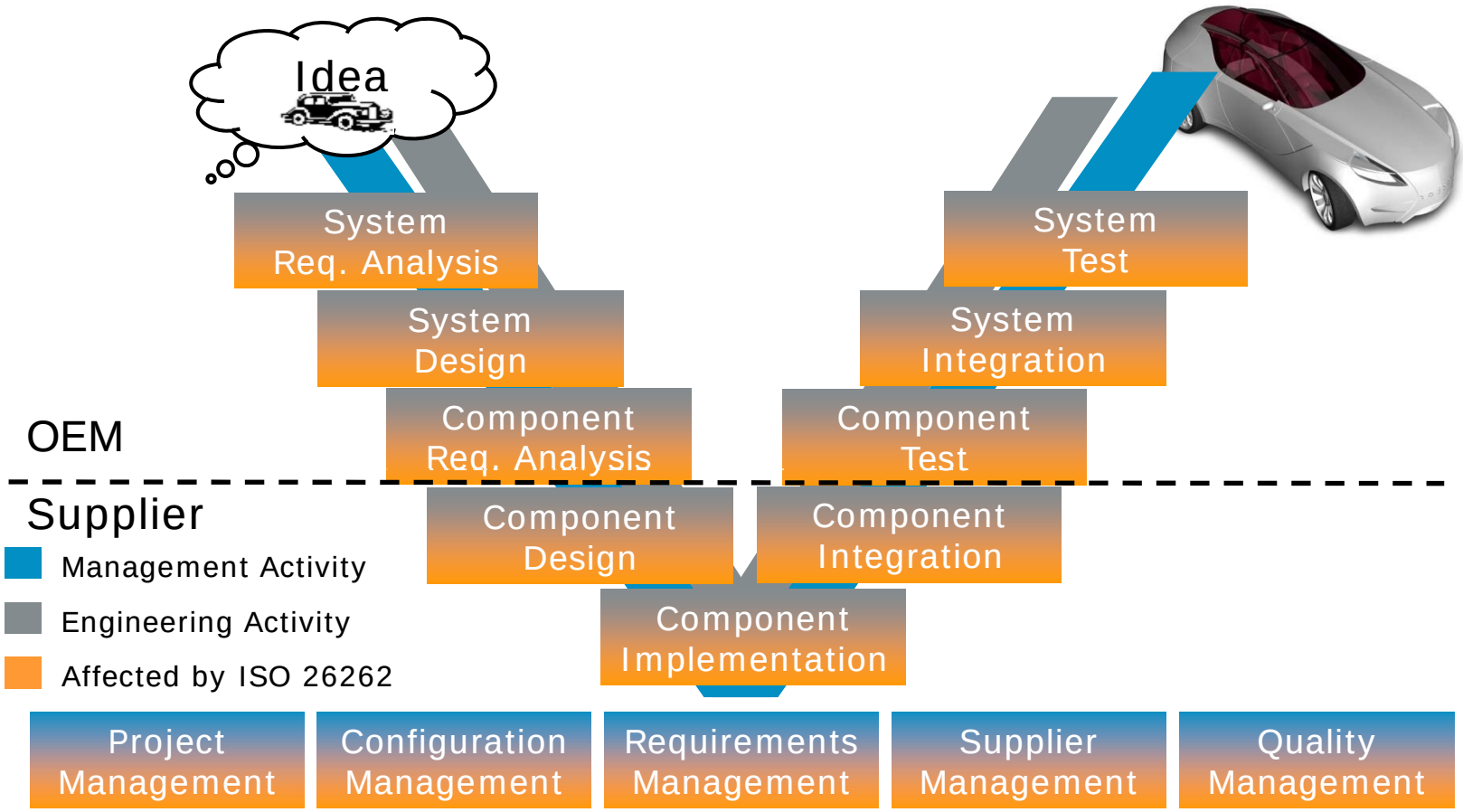
German OEM

Source: autoservicepraxis.de

Increasing amount of incidents ➔ Risk of global visibility

VECTOR

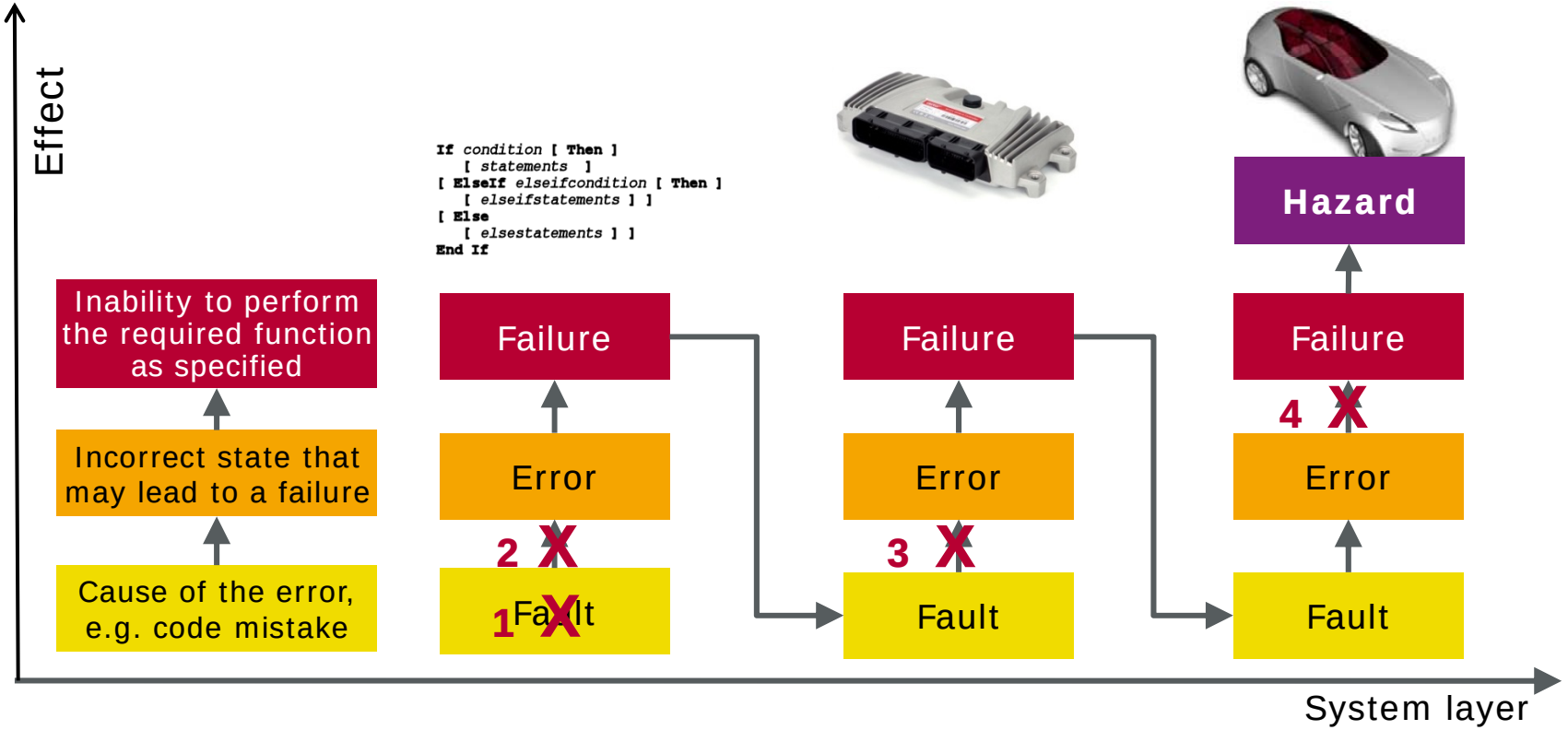
Functional Safety – Wide Impact



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

VECTOR

Functional Safety – Many Methods



1 Fault prevention	2 Fault detection	3 Fault tolerance	4 Robustness
▶ Guidelines	▶ Code analysis	▶ Redundant design	▶ Redundant shut-off
▶ Processes	▶ Review, Test	▶ Memory protection	▶ Fail-operational

Many methods and techniques ➔ Risk of uninformed usage

VECTOR

Functional Safety – Complex Standard

10 Parts

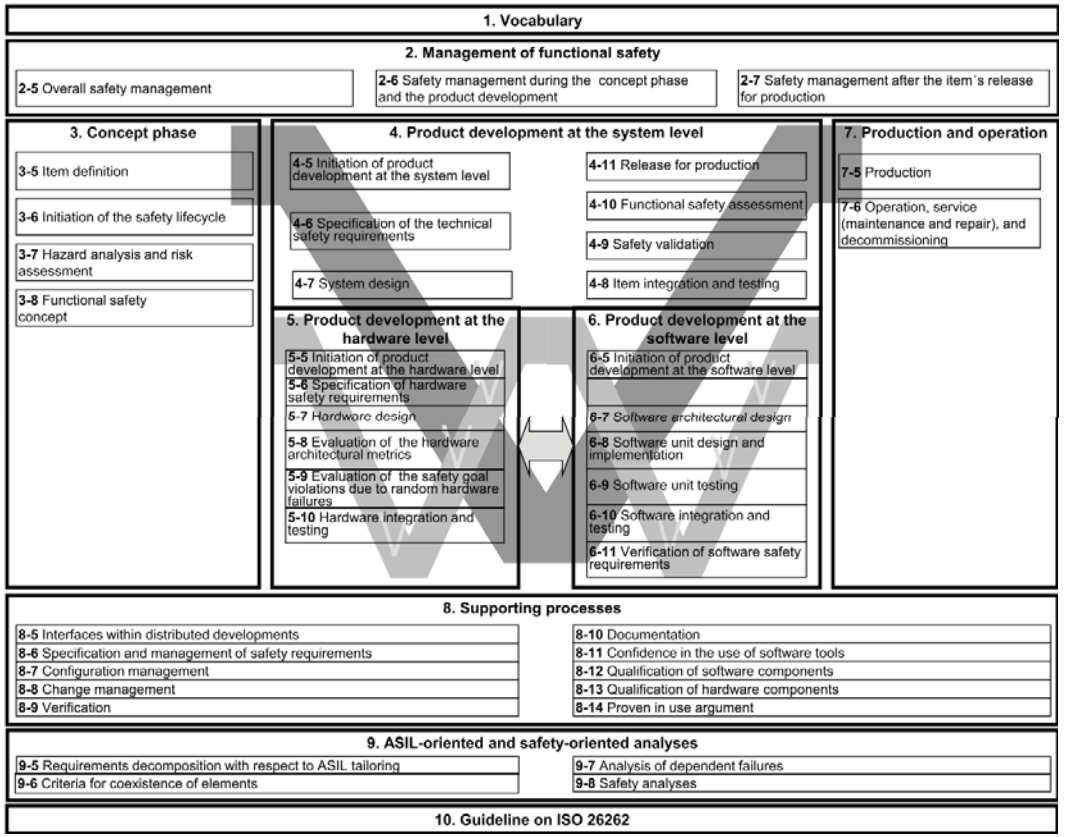
43 Chapters

100 work products

180 engineering methods

500 pages

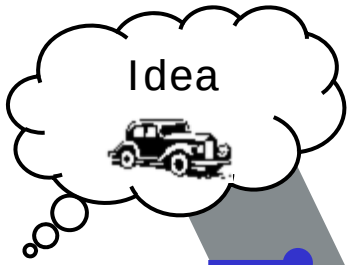
600 requirements



Source: ISO 26262

Complex standard ➔ Risk of overheads and bureaucracy

Liability



Manufacturer's Liability

The manufacturer has to organize the company in a way that design, production and documentation faults are eliminated or detected by checks.

Reversal of Evidence

The manufacturer has to show that he is not responsible for a fault.

Product Liability

A product, that is put in service, must provide the level of safety which can be expected by general public.

Manufacturer's liability is excluded, if a failure can not be detected using current state of science and technology at the time the manufacturer put the product into market.

VECTOR

Legal Liability: State of the Practice

Functional Safety

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
- ...

