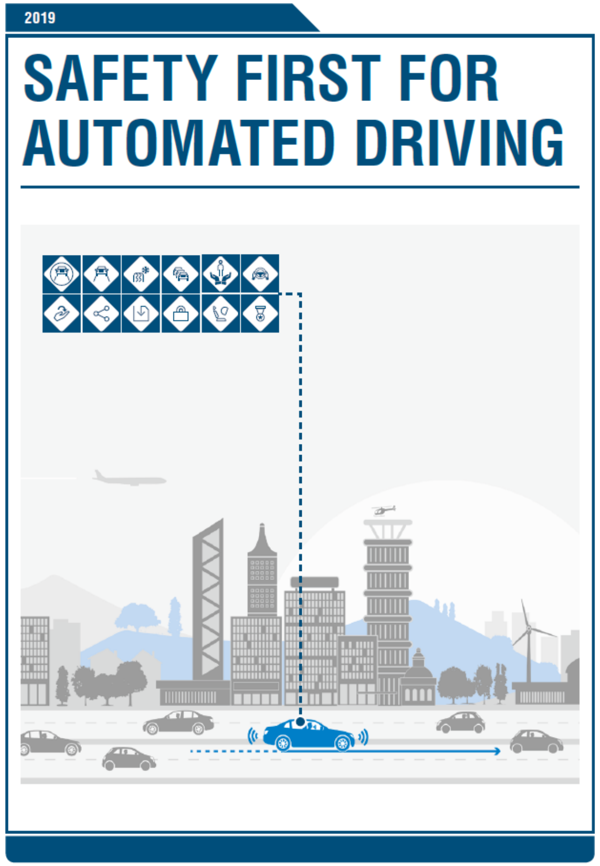
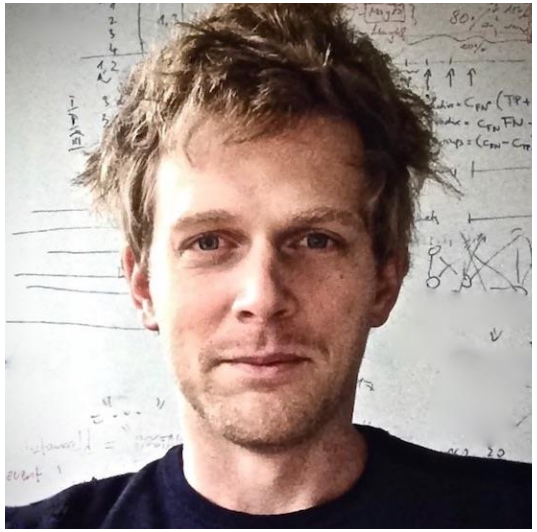
The Future in Motion



Safety First for Automated Driving

ADA/ITU Workshop in Budapest on the 10th September

Anti trust note: All following information need to be understood as a minimum basis shared commonly by the partner consortium. A complete safety case for a concrete product depends heavily on the specific operational design domain and needs always specific additional measures.



David Lanyi

Head of Machine Learning Methods
Continental BU ADAS – Deep Learning Competence Center

- 2018- Continental
- 2012-2018 IBM Research Zurich
- 2014-2015 ETH Zurich
- MS in computer science, Budapest University of Technology and Economics

