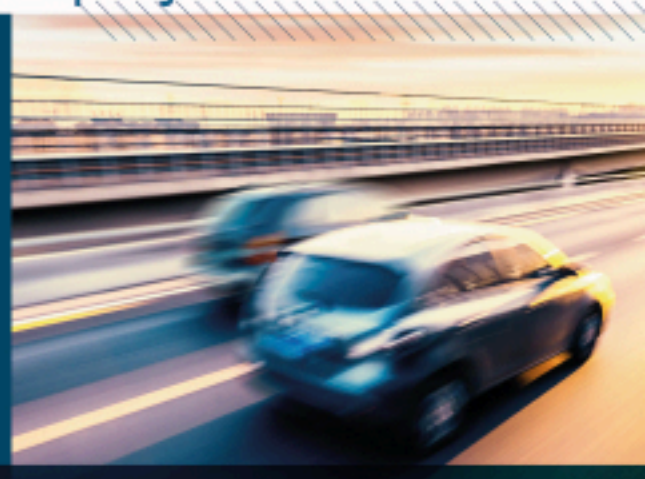
www.pegasusprojekt.de

Requirements & Conditions – Stand 2

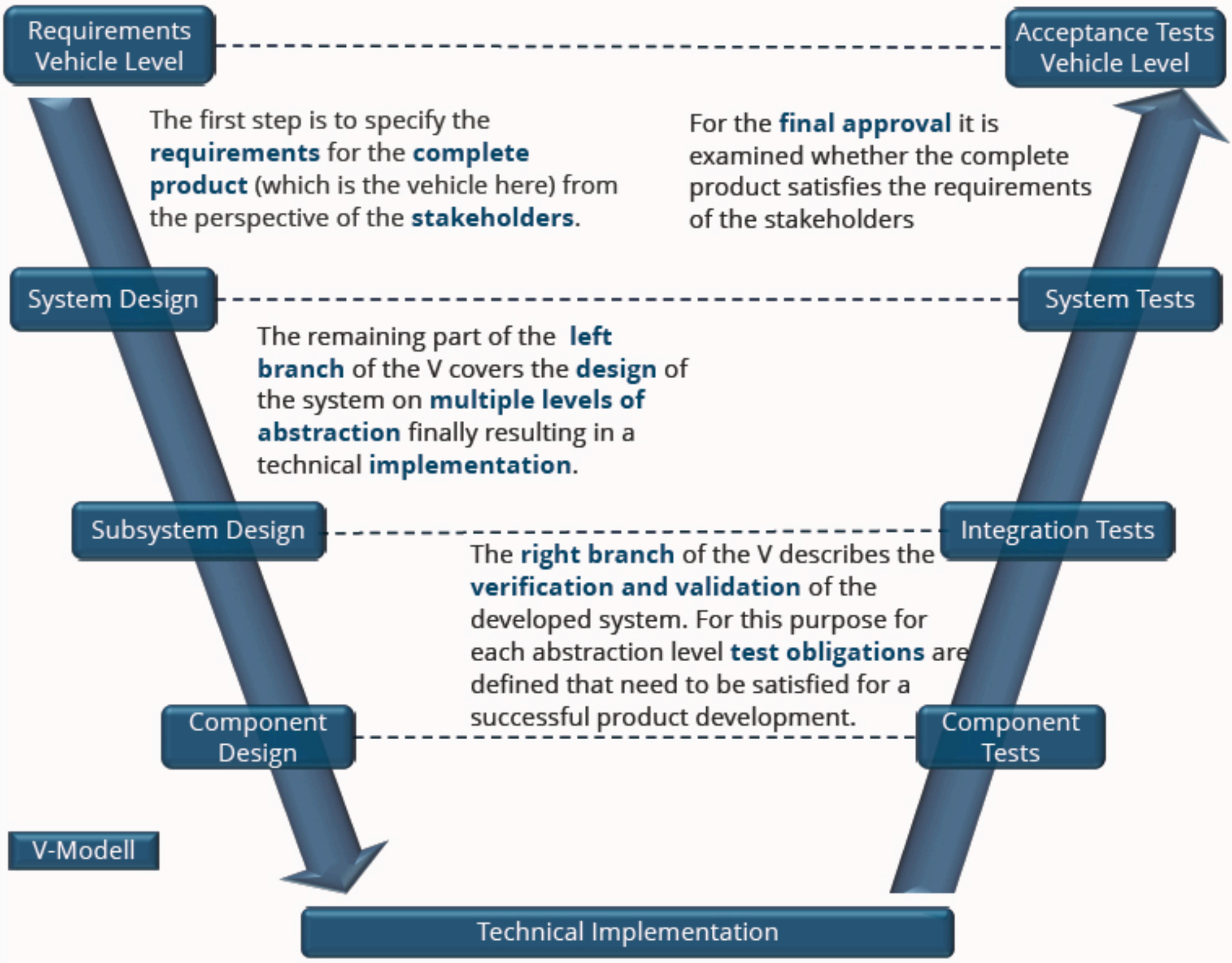
# V-MODEL AND PROCESS ANALYSIS



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 the software development that has established itself as well for the development of complex safe-critical systems in the avionics and **automotive domain**.




