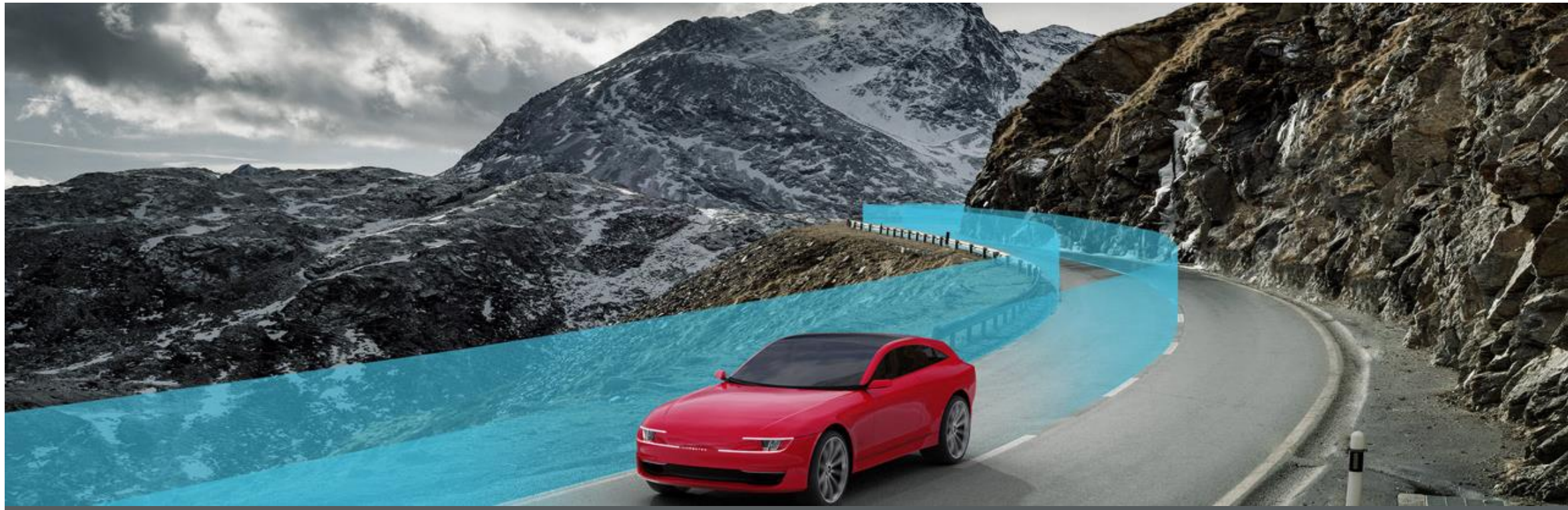
VECTOR



Functional Safety (ISO26262) and SOTIF (ISO/PAS21448) Webinar

Dr. Arnulf Braatz/Andreas Horn, June 16th 2020

V1.10 | 2020-05-12

Webinar: Functional Safety and SOTIF

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.

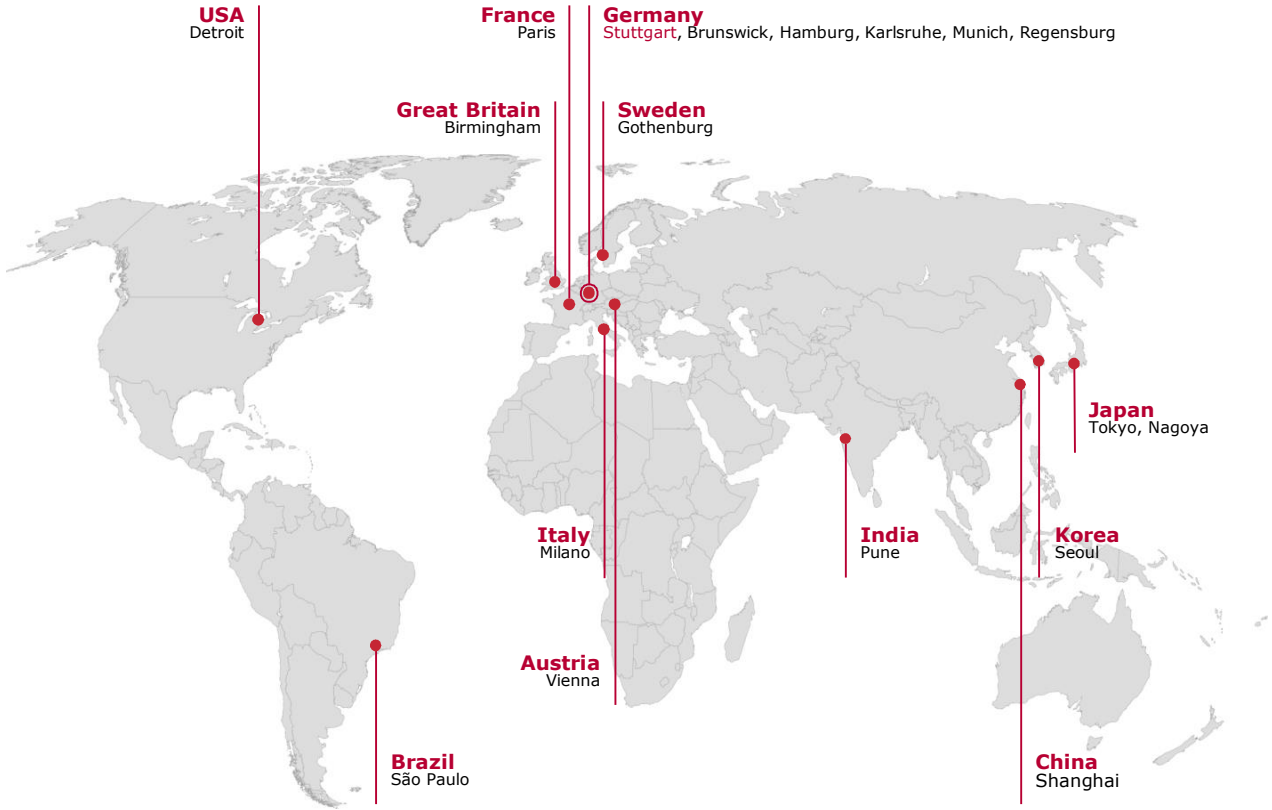
© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Vector Group

- **Development**
  Vector provides tools for developing, testing, calibration and diagnostics as well as software components and development services.