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

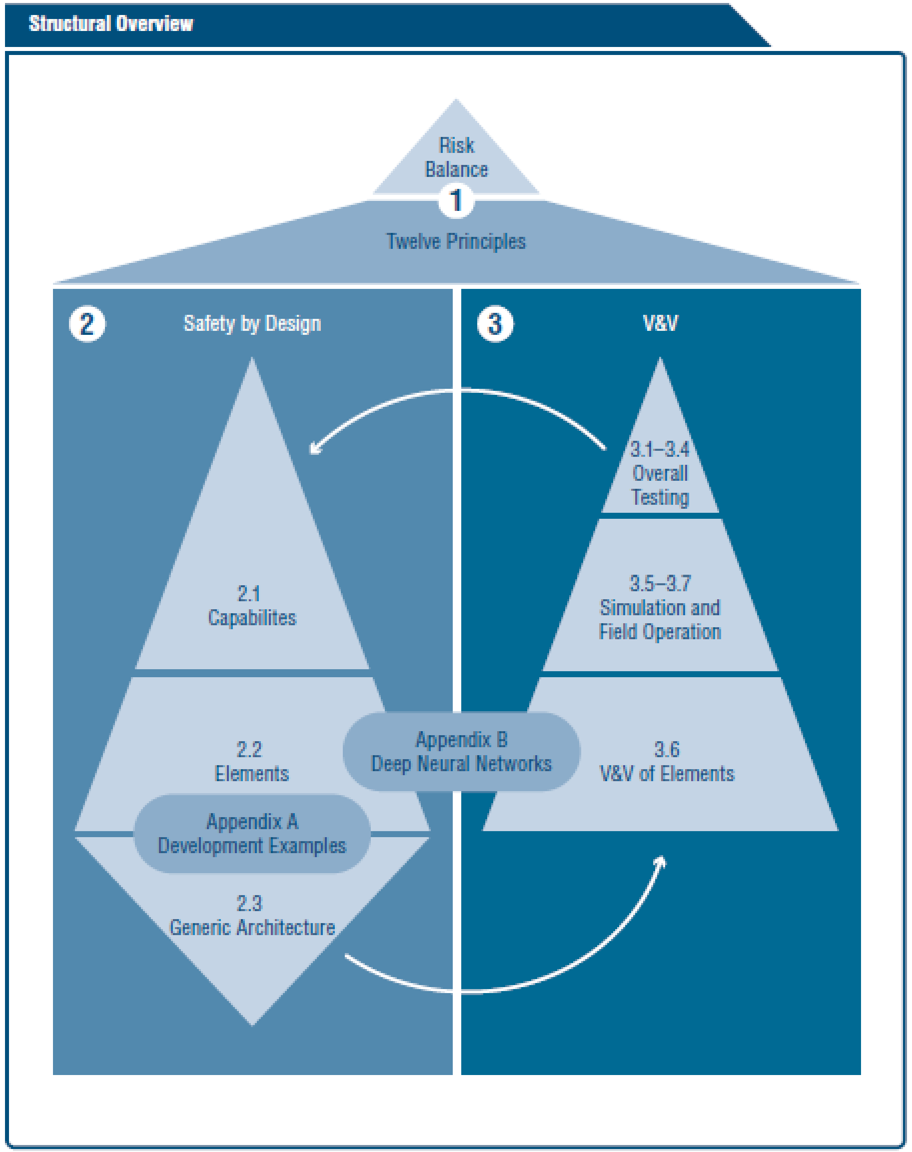
- Intends to collaborate to industrywide standardization

