Analysis of established processes regarding automated driving
In which steps do the established development and safety processes need to be extended to enable the development and safeguarding of automated driving functions?

The V-model is a process model originating from software development that has been established for the development of complex safe-critical systems in the avionics and the automotive domain.

The first step is to specify the requirements for the complete product (which is the vehicle here) from the perspective of the stakeholders.

For the final approval it is examined whether the complete product satisfies the requirements of the stakeholders.

The remaining part of the left branch of the V covers the design of the system on multiple levels of abstraction finally resulting in a technical implementation.

The right branch of the V describes the verification and validation of the developed system. For this purpose for each abstraction level test obligations are defined that need to be satisfied for a successful product development.
The ISO 26262 is a standard for safeguarding electric and electronic (E/E) systems in passenger cars.

Based on the V-model the standard defines a process to ensure the functional safety of such systems before putting them into operation.

This process has been and still is successfully applied for vehicles that are exclusively operated by human drivers and for vehicles equipped with advanced driver assistance systems (ADAS).

It does not address the nominal performance of the E/E systems.

Preferences and Conditions – Booth No. 03

V-Model and Process Analysis

After defining the functional specification of the system under development a hazard analysis and risk assessment is performed. Based on these results the system is designed and a safety concept is developed. The hardware and software development then takes place in further parallel runs of the V-model.

On the right branch of the V integration tests for the developed components are performed and a validation of the safety goals (safety validation) takes place as well as a functional safety assessment of the complete vehicle against the functional specification.
The ISO/PAS 21448 provides guidance on the applicable design, verification and validation needed to archive the Safety of the Intended Functionality (SOTIF) for SAE Level ≤ 2.

- does not apply to faults covered by the ISO 26262
- is intended to be applied where proper situational awareness is critical to safety.

Functional safety (ISO 26262) and SOTIF (ISO/PAS 21448) are distinct and complimentary aspects of safety.

The ISO/PAS 21448 and ISO 26262 are both important in ensuring the safety of vehicles. ISO 26262 focuses on functional safety, which is crucial for the overall operation and performance of the system. SOTIF, on the other hand, addresses the specific requirements for the safety of the intended functionality, which is essential for the prevention of malfunctions that could lead to accidents.

The V-model is a visual representation of the process analysis and requirements for implementing SOTIF. It includes several steps:

1. **Hazard Analysis and Risk Assessment**
   - **ISO/PAS 21448**
   - **ISO 26262**

2. **Software Development**
   - **ISO/PAS 21448**

3. **Hardware Development**
   - **ISO/PAS 21448**

4. **Requirements**
   - **ISO/PAS 21448**

5. **Vehicle Level**
   - **ISO/PAS 21448**

6. **System Tests**
   - **ISO/PAS 21448**

7. **Component Tests**
   - **ISO/PAS 21448**

8. **Integration Tests**
   - **ISO/PAS 21448**

9. **Identification and Evaluation of Triggering Events**
   - **ISO/PAS 21448**

10. **Technical Implementation**
    - **ISO/PAS 21448**

11. **Validation of the SOTIF**
    - **ISO/PAS 21448**

12. **Release Validation of the SOTIF**
    - **ISO/PAS 21448**

The V-model is a comprehensive approach to ensuring the safety of vehicles, particularly in the context of SOTIF. It involves systematic analysis, design, and testing to ensure that all possible safety issues are addressed.

---

**Supported by:**
Federal Ministry for Economic Affairs and Energy

---

**on the basis of a decision by the German Bundestag**
**New Challenges** arise with the introduction of highly automated driving functions, thus requiring extensions of established development and safeguarding processes:

- Interaction with other human traffic (mixed traffic)
- Operation in highly complex and hardly predictable environment (open world)
- Loss of human driver as a fallback (fail operational instead of fail-safe)
- Changing safety-critical functional requirements during product life
- Intensive use of machine learning techniques

**V-Model and Process Analysis**

- **Requirements and Conditions**
- **Vehicle Level**
- **Functional Specification**
- **Hazard Analysis and Risk Assessment**
- **System Design**
  - **System Design and Safety Concept**
  - **Development Fallback Concepts**
  - **Subsystem Design**
  - **Component Design**
- **Technical Implementation**
  - **V Model**
  - **ISO 26262**
  - **ISO/PAS 21448**
  - **Extensions**

- **Software Development**
  - **Software Development**
  - **Test Update Strategy**
  - **Consideration of Systematic Faults (Design / Software)**
  - **Safeguarding Self-learning Algorithms**

- **Hardware Development**
  - **Development Update Strategy**
  - **Test Update Strategy**

- **Integration Tests**
  - **Test Fallback Concepts**

- **System Tests**
  - **Safety Validation**

- **Functional Safety Assessment**
  - **Acceptance Tests Vehicle Level**

- **Tests under Consideration of Human Behavior**
  - **Test HMI Concept**

- **Treatment of Human Behavior**
  - (Driver and Other Traffic Participants)

**Lifting ISO/PAS 21448 to Level 3**

**Scenario-based Approach to Handle Complex Environments**

**ISO/PAS 21448 Extensions**

**V-Model** and process analysis meet new challenges arising with the introduction of highly automated driving functions, thus requiring extensions of established development and safeguarding processes. Key areas include:

- Interaction with other human traffic (mixed traffic)
- Operation in highly complex and hardly predictable environment (open world)
- Loss of human driver as a fallback (fail operational instead of fail-safe)
- Changing safety-critical functional requirements during product life
- Intensive use of machine learning techniques

**Technical Implementation** provides a holistic approach to address these challenges, integrating various aspects of development and validation to ensure safety and reliability in highly automated driving systems.