# Validation, Verification & Quality Assurance of Machine Learning Systems


- Dr. Ernest Wallmüller
  - www.itq.ch
  - wallmueller@itq.ch
- Dr. Martin Reber
  - www.nviso.ai
  - martin.reber@nviso.ch


# Outline

- Computer Vision and neuronal processing at NVISO (Introduction)
- Data driven programming at NVISO: Key properties of the NVISO AI & Machine learning process
- ML process details and tools: How to do data driven programming
- QA & QM of ML Software/Systems
- Experiences & discussion
- Summary & Conclusion

# NVISO in brief

- **NVISO is a global leader in human behaviour artificial intelligence software, for safe secure and personalised autonomous machines with advanced, emotional HMI.**
- **NVISO AI software is licensed worldwide to global manufacturers of user centric products and service-based industries within the healthcare, automotive, consumer and financial services sectors.**
- **Proprietary technology developed over 10 years with collaborative R&D funding from Europe's leading AI funding. Collaboration with Europe's top tier world leading AI researchers (EPFL, ETHZ, University of Edinburgh, Technical University of Munich).**


- Founded in Lausanne (HQ), Switzerland as a spin out from EPFL in 2009.
- Owns massive real-world database of over 1Billion data points.
- Global customer footprint, 35 employees and offices in Switzerland, Japan & Australia.
- Market focus on Smart Mobility, Smart Health, Smart Home and Smart Finance.

# NVISO **BUSINESS AREAS**

Applications Touching Every Consumer where Human Behaviour AI is Mission Critical

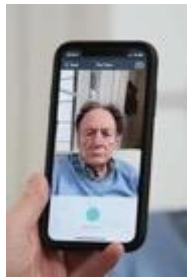
## Smart Health and Living

### COMPANION ROBOTS

Social robots reduce loneliness and increase independence in people living at home alone.

### HEALTH ASSESSMENTS

The aged care sector is in desperate need of technological solutions to support the care of the elderly and particularly those living with dementia.



## Smart Mobility

### ADVANCED DRIVER MONITORING SYSTEMS

Understand driver state and his distracting activities is key in advanced DMS systems.

FOR SAFER CARS EURO NCAP

### INTERIOR SENSING SYSTEMS

Next generation mobility requires AI for interior sensing for safety, security, and experience.