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

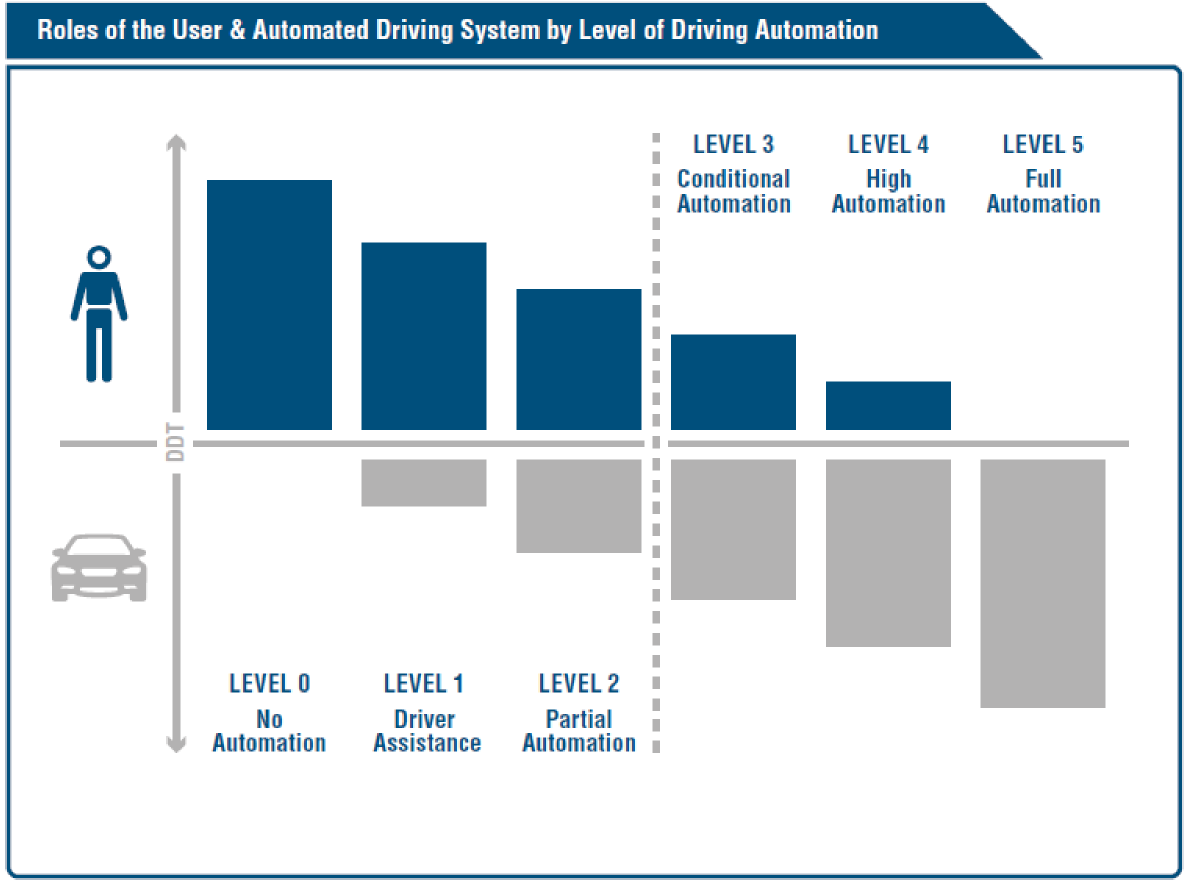
Structure of this Publication

- 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



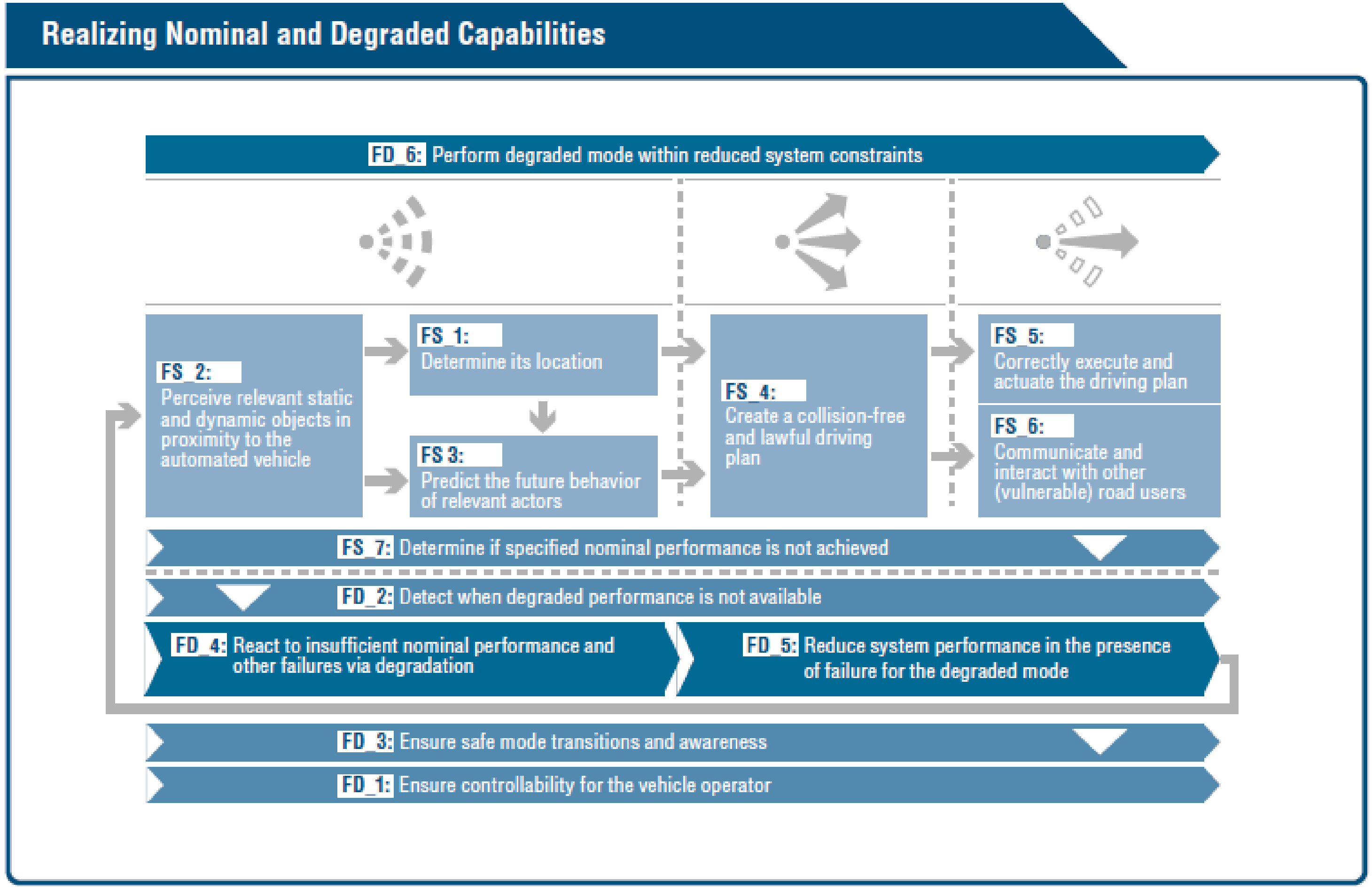
levels of automation according to SAE J3016

