VECTOR

Functional Safety and SOTIF – Principles and Practice

Vector Technology Days 2019 - 2019-10-23, Böblingen, Germany

V1.0 | 2019-10-23

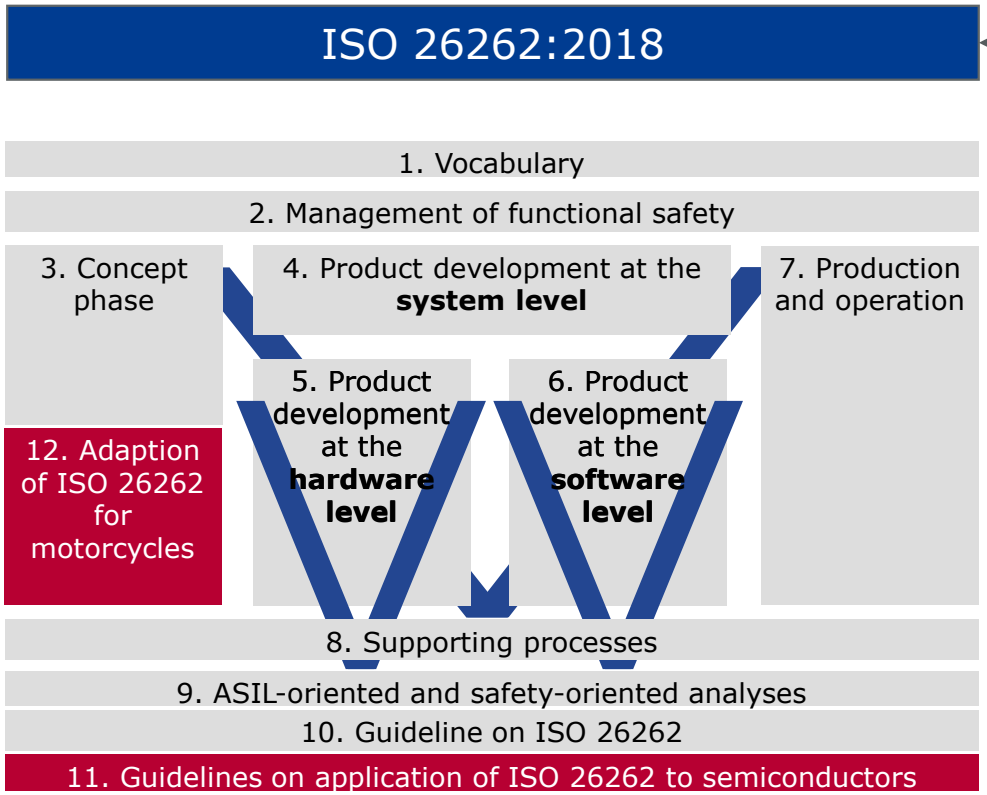
Agenda

1.	The Need for SOTIF
2.	Approach of ISO/PAS 21448 of SOTIF
3.	Best Practices to achieve SOTIF
4.	Outlook

***SOTIF: S**afety **O**f **T**he **I**ntended **F**unctionality*

VECTOR

Safety of the Indented Functionality (SOTIF) – Extension of the Safety Scope



Reference

ISO/PAS 21448

Road vehicles –
Safety of the intended functionality

Scope of ISO/PAS 21448

- SAE J3016 Level 1: Driver Assistance
- SAE J3016 Level 2: Partial Automation

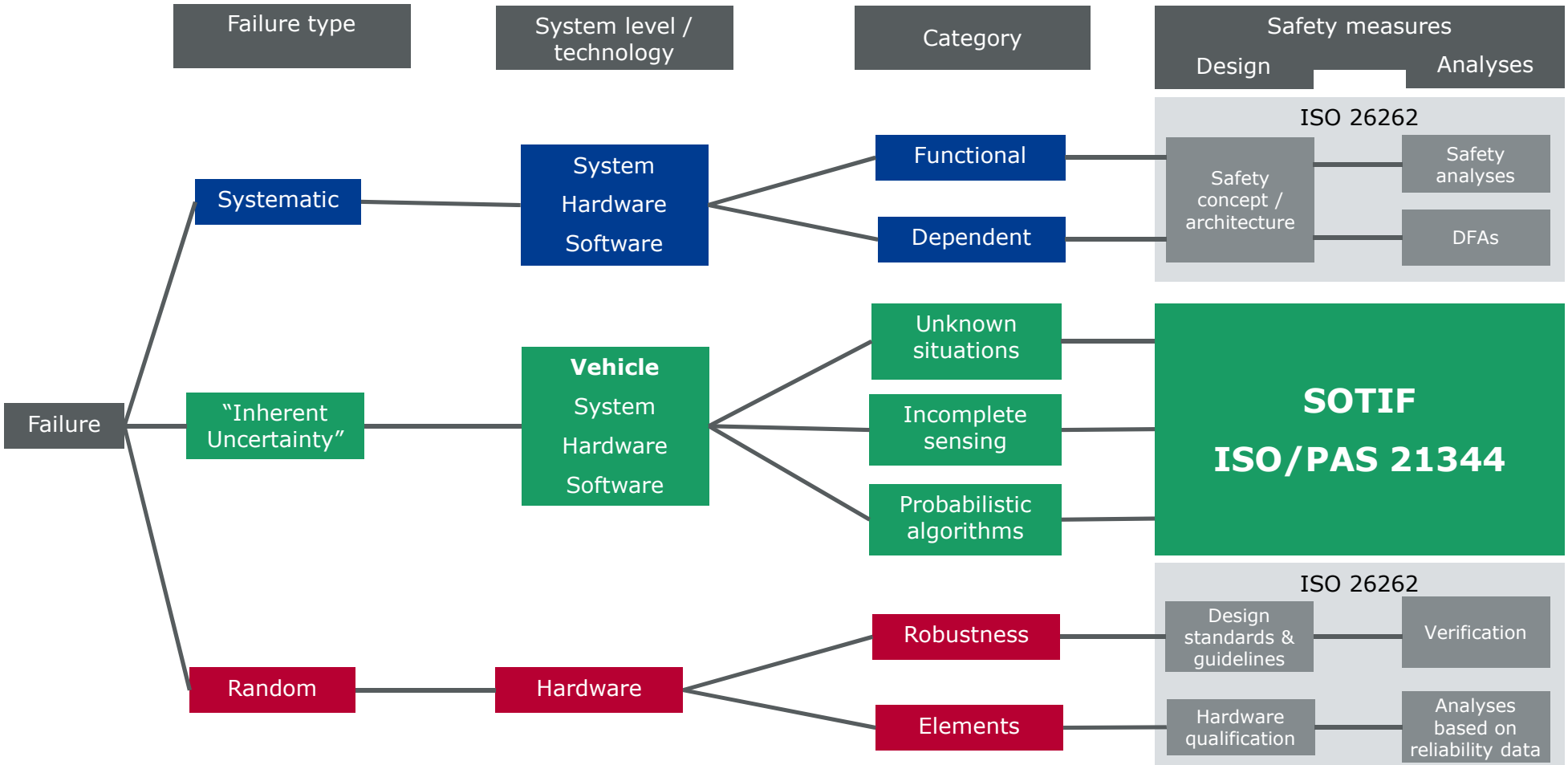
Qualitative approach to uncertainties

- Environment
- Complex sensors
- Algorithms and decisions
- Human machine interaction
- Actuation