## Edge Computing Platforms

**IOT** @ 1fps

NXP

**Low power edge computing platform** with camera attached to device.

**EDGE** @ 30fps

RENESAS

**Low power edge computing platform** supporting attached cameras.

**MOBILE** @ 20fps

android iOS

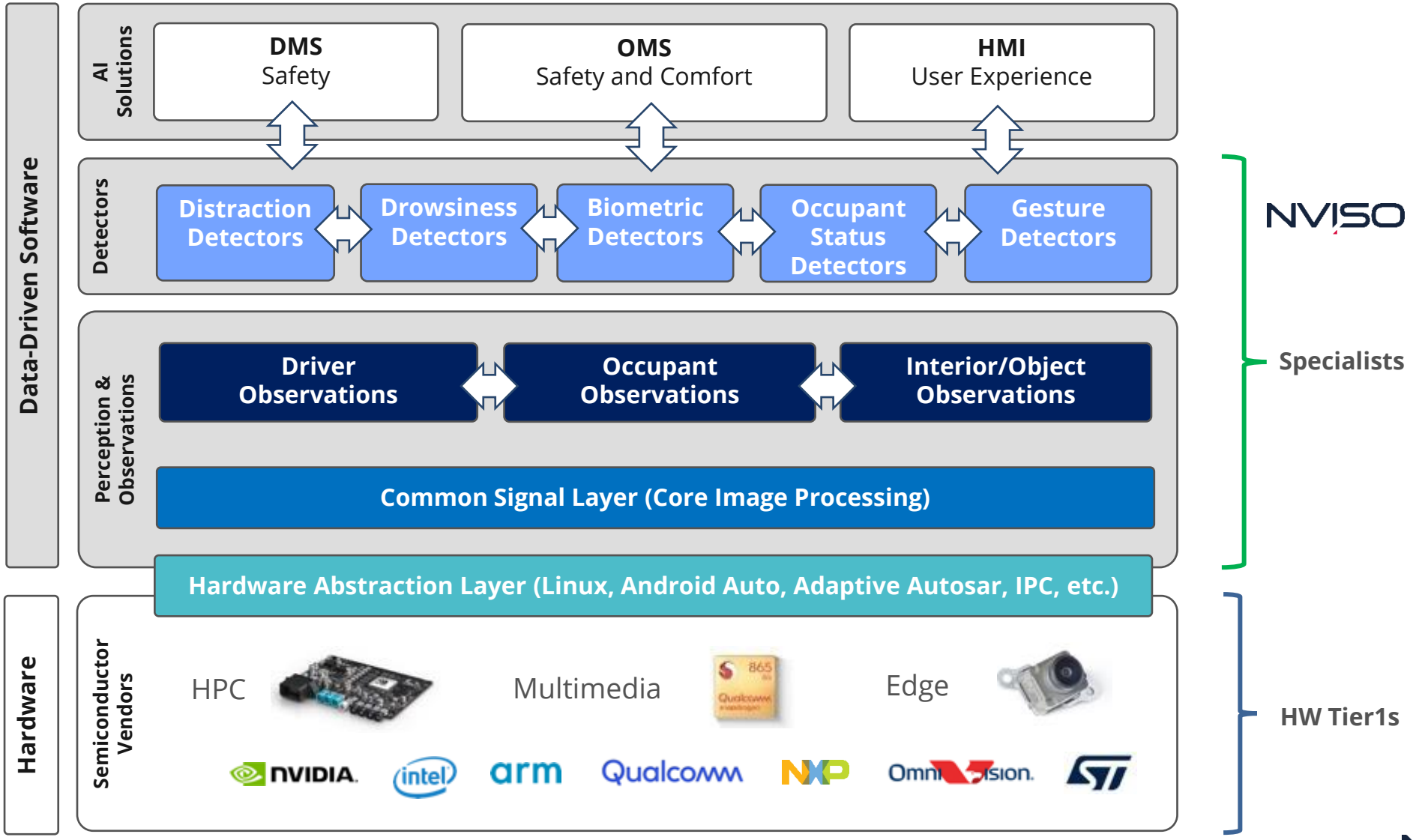
**Phone or tablet with embedded camera** in screen with restricted placement.

**HPC** @ 60fps

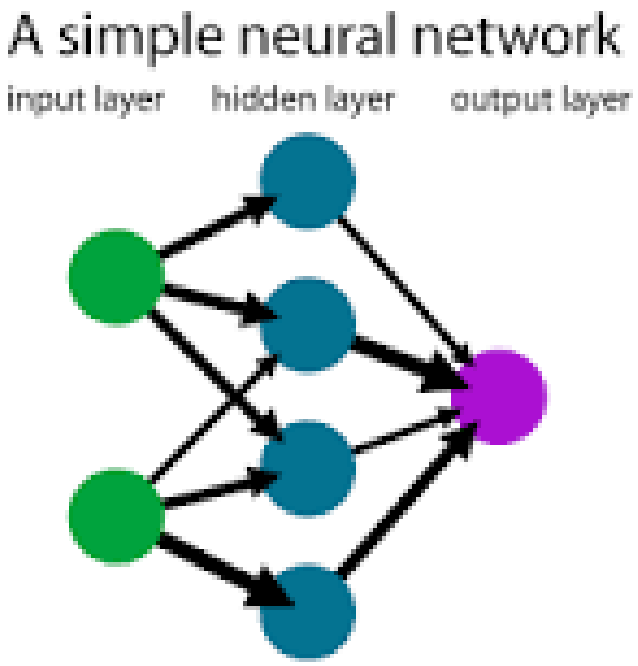
NVIDIA

**High power edge computing platform** supporting attached cameras or non-attached cameras.

**On-Device Intelligence** with Embedded Cameras in Cars, Robots, and Medical Devices


Data-Driven Software
AI Solutions
DMS
Safety
OMS
Safety and Comfort
HMI
User Experience
Detectors
Distraction Detectors
Drowsiness Detectors
Biometric Detectors
Occupant Status Detectors
Gesture Detectors
Perception & Observations
Driver Observations
Occupant Observations
Interior/Object Observations
Common Signal Layer (Core Image Processing)
Hardware Abstraction Layer (Linux, Android Auto, Adaptive Autosar, IPC, etc.)
Hardware
Semiconductor Vendors
HPC
Multimedia
Edge
NVIDIA
intel
arm
Qualcomm
NXP
OmniVision
NVISO
Specialists
HW Tier1s

# How do artificial neural networks work?




An artificial neuron **simulates how a biological neuron behaves by adding together the values of the inputs it receives**.

