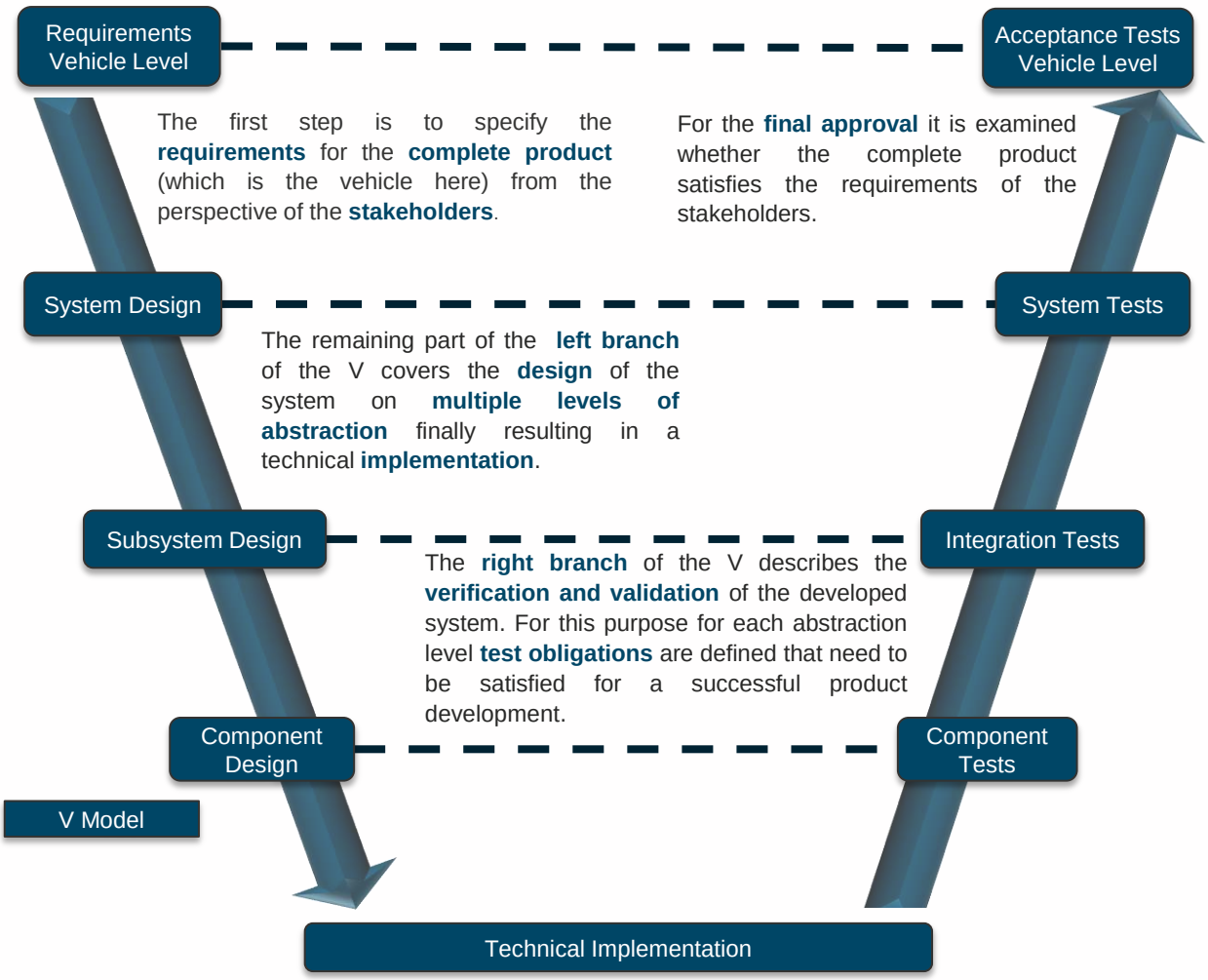
REQUIREMENTS AND CONDITIONS – Booth No. 03

V-MODEL AND PROCESS ANALYSIS

PEGASUS

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**.