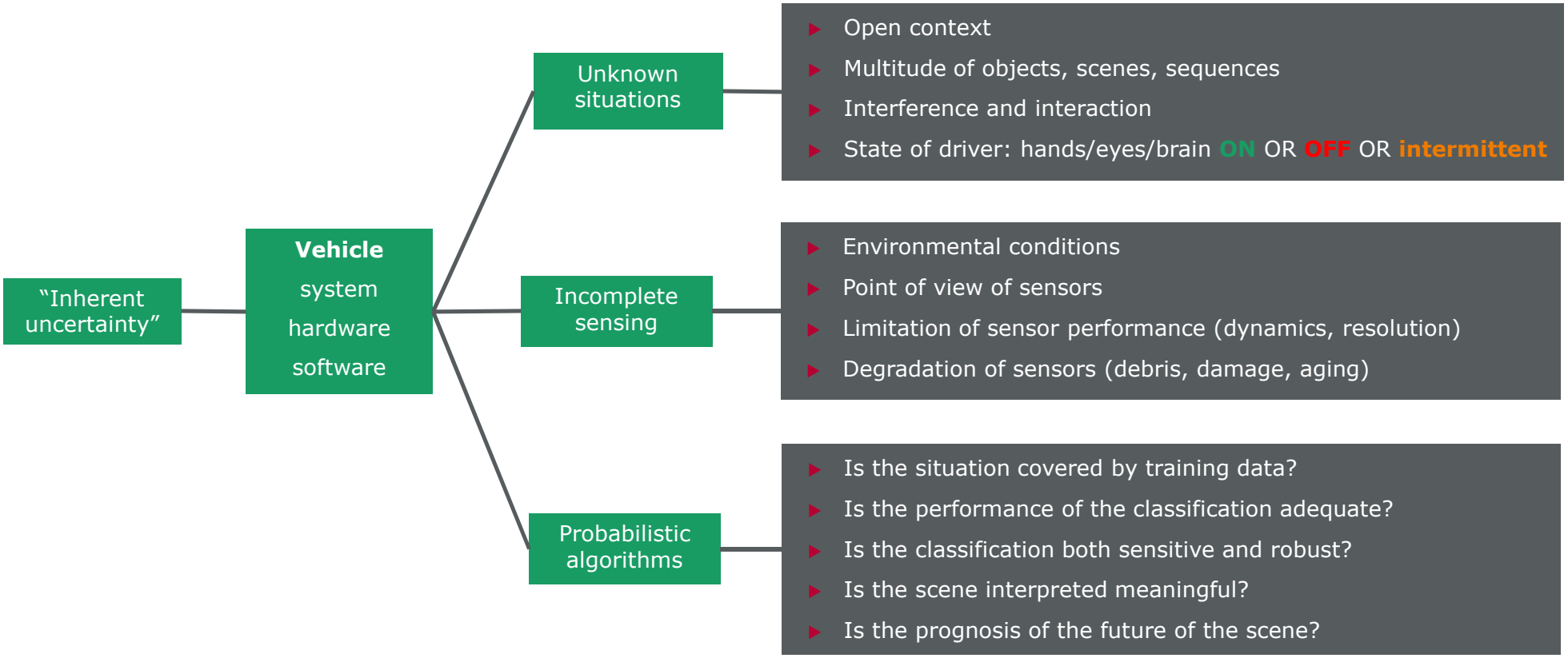
PAS: Publicly Available Specification

ISO/PAS 21448 is related to ISO 26262: Extension of safety for uncertainties

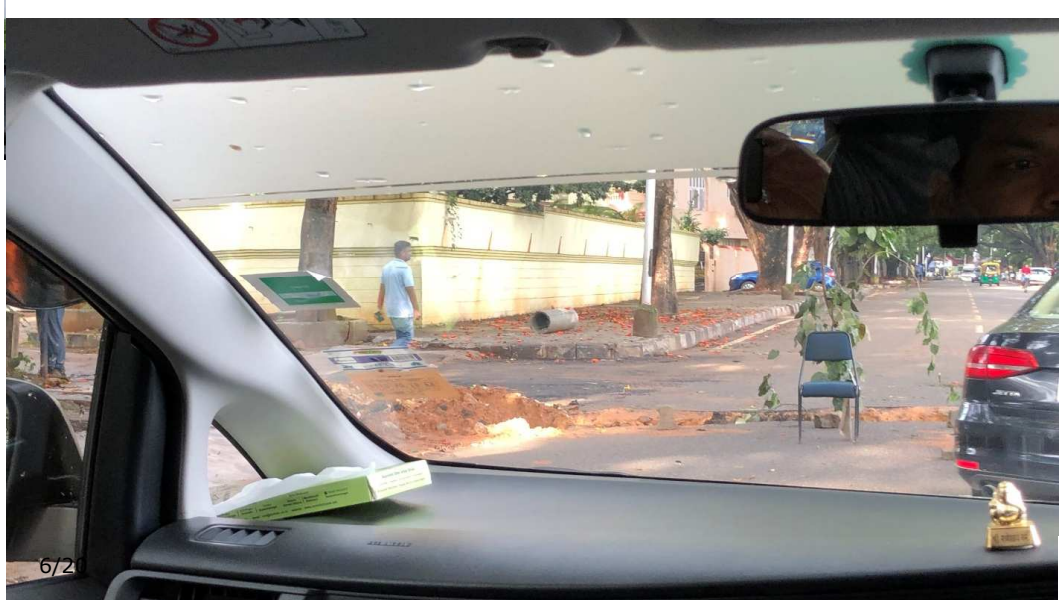
Failures Categories of ISO 26262 and SOTIF



Challenges related to SOTIF