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

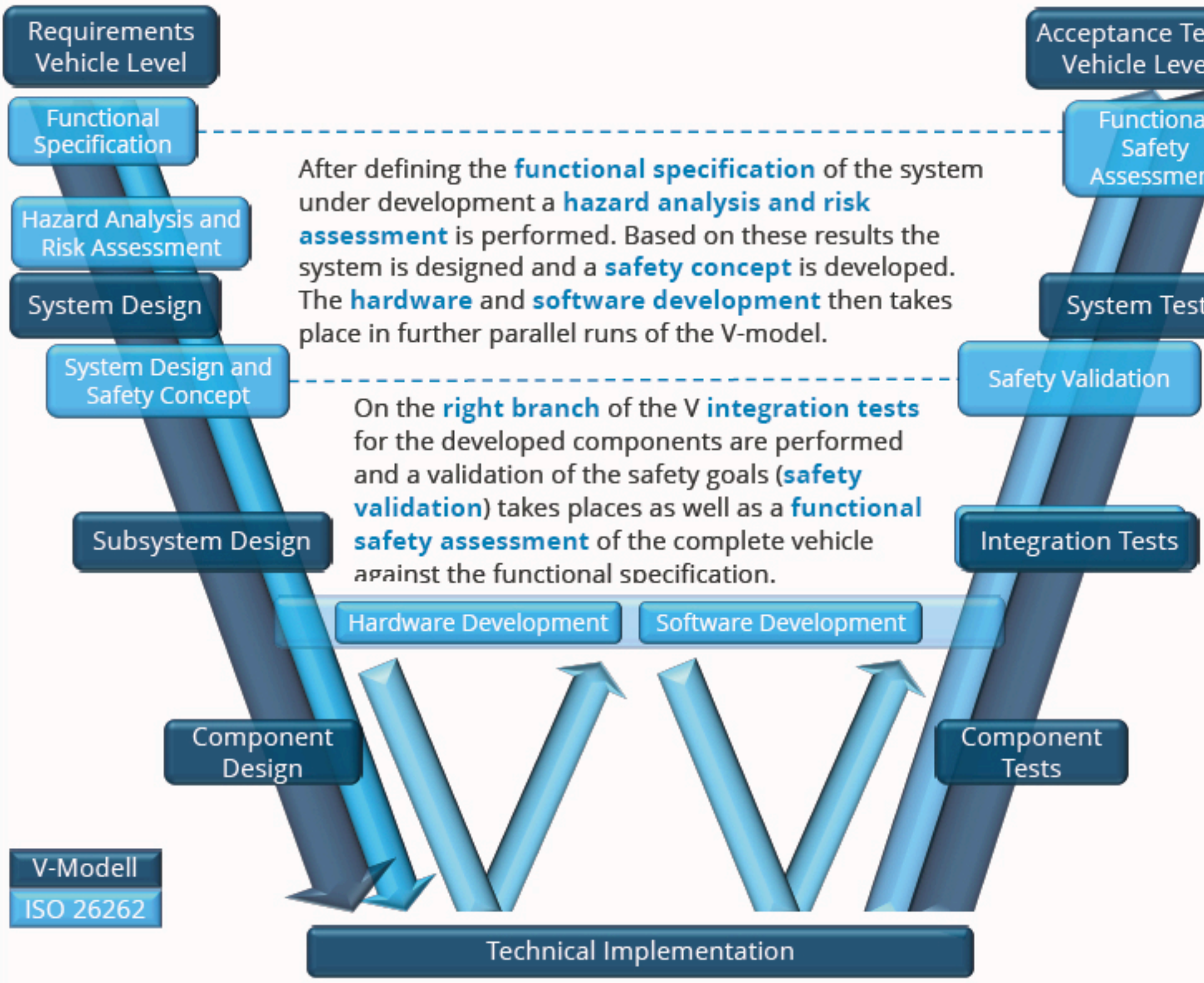
www.pegasusprojekt.de

Requirements & Conditions – Stand 2

# 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 **prove** the safety of such systems before putting them into operation.
- This process was and still is successfully applied for both vehicles that are exclusively operated by human drivers and advanced driver assistance systems (ADAS).