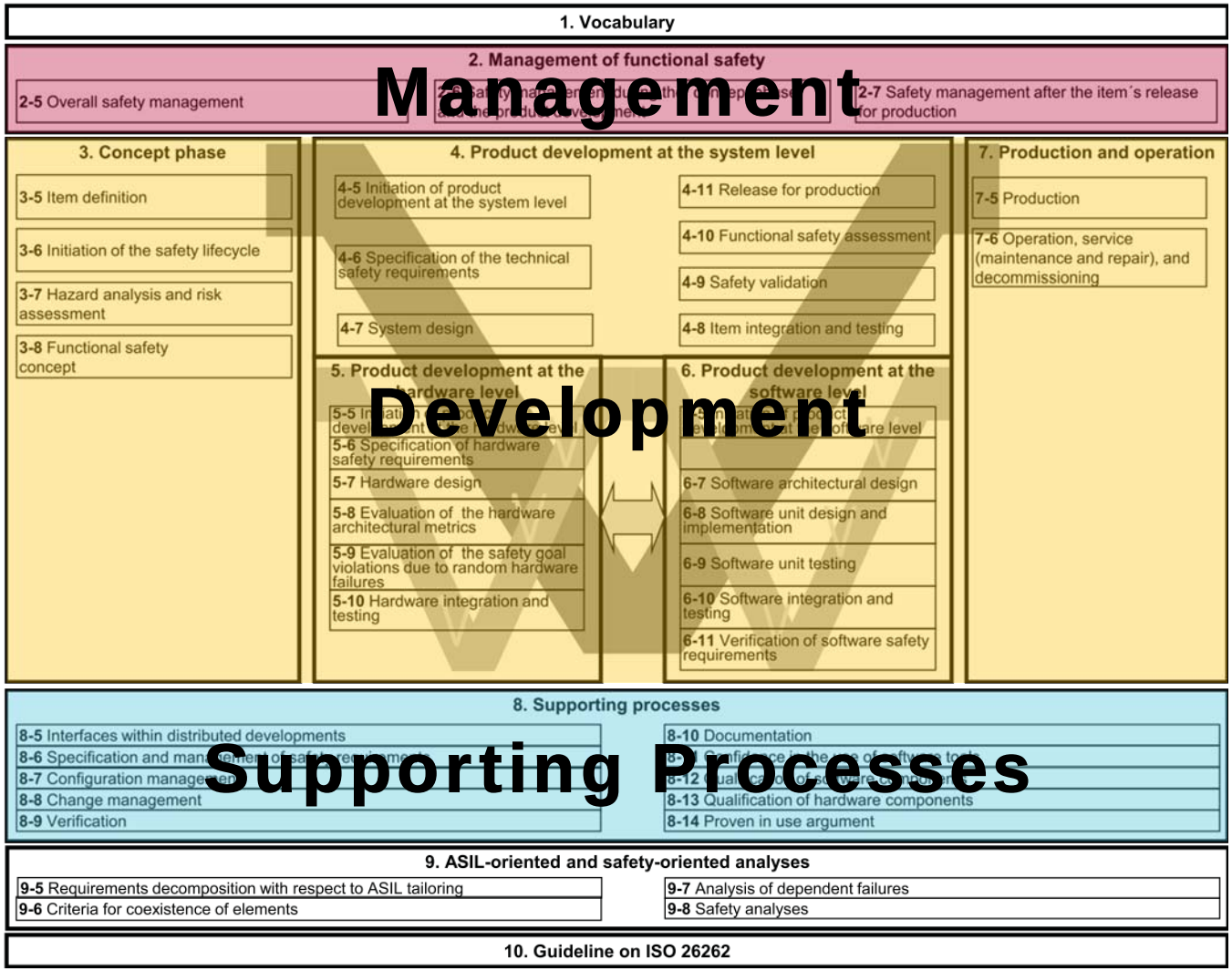
Process Maturity

Application of methodological Frameworks Automotive SPICE® or CMMI

Product Development Process

ISO/TS 16949 ISO 9001

A Structured Approach



Source: ISO 26262-1:2011

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

Risk = Severity x Probability

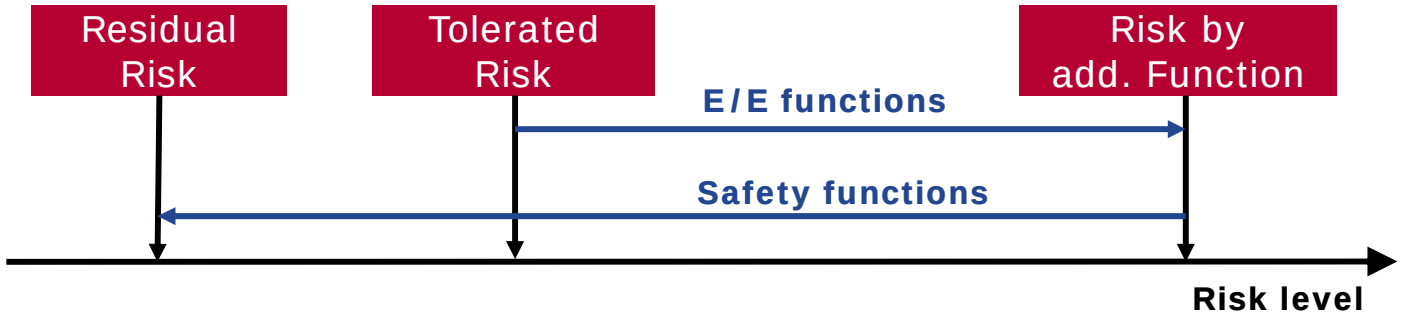
$$R = S \times P_E \times P_C \times P_I$$