Are the uncertainties addressed by the design covering the real world environment?



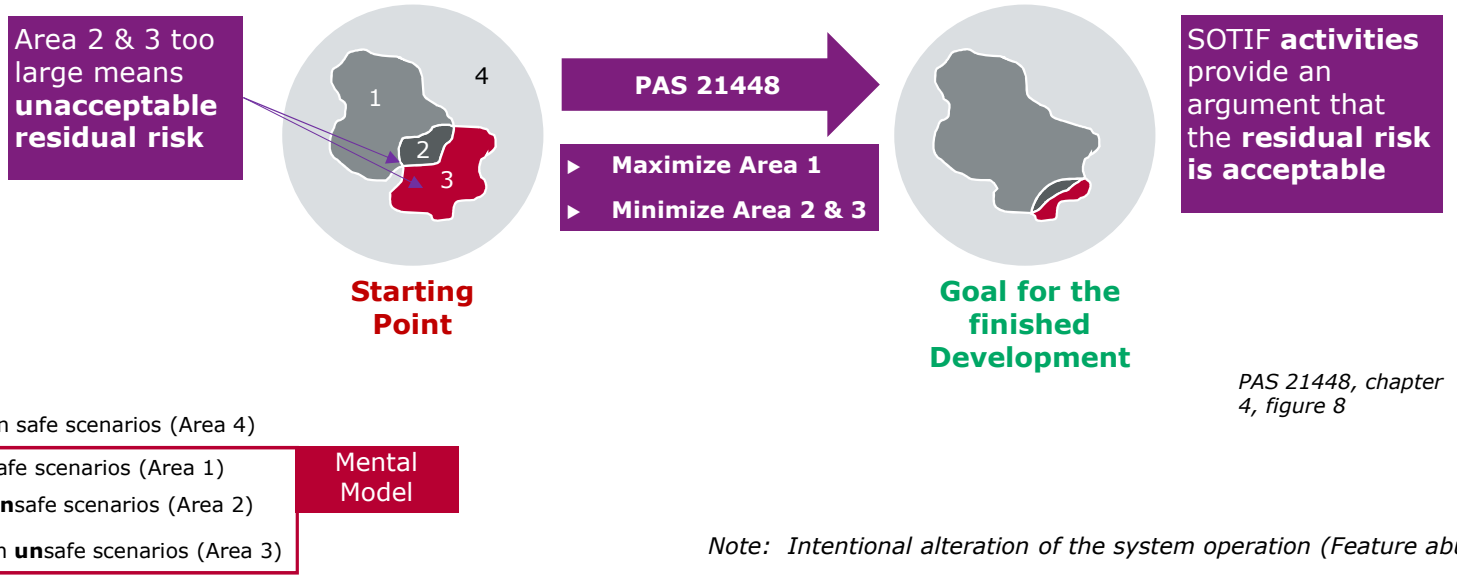
Agenda

1.	The Need for SOTIF
2.	Approach of ISO/PAS 21448 of SOTIF
3.	Best Practices to achieve SOTIF
4.	Outlook

SOTIF: ***S****afety* ***O****f* ***T****he* ***I****ntended* ***F****unctionality*

