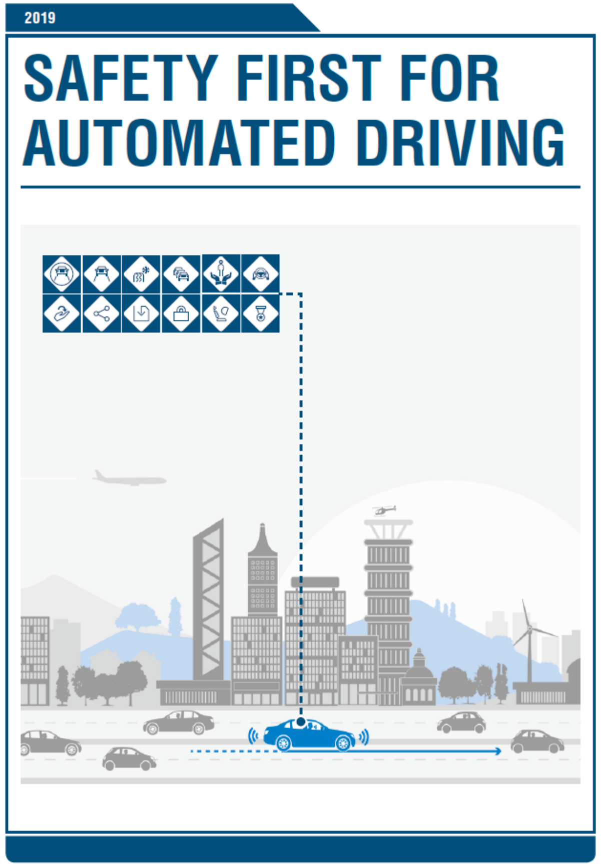
Document FRAV-01-11
Submitted by the expert from Continental



2019

SAFETY FIRST FOR AUTOMATED DRIVING

SAFETY FIRST FOR AUTOMATED DRIVING

White paper globally published on 2nd of July 2019

ABSTRACT
Automated Driving Systems

- Publication merges input of OEMs, tiered suppliers and key technology providers

- Positive risk balance
  - Safety by design and verification & validation methods
  - Comprehensive approach to safety relevant topics

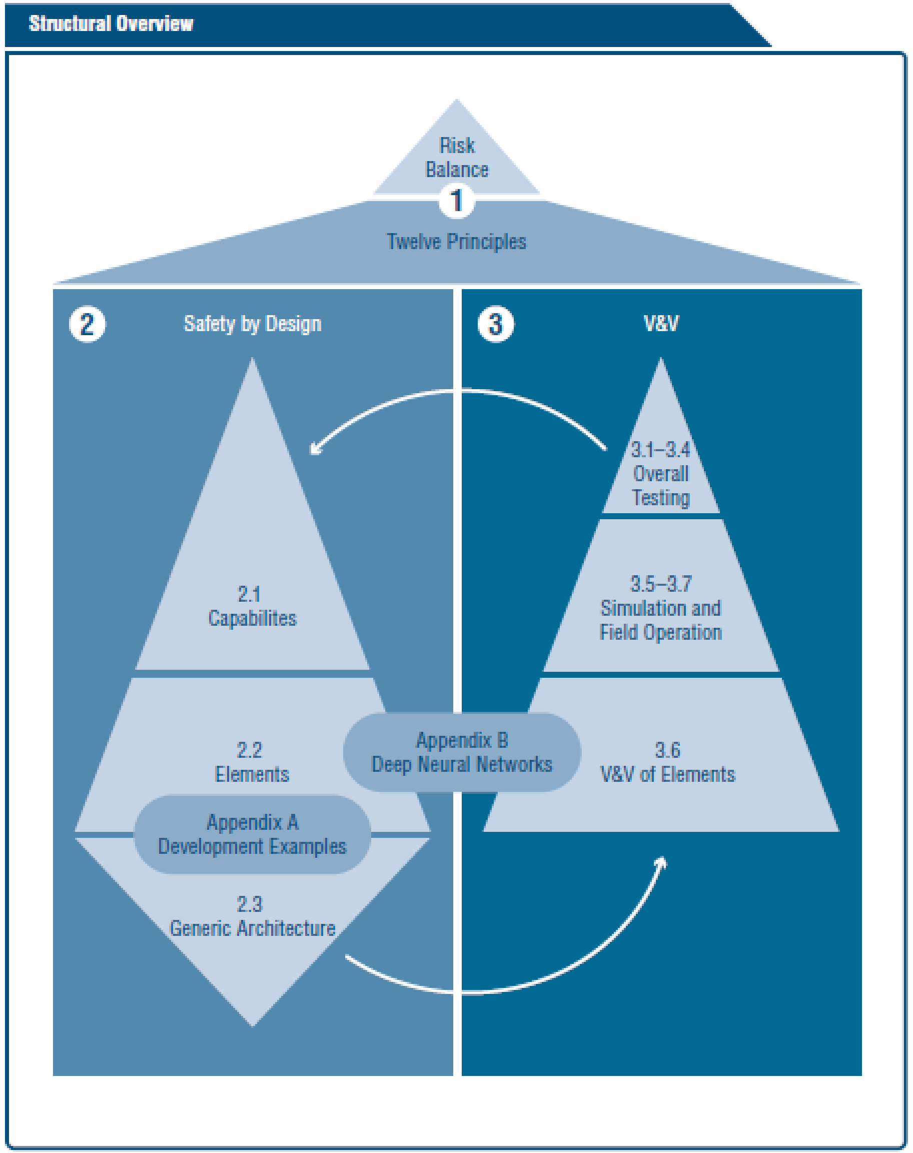
- Intends to collaborate to industrywide standardization

