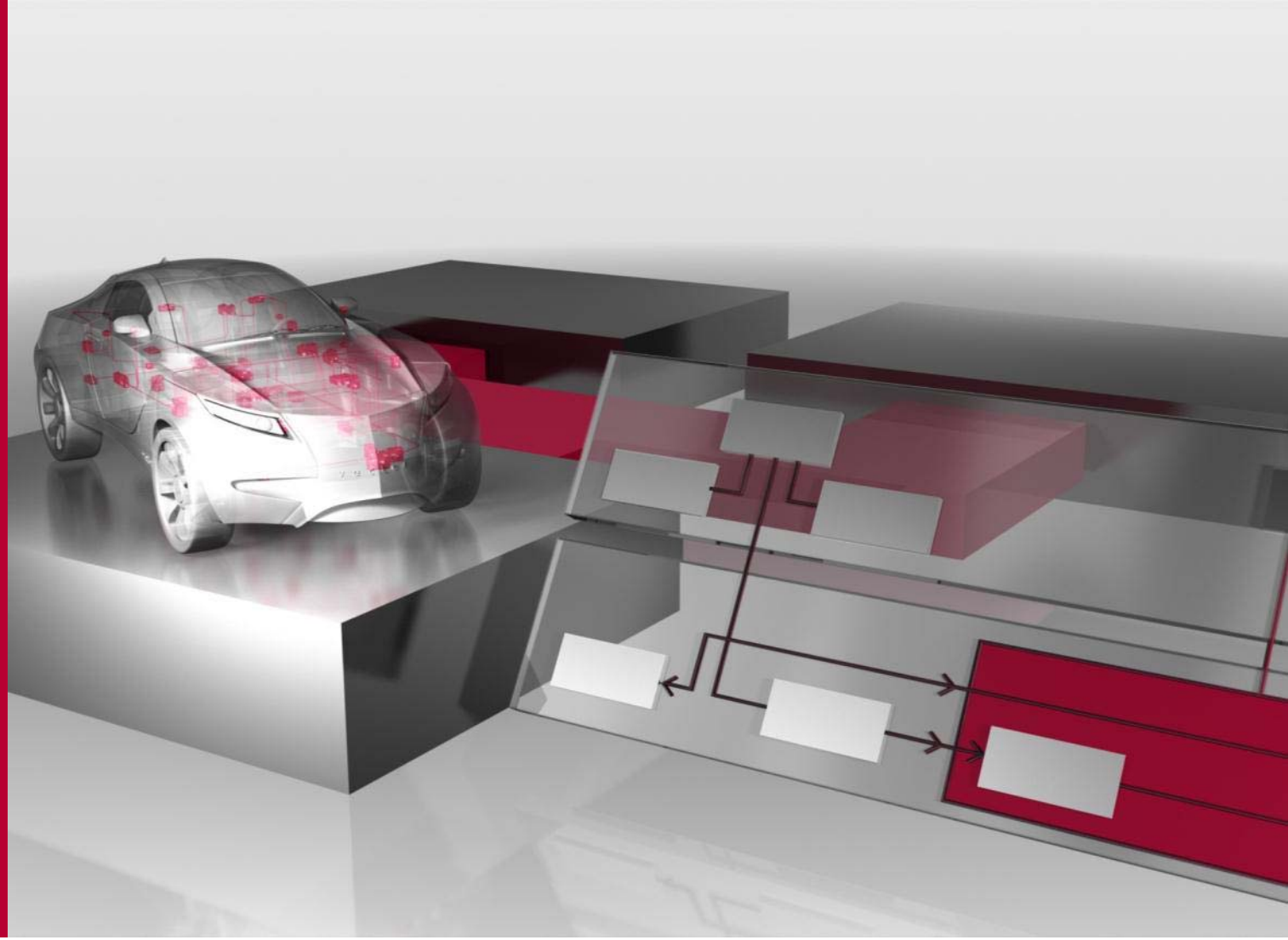


Functional Safety with ISO 26262

Principles and Practice

Dr. Christof Ebert, Dr. Arnulf Braatz
Vector Consulting Services

Welcome to the Webinar

Functional Safety with ISO 26262

Webinar Part 1, Principles and Practice

Speakers: Dr. Christof Ebert, Dr. Arnulf Braatz

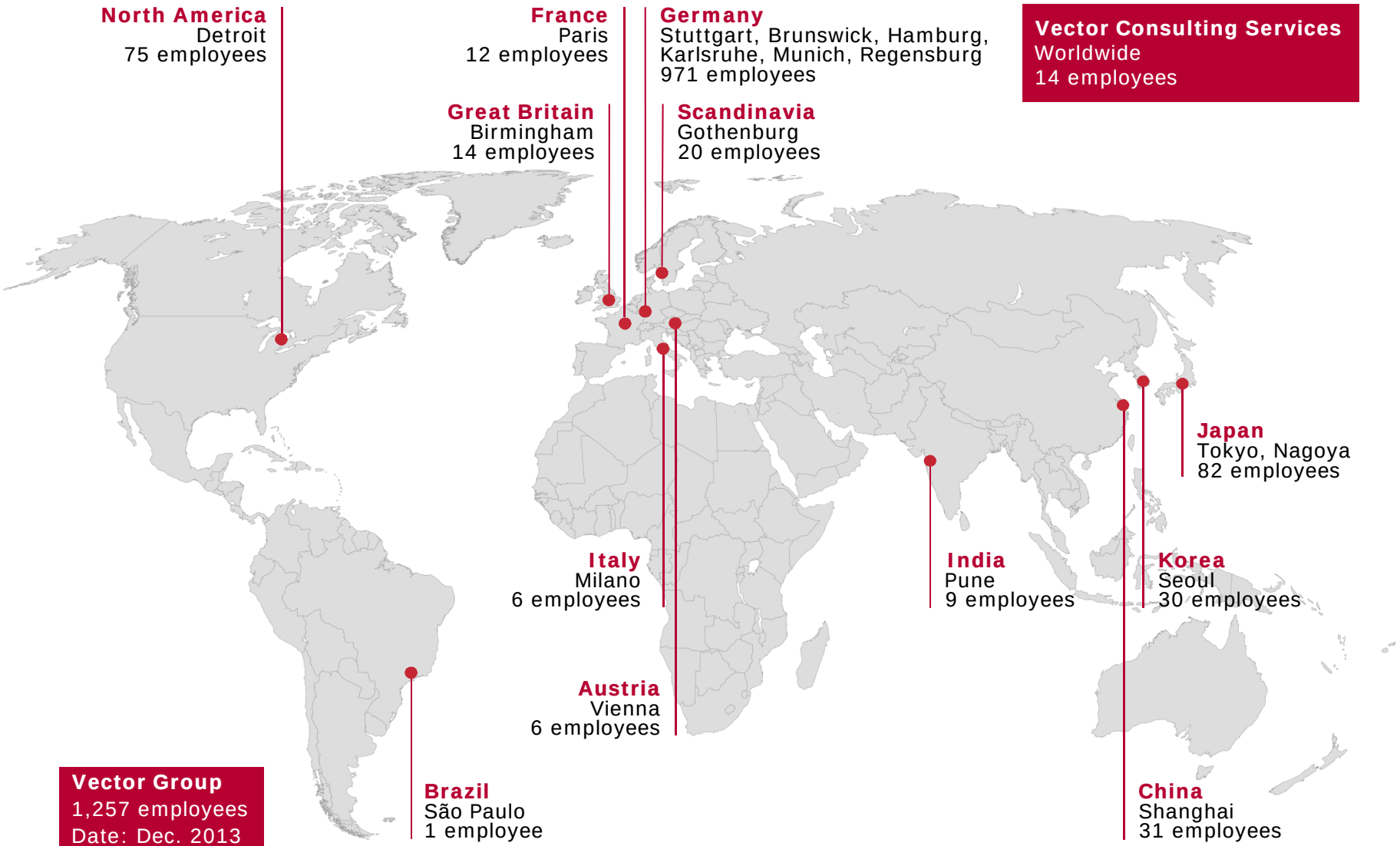
Technical Notes

- **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 presentation 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.