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

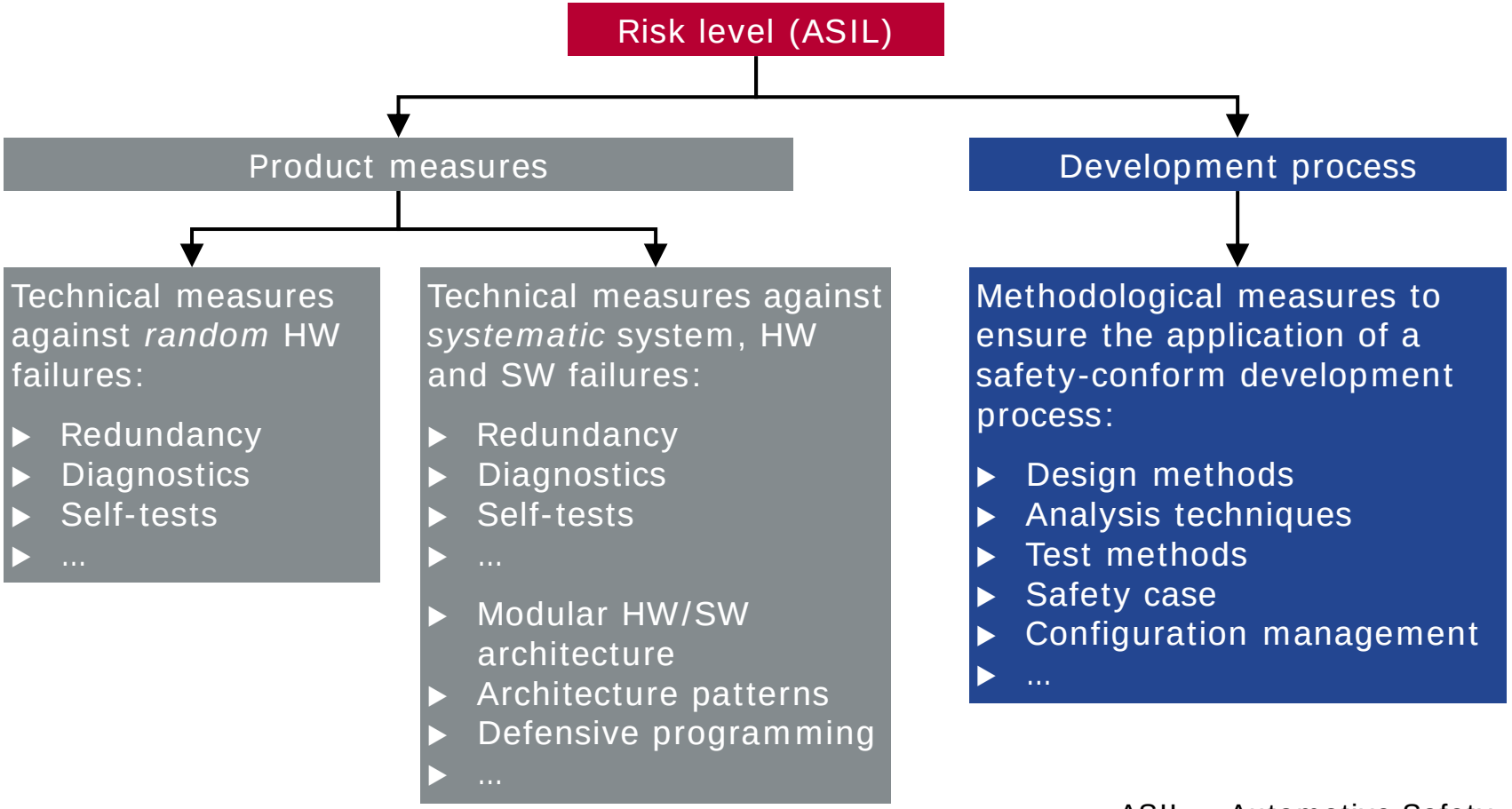
Development – Example Classification Brake-by-wire-System