Approach of ISO/PAS 21448 to SOTIF

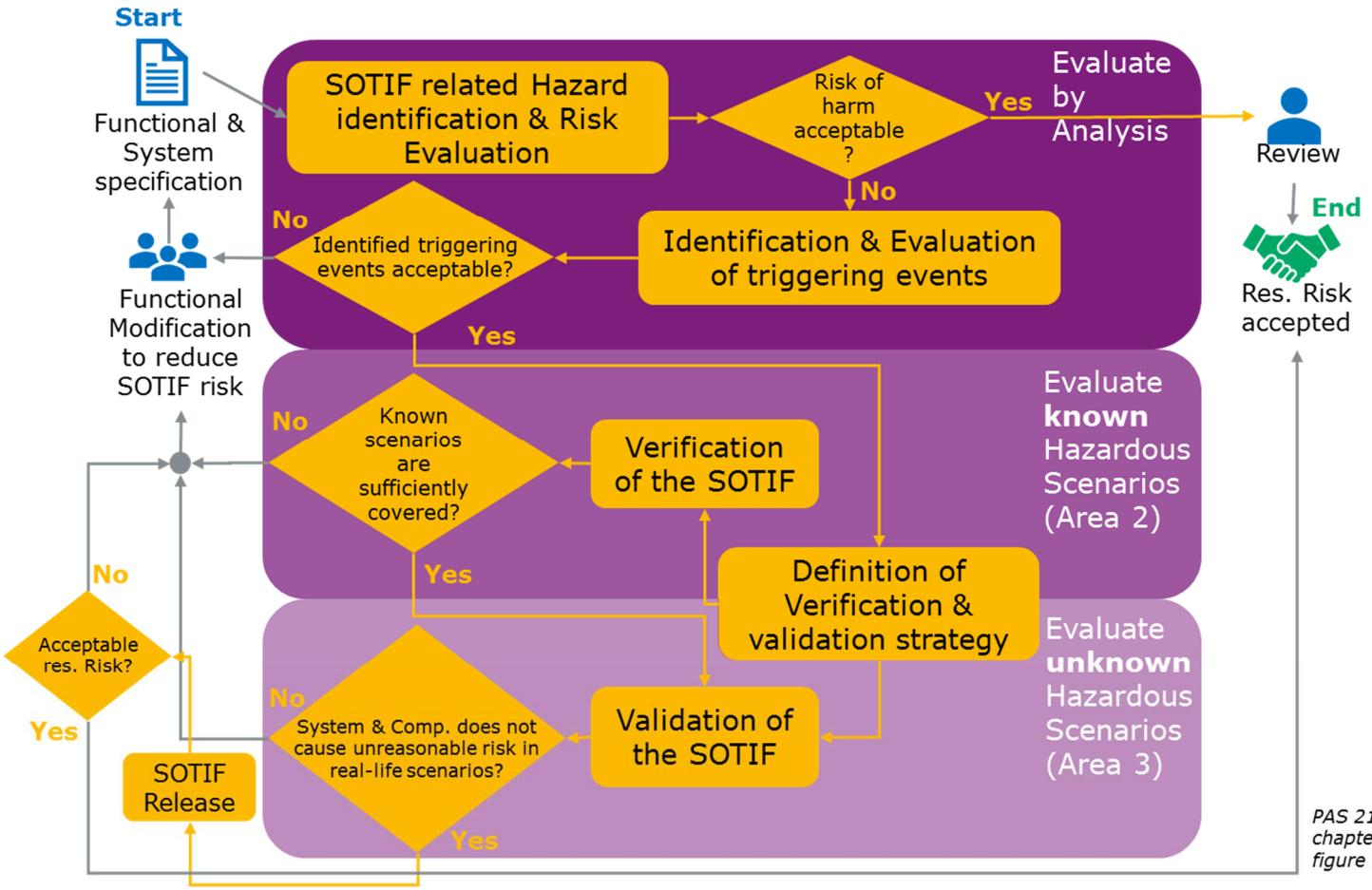
- **Safety of the intended functionality (SOTIF)**
  - The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons.