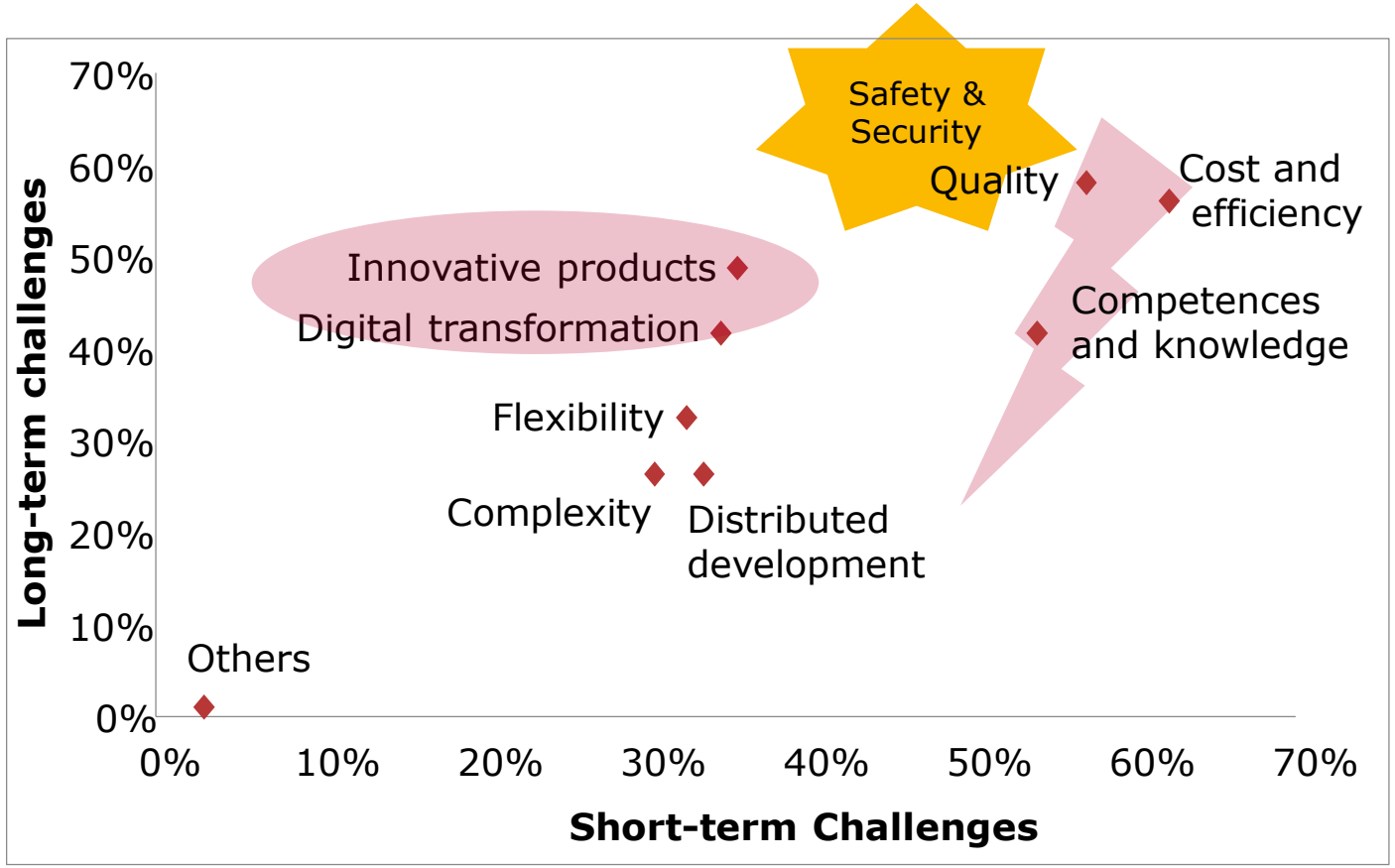
- **Networking**
  Vector provides components and engineering services for the networking of electronic systems.

- **Optimization**
  Vector provides a comprehensive consulting portfolio as well as suitable tools support.



© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Vector Client Survey 2020: Risk of vicious circle



Vicious cycle:
> cost pressure
> lack of competences
> less innovation and quality

Vector Client Survey 2020.
Details: www.vector.com/trends.
Horizontal axis shows short-term challenges; vertical axis shows mid-term challenges.
Sum > 300% due to 5 answers per question. Strong validity with 4% response rate of 2000 recipients from different industries worldwide.

Vector provides tailored consulting solutions to keep OEM and suppliers competitive:
Efficiency – Quality – Competences