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

VECTOR

Approaches to Risk Reduction

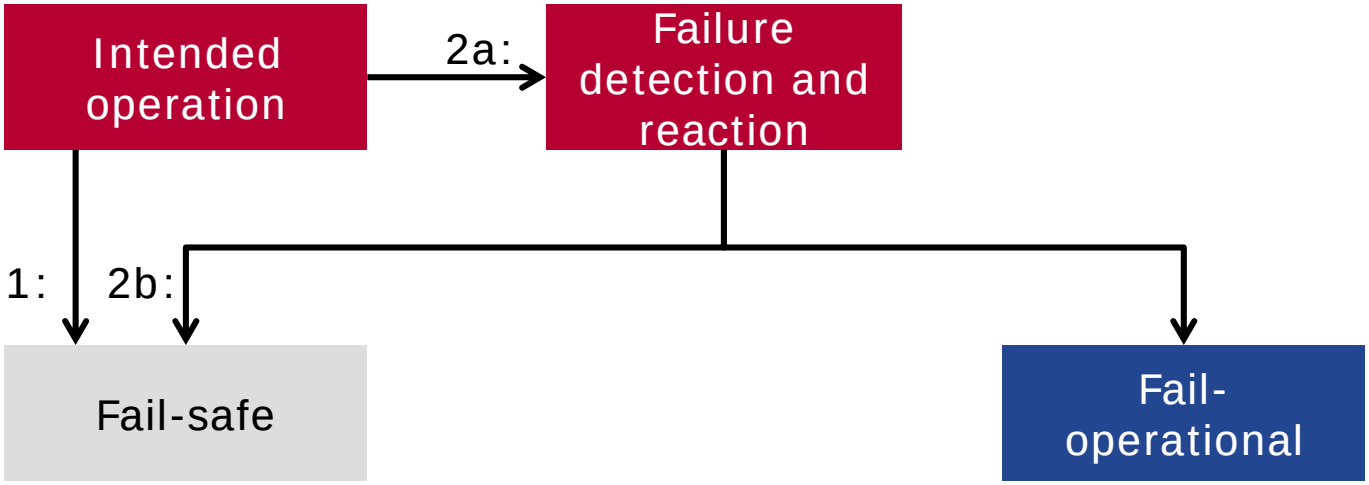


ASIL = Automotive Safety Integrity Level

Goals: Avoid failures – Make unavoidable failures safe

VECTOR

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

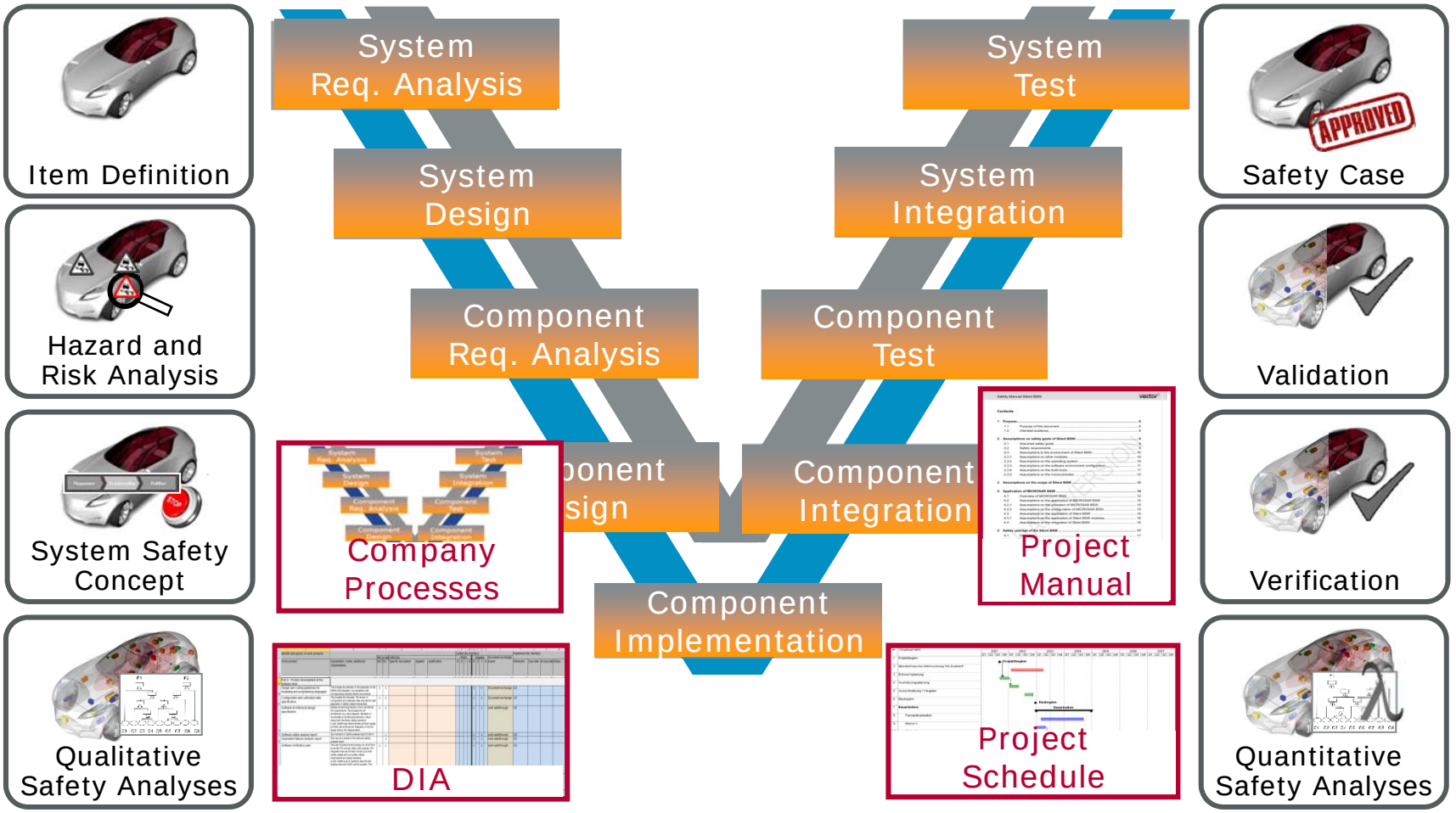
- System remains operational
- E.g. degraded - but safe - operation mode.
- Availability of elements assuring the required safety
- Diverse / redundant architecture
- Required for continuous and automated safe operation

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

Agenda

- Welcome
- 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 – 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 and design

Vector Experiences – Development Interface Agreement (DIA)

List of relevant artefacts

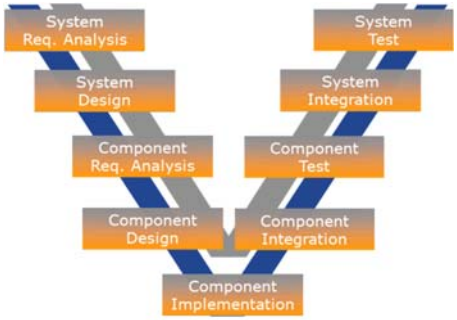
Minimum scope: ~ 60 artefacts

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

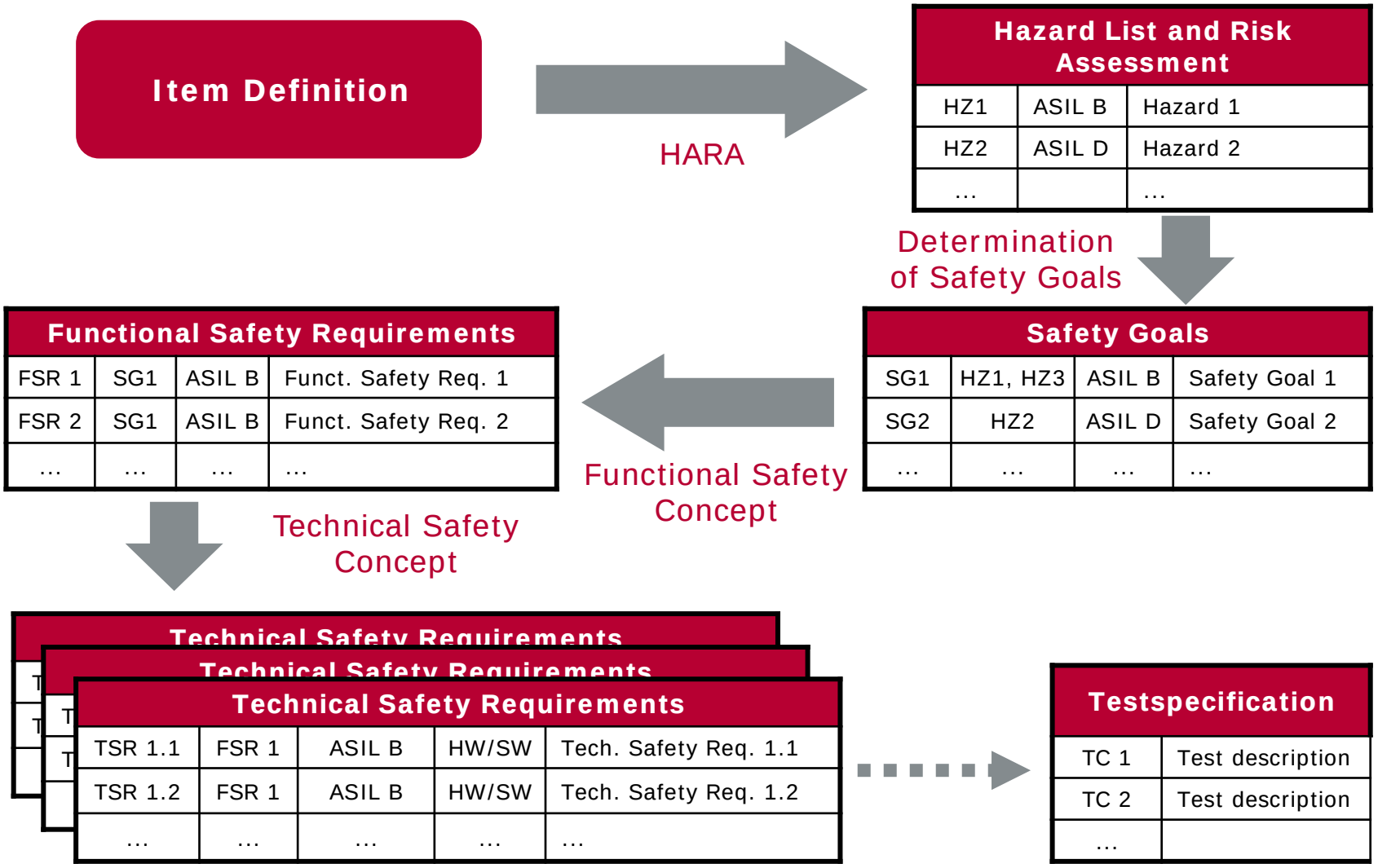
- Purpose: Evaluate implementation of the processes required for functional safety
- Perform periodic audits in projects
- Combine with SPICE assessments
- Perform short supplier audits before nomination, and comprehensive audits in B sample stage