PAS 21448, chapter 4, figure 8

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

ISO/PAS 21448: SOTIF Activities

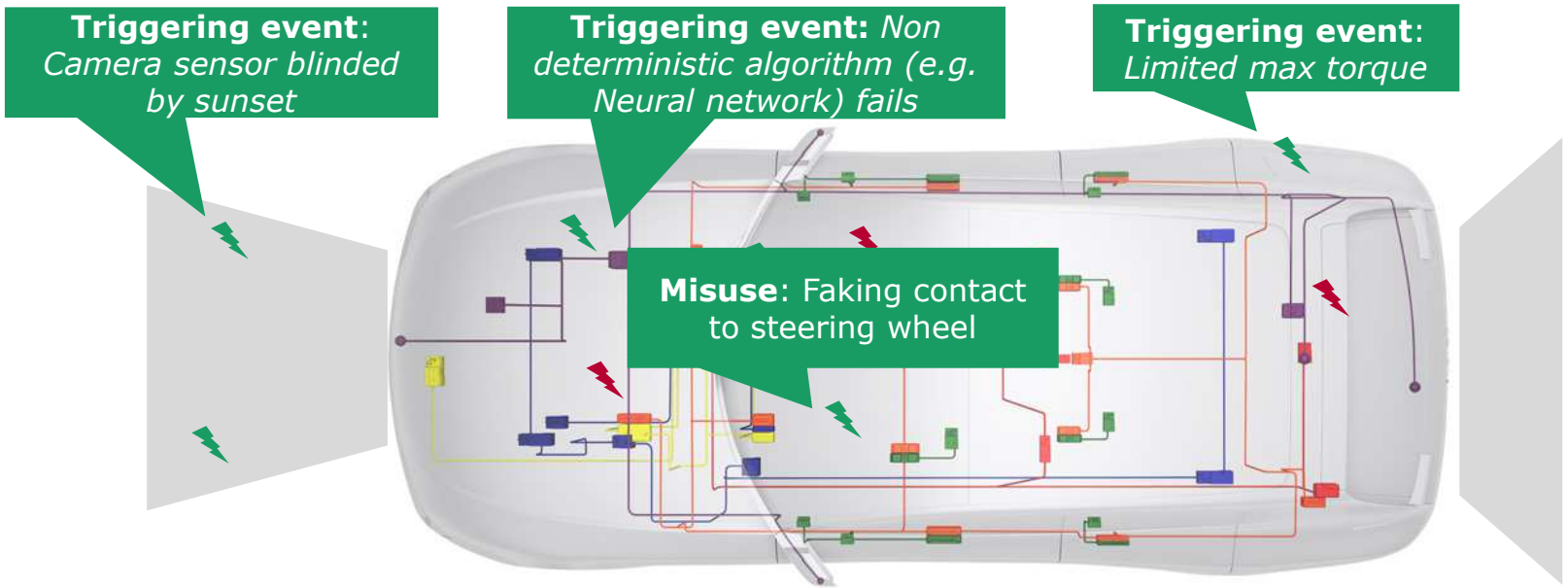


PAS 21448, chapter 5, figure 9

ISO/PAS 21448 – SOTIF Activities: Evaluate by Analysis

1. Systematic identification of the hazards similar to HARA
   Risk evaluation based on exposure, controllability, severity

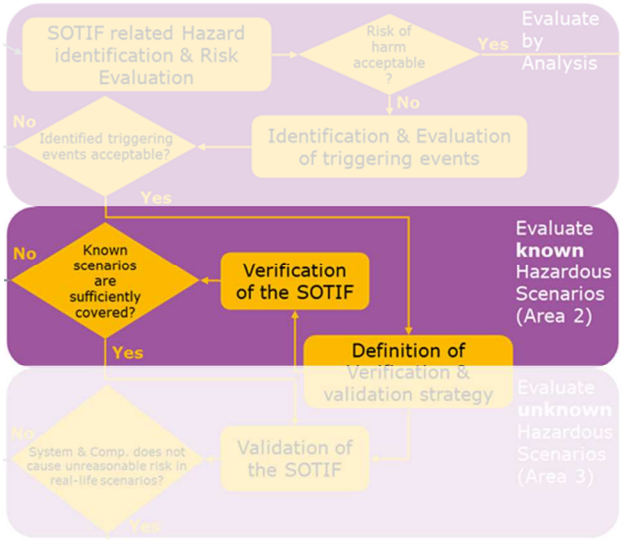
2. Triggering events are identified and analyzed to be acceptable or **function is modified**



= systematic & random faults of HW &SW

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

ISO/PAS 21448 – SOTIF Activities: Evaluate Known Hazardous Scenarios (Area 2)



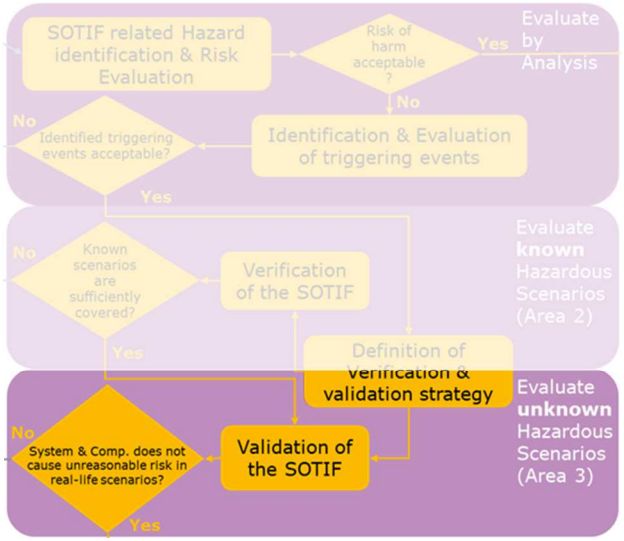
Objective: Verify to the system operates as expected in known hazardous scenarios and reasonably misuse