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

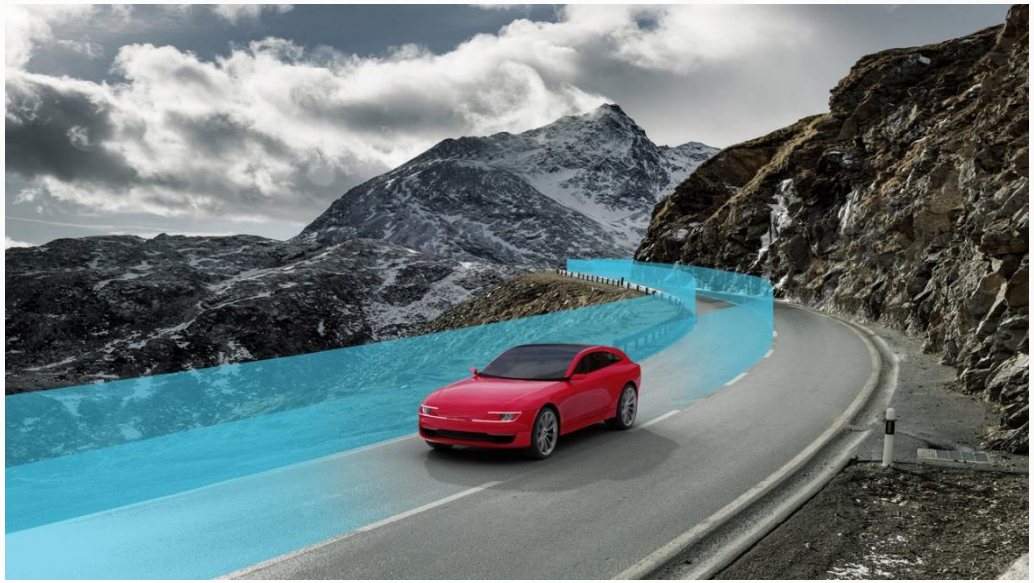
Agenda

Welcome and Introduction

- **Challenges and Concepts**

Vector Safety Experiences

Conclusions and Outlook



© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

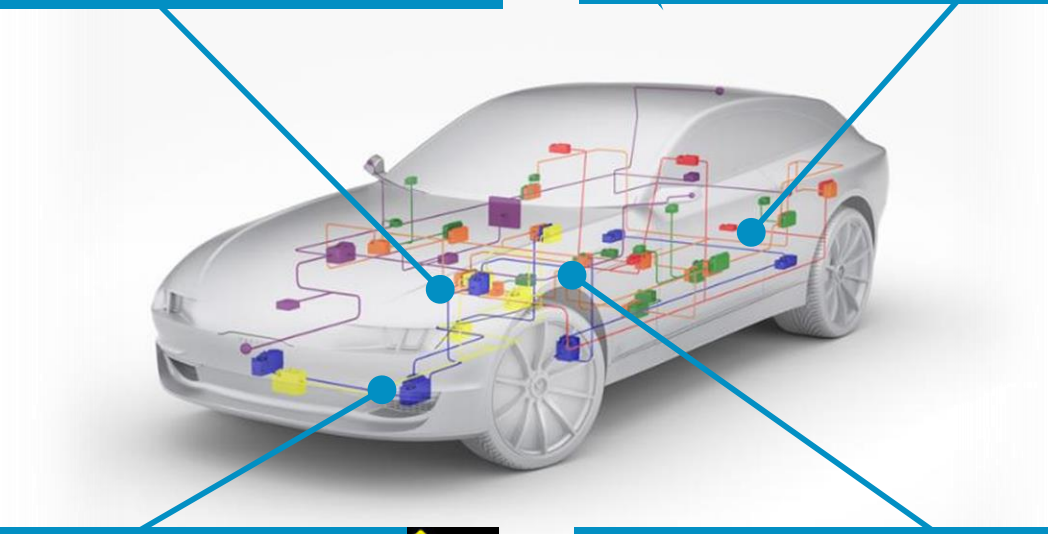
Many functions are safety related

Electrical Power Steering

Unintended steering and loss of steering assist

Electronic Park Brake

Unintended activation in motion



Collision Avoidance

Acceleration instead of deceleration in traffic

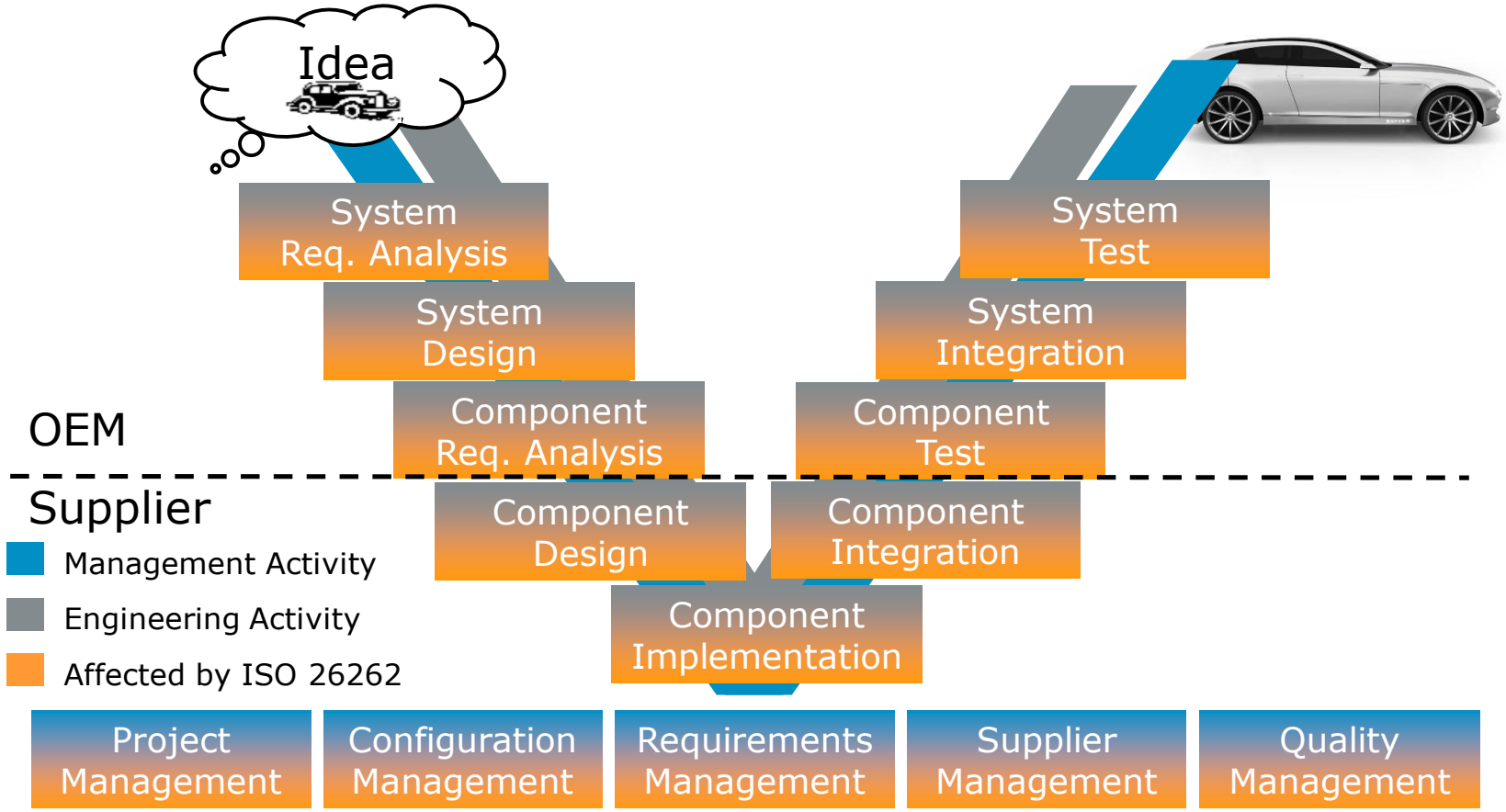
Airbag

Unintended deployment during normal operation

Mal-functions caused by failures of E/E systems

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

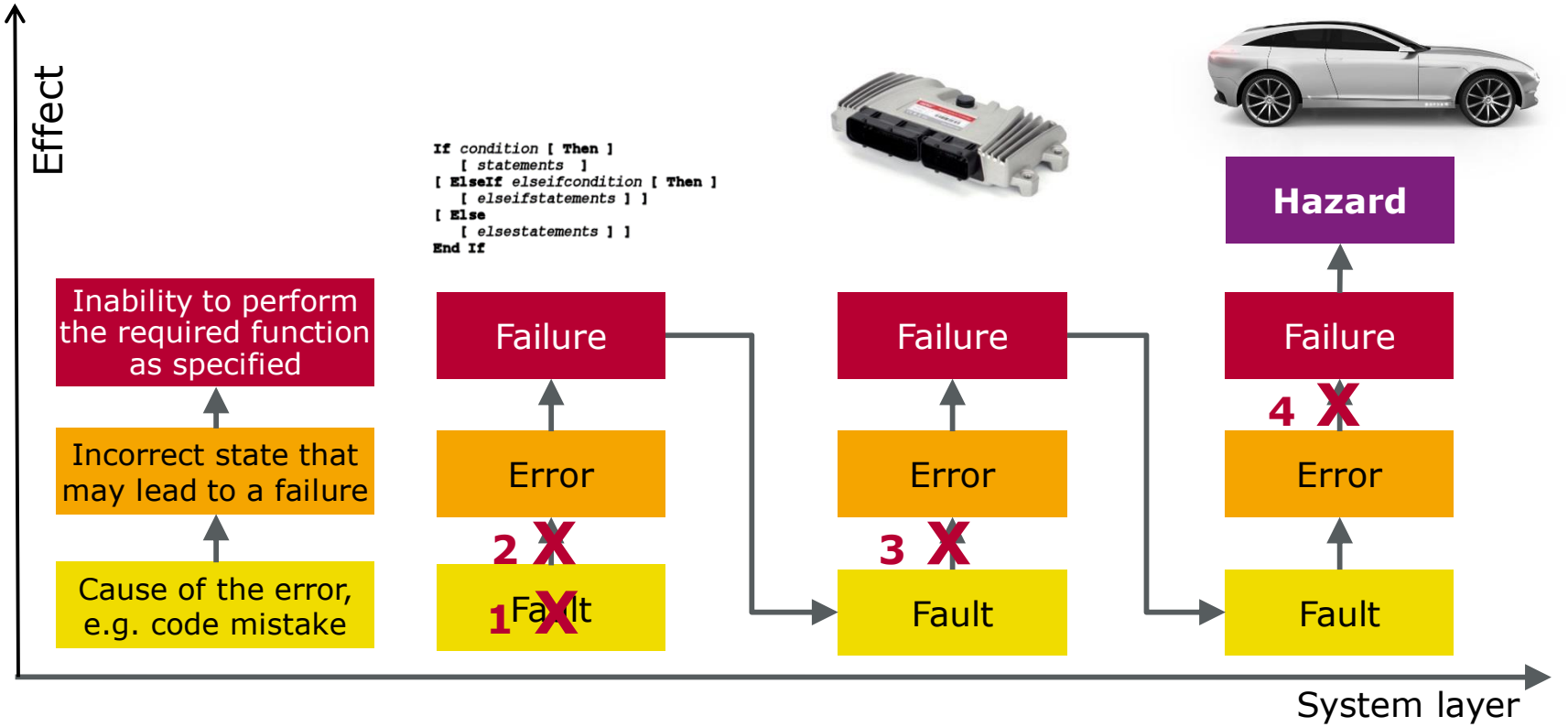
Functional Safety – Wide Impact



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

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Functional Safety – Many Methods