Safety Assessment

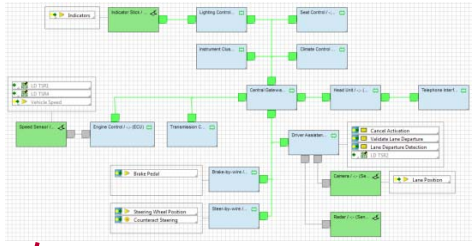
- Purpose: Evaluate achieved functional safety within the defined item for product and process
- Continuously compile the safety case as basis for the assessment
- If the OEM requests assessment by a third party, involve the third party early

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

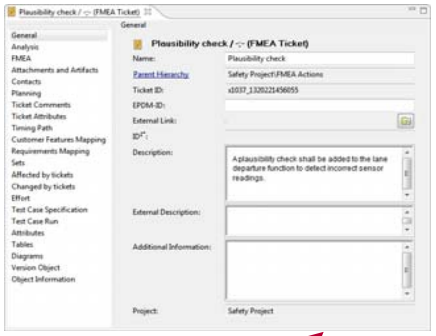
Vector Experiences – Efficient Traceability and Consistency



Vector Experiences – Systematic Analysis and Design



TP.2.2.4.2	*Safety goals*	
LD1-SG.1	*Detect 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 currently qualified to ASIL A	None defined as yet.	10	300	Plausibility check A plausibility check shall be	Metzker	Nov 30, 2011
				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 requirement based tests

Vector Experiences – Master Necessary Analysis Methods

Level	Safety Analyses	Dependent Failure Analyses
Functional Safety Concept	▸ Definition of FSR „can be supported“ safety analyses	▸ Redundancy and independence „can be checked“ by DFA

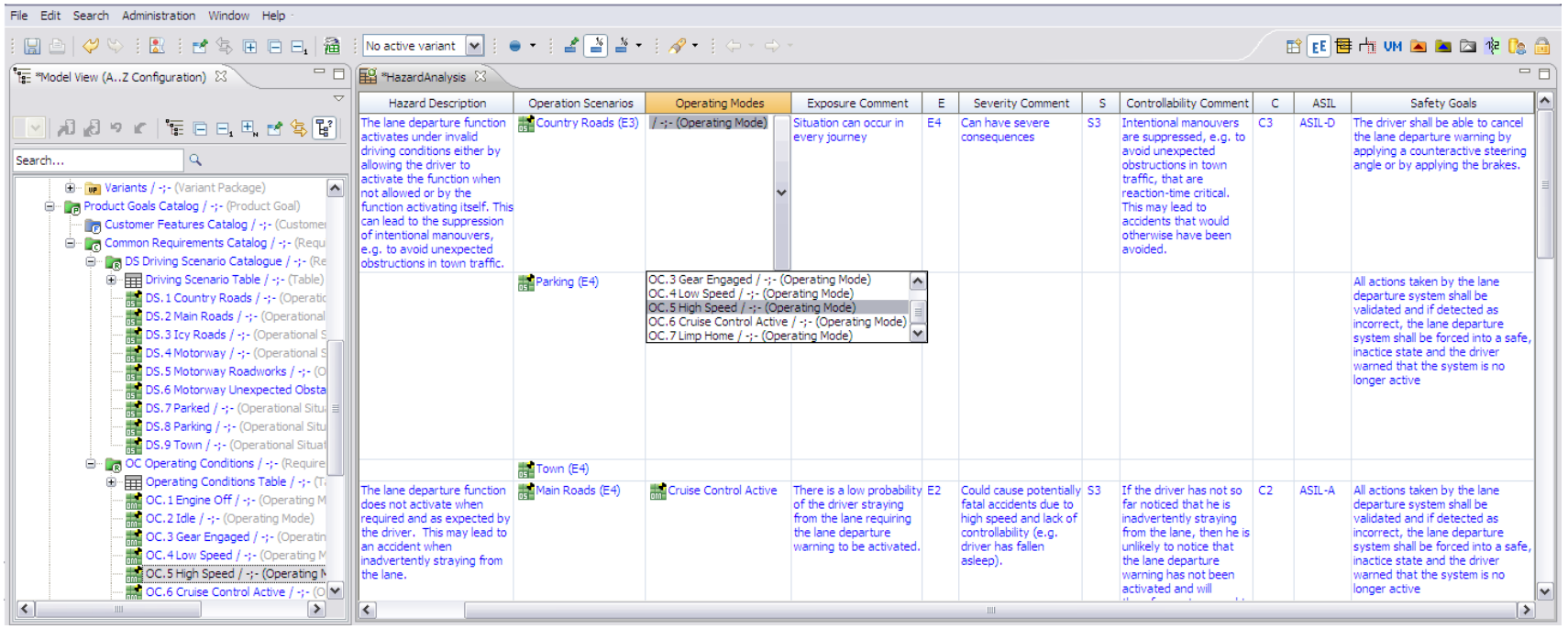
Technical Safety Concept	▸ Avoidance of systematic failures
	  ▸ External sources
	  ▸ Internal sources
	▸ Validation of the technical safety concepts (TSC)
		▸ Independence
		  ▸ Common cause failures and cascading failures
		  ▸ Safety function from safety mechanism
		  ▸ ASIL-decomposition
		  ▸ Allocation and design decisions
		▸ Freedom from interference
		  ▸ Cascading failures only
		  ▸ Partitioning

