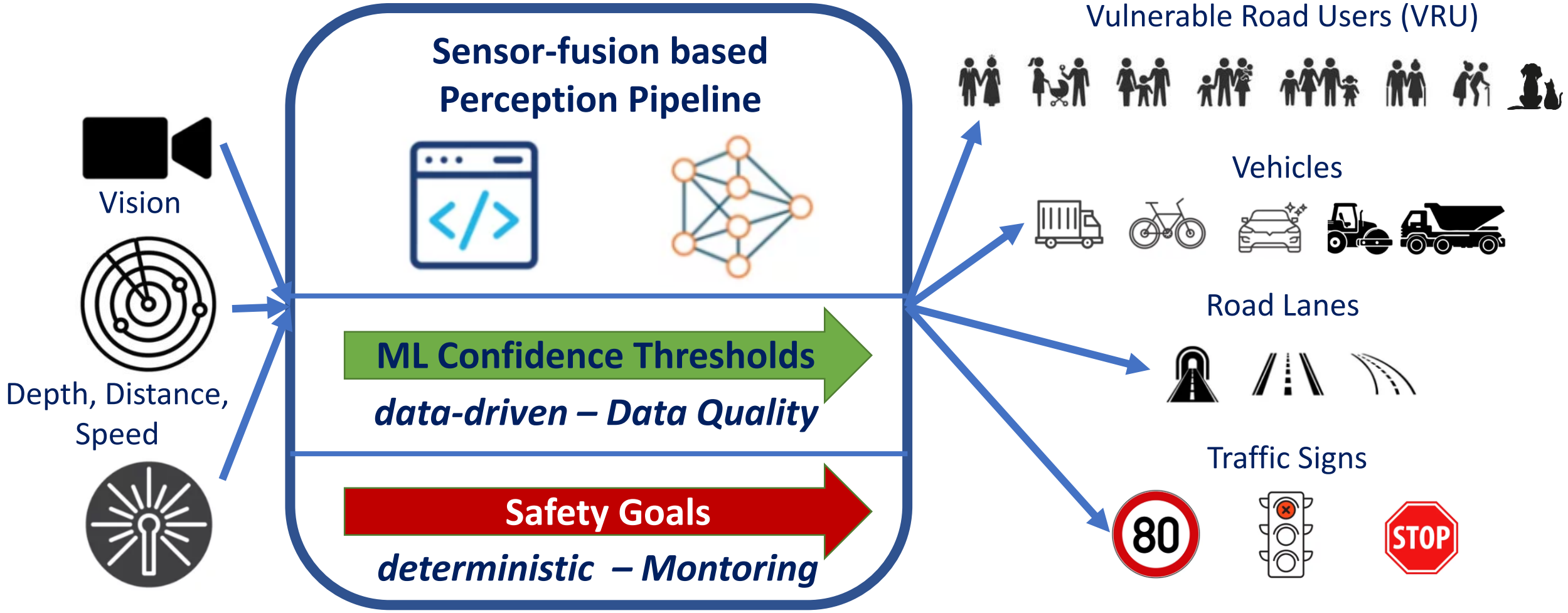
Functional Safety in Advanced Machine Learning Architectures