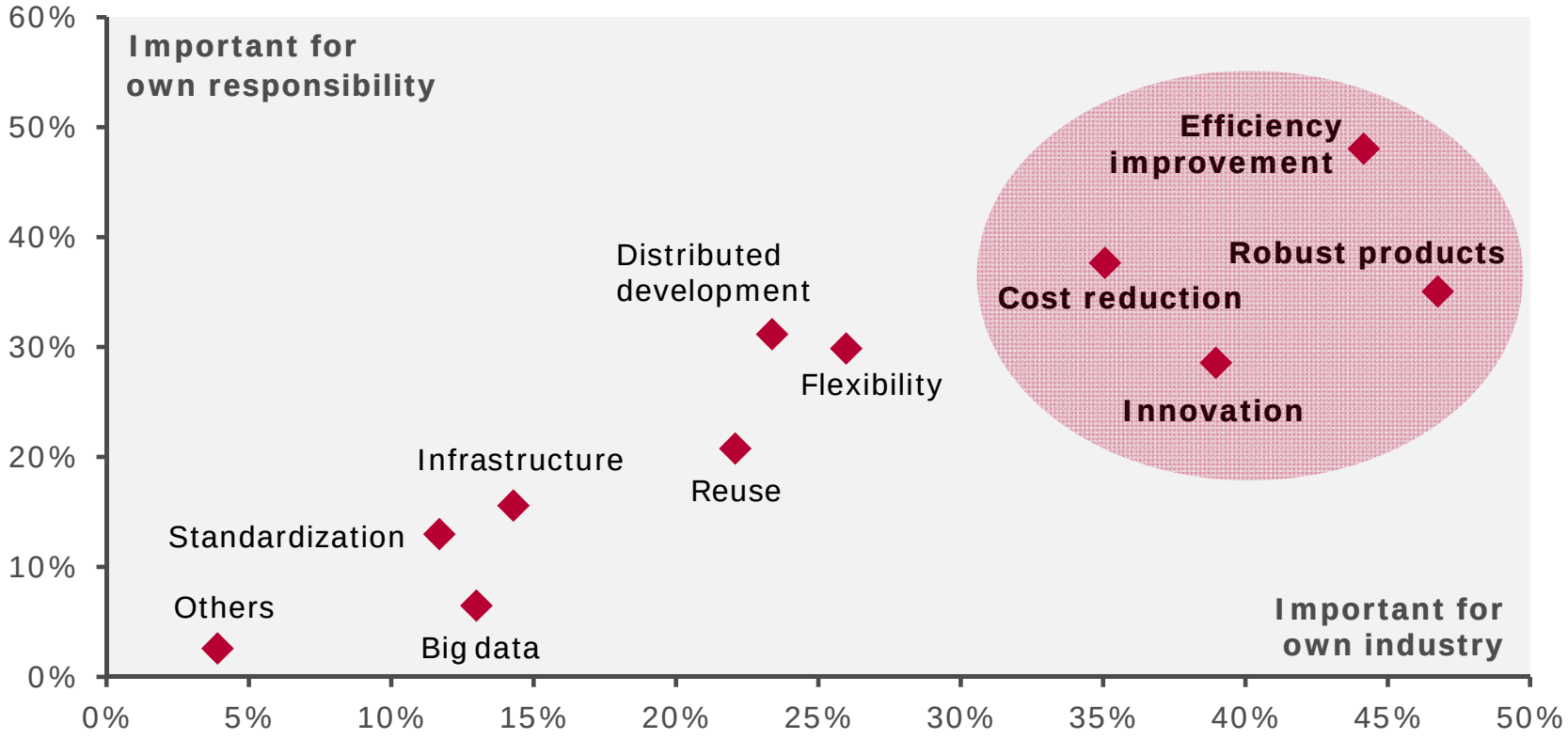
Content

- **Challenges with Implementing Functional Safety**
- Basic Concepts
- Vector Experiences
- Success Factors

Vector Worldwide



Challenges in 2014 – Results from Vector Client Survey

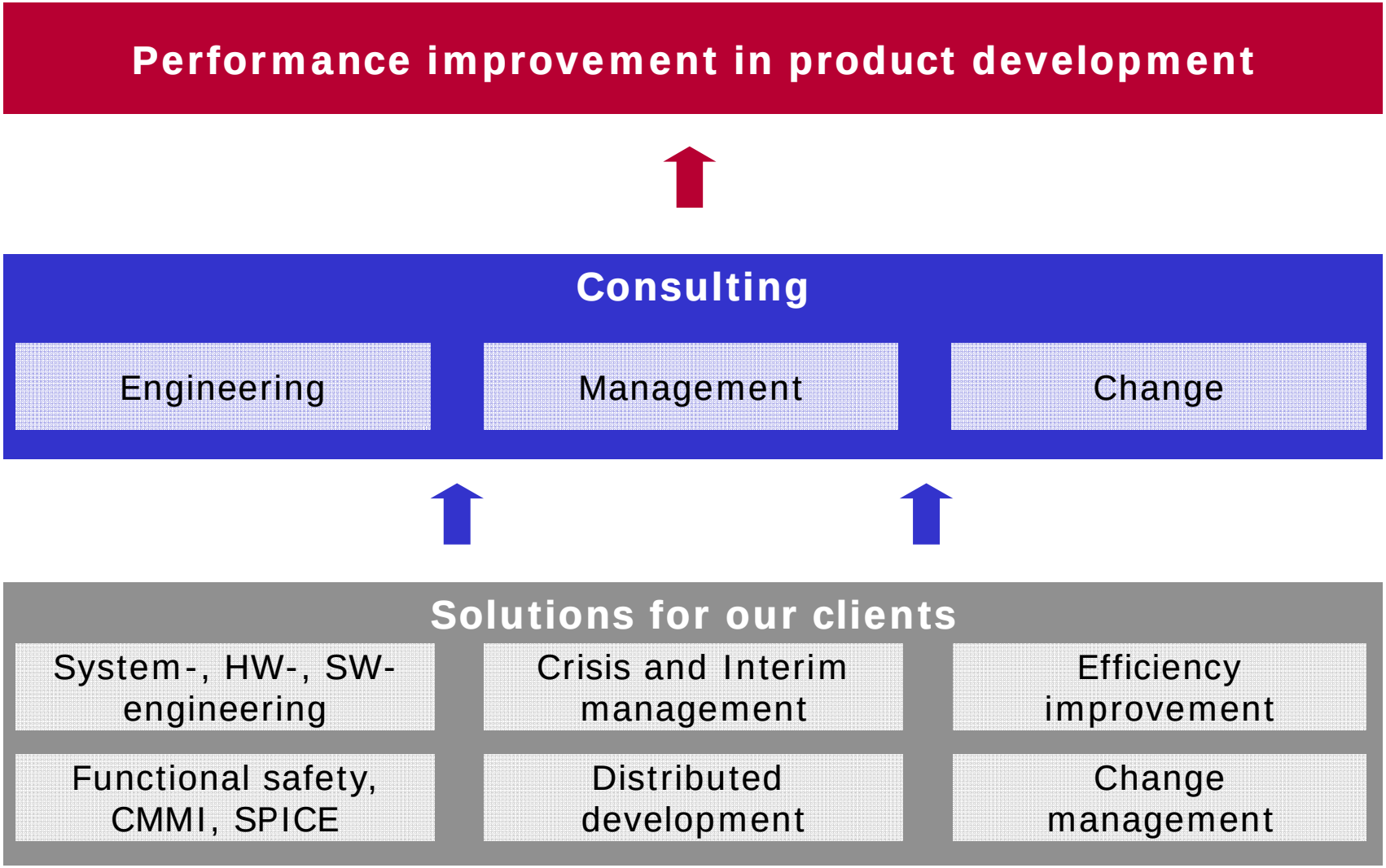


Vector client survey 2014. Details at: www.vector.com/trends-2014
Sum > 100% because 3 answers per question were allowed

Survey results: Four clear focus areas

- Efficiency improvement
- Robust products
- Cost reduction
- Innovation

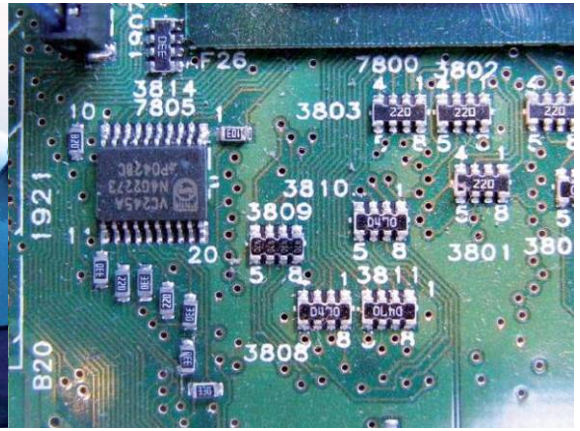
Vector Consulting Services – Business Field



Industry Diversification

Automotive

Aviation & Defense



IT

Energy & Environment

Medical & Health

Railway & Transportation

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, sustainable safety culture
- Implementing consistent tool support, such as PREEvision

Safety Management (Examples)

- Provisioning (interim) safety managers
- Performing safety audits and supplier safety audits

Safety Engineering (Examples)

- Providing software components and platforms, such as MICROSAR Safe
- Facilitating safety analyses, e.g. HARA, FMEA, FMEDA, reviews
- Developing and reviewing safety concepts

Vector Consulting Services – ISO 26262 Customers

vector

Content

- Challenges with Implementing Functional Safety
- **Basic Concepts**
- Vector Experiences
- Success Factors