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

www.pegasusprojekt.de

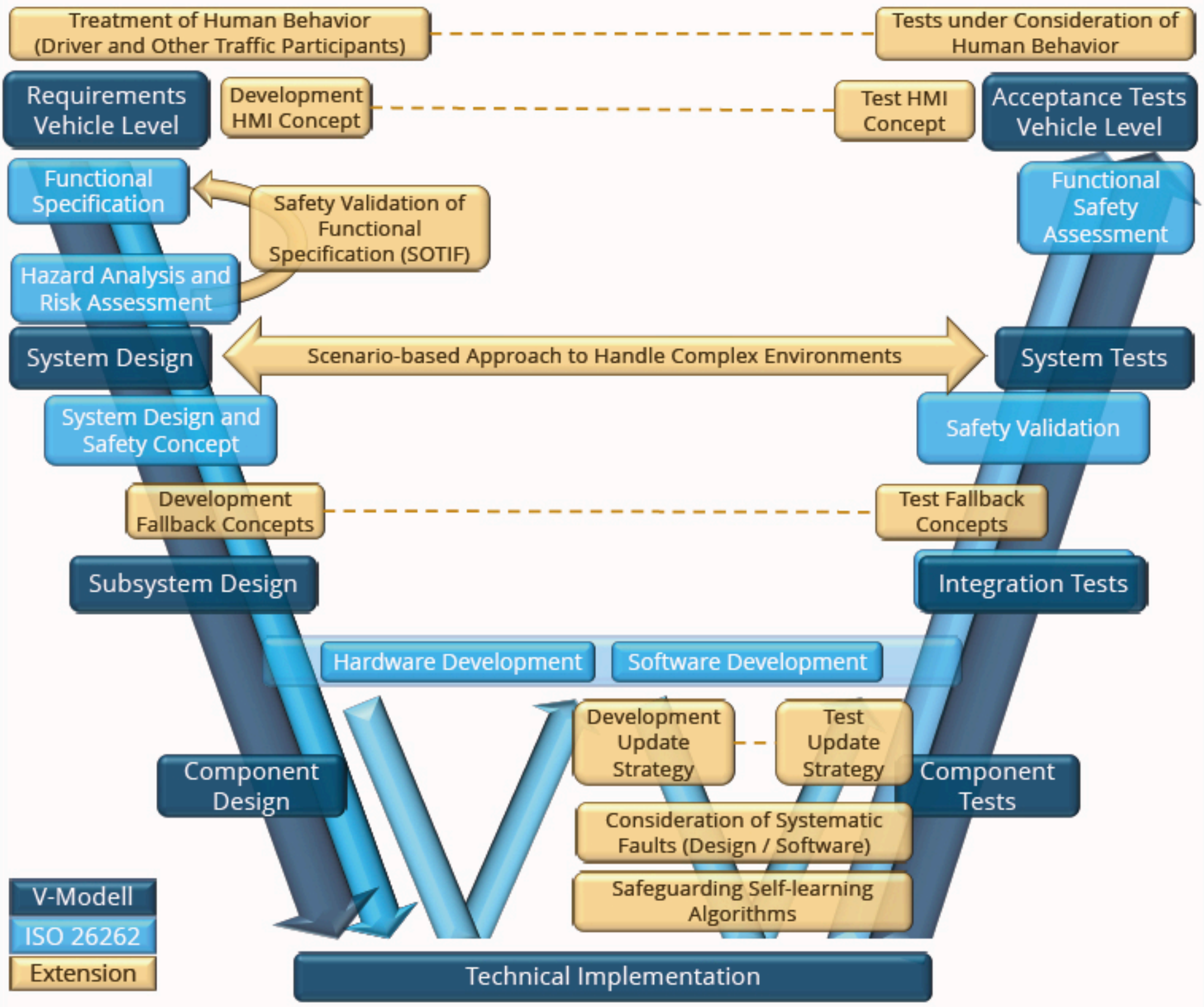
Requirements & Conditions – Stand 2

# V-MODEL AND PROCESS ANALYSIS

PEGASUS

**New Challenges** that arise with the introduction of automated driving functions and the resulting **extensions** of the development and safeguarding processes:

- ➡ Interaction with other human traffic participants (**mixed traffic**)
- ➡ **Takeover situations** between human driver and automation
- ➡ Operation in highly complex and hardly predictable environments (**open world**)
- ➡ Loss of human driver as fallback level (**fail-operational** instead of fail-safe)
- ➡ **Changing** safety-critical functional **requirements** during product life e.g. extension of the range of functions and the operational environment, respectively
- ➡ More intensive use of **machine learning techniques** in software modules




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