- 8 methods for **sensor** verification
  - Sensor characterization
  - 7 test methods, similar to ISO 26262 tailored for SOTIF
- 6 methods for **decision algorithm** verification
  - 3 test methods
  - 2 generic methods (simulation, analysis, tests)
  - Analysis of architectural properties including independence
- 6 methods for **actuation** verification
  - Actuator characterization
  - 5 test methods
- 8 test methods for **system** verification

23 out of 28 verification methods rely on tests

ISO/PAS 21448 – SOTIF Activities: Evaluate Unknown Hazardous Scenarios (Area 3)

Objective: Validate to "show" absence of unreasonable level of risk in real-life use cases



- 12 methods for validation
  - 9 test methods including randomization and misuse
    - Most test methods are extensions of ISO 26262 test methods
    - Additional: Fleet tests
    - Extension: Randomized tests
    - Constraint: Appropriate amount of test data and distribution
  - 2 types of analyses
    - Architecture verification including independence
    - Analysis of worst case scenarios
  - 1 simulation of selected scenarios

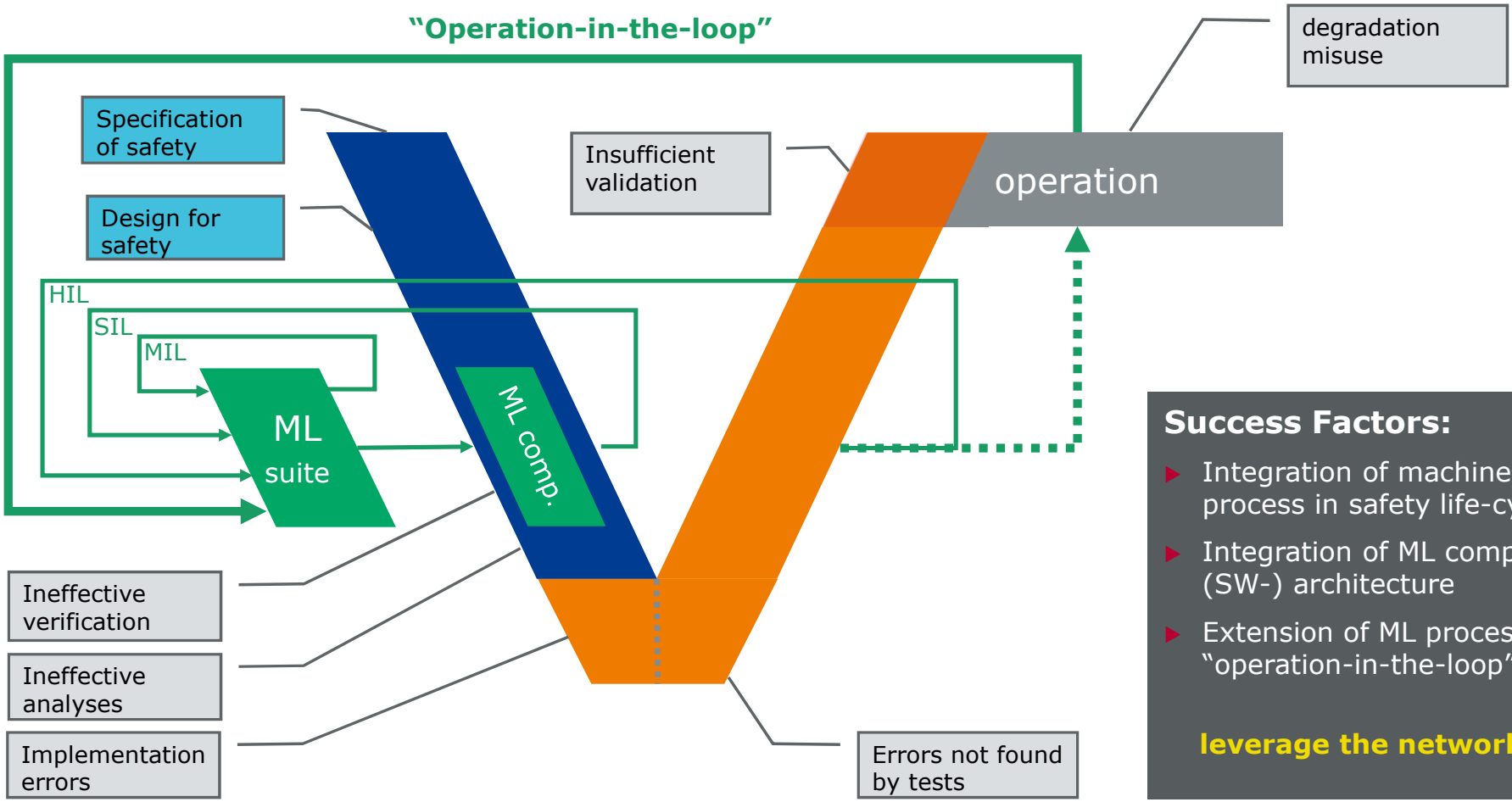
Exploration of the "unknown" with focus on tests