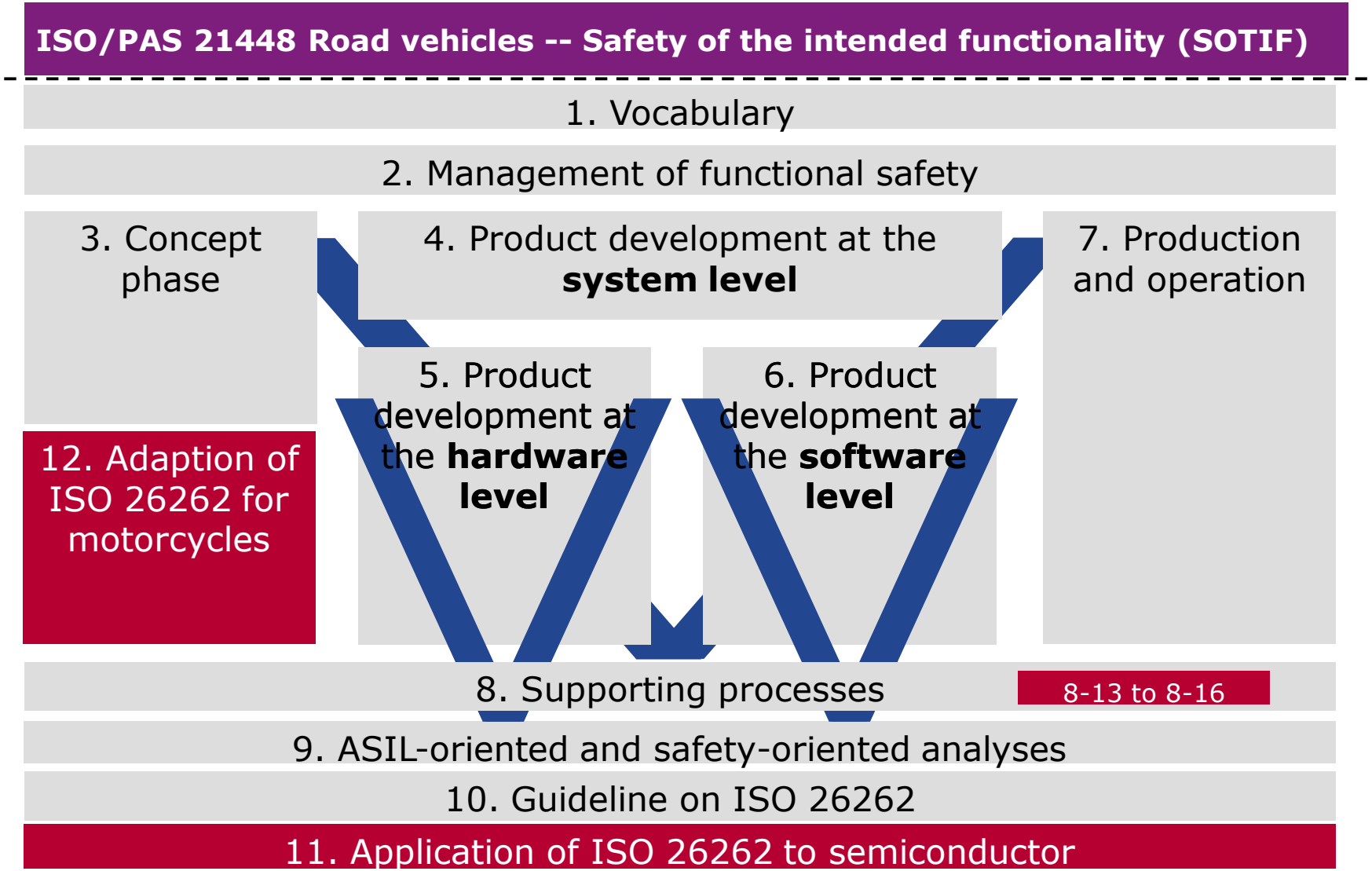


1 Fault prevention	2 Fault detection	3 Fault tolerance	4 Robustness
▶ Guidelines	▶ Code analysis	▶ Redundant design	▶ Redundant shut-off
▶ Processes	▶ Review, Test	▶ Memory protection	▶ Fail-operational

Many methods and techniques ➔ Risk of uninformed usage

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

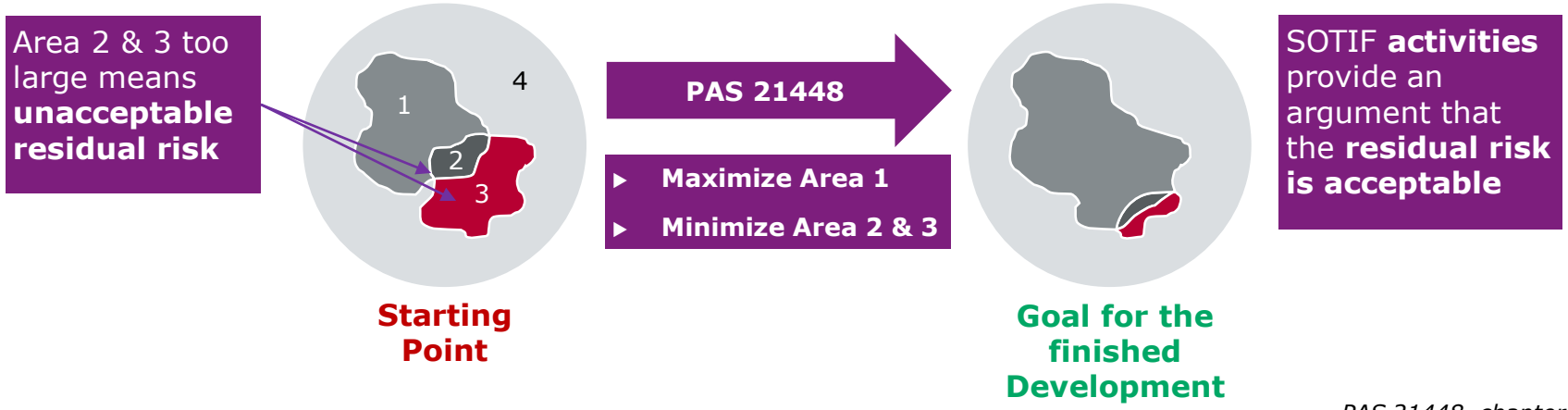
Parts of ISO 26262:2018 – 2nd Edition – Main Changes



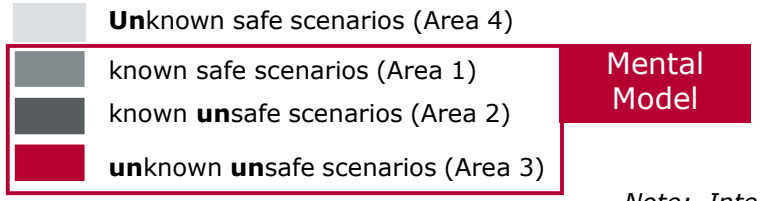
© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Scope of SOTIF (ISO/PAS 21448)

Safety of the intended functionality (SOTIF) – The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons.



PAS 21448, chapter 4, figure 8

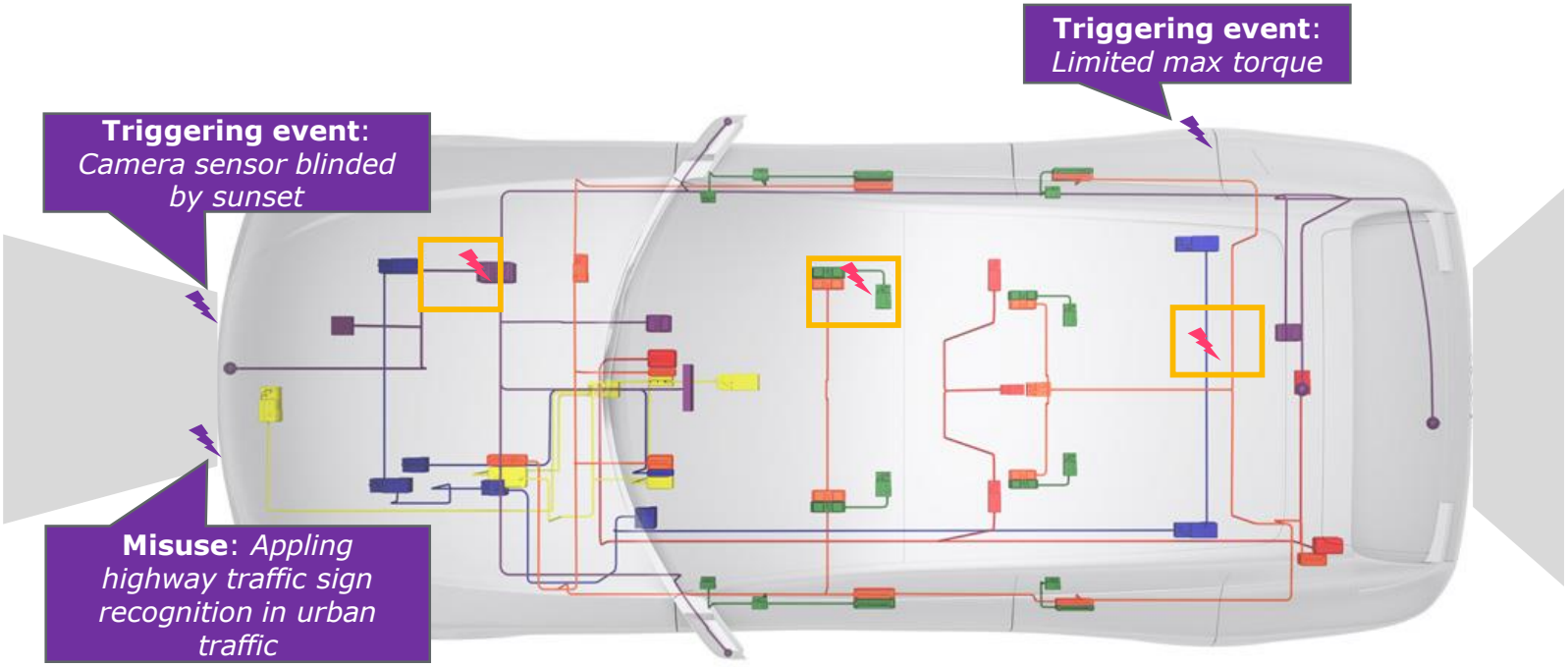


Note: Intentional alteration of the system operation (Feature abuse) is not in scope.