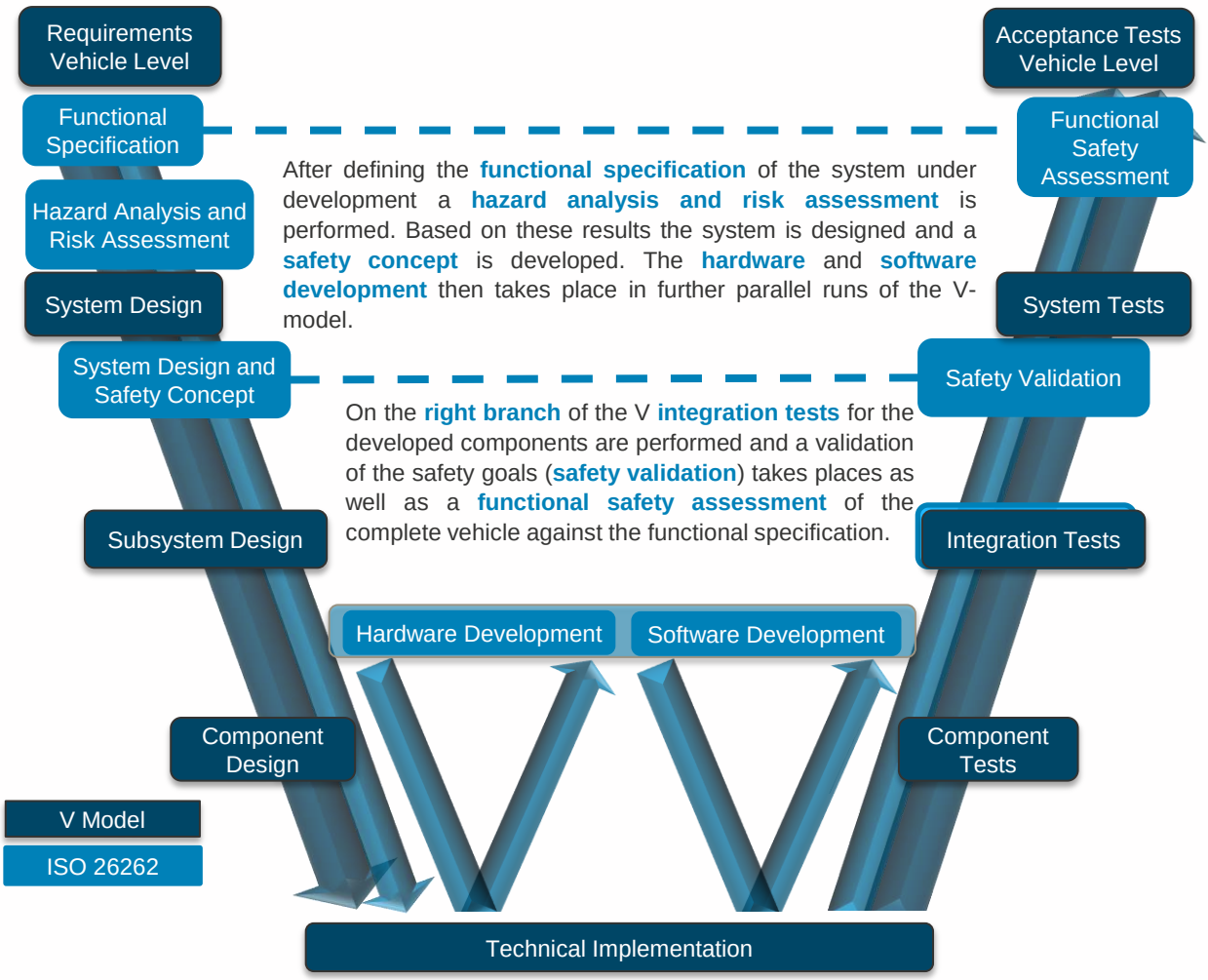
Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

REQUIREMENTS AND CONDITIONS – Booth No. 03

V-MODEL AND PROCESS ANALYSIS

PEGASUS

- 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.



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 places as well as a **functional safety assessment** of the complete vehicle against the functional specification.