Functional Safety – Recent Call-Backs

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

Korean OEM, 2013

Problems with acceleration:
Car unintentionally accelerates thus causing personal damage

Japanese OEM, 2013

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

American OEM, 2013

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

German OEM, 2013

Source: autoservicepraxis.de

Many incidents ➔ Risk of liability

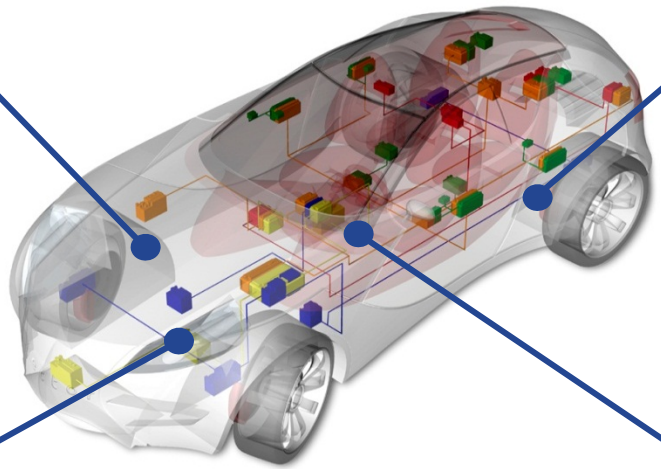
Functional Safety: Broad Exposure

ESP

- Unintended, single-sided brake effect on straight lane

Electronic Park Brake

- Unintended activation in motion



Collision Avoidance

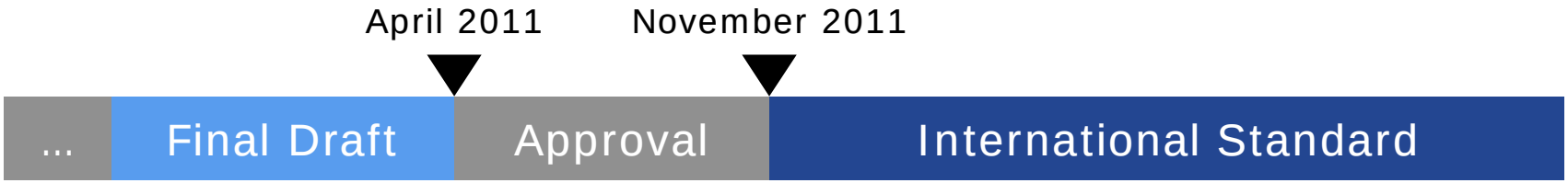
- Acceleration instead of deceleration in traffic

Airbag

- Delayed deployment after crash detection

Exposure of almost many E/E functions ➔ Risk of liability

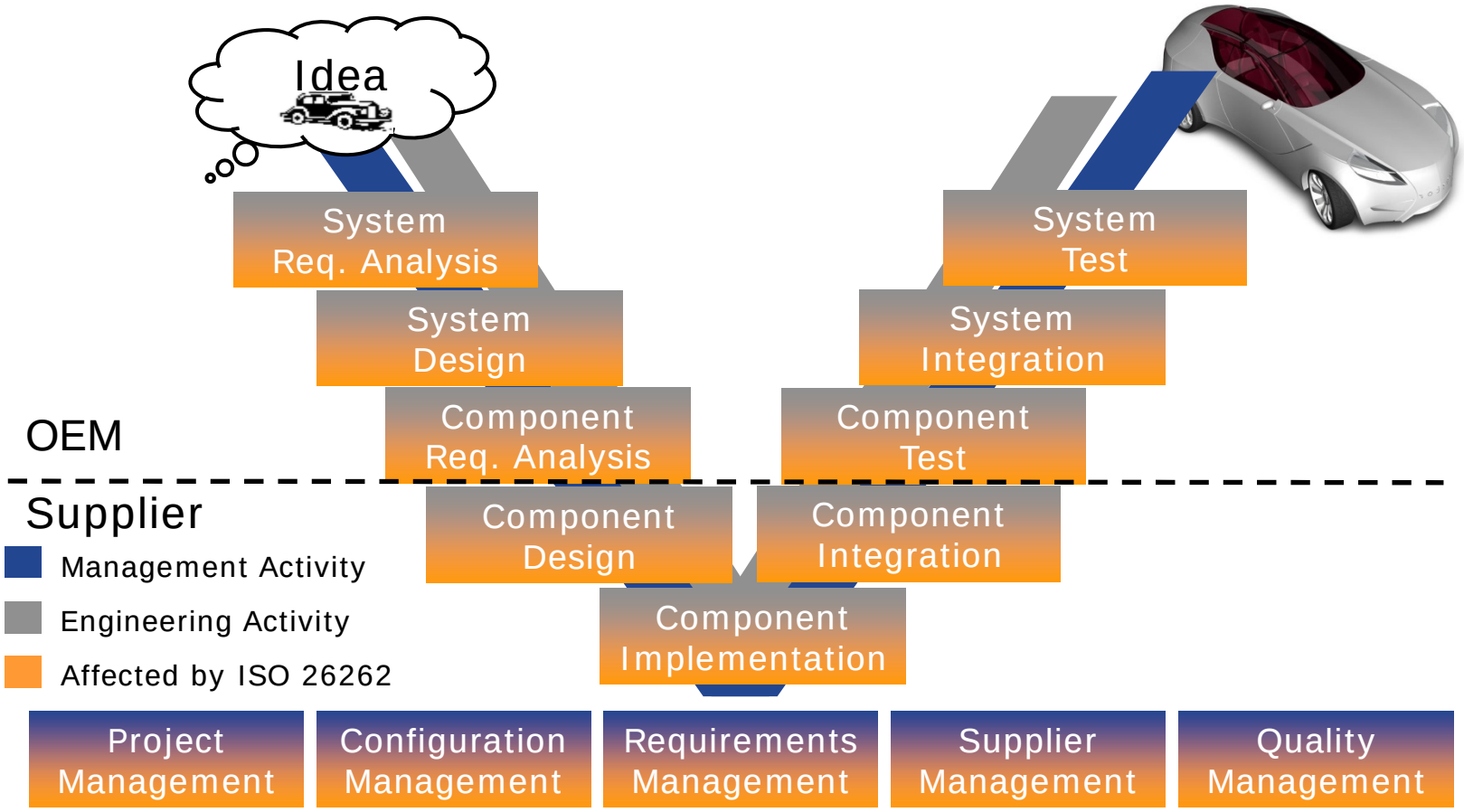
Functional Safety – Mandatory Standard



- ISO 26262 is an „International Standard" for the automotive industry, based on the generic safety standard IEC 61508
- Functional safety is considered critical to product liability
- OEMs demand fulfilling the standard from their suppliers
- Mature development processes (e.g. SPICE L3, CMMI ML3) facilitate implementing ISO 26262

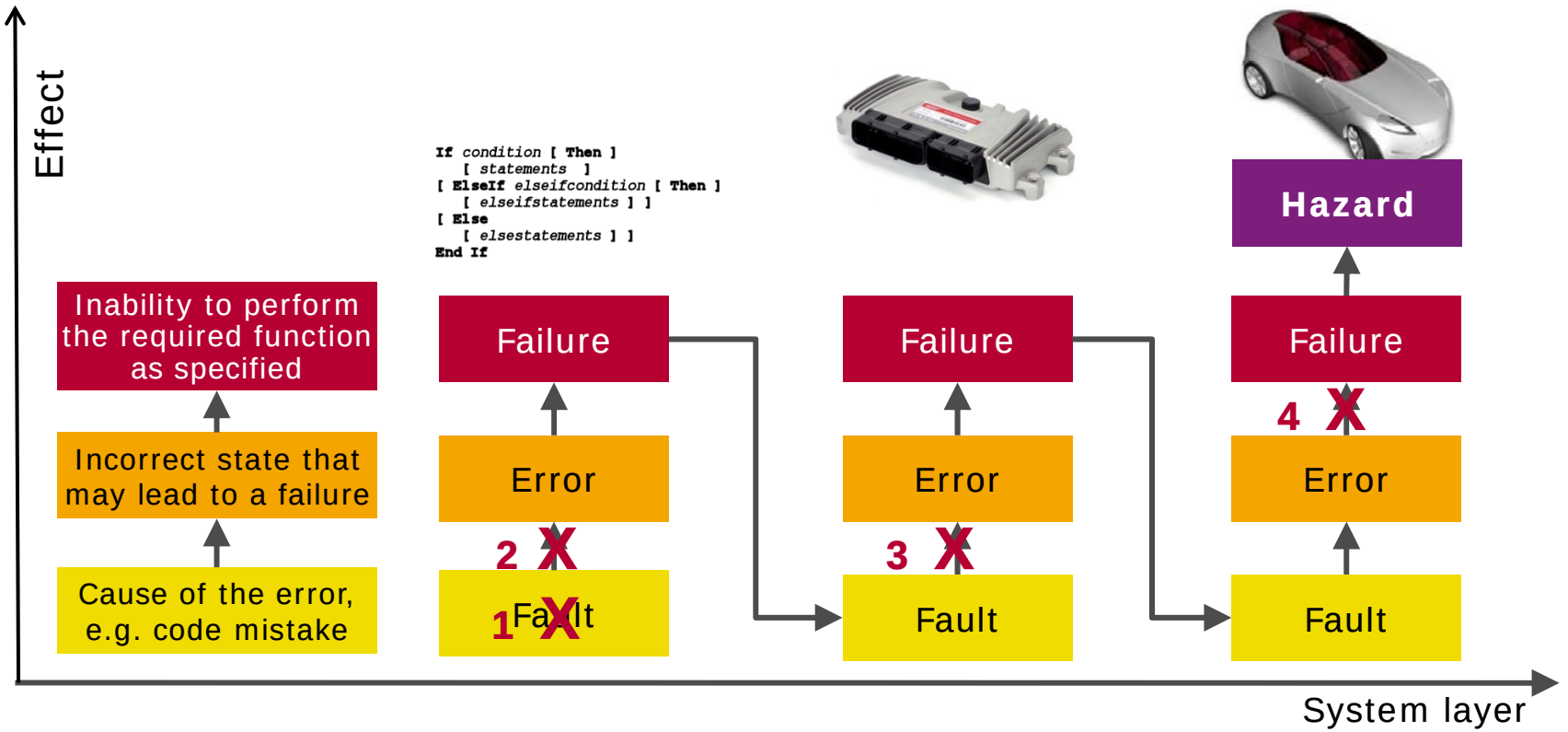
Not yet integrated to product life-cycle ➔ Risk of falling short