Case Study: Perception System for HAD 2+/3

EuroSPI Tech Day, 15.9.2025

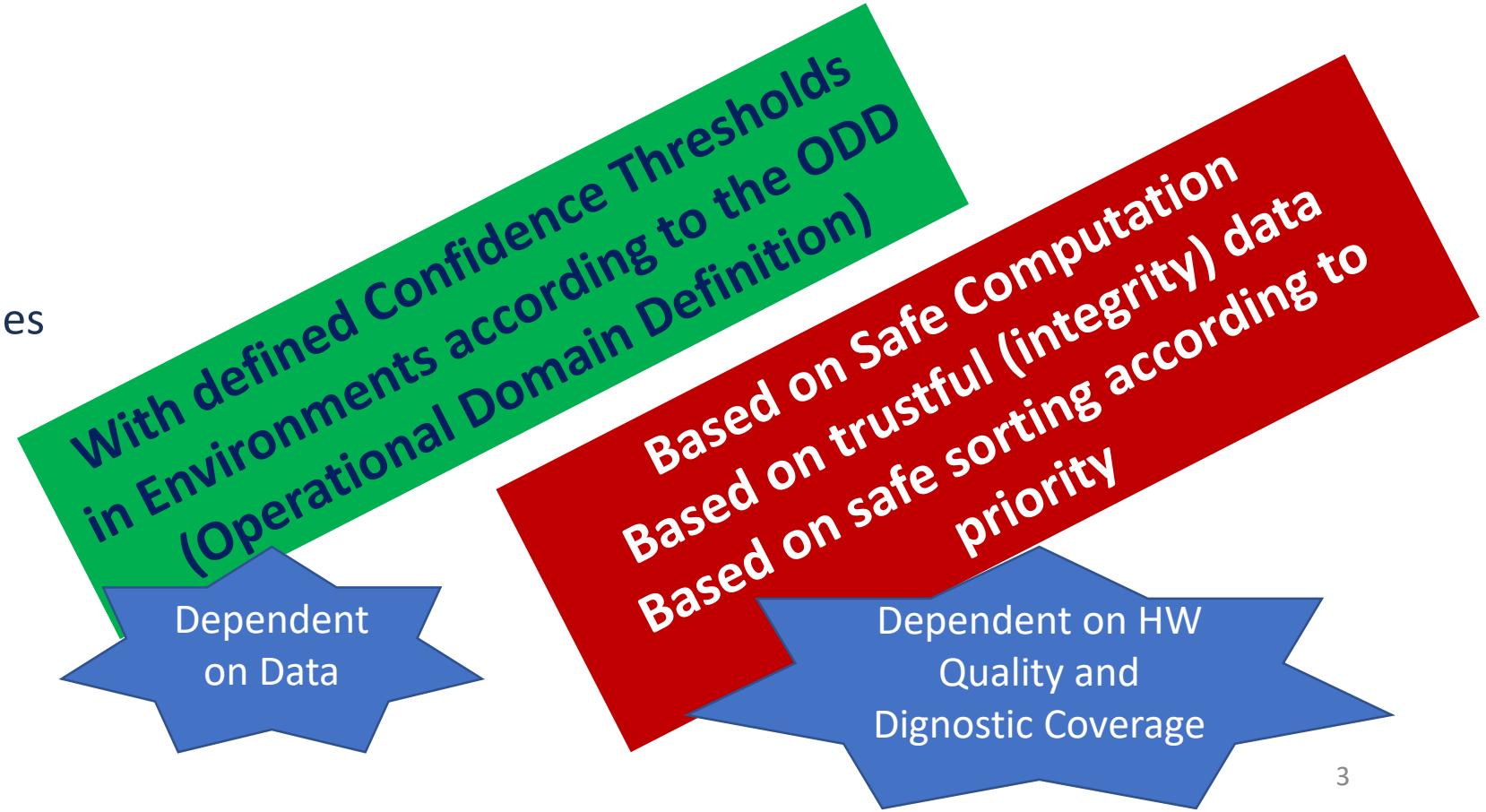
Dr Andreas Riel, Grenoble INP & ISCN Group,
Dr Georg Macher, TU Graz & ISCN Group,
Dr Richard Messnarz, ISCN & EuroSPI GmbH

Technical Foundation for HAD 2+/3



Typical Pipeline Machine Learning Confidence Threshold Objectives

- **Identify Objects in Frames updated at … Hz in a distance of the ego-vehicle of up to … m.**
  - Object Classes
    - Pedestrian
    - Bicycle with riders
    - Animals
- **Recognize Road Lanes**
  - Lane Classes
    - Separation/Middle Lanes
    - Side Lanes
- **Recognize Traffic Signs**
  - Traffic Sign Classes
    - Speed Limits
    - Stop/Priority
    - Traffic Lights
    - …