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Overview Automotive Safety: Functional Safety & SOTIF

SOTIF: **Triggering events** are analyzed if acceptable or **function needs to be modified.**



Functional Safety: Methods required by ISO 26262 focus on those **faults** need to be **identified and mitigated**, which potentially violate a safety goal.

= systematic & random faults of HW &SW

= known limitations of sensors, actuators and algorithms, environmental conditions and foreseeable misuse (PAS 214448, Chapter 7.2)

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Legal Liability: State of the art of science and technology

Conferences, white papers, etc.

ISO 26262

Process governance (e.g. CMMI, SPICE)

Basic regulations:

- Laws,
- statutory provisions,
- nongovernmental standards (ISO 9001, ISO/TS 16949, etc.)

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
- …

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

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

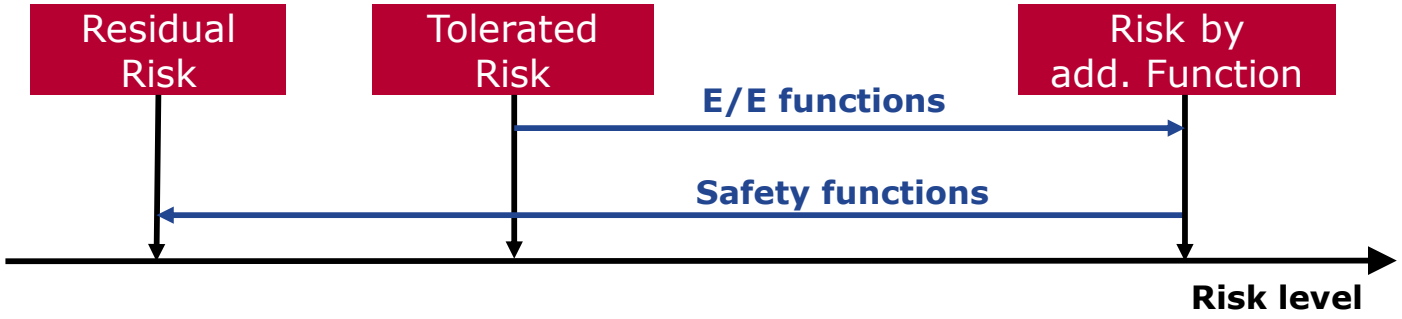
Risk = Severity x Probability

$$R = S \times \underbrace{P_E \times P_C \times P_I}_{\text{ASIL}}$$

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

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Development – HARA for deriving Safety Goals and ASIL

Malfunction of Adaptive Front Steering	Operational Situation			E	C	S	ASIL
No superimposition	> 100 km/h	Highway	Wet road	E3	C1	S3	A
Steering inversion	> 50 km/h < 100 km/h	Main Road	Dry road	E4	C3	S3	D
Oversteering	> 50 km/h < 100 km/h	Main Road	Dry road	E4	C3	S3	D
Oversteering	Parking < 10 km/h	Side Road	Dry road	E4	C1	S1	QM

Exposure:

- E3: 1-10% of average operating time
- E4: >10% of average operation time

Controllability (Average Driver):

- C1: Hazardous situation is simply controllable
- C3: Hazardous situation is usually not controllable

Severity:

- S1: Light to moderate injuries
- S3: Critical injuries

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Efficient Traceability and Consistency

Safety Goals

SG1	HZ1, HZ3	ASIL B	Safety Goal 1
SG2	HZ2	ASIL D	Safety Goal 2
...	...	...	...

Hazard Analysis & Risk Assessment

Item Definition

Functional Safety Concept

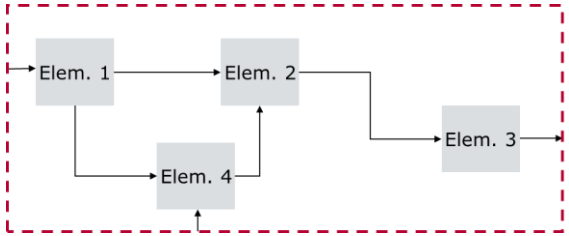
Functional Safety Requirements

FSR 1	SG1	ASIL B	Funct. Safety Req. 1
FSR 2	SG1	ASIL B	Funct. Safety Req. 2
...	...	...	...

Allocation of FSRs to architectural elements

System Architectural Design (external input)

Preliminary Architecture / System Architectural Design



Technical Safety Concept

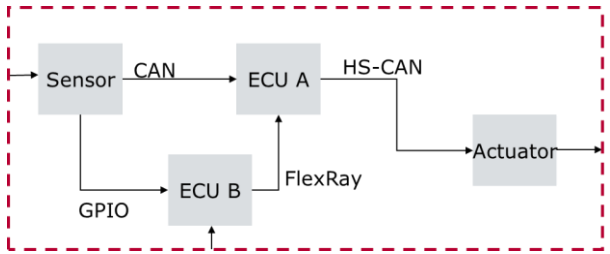
Refinement of Architectural Design

Technical Safety Requirements

TSR 1.1	FSR 1	ASIL B	HW/SW	Tech. Safety Req. 1.1
TSR 1.2	FSR 1	ASIL B	HW/SW	Tech. Safety Req. 1.2
...	...	...	...	...

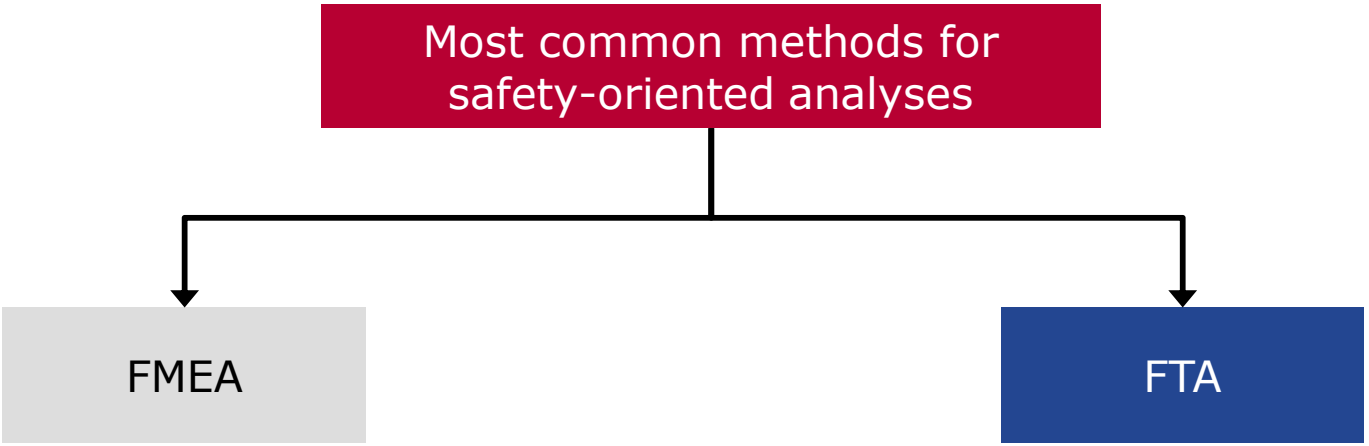
Allocation of TSRs to architectural elements

System Architectural Design



© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

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

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Approaches to Risk Reduction

Objectives:

- Avoid failures
- Make unavoidable failures safe

Failure

- Random Failure
- Systematic Failure

Technical measures against **random** HW failures:

- Redundancy
- Safety mechanisms ("Diagnostics")
- Self-tests
- …

Technical measures against **systematic** system, HW and SW failures:

- Redundancy
- Diagnostics
- Self-tests
- Modular HW/SW architecture
- Architecture patterns
- Defensive programming
- …

Methodological measures to ensure the application of a safety-conform **development process**:

- Top-down design flow
- Requirements based engineering
- Design methods
- Analysis techniques
- Test methods
- Traceability
- Reproducibility
- Detailed process requirements
- …

Product Measures

Process Measures

ISO26262 (ASIL)

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Your Questions

Remark: If we are not able to answer your question within the hour we will send you the answer via mail in the coming days!