Functional Safety – Wide Impact



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

Functional Safety – Many Methods



1 Fault prevention	2 Fault detection	3 Fault tolerance	4 Failure prevention
▶ Guidelines	▶ Code analysis	▶ Redundant design	▶ Redundant Shut-off
▶ Processes	▶ Review, Test	▶ Memory protection	▶ Fail-safe concepts

Many methods and techniques ➔ Risk of uninformed usage

Functional Safety – Complex Standard

10 Parts

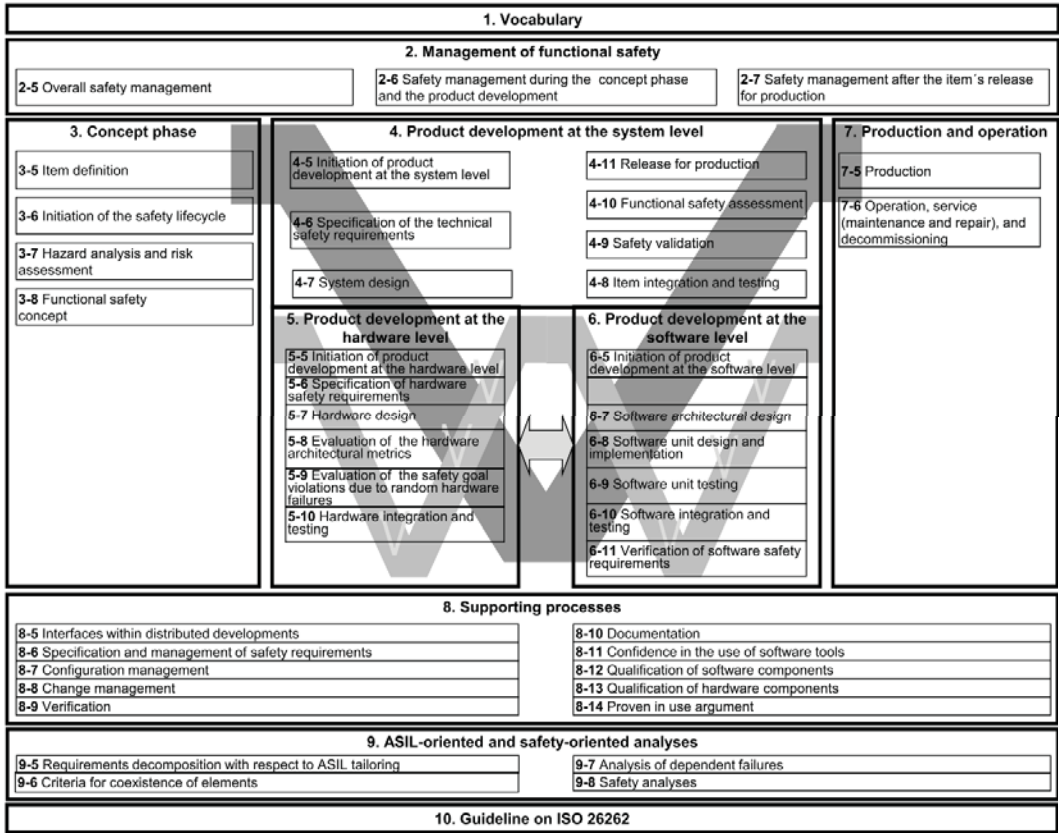
43 Chapters

100 work products

180 engineering methods

500 pages

600 requirements



Source: ISO 26262

Complex standard ➔ Risk of overheads and bureaucracy

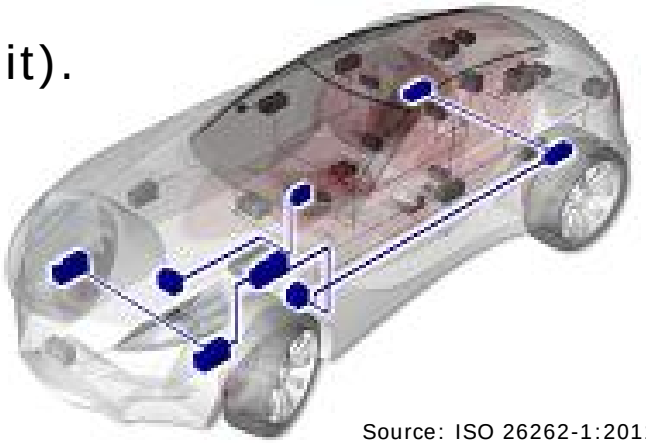
Scope of ISO 26262

ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3 500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

[...]

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.

- Systems with safety-related functions,
- realized in E/E systems (e.g. control unit).
- Common passenger cars.
- Series production.
- < 3,5 t.



Source: ISO 26262-1:2011

Why?

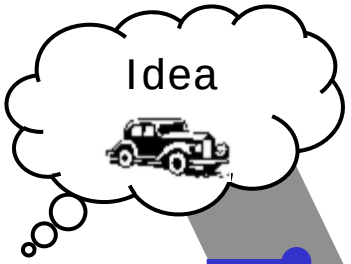
- Trust in products (i.e. contractual liability)
- Moral commitment: „The prevention of accidents must not only be considered as a regulation by law, but as a matter of human commitment and economic reason."
  - Werner von Siemens -
- Legal obligation – Product liability, Manufacturer's liability

How?

- What is „**safe**"? → Conform to current state-of-the-art of science and technology
  - Publications
    - Conference Articles
    - Competitor Analysis
  - Standards

vector

The Question of 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

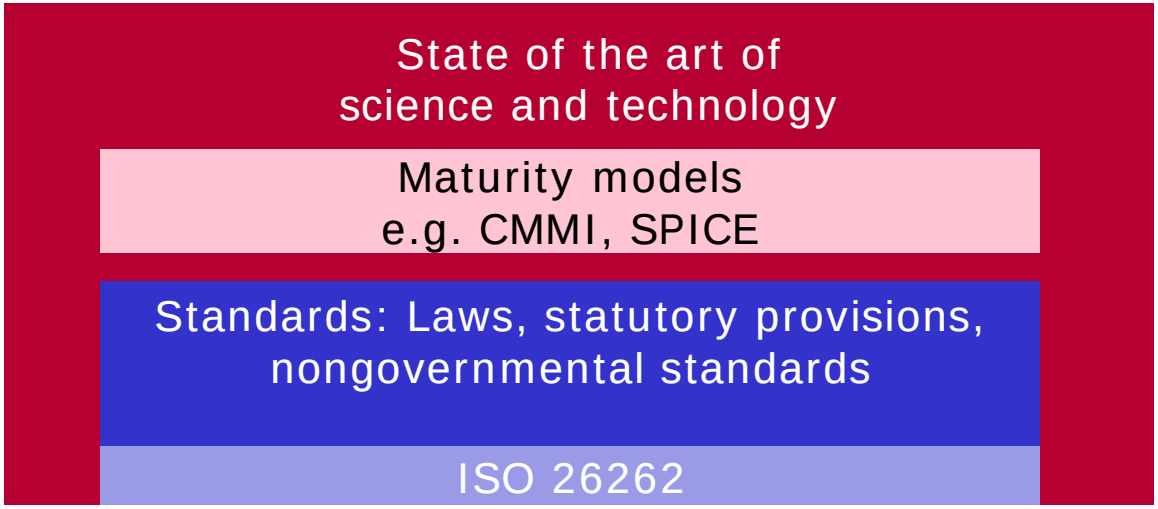
The manufacturer has to show that he is not responsible for a fault.