THE TWELVE PRINCIPLES OF AUTOMATED DRIVING

- **SAFE OPERATION**
  - Deal with degradation
  - Fail operational
- **SAFE LAYER**
  - Recognize system limits
  - React to minimize the risk
- **OPERATIONAL DESIGN DOMAIN**
  - ODD determination
  - Manage typical situations
- **BEHAVIOR IN TRAFFIC**
  - Manners on the road
  - Conforming to rules
- **USER RESPONSIBILITY**
  - Responsibilities
  - Mode awareness
- **VEHICLE-INITIATED HANDOVER**
  - Minimal risk condition
  - Takeover request
- **VEHICLE OPERATER-INITIATED HANDOVER**
  - Engaging and disengaging of AD system
  - Ensure intent of handover with high confidence
- **INTERDEPENDENCY (OPERATOR ↔ AD SYSTEM)**
  - Take effects on the driver due to automation into account
- **DATA RECORDING**
  - Record relevant data when an event or incident is recognized
  - Complies with the applicable data privacy laws
- **SECURITY**
  - Protect the automated driving system from security threats
- **PASSIVE SAFETY**
  - Crash scenarios (vehicle layout modifications)
  - Alternative seating position (new uses for the interior)
- **SAFETY ASSESSMENT**
  - Verification and validation to ensure that safety goals are met
  - Reach a consistent improvement of the overall safety