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

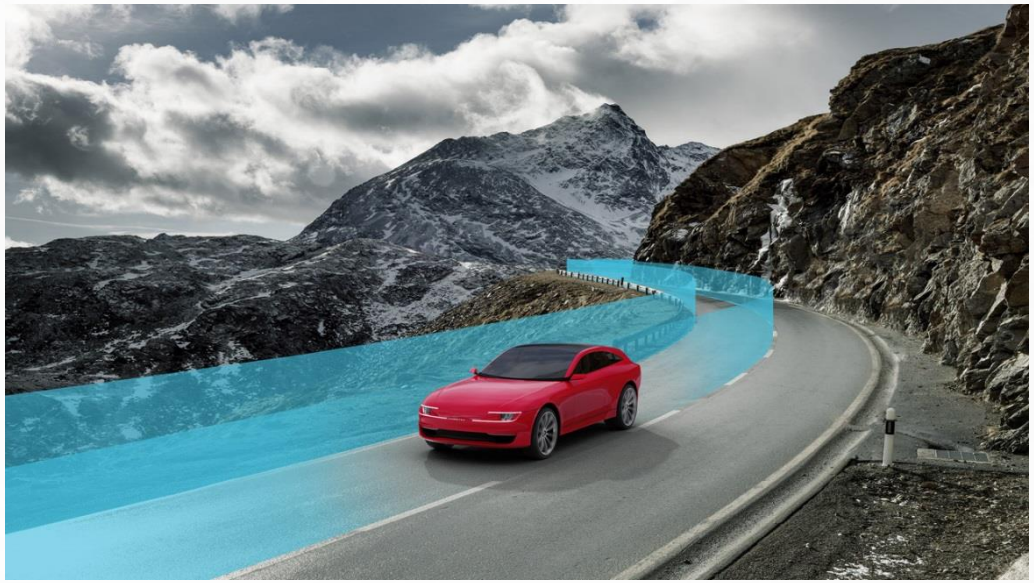
Agenda

Welcome and Introduction

Challenges and Concepts

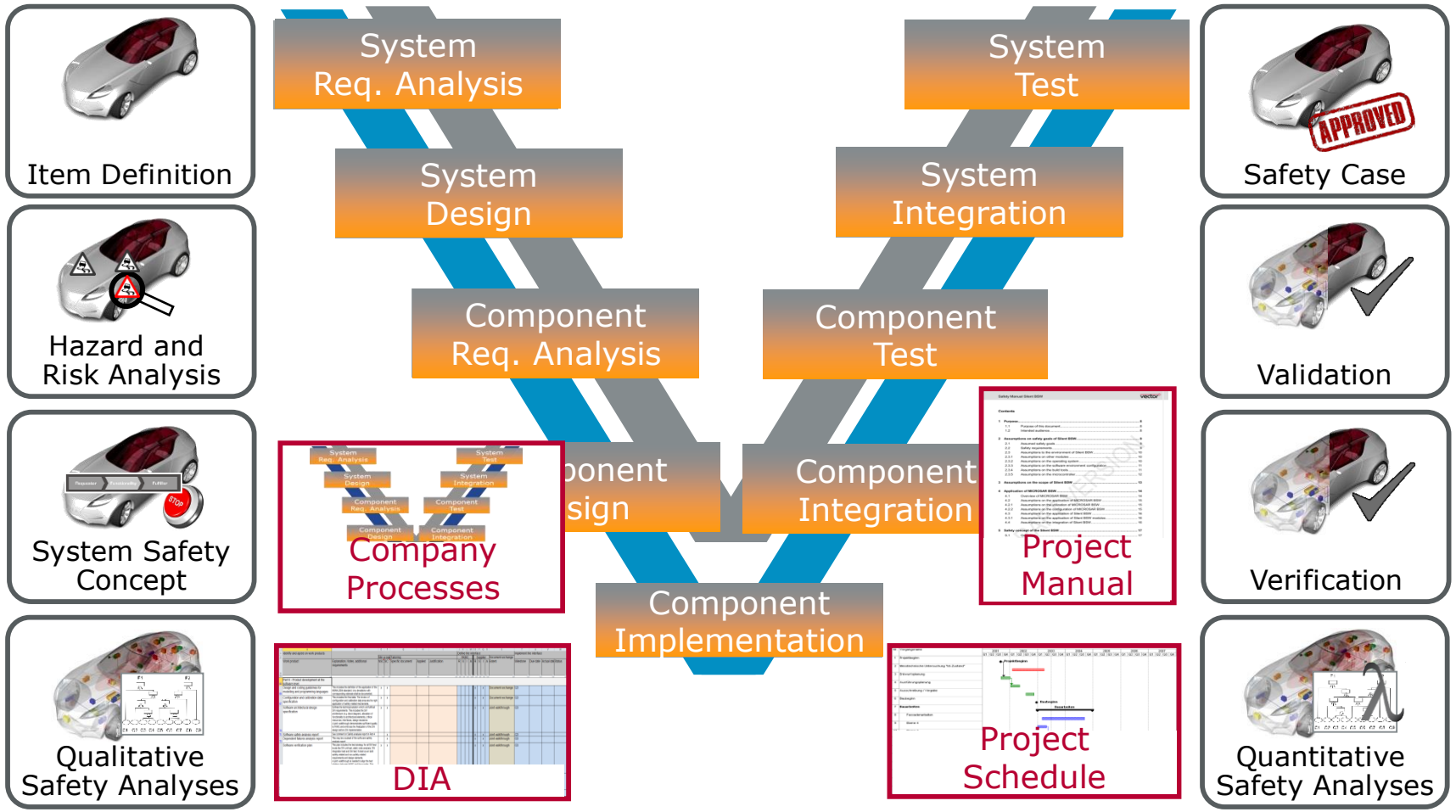
▶ **Vector Safety Experiences**

Conclusions and Outlook



© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

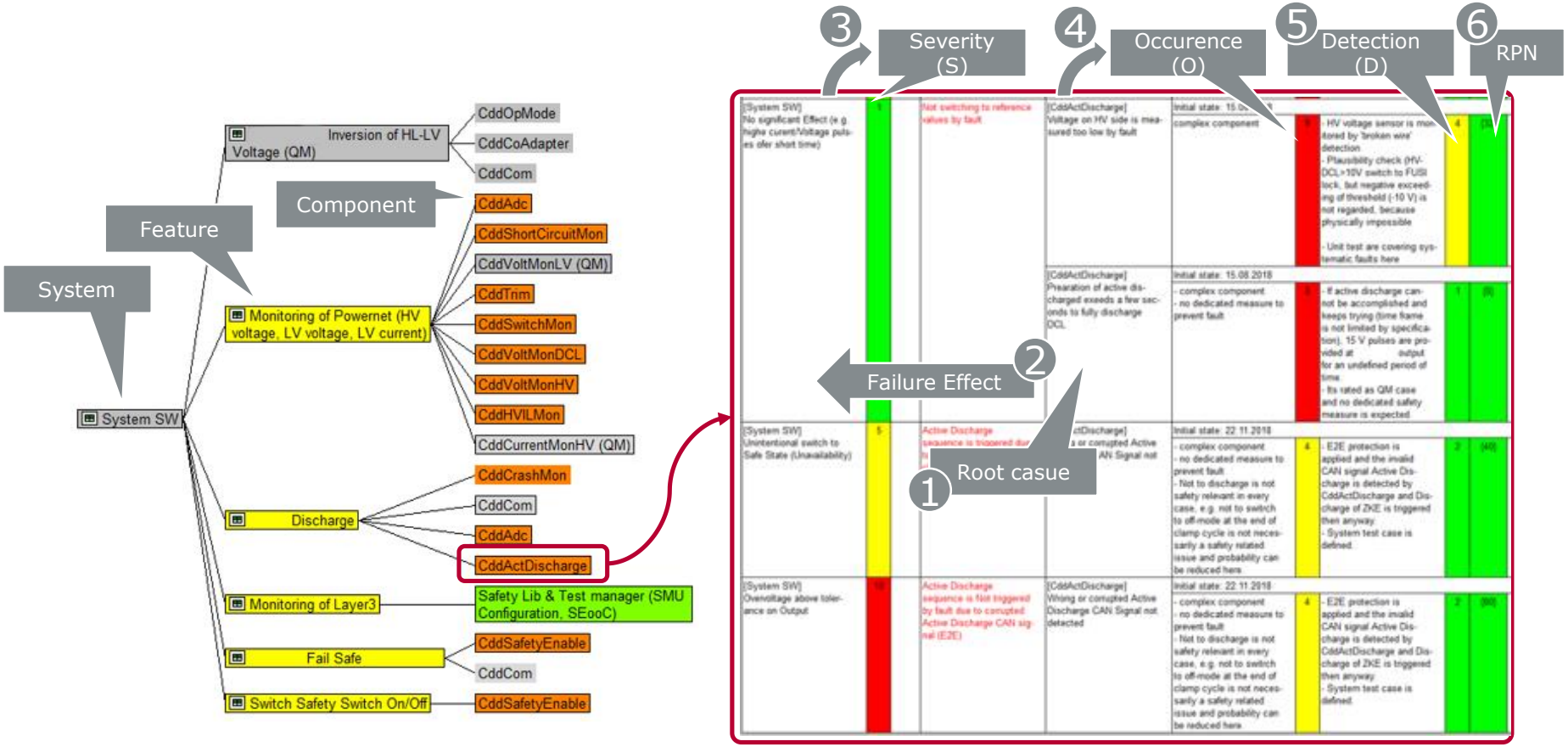
Vector Experiences – Support Throughout the Life-Cycle