If this is above some threshold, it sends its own signal to its output, which is then received by other neurons.

However, a neuron doesn't have to treat each of its inputs with equal weight.

Real world problem / challenge

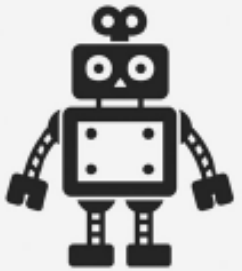
e.g. Driver Observation

Training

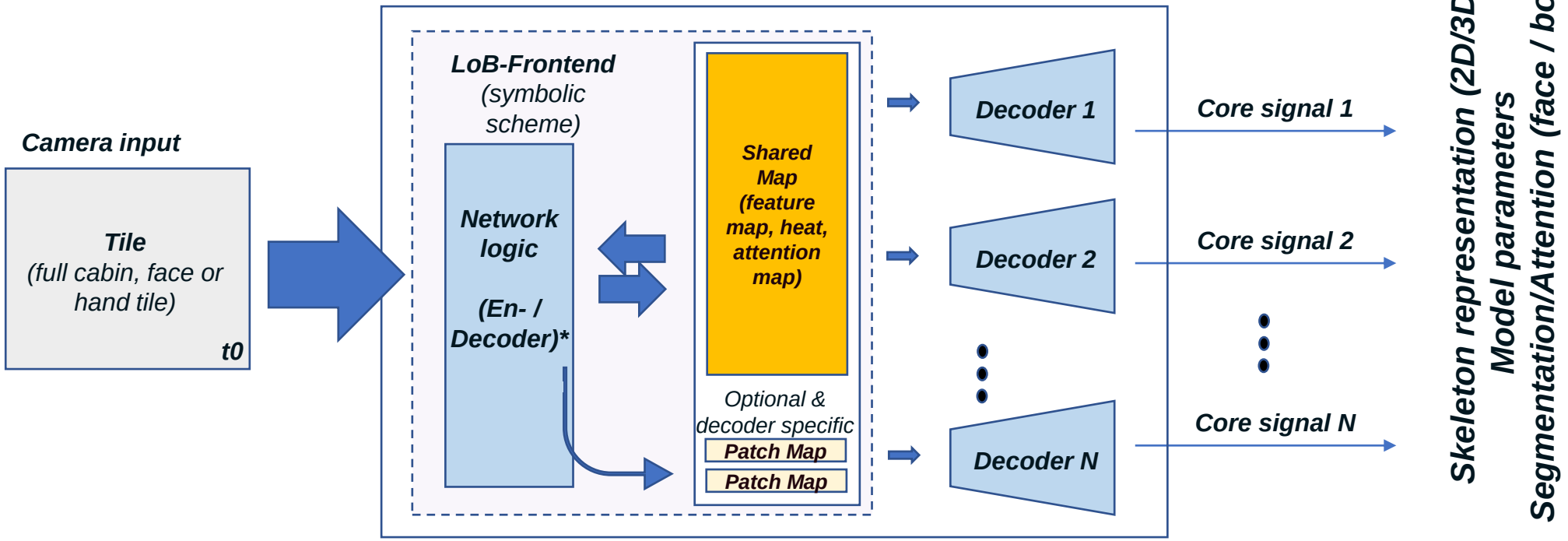
Data

Algorithm

Model



# Automotive Hydra **Net – Life-On-Board (LoB) NN Type** ***– Body, Baby, Hand, Face, Animal, Object Skeletons -***




- **Easy to extent:** Dec1: Adults (body, hand, head, face) Dec2: Baby, Dec3: Animals, Dec3: Selected objects (like Baby seat, Pet-Carrier), Dec4: Face Decoration, Dec5: Seat-belt, Dec6: Clothes, ***Dec7: future options***
- **Enables efficient changes/updates/ticket handling:** without affecting other core signals and min. effect on memory and computational load
- **Model driven:** For highest performance and handling of extreme occlusions (one object in onother one)
- **Superior aproach:** E.g. for Baby seat (with/without baby), Animal box (with/without animal in box).

