Federal Ministry
of Transport and
Digital Infrastructure

bast

Explanatory notes to the introduction of the document FRAV-03-03

From the Framework Document (FD):

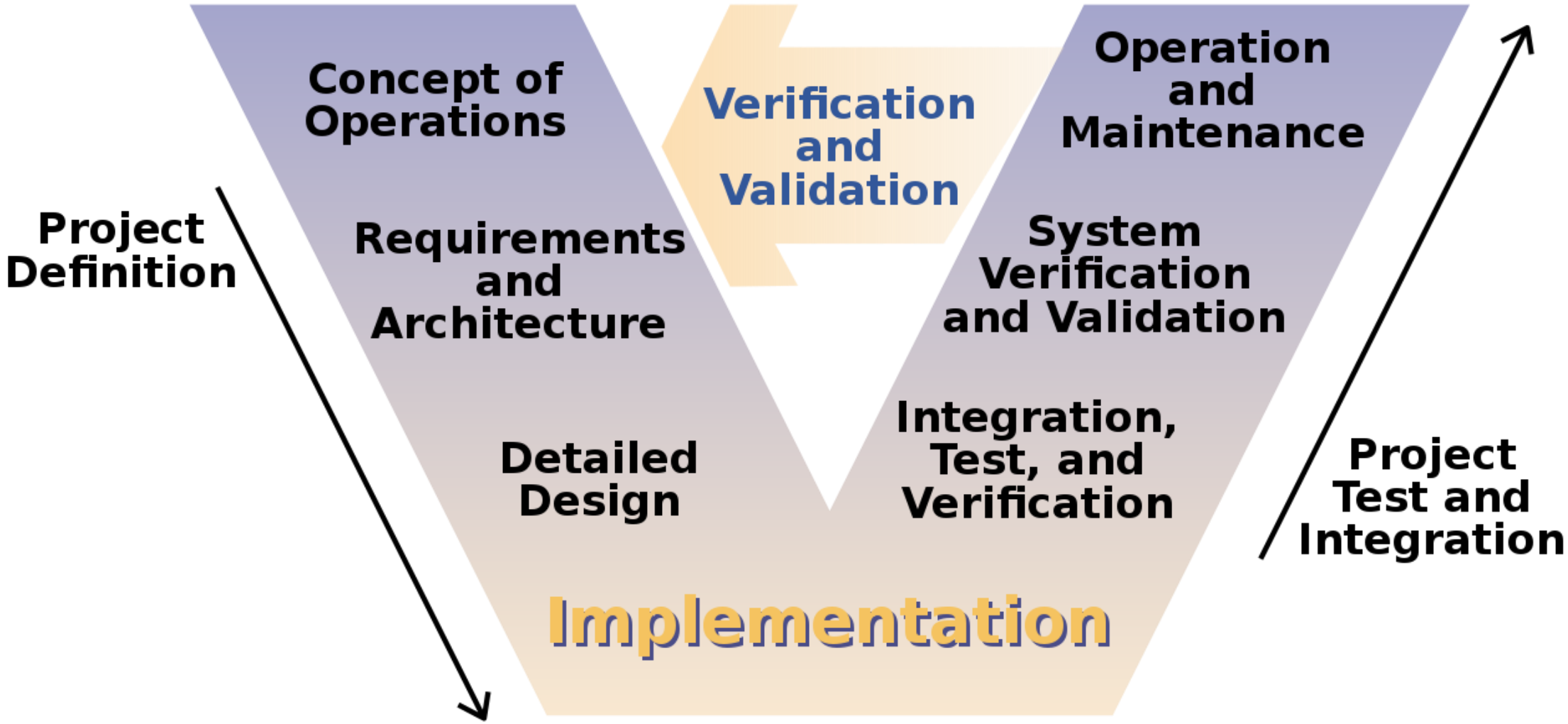
- *"When in the automated mode, the automated/autonomous vehicle should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations.",*
- *"This level of safety implies that an automated/autonomous vehicle shall not **cause** any non-tolerable risk [introduce unreasonable risks], meaning that automated/autonomous vehicle systems, while in automated mode, shall **not cause any traffic accidents** [incidents/events] resulting in [destruction of property,] injury or death that were reasonably foreseeable and preventable."*

Free of unreasonable risks:
This is a strategic decision, acknowledging the residual risk

To cause a risk:
a) cause an accident,
b) to not succeed to avoid a non-caused accident at least as good a human driver.

To cause an accident:
Cause an accident.

V-Model (Wikipedia):



V-Model

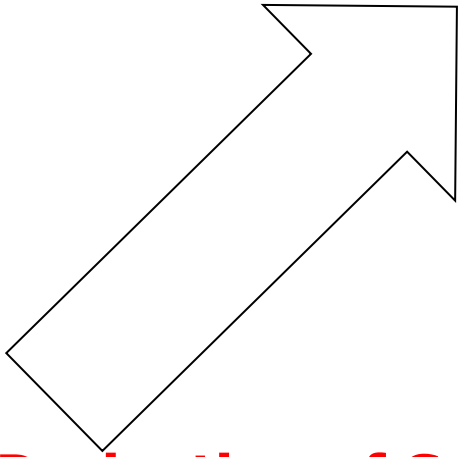
Requirements:
Does not cause unreasonable safety risks

Validation:
Did not cause unreasonable safety risks
(e.g. by balancing method)

Derived specifications

More specs?

…not cause any traffic accidents [incidents/events] resulting in [destruction of property,] injury or death that were ***reasonably foreseeable and preventable.***



Process of Derivation of Specifications intransparent?

Derived specifications

Specification:
Avoid the scenario x and
mitigate an accident in the scenario y

Verification:
Test scenario x and verify avoidance
Test scenario y and verify mitigation

„Reasonably foreseeable and preventable“

- Foreseeable by whom?
  - Expert Driver
  - Computer with sensors
  - Programmer of ADS
  - Neural Network
- Preventable through what?
  - Expert Driver-like control system
  - Fast brake actuator
  - Fast steering system

RFaP needs further specification and interpretation!

Conclusions and Proposal from FRAV-03-03

- Framework Document defines top-level requirements
- Specifications need to be derived
- Some kind of „product development process“ (→ V-Model)
- Define RFaP on a technical basis
- Process proposal: Agree on Specifications top-down!
  - As opposed to collecting requirements where the derivation is unclear
- Technical proposal (as an example):
  - Physical limitations *(DE‘s preference)*
  - (Safety Envelope is a special form of physical limitations)
  - Expert driver model