Hardware	▸ Qualitative analyses (from part 9):
	  ▸ Verification of hardware design
	  ▸ Effectiveness of safety mechanisms
	▸ **(B), C, D: Quantitative** analysis:
	  ▸ Random hardware failures	

Software Architecture	▸ Safety mechanisms
	  ▸ Effectiveness
	  ▸ Error detection
	  ▸ Error handling	

General Requirement	▸ Complete safety item ▸ Confirmation reviews ▸ Verification reviews	▸ Focused analyses ▸ No requirements on reviews

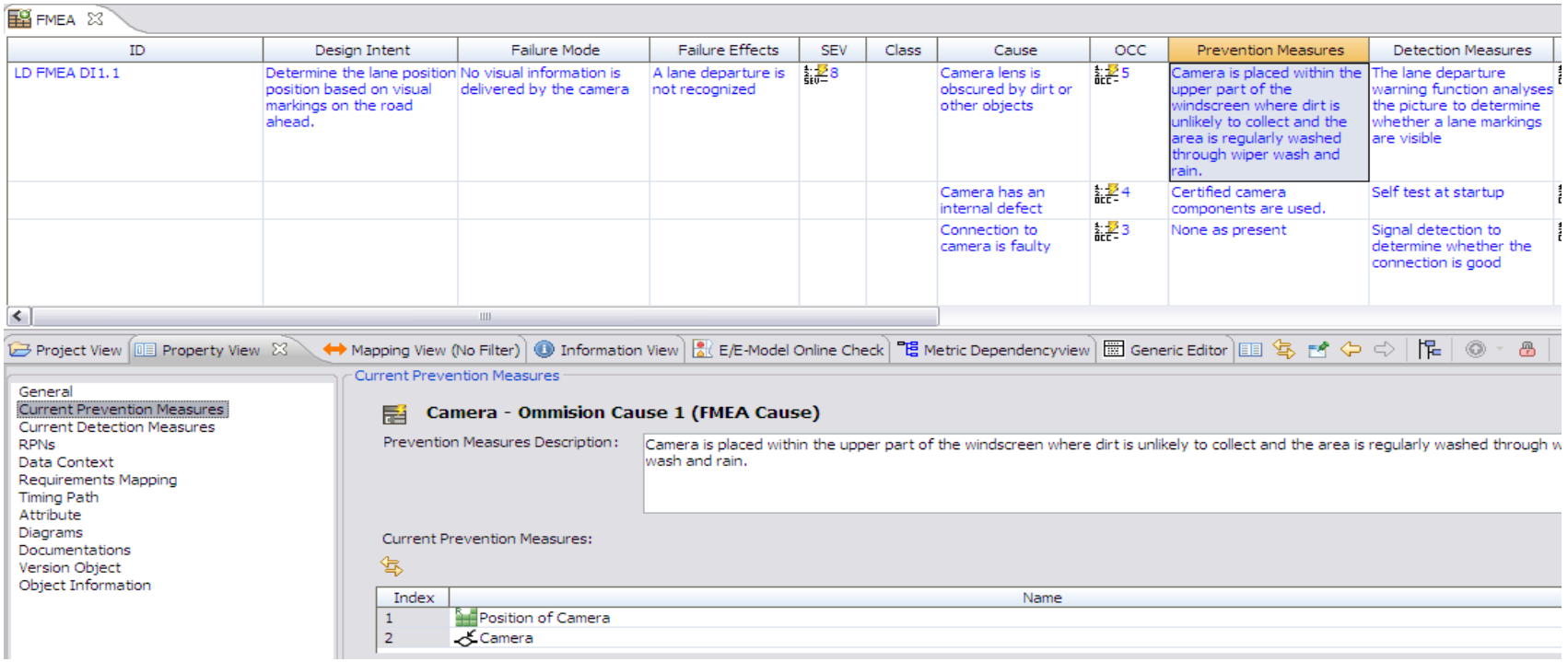
Vector Experiences – Thorough Hazard & Risk Analysis



Support by Vector Consulting Services and PREEvision tool:

- Predefined operation scenarios and operating modes
- Automatic ASIL calculation
- Traceability of safety goals to requirements and design artefacts

Vector Experiences – Consistent Support for FMEA



Support by Vector Consulting Services and PREEvision tool:

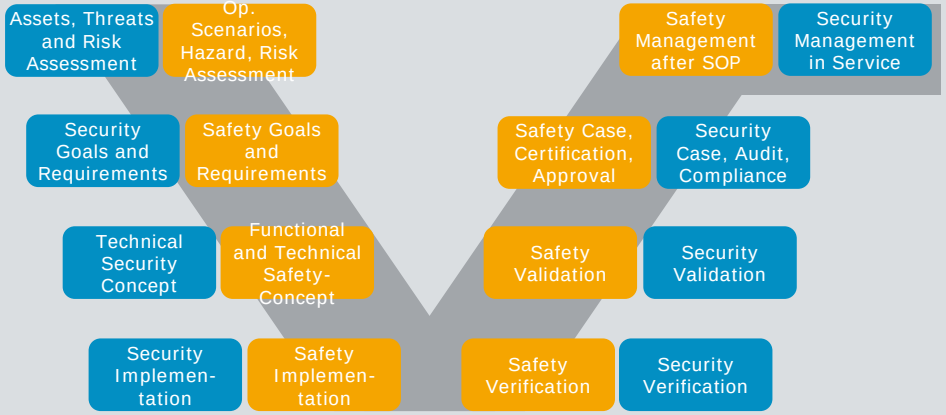
- System requirements and design data with full traceability, thus avoiding to replicate system structure in a separate FMEA tool, while achieving significant cost savings
- Automatic consistency checks to ensure coverage