Consistently plan and systematically maintain safety artefacts

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Example SW Safety Analysis - *SW-FMEA*: Vector Best Practice

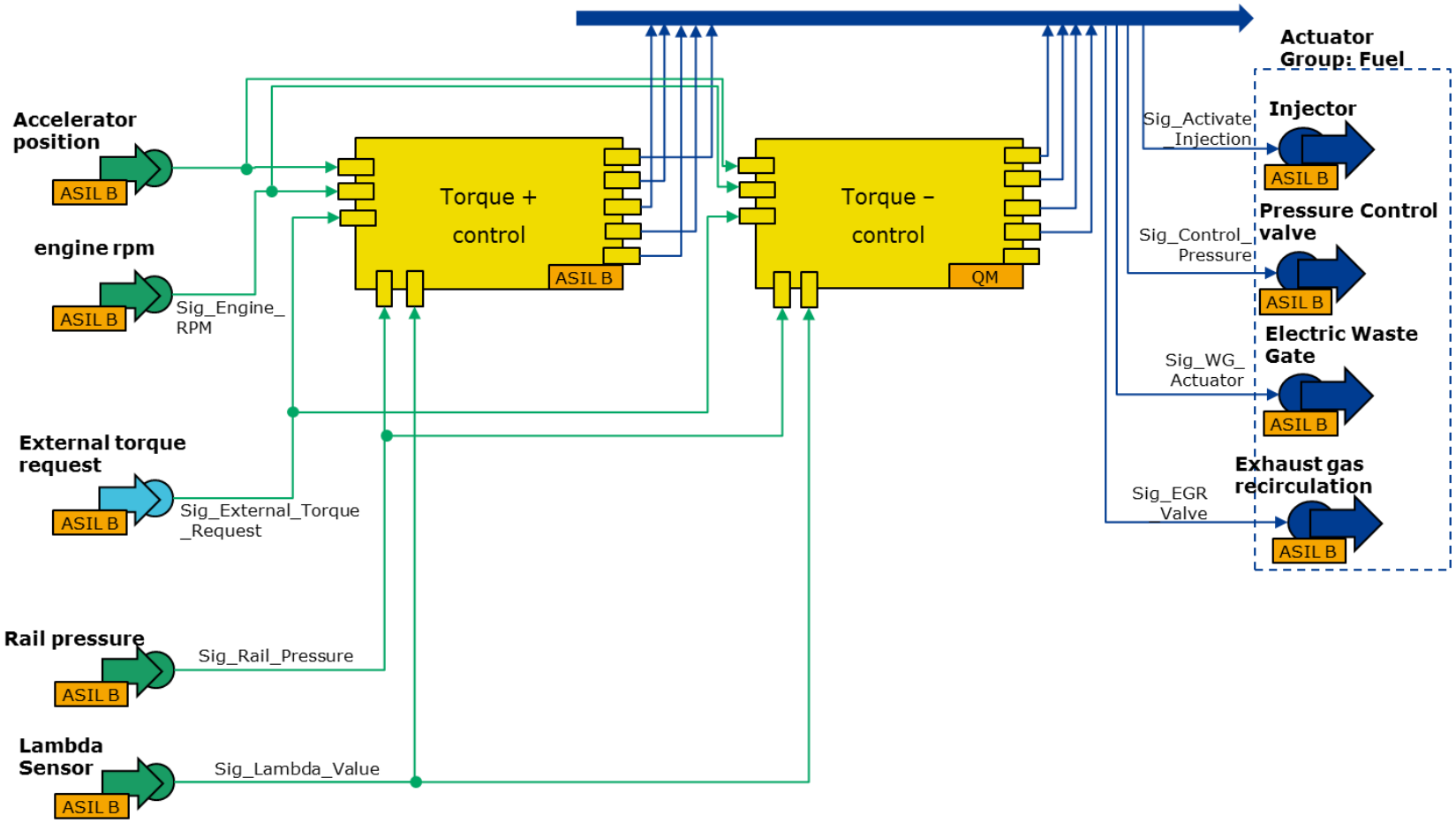


SW Safety Analysis assumes **occurrence** of SW faults based on complexity of SW.

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Example FSC – SysML Block Diagram as *Vector Best Practice*

SysML is a semi-formal notation and recommended by ISO 26262:



Functional safety is about **requirements** & **solution** development (*Two-Pillar approach*)

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

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 dat	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

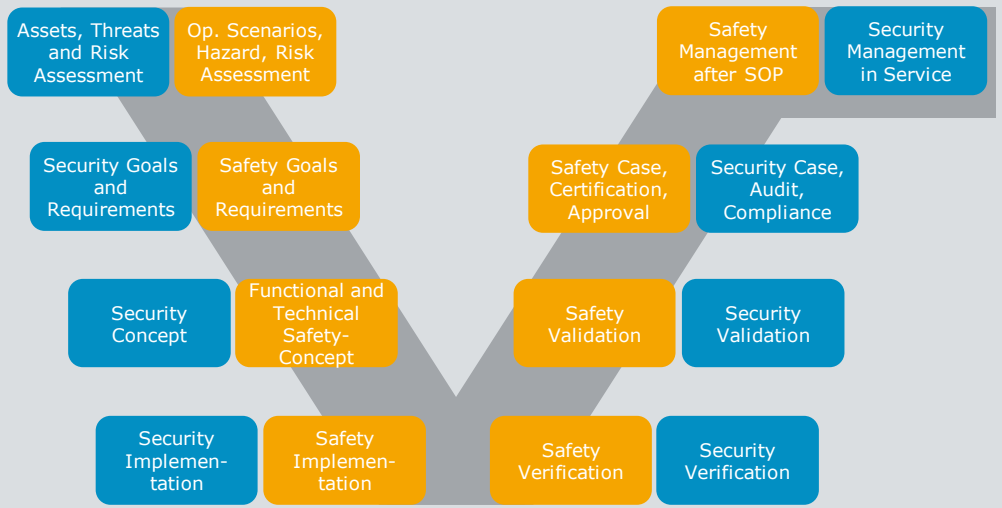
© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Vector Experiences – Security Directly Impacts Safety

Functional Safety (ISO/PAS21448, ISO 26262)

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

Security not sufficiently addressed



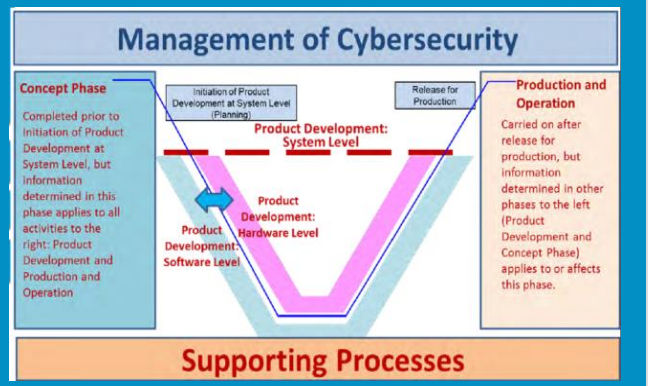
+ Security

(J3061, ISO/SAE 21434)