***** *Encoder accounts for most of the computation al load*

# IMS: Life-on-Board Detection (Latest Gen.)

*Step 4: In parallel to step 1,2,3: Surface segmentation (Under-stand decoration & relevance)*

*Modell support also for face (Understand occlusions, All Passengers)*


*Face / (body) Segmentation*

*Understand Relevance and Decoration:*

*Skin parts, Glasses, Hair, Hat, Mask, Headgear, Headphones*

*3D Face Model and Skeleton (unconnected)*

*Attention map*

*Image (Occluded by Glasses)*

*Face Model (Reconstruction)*

*3D Skeleton (legacy landmarks)*

*3D Head Model*

*3D Hands Model*

*2D Body Parts*

*3D Body Parts*

*3D Body Model*

***Unified Interface** e .g. 3D skeleton representation for full body, hands, head, including face*

*Understand ALL moving parts:*

*Pose*
*Activity*
*Gestures*

*Usage of baby seat or pet-carrier*

*Step 1: 2D skeleton extraction*

*Step 2: 3D skeleton regression*

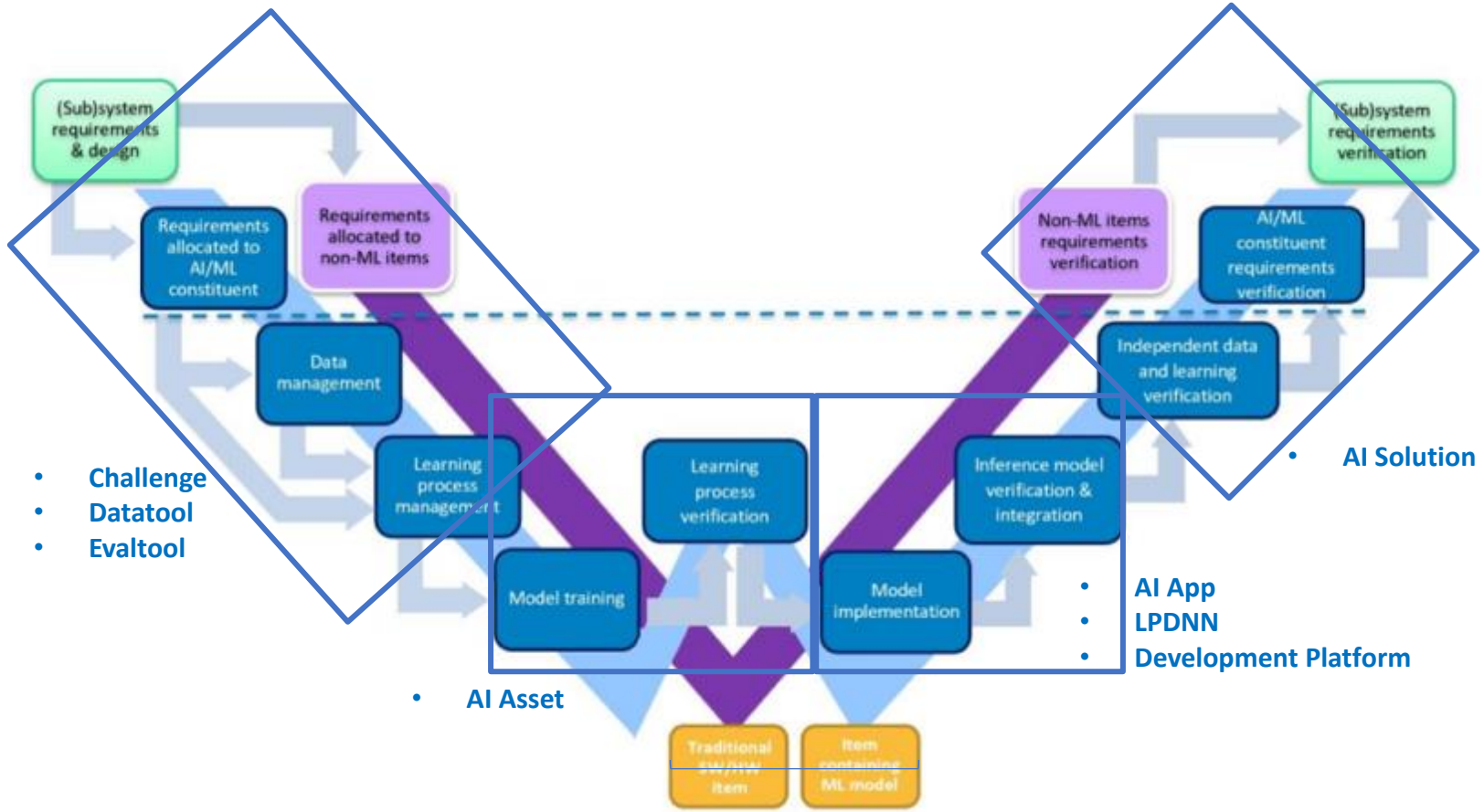
*Step 3: Match to 3D Model*

**=> Deep NN System, 3D, Model based, Complete, Extremely robust**

# Model implementation for guessing occluded parts & body metric

# ML Specific Engineering: Learning Assurance | Cycles and Synchronization with V&V

- Highly automated and well thought trough ML process.
- Optimized processes for traditional SW development (above dotted line) and specialized ML processes (below dotted line).
- It is critical to have automated tooling through-out the life-cycle to ensure that iterations triggered by training or implementation can be measured reliability and efficiently, especially for many systems which have many AI-based subsystems e.g. > 10 ML models.
- Comes with HIL / SIL