Clear Separation of Concerns

ML Confidence Thresholds

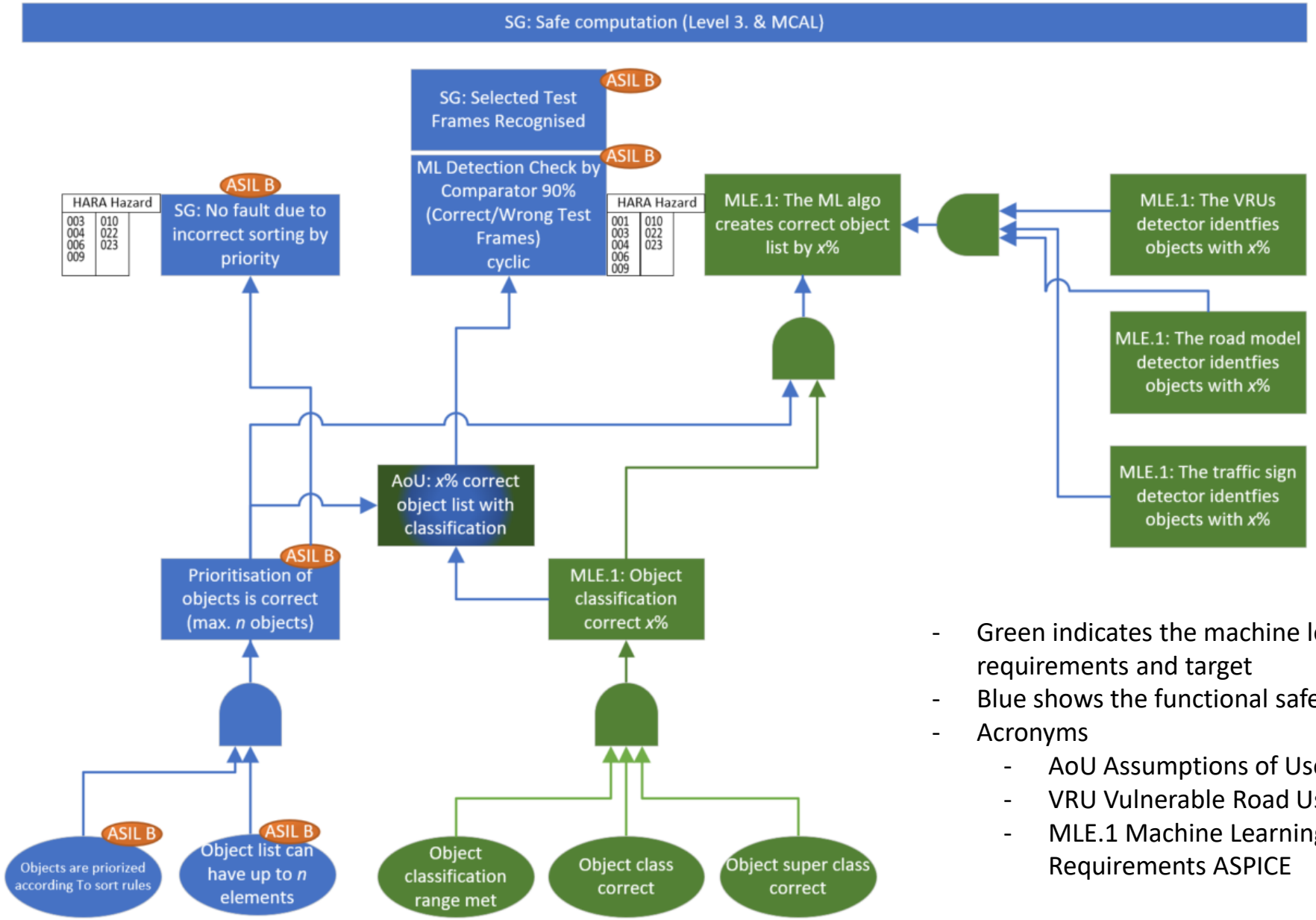
- Object Identification
- Object Recognition
- Object Motion Prediction
- Lane Tracking
- Traffic Sign Recognition
- Ego Lane Tracking