Realizing Nominal and Degraded Capabilities

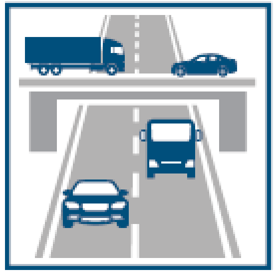
› Capabilities based on Sense – Plan – Act to achieve **nominal** performance

› Ensure **degradation** in case of insufficient nominal performance or other failures

› Ensure safe mode **transitions**



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

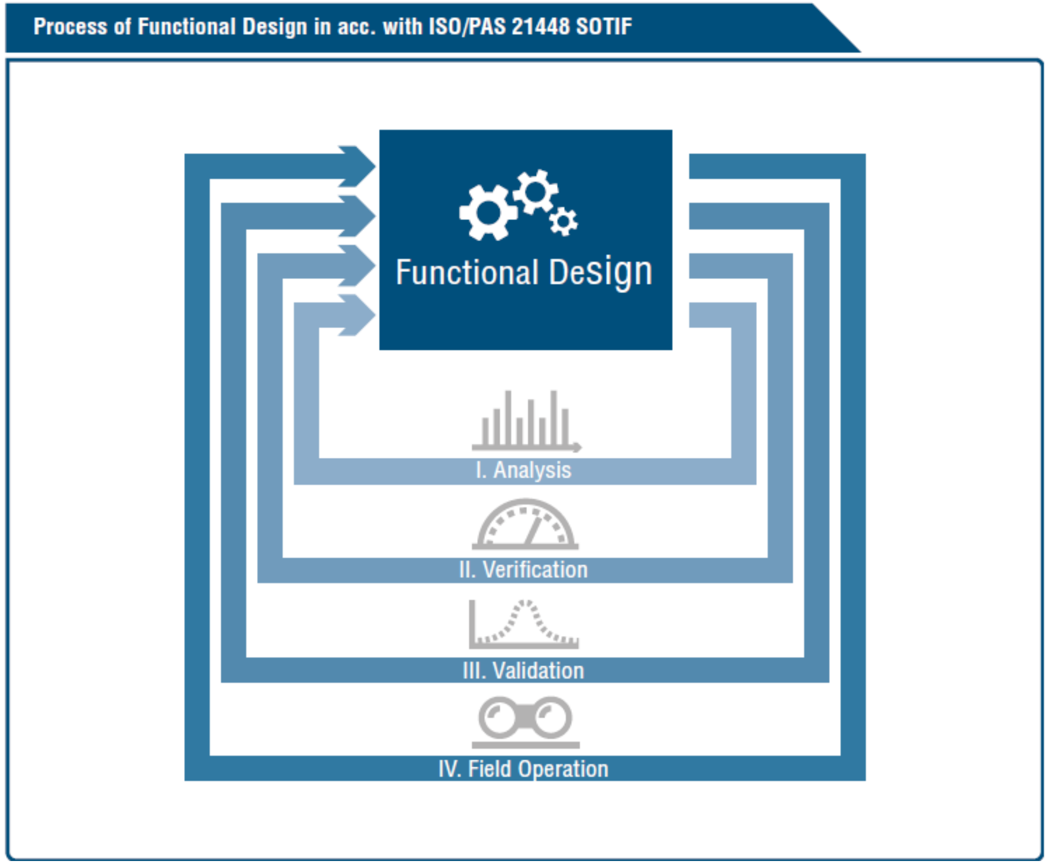
Minimal Risk Conditions	› **Driver** has taken over control
	    › Deactivate as soon driver has control or the vehicle is stopped
	› Vehicle is stopped **in-lane**
	    › **Immediately** stop the vehicle with **fixed** deceleration
	    › **lateral** vehicle movement based on **last valid** trajectory