# End-to-End Tooling Requirements | NPU Edge Enablement on SoCs

## Fully integrated training and deployment workflows accelerate feedback loops

**Data**
Collection

**Training**
Model compression

**Hardware-in-the-Loop Deployment**
Model optimization, deployment, and benchmarking

**Solution Integration**
Model verification

3

**Data**
Collection and labeling of data. Data augmentation and export of training and benchmarking datasets.

4

**Training**
Model training and compression

**Infrastructure**

5

**Optimization**

LPDNN
DEEP EDGE AI

**Benchmarking**
Code optimization on target hardware

**Deployment**

6

**Test Protocol**
Protocol and testing results.

**Bias / Sensitivity Analysis**
Model analysis for bias and sensitivity to noise.

7

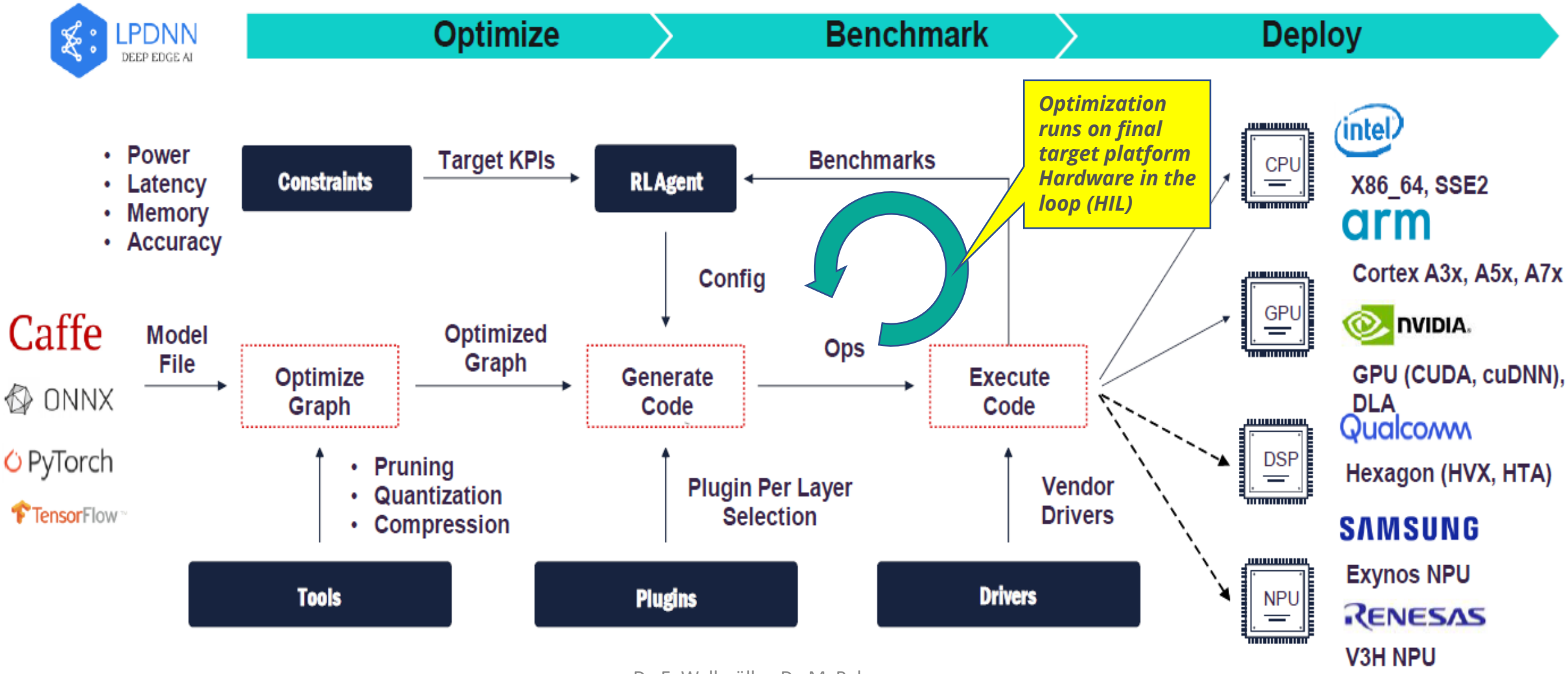
**Integration**
AI App integrated into system.