Agenda

1.	The Need for SOTIF
2.	Approach of ISO/PAS 21448 of SOTIF
3.	Best Practices to achieve SOTIF
4.	Outlook

***SOTIF: S**afety **O**f **T**he **I**ntended **F**unctionality*

Best Practice (1/3): Achievement of SOTIF in the Safety Life-Cycle

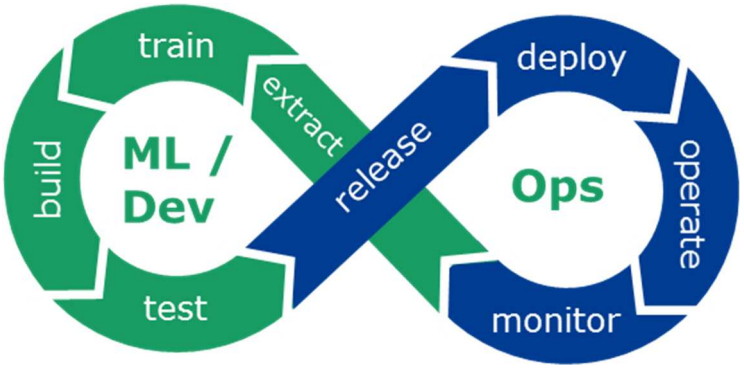


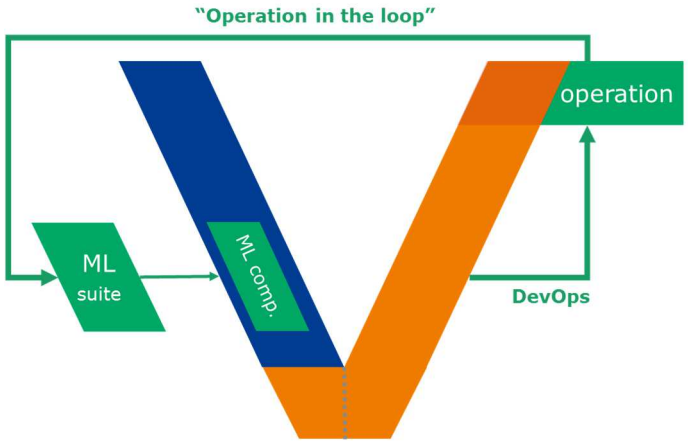
Success Factors:

- Integration of machine learning process in safety life-cycle
- Integration of ML components in (SW-) architecture
- Extension of ML process for "operation-in-the-loop"

leverage the network effect

Best Practice (2/3): Acceleration of the "Safety Performance" in **S**OTIF





- **DevOps** is the tight integration of
  - **Dev**elopment and
  - **Op**eration
- **Effective utilization of DevOps**
  - Accelerates error detection and correction
  - Reduces false change rates
  - Increases efficiency
- **Preconditions**
  - SW design principle beyond ISO 26262 scope
  - Segregation of elements in scope of DevOps
  - Continuous integration established
  - OTA infrastructure and vehicle capability
  - Benchmark execution by embedded systems
- **Straight forward adaption** form classic code-base SW development to ML Learning

DevOps enables "operation-in-the-loop" to accelerate and leverage the network effect

VECTOR

Best Practice (3/3): Right-Positioning of Testing for SOTIF

- Testing can only proof the **presence of errors, never the absence**
  - Primary intend: Defect detection and exploration of limitations
  - Secondary intend: Demonstrate capabilities and functionality

- Testing has **sampling character** - testing is by nature incomplete
  - Avoid redundant sampling, e.g. by boundary values, equivalence classes
  - Focus on relevant combinations, e.g. classification tree, combinatorial testing

- Practical **tests cannot provide statistical evidence** to comply with target values
  - Compliance with target values is typically provided by quantitative analysis

ISO 26262

- The **test methods of ISO 26262 can be tailored and extended** for SOTIF
  - Randomizing, exploring limitations, out-of-environmental context

- A **systematic approach** enables effectiveness tests
  - 1. Objectives 2. Methods 3. Design/implementation, 4. Execution, 5. Analysis

Considering principles and properties of tests to demonstrate sufficient evidence

Agenda

1.	The Need for SOTIF
2.	Approach of ISO/PAS 21448 of SOTIF
3.	Best Practices to achieve SOTIF
4.	Outlook

SOTIF: ***S****afety* ***O****f* ***T****he* ***I****ntended* ***F****unctionality*

VECTOR

Outlook: The evolution of ISO/PAS 21448 to future Standard ISO 21448

ISO/PAS 21448

published Jan 2019

- Snapshot of ongoing standardization as "public available specification"
- Focus on automation levels 1, 2
- Qualitative approach
- No elaborated architectural approach, no dedicated evaluation of architecture
- Focus of evidence by testing

ISO standard 21448

targeted for 2022

- **Fully elaborated ISO standard** with defined relations to ISO 26262
- Coverage of all automation levels **1 to 5**
  - Focus on **autonomous driving**
  - More safety goals and **higher ASILs**
- Qualitative and **quantitative** approach
  - In addition quantitative methods to indicate probabilities and residual risk
- New **Focus on software architecture**
  - Evolutionary architecture
  - Integration of AI/ML
  - Dedicated evaluation of AI/ML
- Right-positioning of testing
- New Dedicated support processes