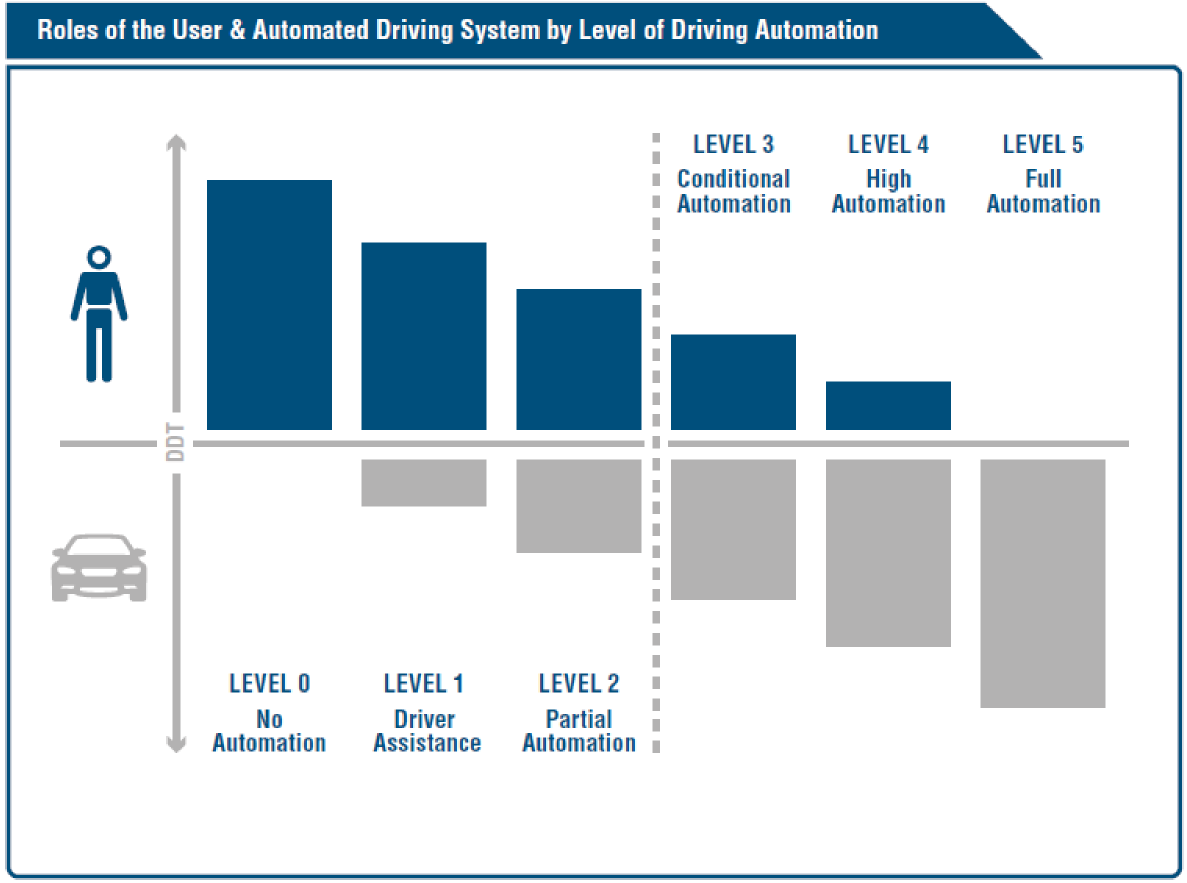
STRUCTURE OF THIS PUBLICATION

- This publication is structured as interconnected topics which build upon one another to achieve an overall **safety vision**.
- The roof ridge in the figure represents the **positive risk balance** as an initial starting point and the overall goal.