- Threat, Attack and risk analysis
- Attack paths and vulnerabilities
- Security engineering

- Security & Safety are interacting and demand holistic systems engineering

- For fast start security engineering should be connected to safety framework



© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

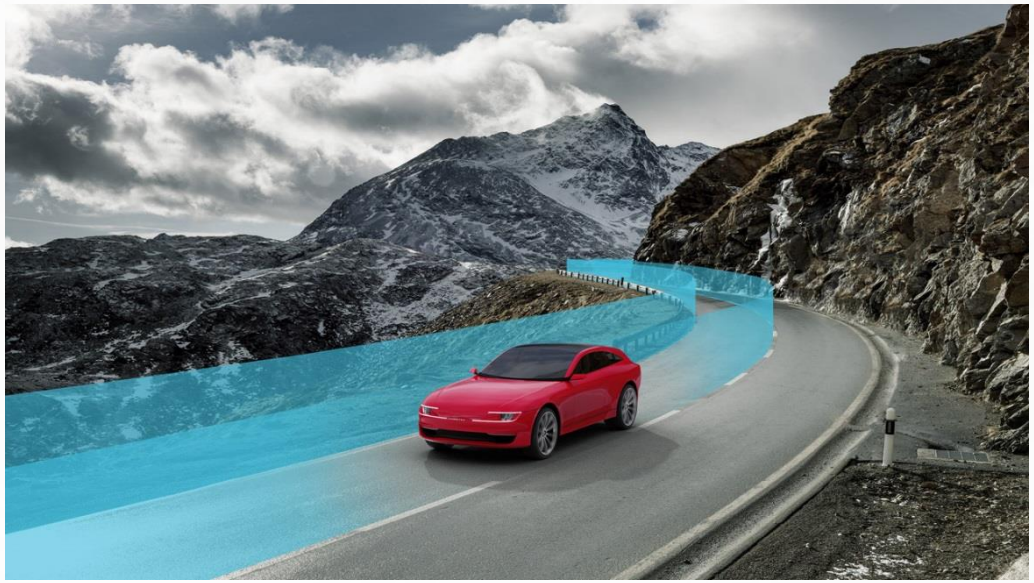
Agenda

Welcome and Introduction

Challenges and Concepts

Vector Safety Experiences

▶ **Conclusions and Outlook**



© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

VECTOR

ISO26262 Experience

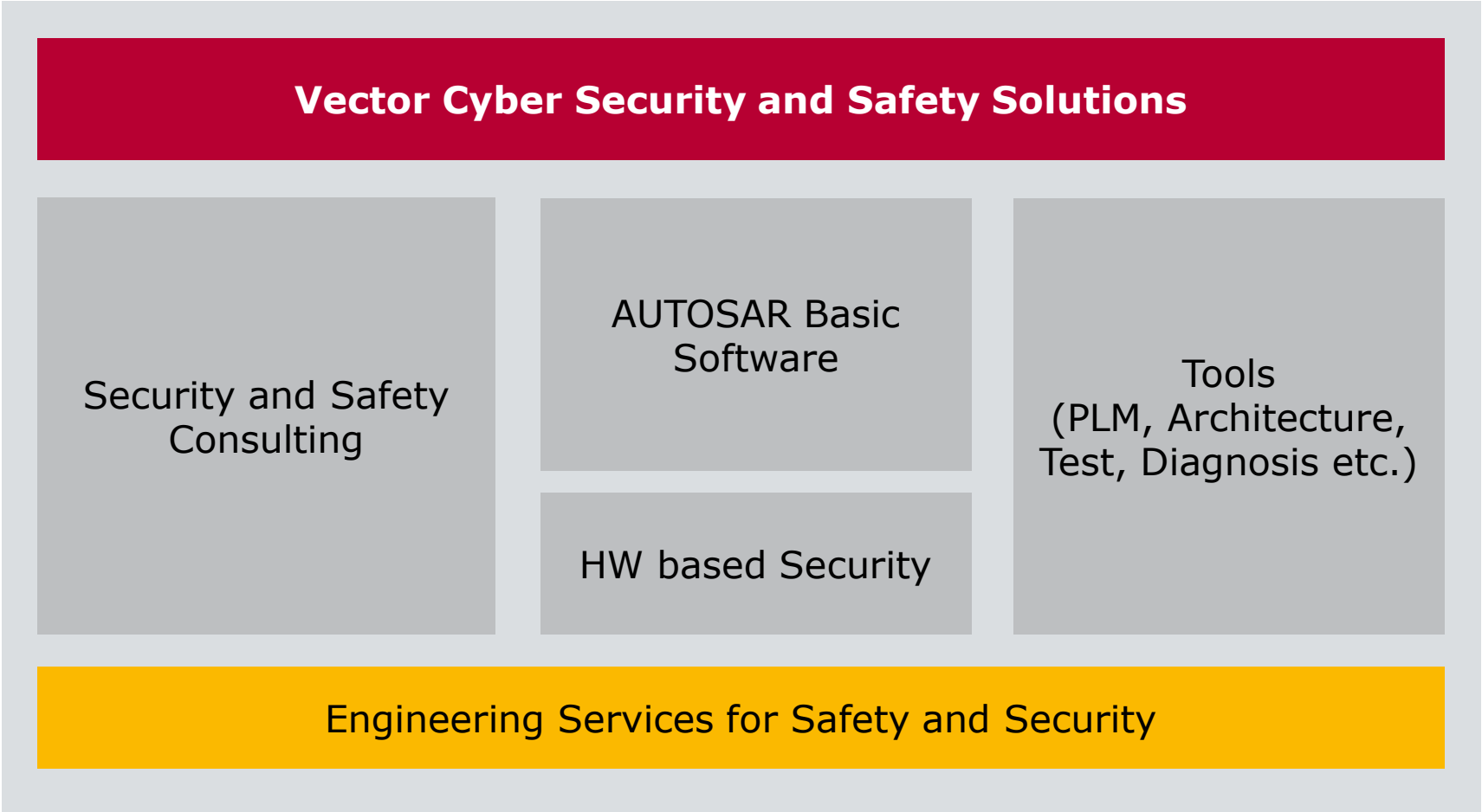
- **Increasing functional safety capabilities**
  - Majority of OEM´s include ISO26262 compliance in their contracts
  - Independent audits and assessments are performed
  - Methods for qualitative and quantitative analysis are available
  - ASIL D HW and SW components are available as SeooC

- **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.

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Vector: Comprehensive Portfolio for Security and Safety



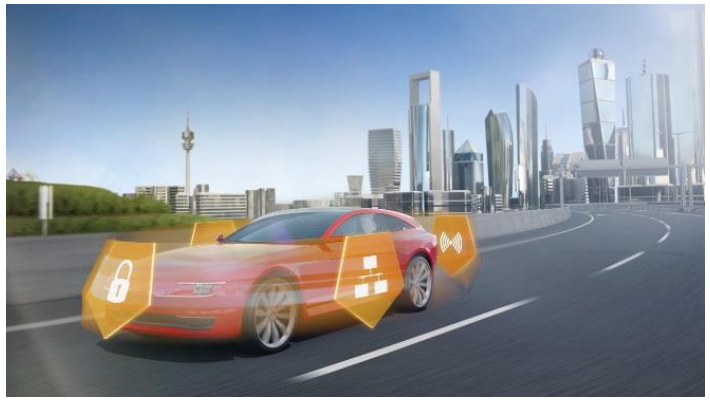
www.vector.com/safety www.vector.com/security www.vector.com/consulting

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12

Vector Safety Solutions

Trainings and media

- Training "Functional Safety with ISO 26262" Stuttgart, continuously www.vector.com/training-safety
- Virtual trainings
- Free white papers… www.vector.com/media-safety



- **Vector Forum – Achieving Engineering Competitiveness (25 June 2020), on your computer – It is a virtual event** https://consulting.vector.com/int/en/company/vector-forum/2020/

- **Further free Webinars:**
  - 2020-06-17 Automotive Cybersecurity – Challenges and Practical Guidance

https://www.vector.com/int/en/events/webinars/

© 2020. Vector Consulting Services GmbH. All rights reserved. Any distribution or copying is subject to prior written approval by Vector. V1.10 | 2020-05-12