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

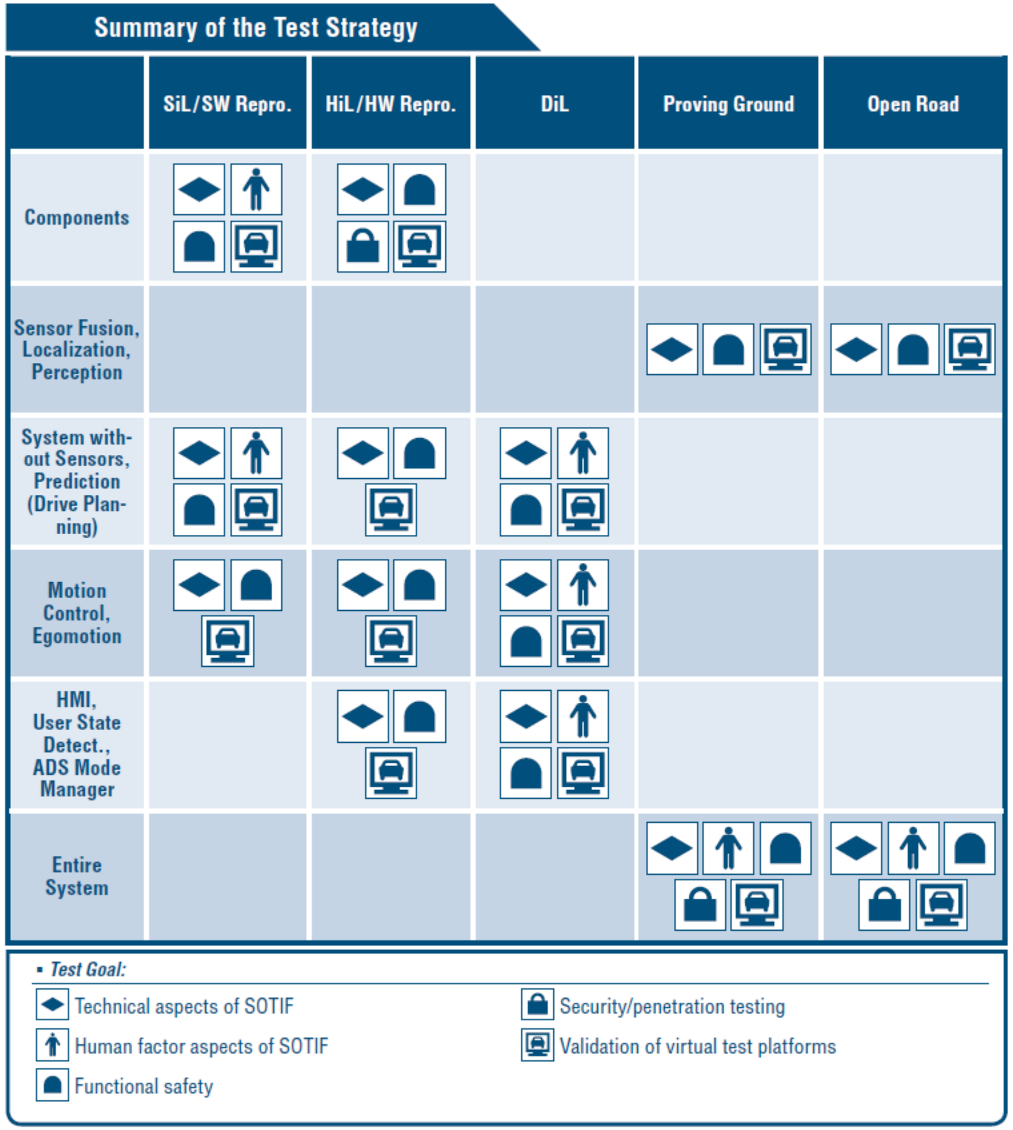
Verification and Validation
Key Challenges for V&V of L3 and L4 Systems