HUMAN - MACHINE INTERACTION

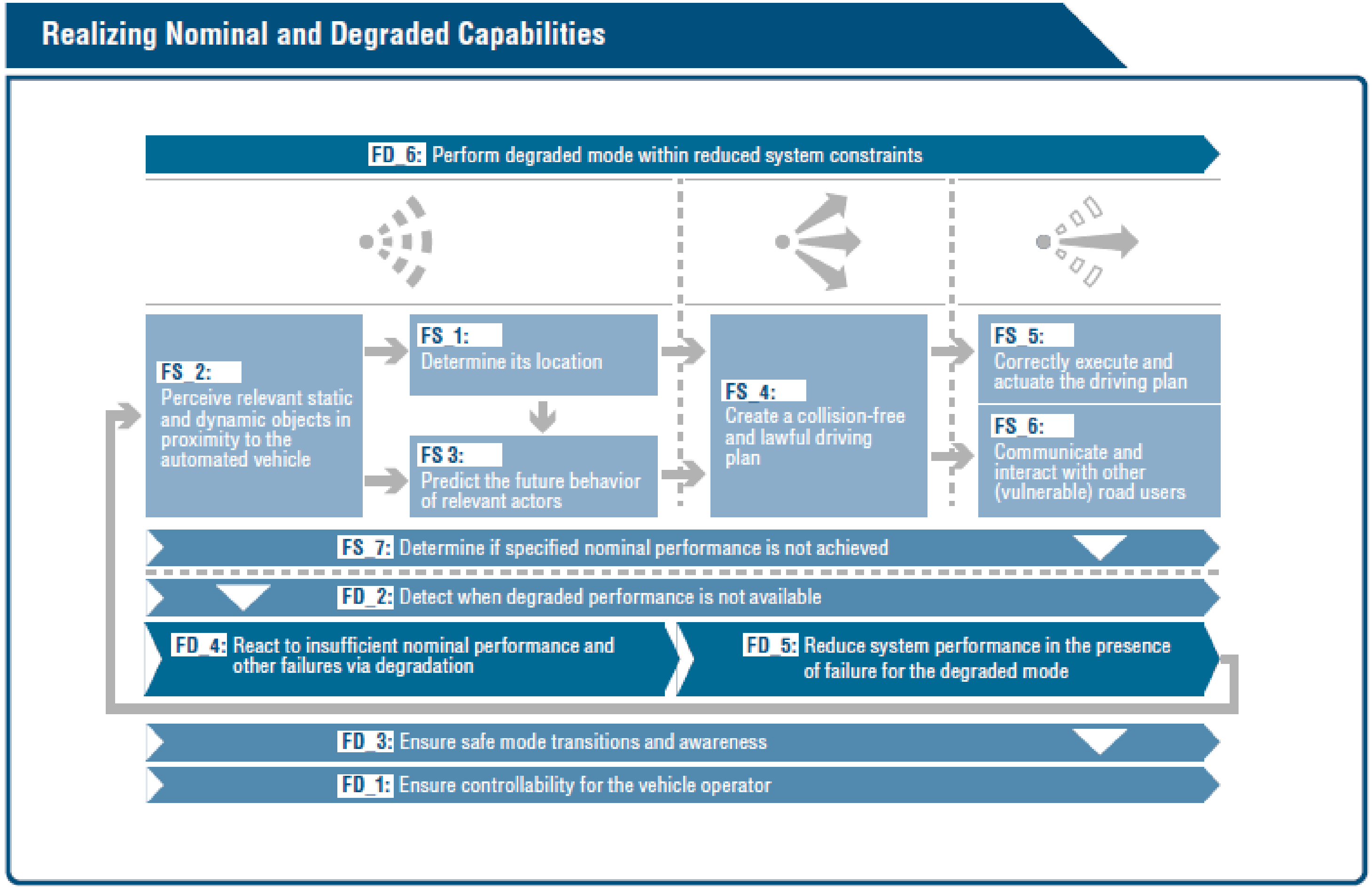
- Introducing L3 automated driving system,
  - the vehicle operator is allowed to **cede full control to the vehicle** during the nominal driving task **within** ODD
  - user’s **correct interpretation** of the actual driving mode and related **responsibility** for dynamic driving tasks (DDT) is crucial to enable safe driving



levels of automation according to SAE J3016

REALIZING NOMINAL AND DEGRADED CAPABILITIES

- Capabilities based on Sense – Plan – Act to achieve **nominal** performance
- Ensure **degradation** in case of insufficient nominal performance or other failures
- Ensure safe mode **transitions**



Realizing Nominal and Degraded Capabilities

FD_6: Perform degraded mode within reduced system constraints

FS_2: Perceive relevant static and dynamic objects in proximity to the automated vehicle

FS_1: Determine its location

FS 3: Predict the future behavior of relevant actors

FS_4: Create a collision-free and lawful driving plan

FS_5: Correctly execute and actuate the driving plan

FS_6: Communicate and interact with other (vulnerable) road users

FS_7: Determine if specified nominal performance is not achieved

FD_2: Detect when degraded performance is not available

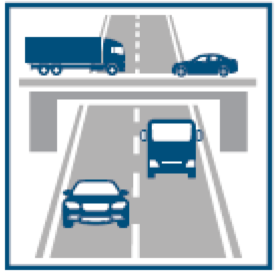
FD_4: React to insufficient nominal performance and other failures via degradation

FD_5: Reduce system performance in the presence of failure for the degraded mode

FD_3: Ensure safe mode transitions and awareness

FD_1: Ensure controllability for the vehicle operator

EXAMPLE TRAFFIC JAM PILOT (L3)