Product Liability

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

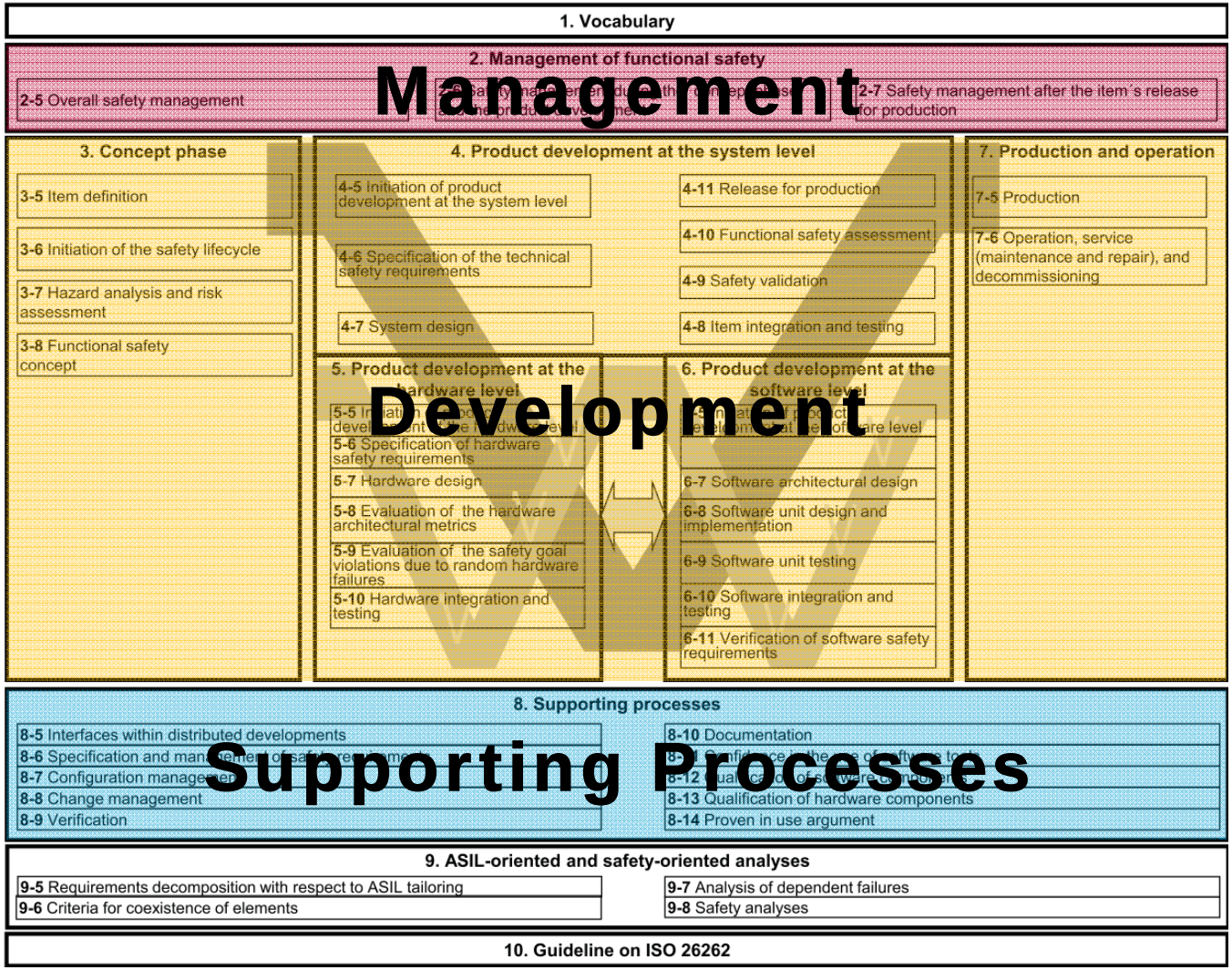
Manufacturer's liability is excluded, if a failure can not be detected using current state of science and technology at the time the manufacturer put the product into market.

Legal Liability



- Standards are the lower limit of the state of the art of science and technology.
- ISO 26262 is published and thus part of the state of the art of science and technology.
- Maturity models, like CMMI and SPICE, are also part of the state of the art of science and technology.
- Their application is therefore expected.

A Structured Approach



Source: ISO 26262-1:2011

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

Risk Severity Probability

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

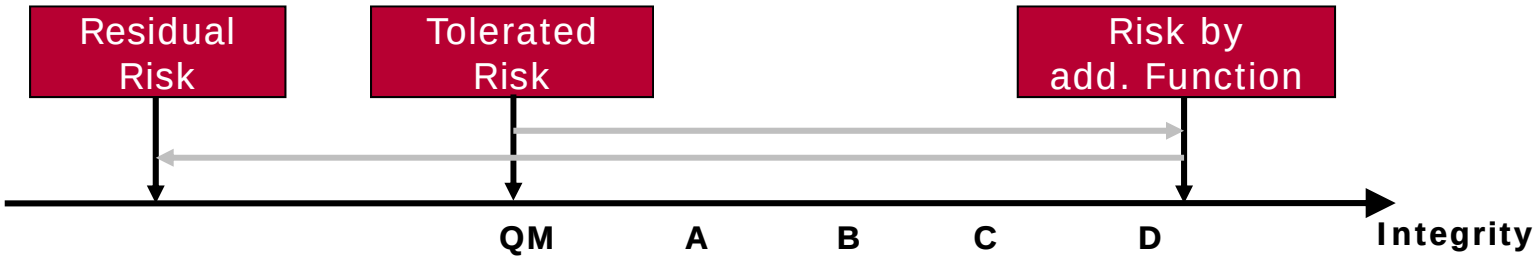
P_E: Exposure; P_C: Controllability; P_I: Integrity

ASIL

Automotive Safety Integrity Level

(= required integrity of a function)

S: Severity
E: Exposure
C: Controllability
I: necessary Integrity
QM: Quality Management



vgl. IEC 61508:2010

Development – Determination of ASIL

Risk Severity Probability

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

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

S: Severity
E: Exposure
C: Controllability
I: necessary Integrity
QM: Quality Management