- 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**



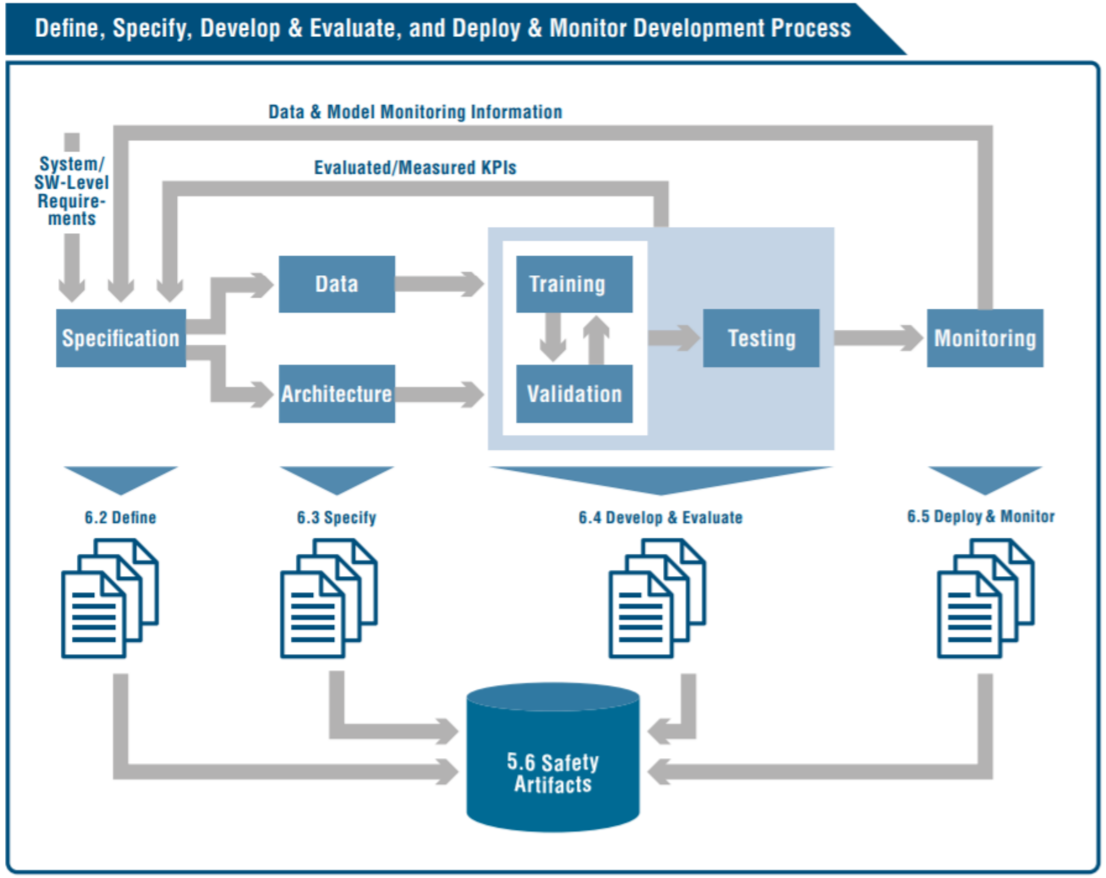
Test Strategies

- 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



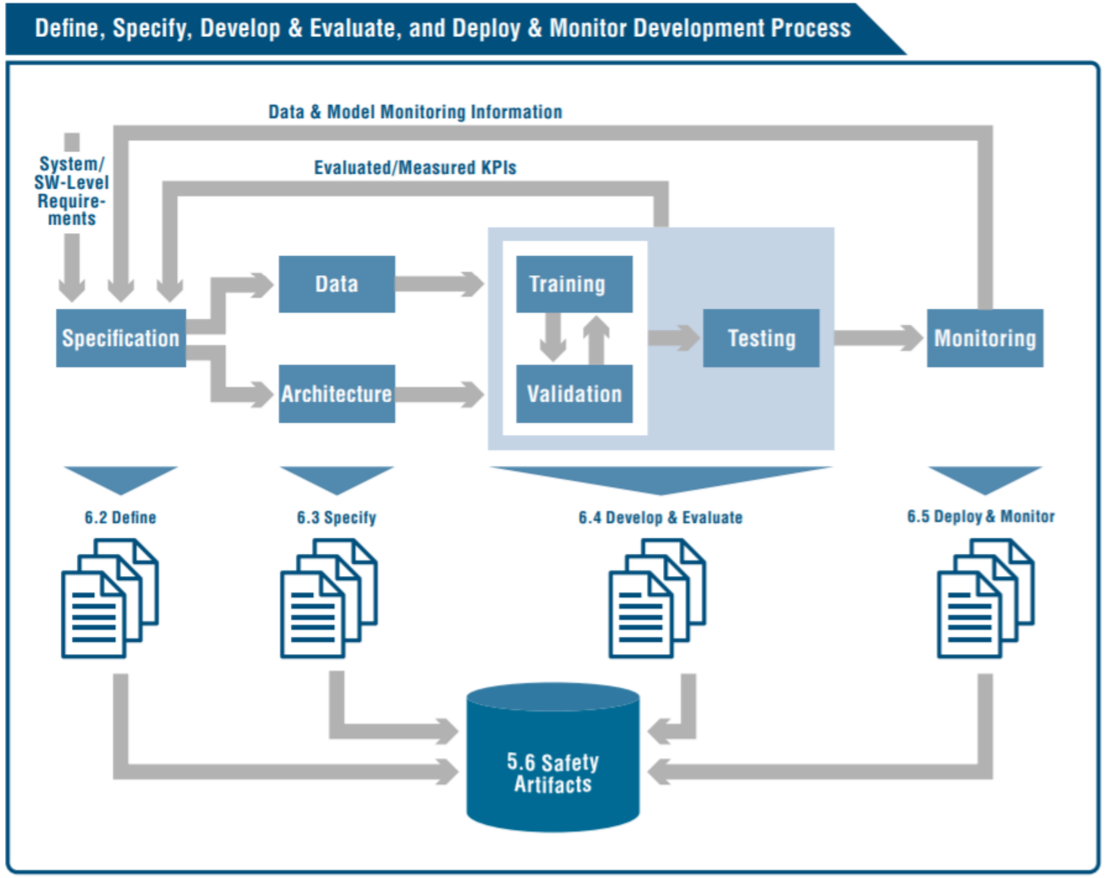
Safety Aspects of Machine Learning Systems

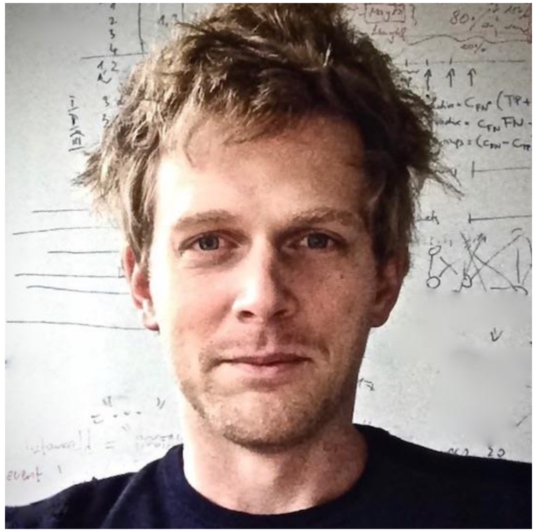
- **General considerations**
  - Be agnostic to means of implementation; documentation during full process chain, creation of safety artefacts.
- **Define**
  - ODD, data set, probabilistic output, KPIs, target hardware
- **Specify**
  - Data set specs, labelling specs, labelling quality, DL model architectures,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



Safety Aspects of Machine Learning Systems

- **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.





David Lanyi

Head of Machine Learning Methods
Continental BU ADAS – Deep Learning Competence Center

- 2018- Continental
- 2012-2018 IBM Research Zurich
- 2014-2015 ETH Zurich
- MS in computer science, Budapest University of Technology and Economics