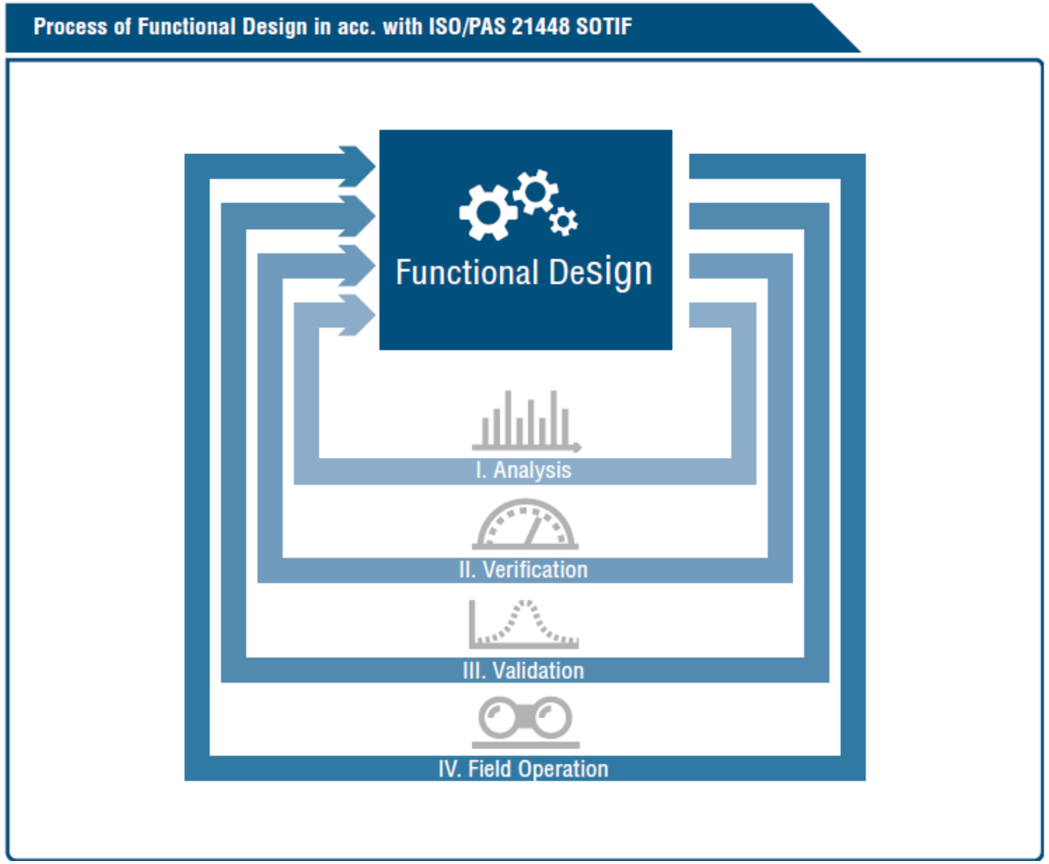


Nominal Function **Definition**	› **Vigilant** driver with driver's license, › driving only on **structurally separated roads** › typically **no** pedestrians or cyclists › 60 km/h **max** › **only** with leading vehicles › **no** lane changing › **no** construction sites › **only** during daylight, without rain › **only** temperatures higher than freezing point
Minimal Risk Conditions	› **Driver** has taken over control › Deactivate as soon driver has control or the vehicle is stopped › Vehicle is stopped **in-lane** › **Immediately** stop the vehicle with **fixed** deceleration › **lateral** vehicle movement based **on last valid** trajectory

Sensing Elements for **Localization**	› Determine whether the vehicle is on the **highway**
Sensing Elements for Perceive **Relevant Objects**	› Leading **vehicles in front** of the ego vehicle › Lane markings › **(vulnerable) road users** (even though they are excluded from the ODD) › **Diversity object detection methods** are preferred to cover the performance weakness of single sensors › **High-level object fusion** is considered a meaningful measure
ADS Mode Manager	› Check **activation** conditions › Check **deactivation** conditions › Ensure that the vehicle has either reached a **fail-safe state** › Or that the user has **safely taken over** control