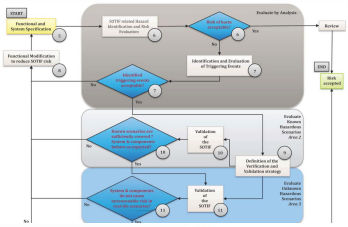
Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

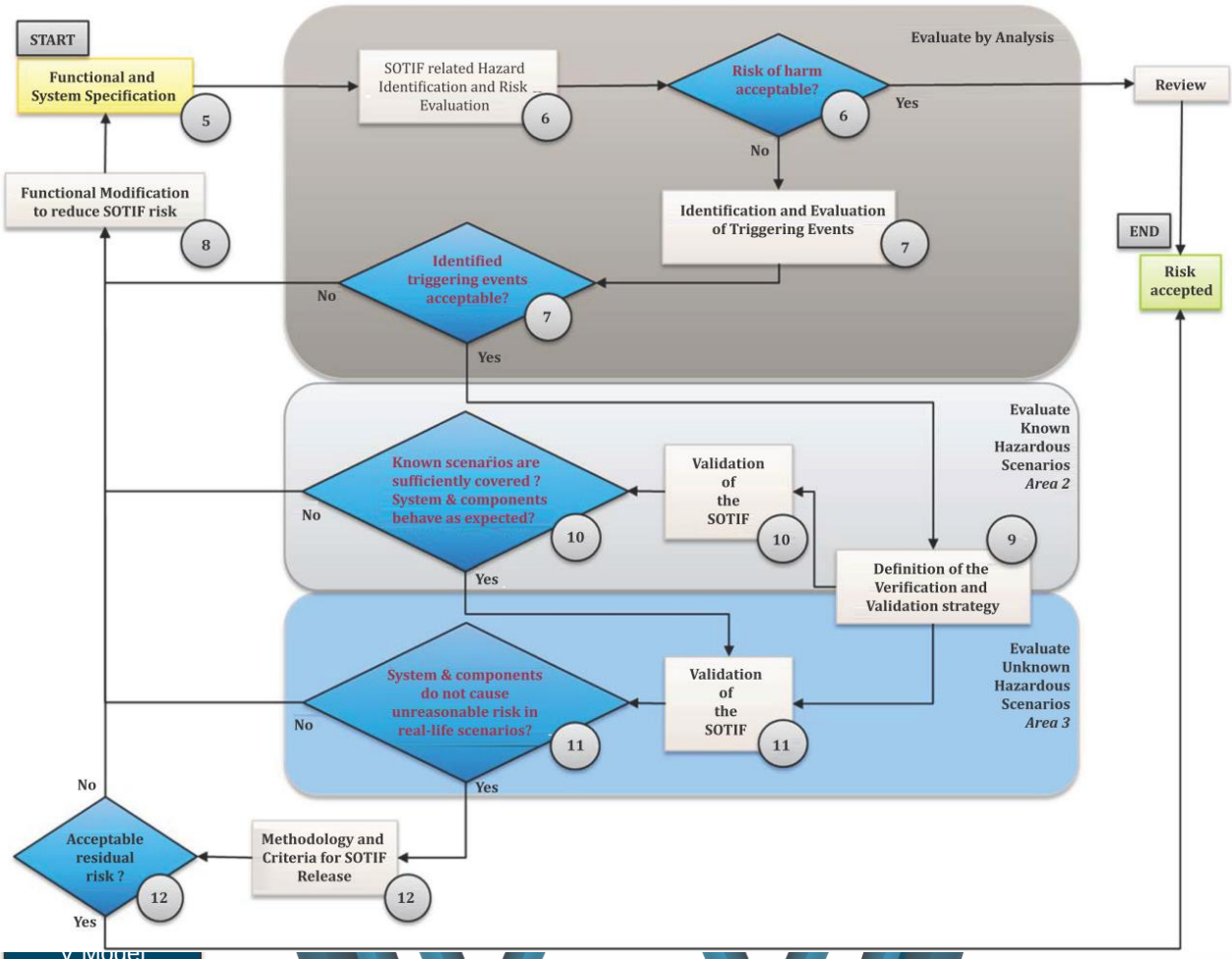
REQUIREMENTS AND CONDITIONS – Booth No. 03

V-MODEL AND PROCESS ANALYSIS

PEGASUS

- 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 safetv.