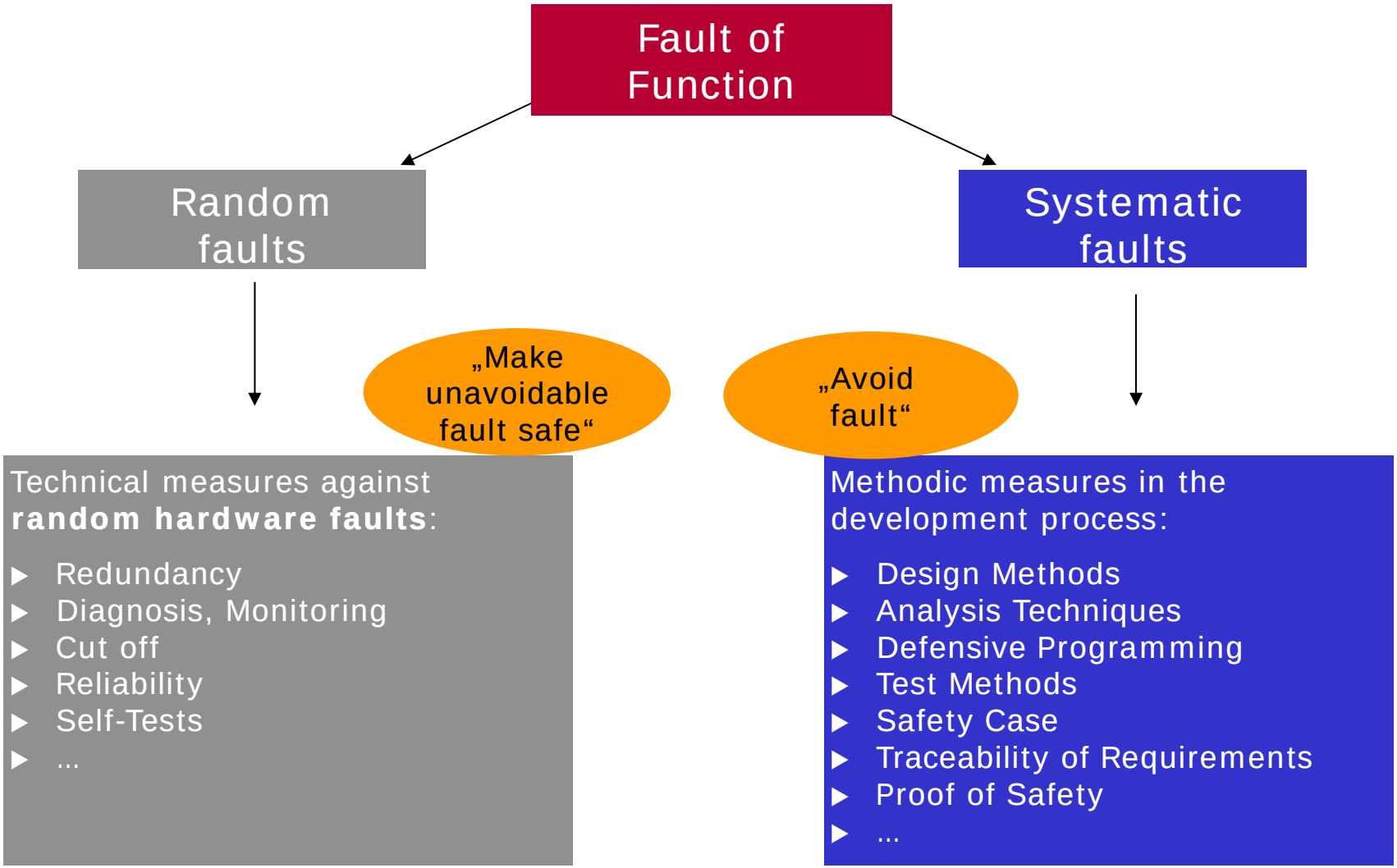
Source: ISO 26262-3:2011

Development – Classification Example 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

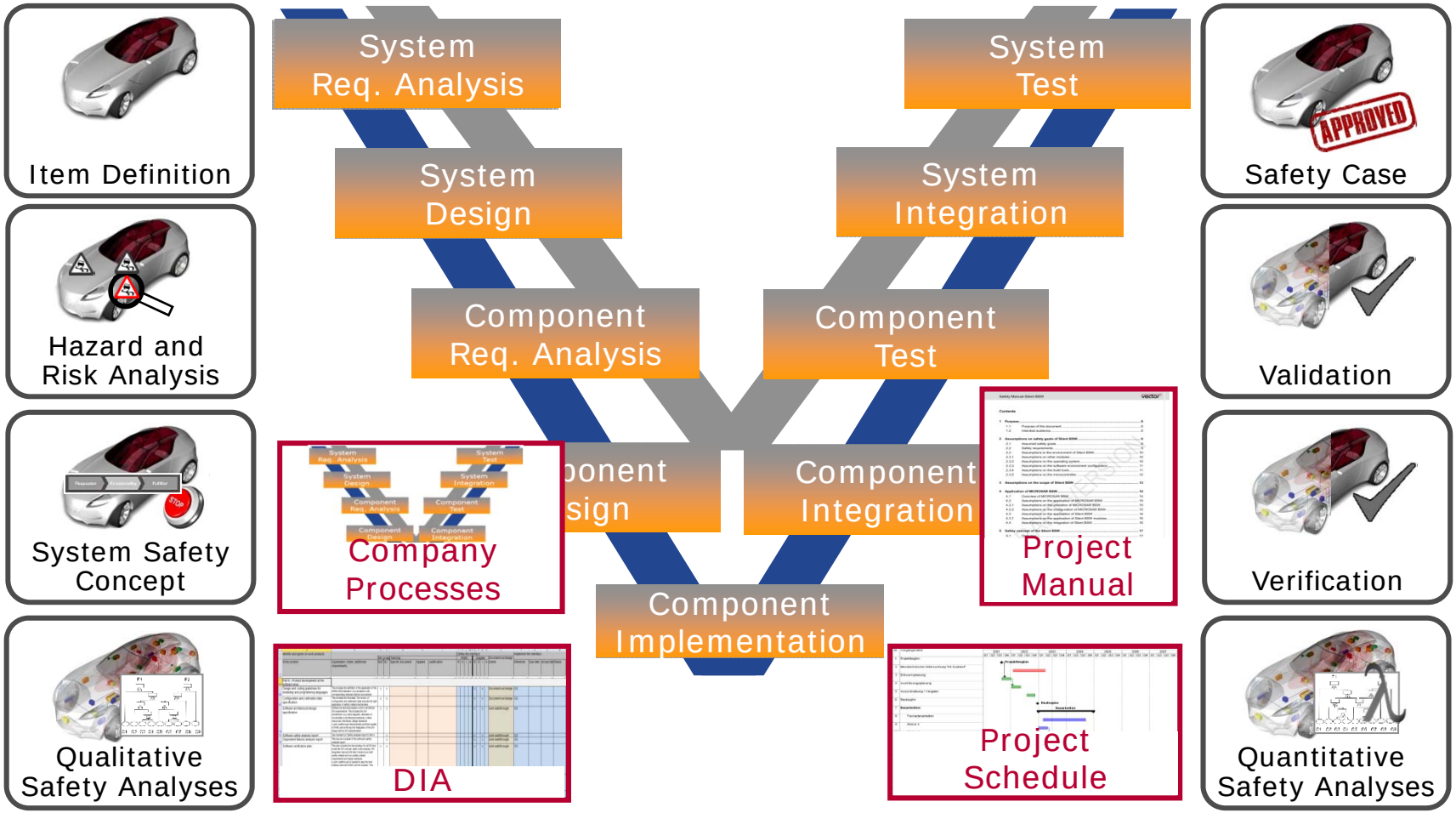
Approaches to Risk Reduction



Content

- Challenges with Implementing Functional Safety
- Basic Concepts
- **Vector Experiences**
- Success Factors

Vector Experiences – Safety Plan



Use consistent process, DIA, project schedule and manual for Safety Plan

Vector Experiences – Development Interface Agreement (DIA)

List of relevant artifacts

Minimum scope: ~ 60 artifacts

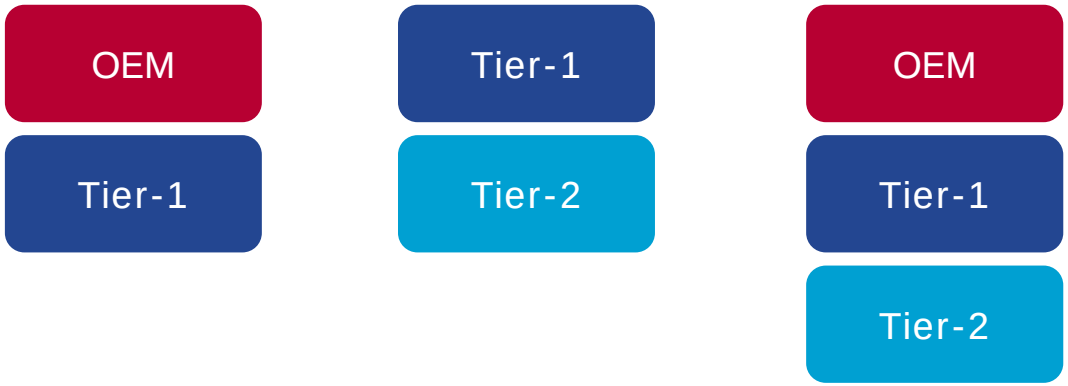
Project specific tailoring, application and tracking

	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 interface to your customer and/or supplier, extend the usage to not safety related artifacts

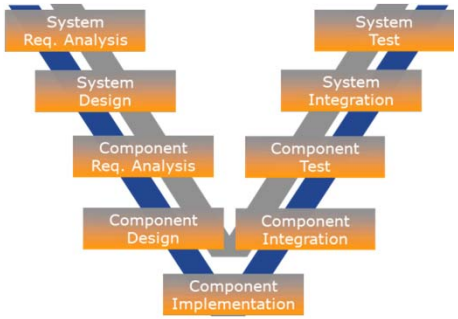
Vector Experiences – Including the Customer and Supplier

- 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 – Performing Audits and Assessments