Vector Experiences – Security Directly Impacts Safety

Functional Safety (IEC 61508, ISO 26262)

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

Security only implicitly addressed

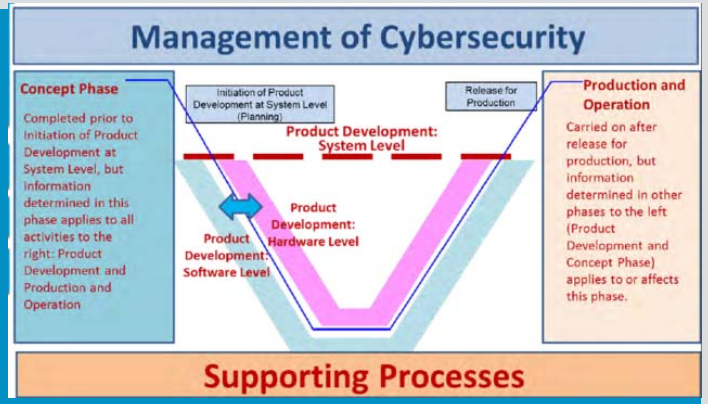


+ Security (ISO 15408, J3061)

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

Security and Safety are interacting and demand holistic systems engineering

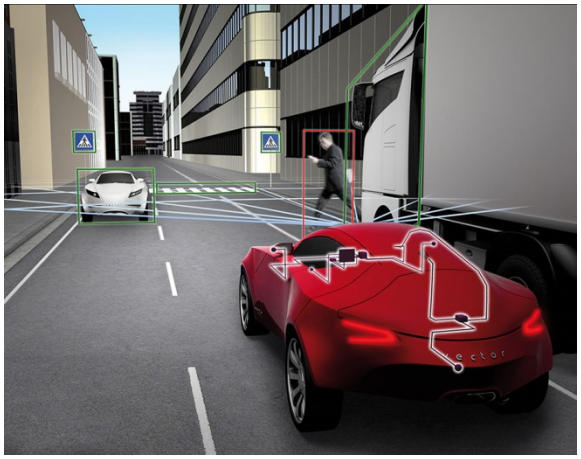
For fast start security engineering should be connected to safety framework



Safety and Security must be addressed in parallel

Innovative functionality...

- Distributed systems
- Complex feature interaction
- High data volume
- External interfaces (V2X; vehicle as IP node)



... Drives new challenges

- Fail-operational robust behaviors
- High-performance micro-controllers
- Software development for critical systems
- Safety functions must be secured against attacks
- Cost-effective evolution and support over the entire life-cycle

Apply holistic systems engineering for safety and security

Agenda

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

VECTOR

Success Factor – Change Towards Safety Culture

Classic Development Culture	Safety Culture
Insufficient budget and time for relevant safety measures	Necessary measures are planned according to safety analysis – and reliably implemented
Shadow organization of safety experts and staff teams	Safety expertise is embedded into the regular line and project organization
Risk analysis is done superficially for documentation purposes and not maintained	Risk analysis and FMEA are developed at the beginning of system development and are continuously updated
System architecture is not considered in safety goals and requirements	System architecture explicitly covers the safety goals and requirements
Changes are accepted at any time for practically all system parts	Changes are analyzed with respect to their effects on functional safety using a strict change management
Safety audits are conducted only sporadically	Safety audits are established as a normal and standardized behavior
...	...

Implementing functional safety implies a profound culture change

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

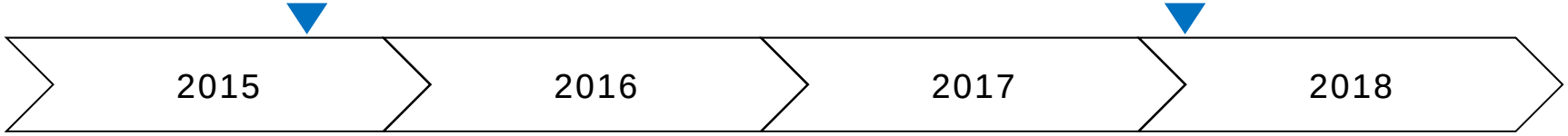
Functional safety can be efficiently achieved on the basis of mature development processes together with a competent partner.

VECTOR

ISO26262 Will Further Evolve

Committee Draft (CD) on 17. Dec. 2015

Release ISO26262 ed. 2



Evolution – Some Topics

1. Extension of scope by 50% to 729 pages
2. Application to commercial vehicles and motor cycles
3. Fully new section on semiconductors
4. Improved Safety Analysis Methods for software
5. Support for safety case for ADAS, fail-operational, diversified redundancy
6. “Objective” Assessment and Audit process improvement

Vector with its partners contributes to the evolution of ISO 26262

VECTOR

Vector – Complete Safety Solution Portfolio

Introduction of Safety Processes (Examples)

- Introducing ISO 26262, starting with analysis of the current state, including technical and process measures and building up safety culture
- Training und coaching for functional safety and safety culture
- Implementing consistent tool support, such as PREEvision

Safety Management (Examples)

- Operationally supporting with interim safety managers
- Performing safety audits and supplier safety audits

Safety Engineering (Examples)

- Providing software components and platforms, such as MICROSAR Safe
- Developing and reviewing safety concepts and safety analyses
- Combined safety and cyber security concepts

Vector Safety Portfolio

Safety Solutions

- **Consulting**
  Vector Safety Check, Interim Safety Manager, …
- **Tools**
  PLM with PREEvision, Test, Diagnosis, …
- **Software**
  AUTOSAR up to ASIL-D…
- www.vector.com/safety

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

Thank you for your attention.
Contact us for further support on functional safety, cyber security, and product development.

Passion. Partner. Value.

Vector Consulting Services

Phone +49 711 80670-0
Fax +49 711 80670-444

www.vector.com/consulting
consulting-info@vector.com