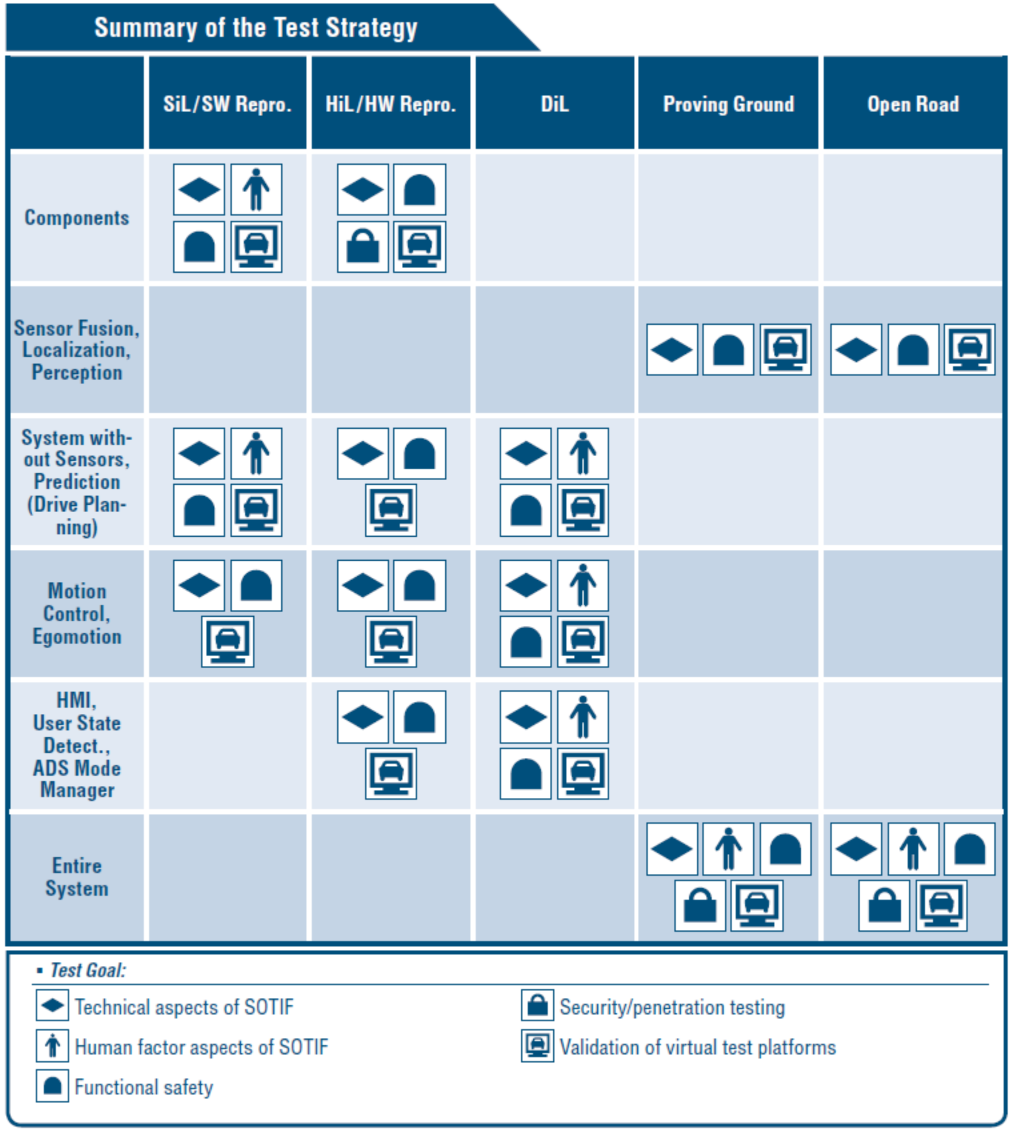
VERIFICATION AND VALIDATION
KEY CHALLENGES FOR V&V OF L3 AND L4 SYSTEMS

- Statistical demonstration of system safety and a **positive risk balance** without driver interaction
- System safety with driver **interaction** (especially in takeover maneuvers)
- Consideration of scenarios currently **not known** in traffic
- Validation of various system **configurations** and **variants**
- Validation of (sub) systems that are based on **machine learning**



TEST STRATEGIES

- A viable test strategy responds to the **key challenges** in the V&V of automated driving systems
  - by carefully breaking down the overall **validation objective** into **specific test goals** for every object under test
  - and by defining **appropriate** test platforms and test design techniques