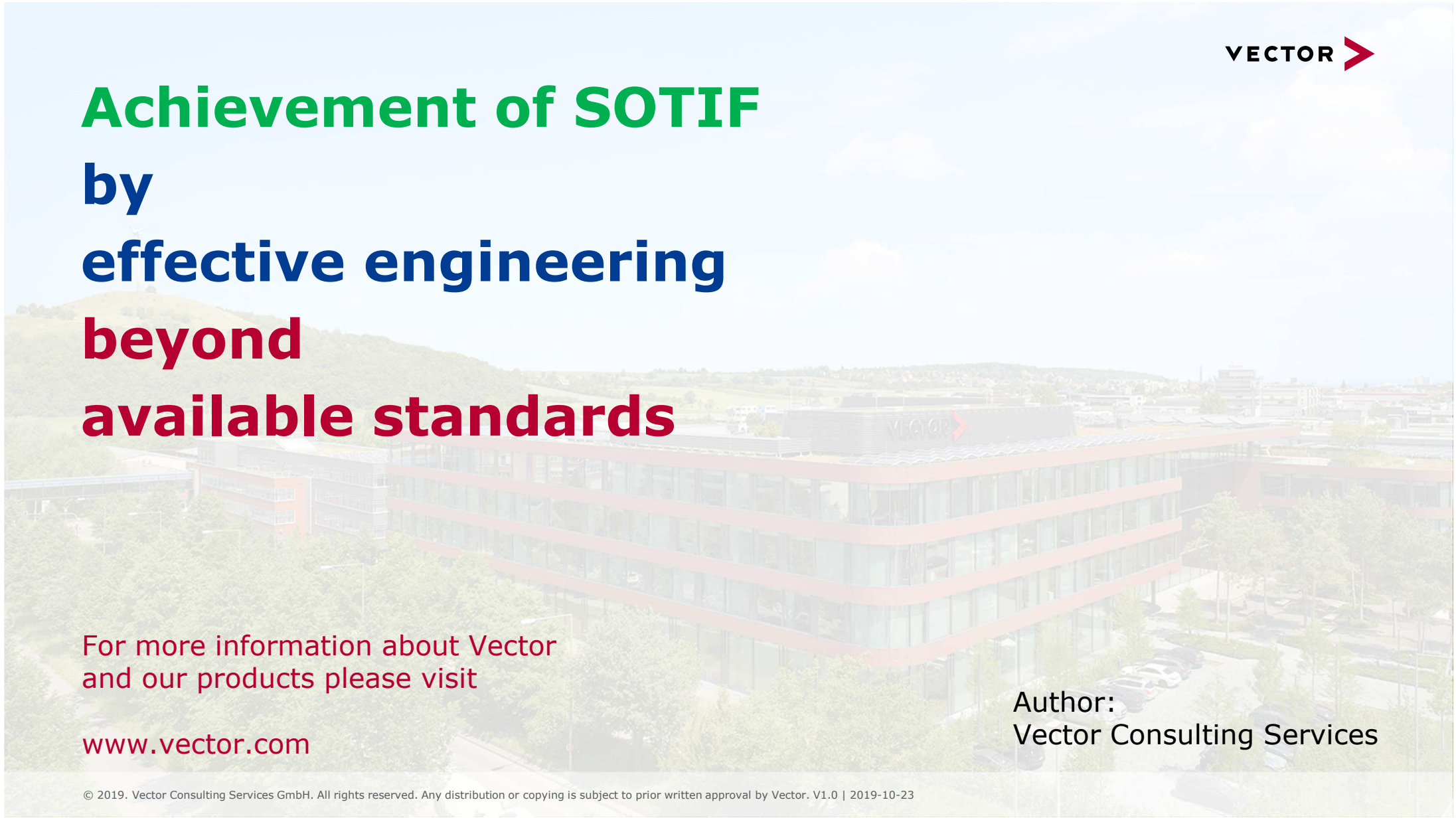
VECTOR

Outlook: A Pragmatic Approach Towards SOTIF

- **Constant**
  - **Principles** of safety engineering and safety concepts
  - **Acceptance of reasonable residual risks** by individuals and societies
  - Practitioner and teams remain endangered by **cognitive biases related to safety**
- **Change**
  - The "inherent uncertainty" of SOTIF constitutes a **new type of failure**
  - Stronger emphasis on **evolutionary software architectures** embedding ML-elements
  - **Continuous learning about SOTIF**, e.g. white paper ‚Safety First for Automated Driving'
- **New**
  - Advent and **progress of machine learning** will further boost SOTIF despite inherent uncertainties
  - **Acceleration of safety** by adoption of agile paradigms: Continuous integration and **DevOps**
  - Evolution of **technologies enabling networked SOTIF**, e.g. semiconductor, 5G, quantum computing

Achievement of SOTIF is a challenging endeavor into the future

Achievement of SOTIF by effective engineering beyond available standards



For more information about Vector and our products please visit

www.vector.com

Author:
Vector Consulting Services