Safety Audit

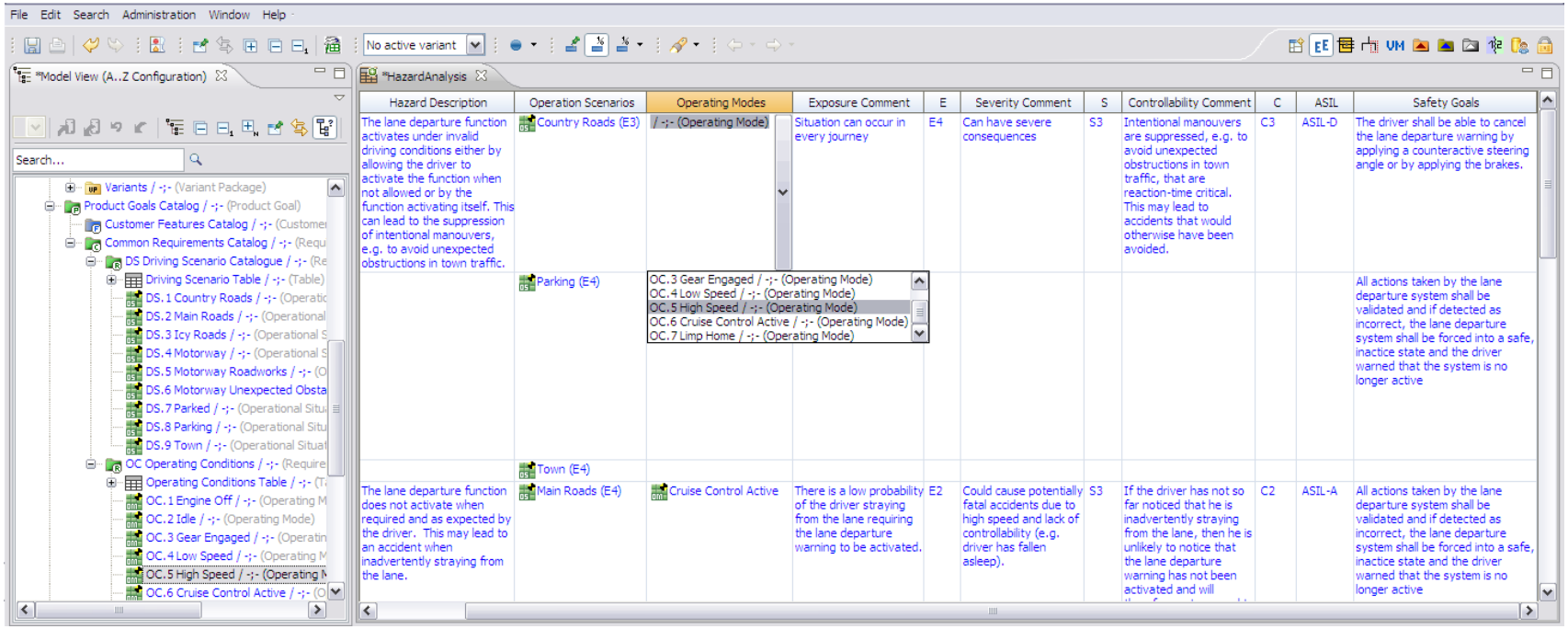
- Purpose: Evaluate implementation of the processes required for functional safety
- Perform periodic audits in projects
- Combine with SPICE assessments
- Perform short supplier audits before nomination, and comprehensive audits in B sample stage

Safety Assessment

- Purpose: Evaluate achieved functional safety within the defined item
- 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

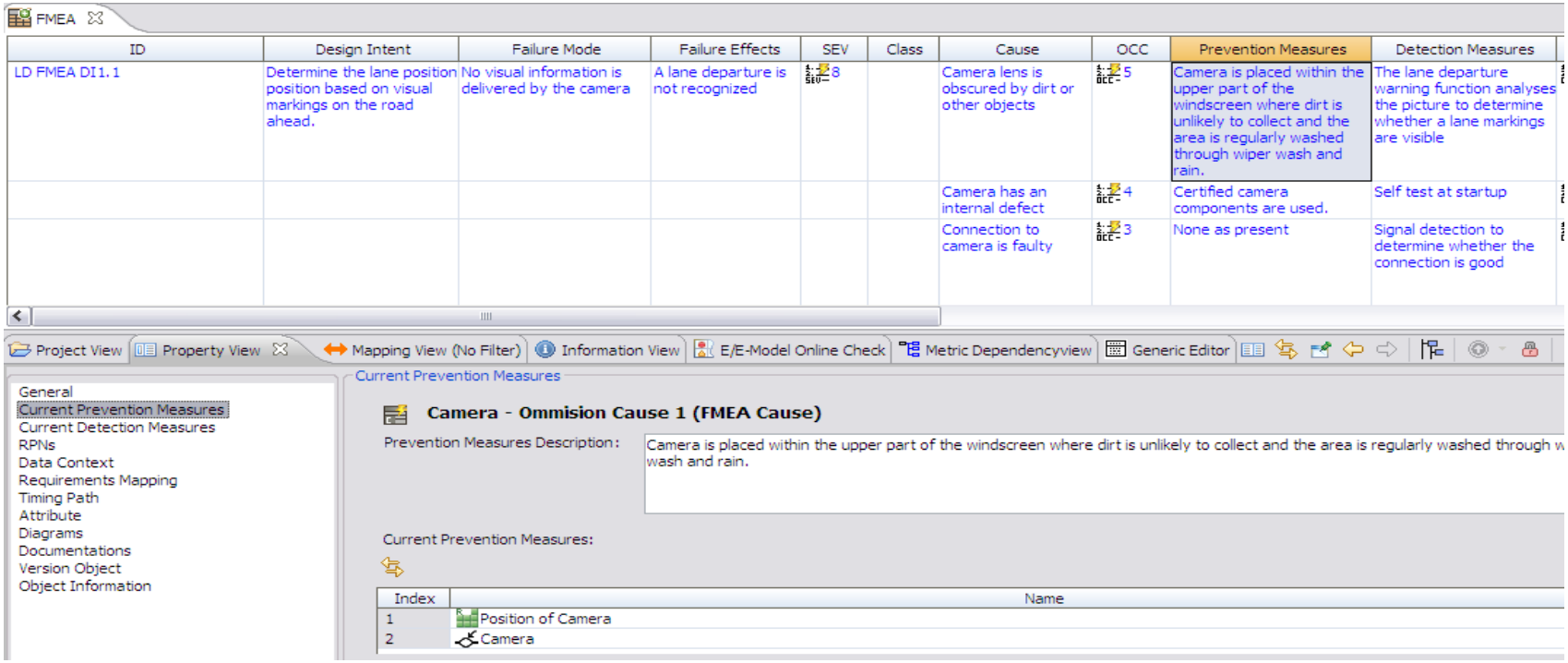
Vector Experiences – Tool Support for Hazard & Risk Analysis



Vector PREEvision:

- Supports working with predefined operation scenarios and operating modes
- Supports automatic ASIL calculation
- Supports traceability of safety goals to requirements and design artifacts

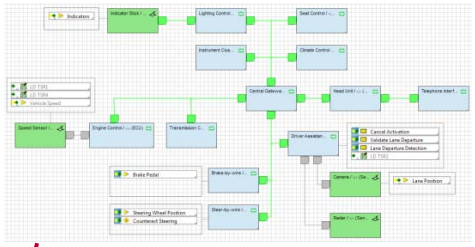
Vector Experiences – Tool Support for FMEA

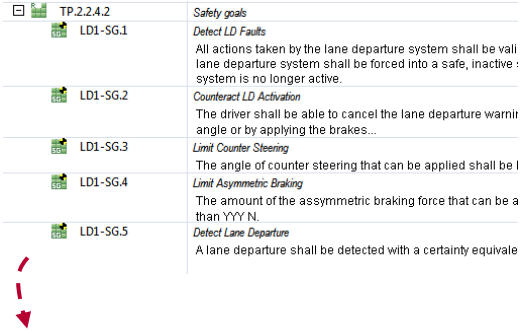


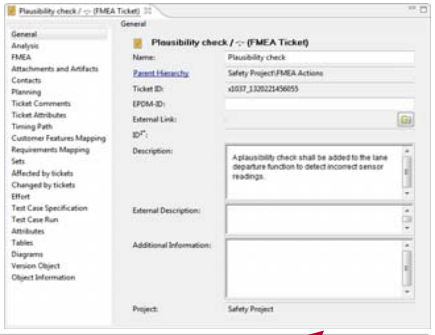
Vector PREEvision:

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

Vector Experiences – Tool Support for Analysis and Design







*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
				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			