Summary of the Test Strategy

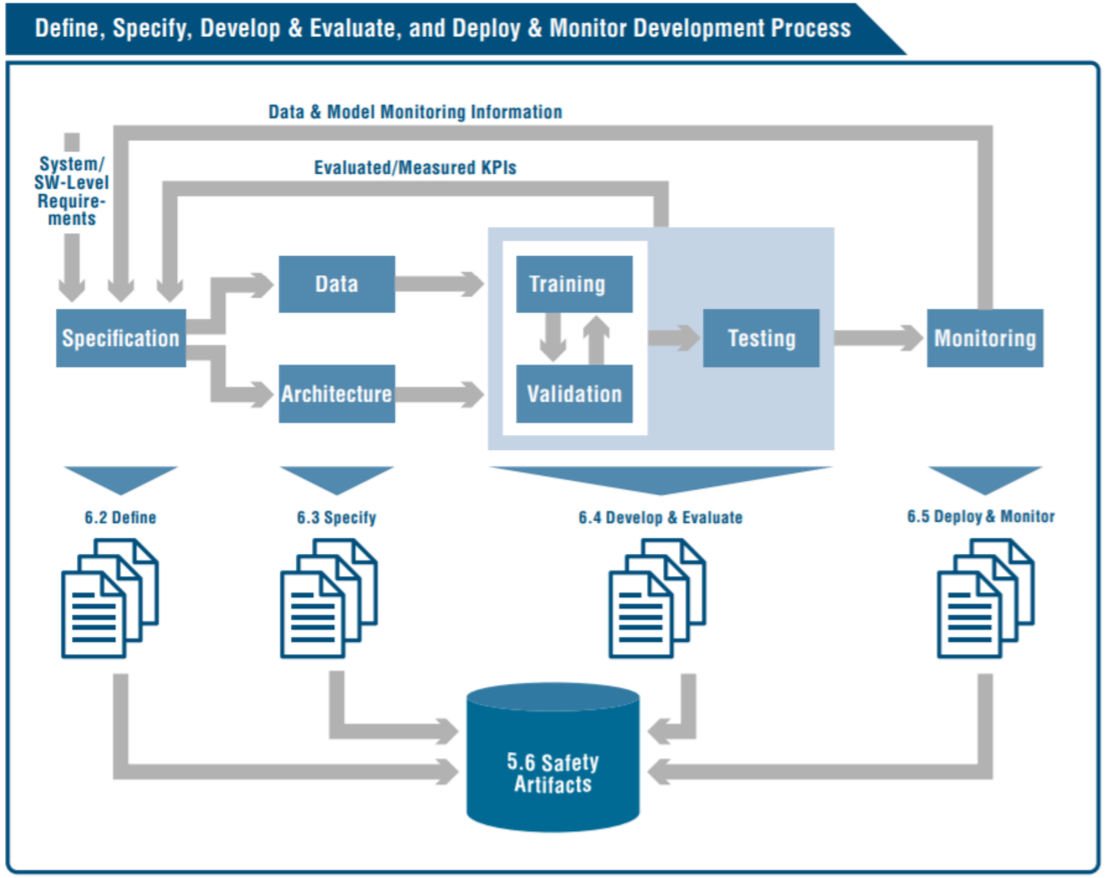
	SiL/SW Repro.	HiL/HW Repro.	DiL	Proving Ground	Open Road
Components	◆ 🚶 ● 🖥	◆ ● 🔒 🖥			
Sensor Fusion, Localization, Perception				◆ ● 🖥	◆ ● 🖥
System without Sensors, Prediction (Drive Planning)	◆ 🚶 ● 🖥	◆ ● 🖥	◆ 🚶 ● 🖥		
Motion Control, Egomotion	◆ ● 🖥	◆ ● 🖥	◆ 🚶 ● 🖥		
HMI, User State Detect., ADS Mode Manager		◆ ● 🖥	◆ 🚶 ● 🖥		
Entire System				◆ 🚶 ● 🔒 🖥	◆ 🚶 ● 🔒 🖥

▪ *Test Goal:*

◆ Technical aspects of SOTIF	🔒 Security/penetration testing
🚶 Human factor aspects of SOTIF	🖥 Validation of virtual test platforms
● Functional safety	