**Verification**
Correct performance is verified.

**Evaluation Report :** Feedback for next KPI target.

**Verification Report**

# LPDNN: Low-Power DNN Inference Engine



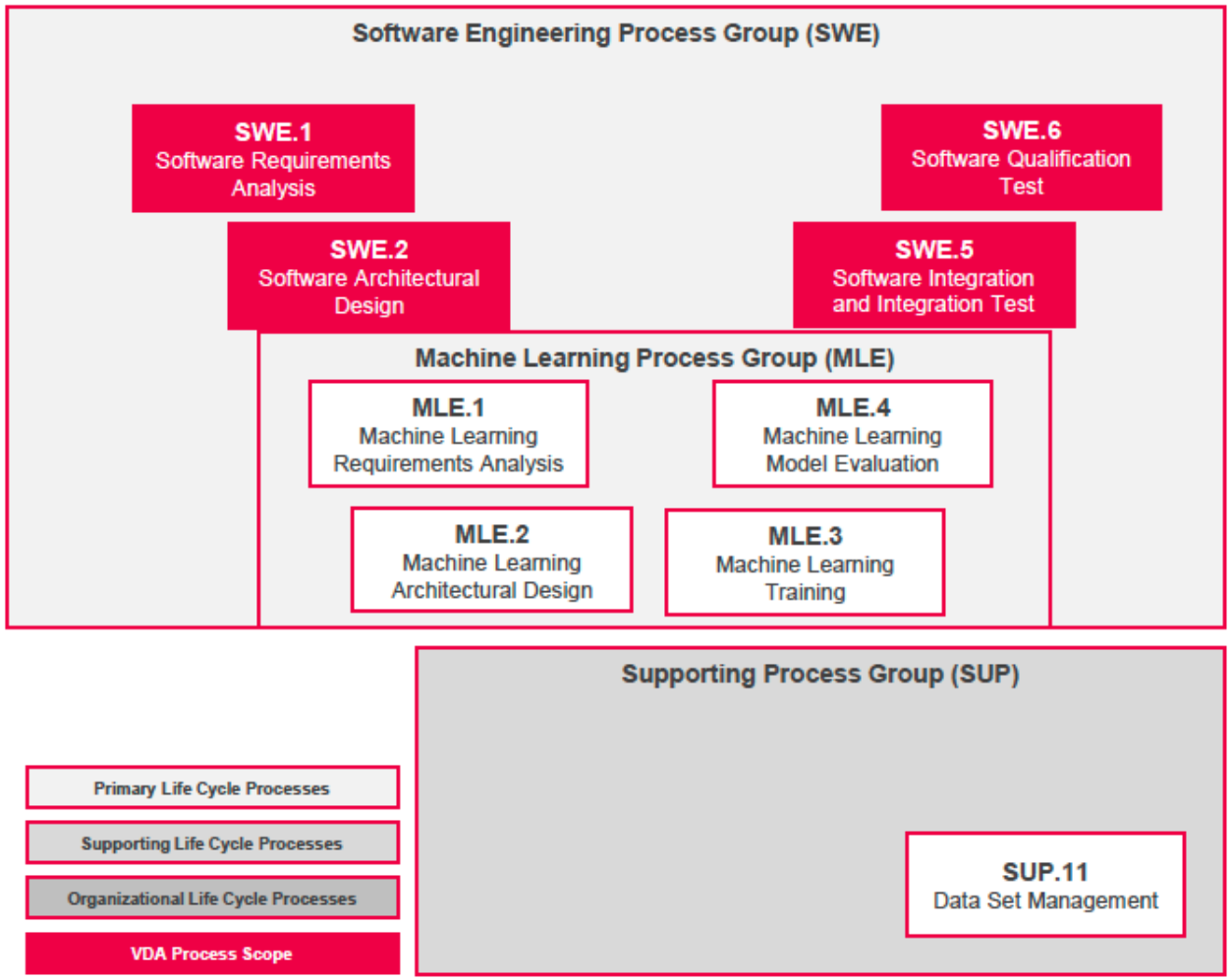
# Observations: Low Success Rate (20-40%) to create Business Value with AI Technology

- Insufficient alignment of business goals and processes to the AI technology
- Lack of data strategy
- Shortage of skilled people who can combine domain knowledge and the relevant AI technology
- Unique concerns about AI (e.g. model transparency, explainability, fairness/bias, reliability, safety, maintenance, etc.)
- Need for better engineering infrastructure for data and model provenance.

# The Need for QA/QM and Process Assessment (SPICE)

- As the application of AI moves to business/mission critical tasks with more severe consequences, there is a need for a rigorous quality management, such as **frameworks** and
- **Verification and validation methods**
- QM have been in place for IT projects over many decades
- QM, V & V (QS) for AI and machine learning gets more and more importance, but is a young discipline with some open questions

# SPICE for Machine Learning




June 30th 2022
VDA Automotive SYS Conference 2022, Potsdam
Christina Stathatou, Bhaskar Vanamali

KUGLER MAAG CIE

# Conclusion 1 – Data driven programming at NVISO

The ML approach at NVISO was presented. It‘s highly automated development covers five high-order themes:

- Assuring robustness of NNs (design and deployment phase)
- Improving the failure resilience of NNs (design and deployment phase)
- ML concept with level/task specific test, completeness of tests
- Designer can focus on relevant data to assure safety properties of NN-based control software, and
- Improving the interpretability of NNs.

From the industry perspective, improving the interpretability of NNs is a crucial need in safety-critical applications.

# Conclusion 2 – QA and QM at NVISO

- It should be clear that ML applications need a different mindset from the start of a project/product.
- Since AI is really a software component, we need to apply the relevant software quality attributes (ISO/IEC 25000) to it e.g. fairness („Angemessenheit“), explainability, etc.
- In spite of an extraordinary worldwide effort devoted to Machine Learning technology, the quality management of AI systems is fragmented and incomplete.
- In order to meet the needs of society, we need an AI engineering framework that meets the rigor needed.



- Dr. Ernest Wallmüller
  - www.itq.ch
  - wallmueller@itq.ch
- Dr. Martin Reber
  - www.nviso.ai
  - martin.reber@nviso.ch