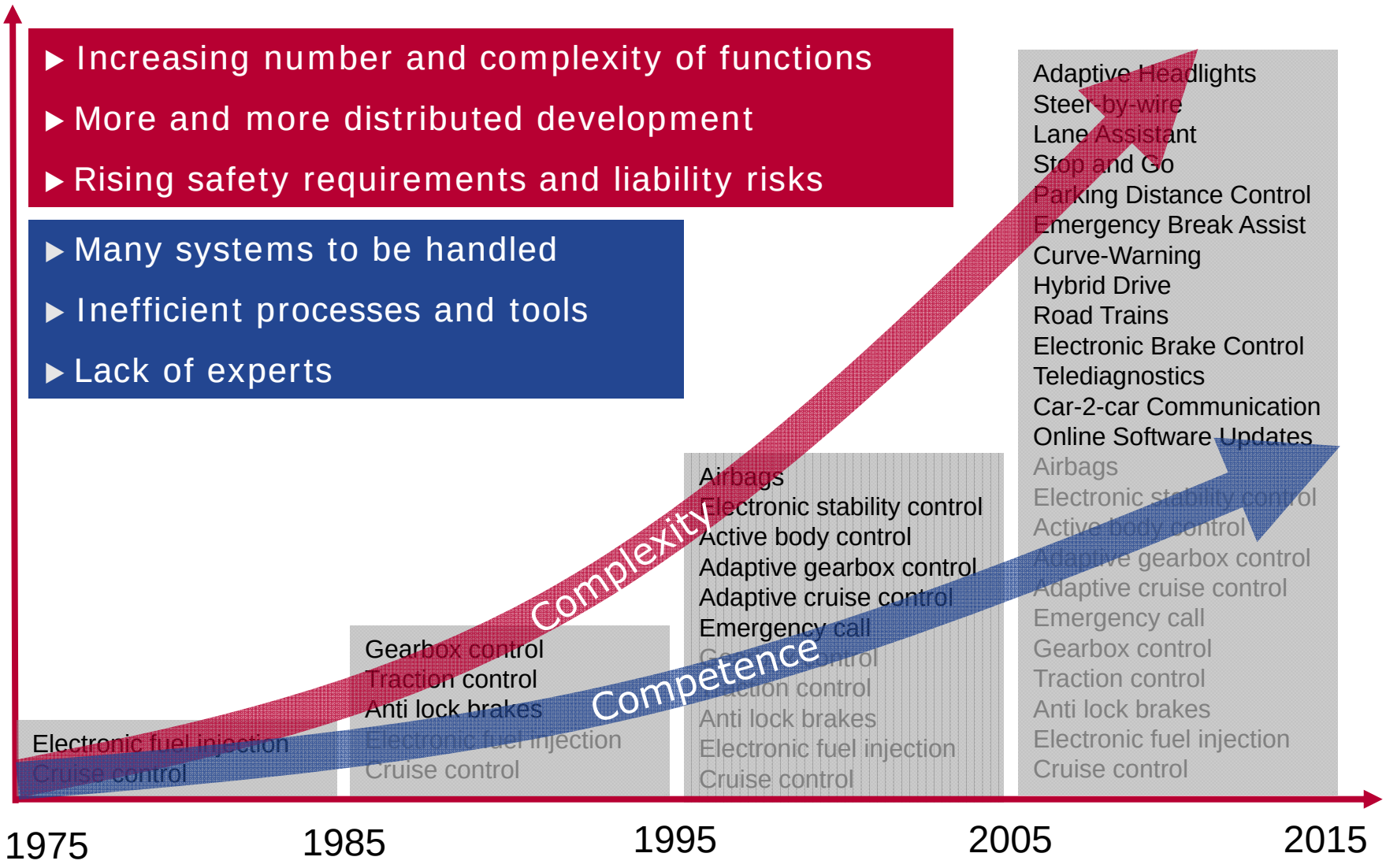
Vector PREEvision:

- Provides single source for item definition, based on features, requirements, operating scenarios, dependencies
- Facilitates model-based design of functional and technical safety concept, including ASIL decomposition and requirement based tests

Content

- Challenges with Implementing Functional Safety
- Basic Concepts
- Vector Experiences
- **Success Factors**

Functional Safety Challenge: Complexity and Competences



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

Success Factor – Implement Functional Safety

Products

Technical measures against hardware and software failures to
- **avoid failures** and
- make **unavoidable** failures **safe**.

Examples: **Redundancy, Reuse** with AUTOSAR

Processes

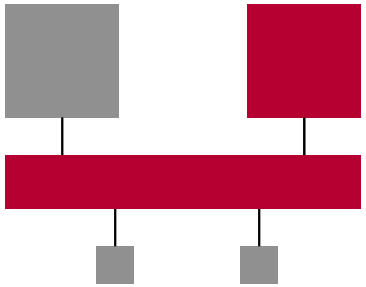
All development activities are concerned as well as **production** and **field observation**.

Examples: **Hazard analysis** during concept definition, **consistent modeling** in PREEvision

People

New **roles** and **skills** as well as **cultural changes** for engineering and management staff.

Examples: **Safety engineering** skills, **safety manager** role, **safety culture**



Implementation needs to address products, processes and people

vector

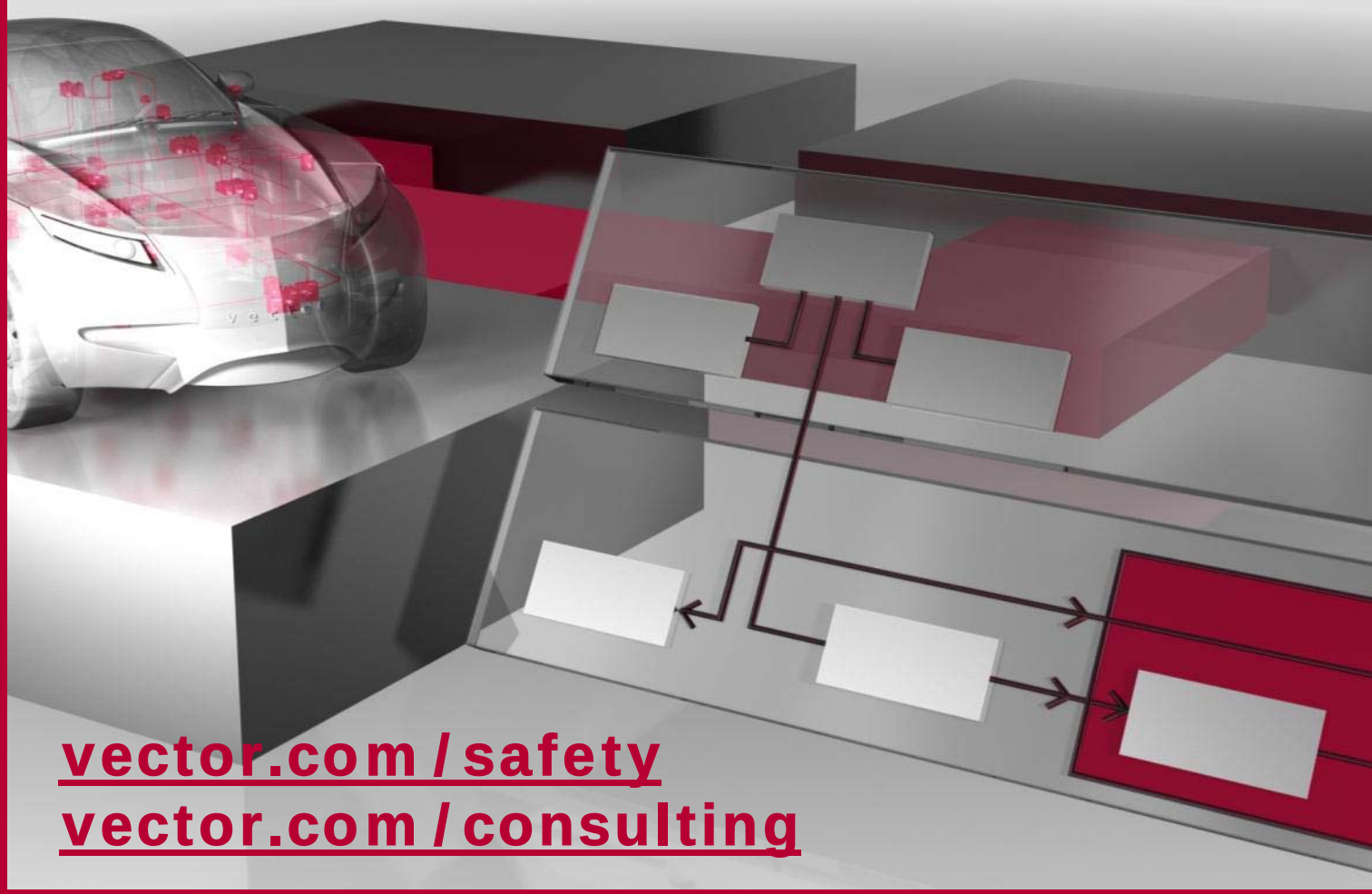
Outlook

- **Automotive OEMs** in many cases still need to improve their process capabilities to fulfill the requirements of the safety standards and to better collaborate with suppliers
- **Suppliers of established safety critical components** need to further improve field observation and abilities for complete safety case.
  Examples: Engine management systems, driving dynamics
- **Suppliers of new and innovative components** need to build up good basic process capabilities as a reliable foundation for safety.
  Examples: Innovative driver assistance functions and powertrain
- **ISO 26262** will evolve based on experiences and to cover new challenges and development techniques
- **Safety capabilities** will become part of standard supplier evaluations

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

Questions?

Good success with implementing Functional Safety!



vector.com/safety
vector.com/consulting

vector

Your Partner in Achieving Engineering Excellence.