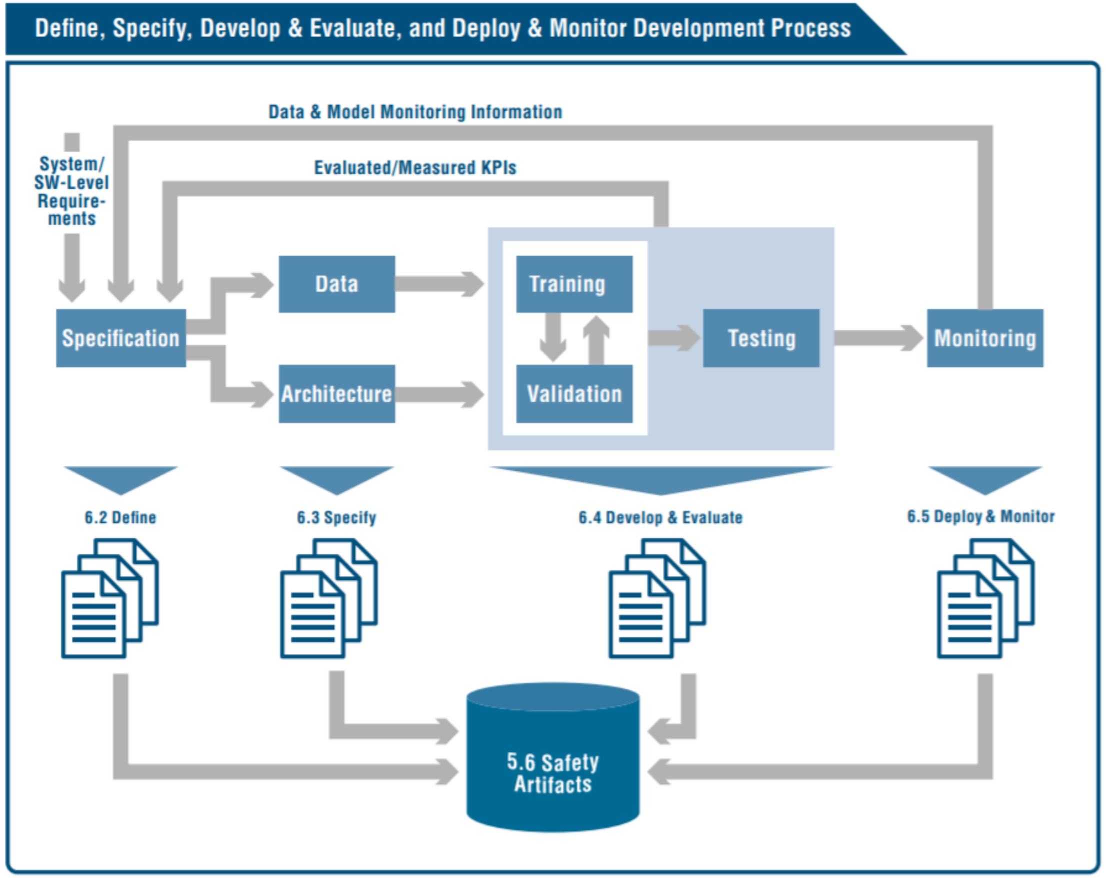
SAFETY ASPECTS OF DEEP LEARNING IMPLEMENTATION

- **General considerations**
  - Be agnostic to means of implementation; documentation during full process chain, creation of safety artefacts.
- **Define**
  - ODD, Data set, probabilistic output, KPIs, target hardware
- **Specify**
  - Data set specs, labelling specs, labelling quality, DL model architectures, observers.



SAFETY ASPECTS OF DEEP LEARNING IMPLEMENTATION

- **Develop & Evaluate**
  - DL model architecture (layers, connectivity, activations, pooling/upsampling, stride, …); composition of loss, regularization, optimization methods (solver, learning rate, …).
- **Deploy & Monitor**
  - Challenges: unseen data, confidence interpretation, emerging features, distributional shift.


Define, Specify, Develop & Evaluate, and Deploy & Monitor Development Process
Data & Model Monitoring Information
Evaluated/Measured KPIs
System/ SW-Level Require- ments
Specification
Data
Architecture
Training
Validation
Testing
Monitoring
6.2 Define
6.3 Specify
6.4 Develop & Evaluate
6.5 Deploy & Monitor
5.6 Safety Artifacts