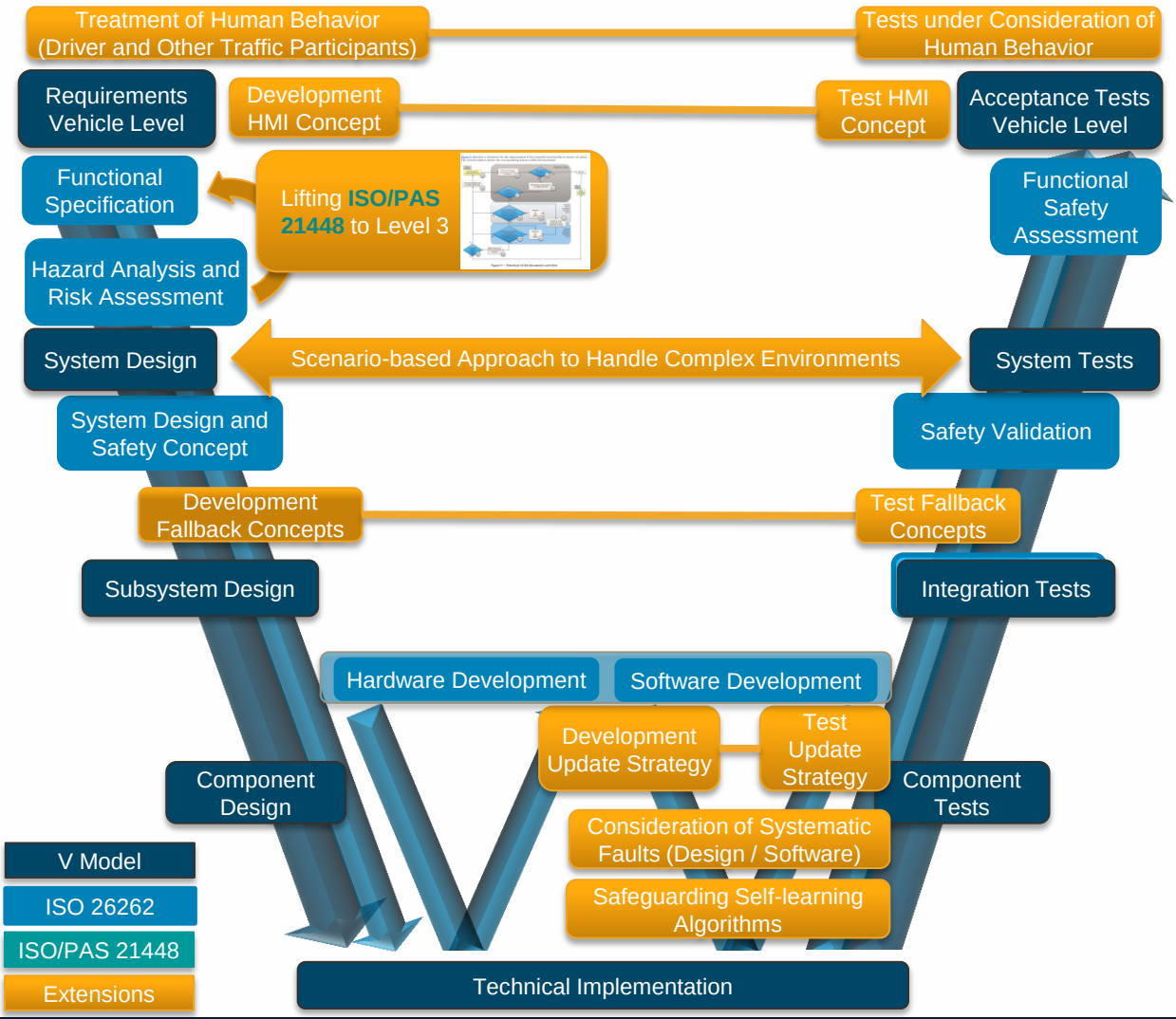
Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag

REQUIREMENTS AND CONDITIONS – Booth No. 03

V-MODEL AND PROCESS ANALYSIS

PEGASUS

- **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



Supported by:
Federal Ministry for Economic Affairs and Energy
on the basis of a decision by the German Bundestag