Algorithms for Pre- and Post-Processing of ML Calculation & Results

Safety Goals

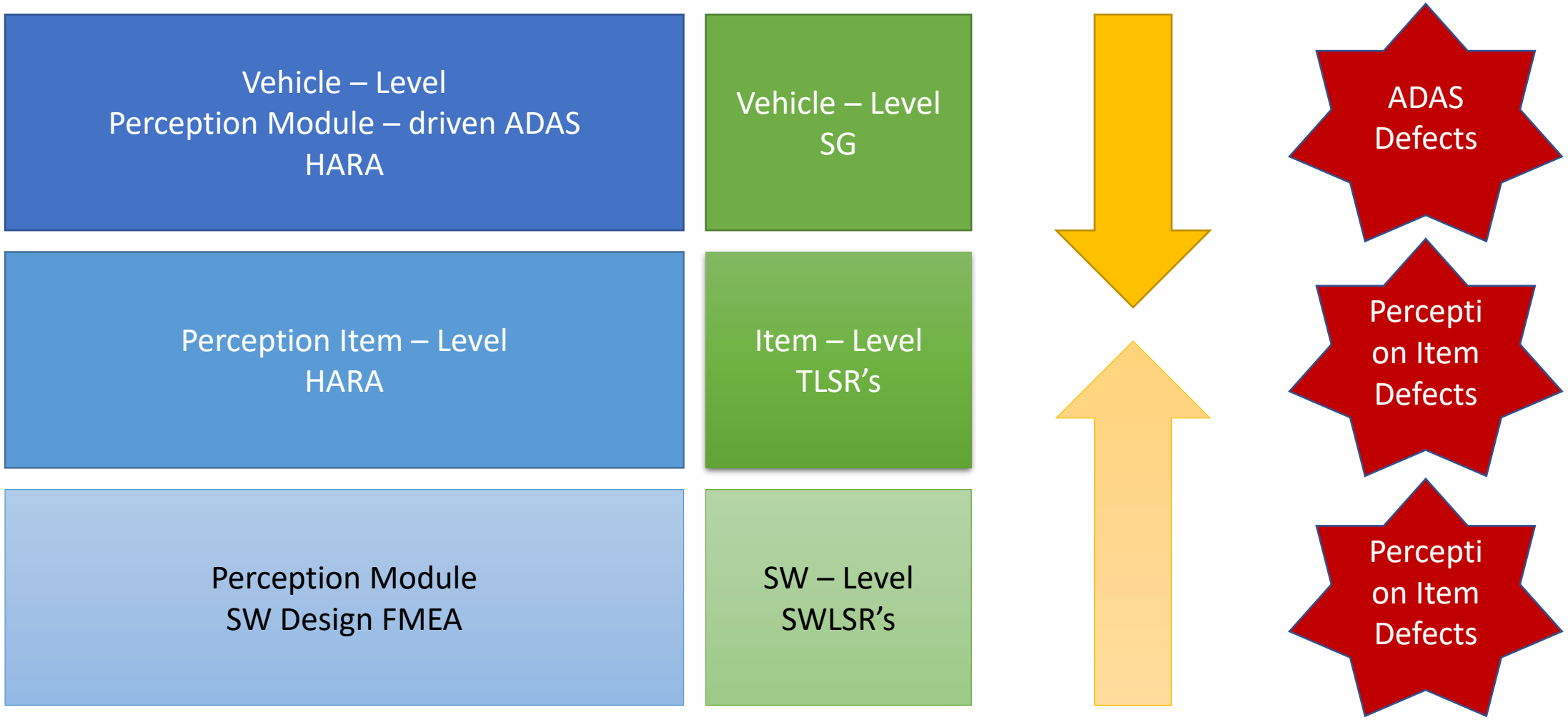
- Safe Computation
- Safe Data Transfer/Communication
- Program Flow Monitoring
- Code Isolation/Redundancy
- Data/Parameter Isolation/Redundancy
- Code/Data Integrity Protection

Particular Data:
Neural Network Node Weights & Biases
Sensor Data during Transfer and Preprocessing



- Green indicates the machine learning requirements and target
- Blue shows the functional safety path
- Acronyms
  - AoU Assumptions of Use
  - VRU Vulnerable Road User
  - MLE.1 Machine Learning Requirements ASPICE

Derivation of SG, TLSR's, and SWLSR's (System of Systems in the SDV)



Selective Degradation Strategy in the SDV

- How many sensors fail, and how do they fail?
- What is the impact on each ADAS function?
- What is the required level of degradation?
- Who can detect the failure and when (Vehicle/Item State)?
- Can the failure, once detected, by cured/compensated?

Malfunction Category	Sensor Malfunction	ADAS Function used	Impact on Traffic Sign Path	Explanation of Impact	Degradation required Y/N (-> FuSa)	Impact on Object Perception Path/List	Explanation of Impact	Degradation required Y/N (-> FuSa)	Impact on Road Lane Model	Explanation of Impact	Degradation required Y/N (-> FuSa)	Detectability Sensor Provider	Detectability Perception Item
Front camera performance failure	Fisheye front camera completely obstructed	ACC	No	n/a	No	Yes	No wide-angle/ surround view to detect and track VRU's	No	Yes	No wide-angle/ surround view used for tracking the side lanes	No	See the Camera's Safety Manual	Dark image over several frames
		Speed Assistance Mode			No			No			No		
		AEB			No			Yes			No		
Sensor synchronization Issues	Camera Signals not synchronized	ACC	Yes	Tracking	No	Yes	Tracking	No	Yes	Tracking	No	No	Implementation of a sensor signal synchronization and alignemnt module
		Speed Assistance Mode			Yes			No			No		
		AEB			Yes			Yes			No		

Example: Sony IMX 728 Built-In Diagnosis

- Concept is an FPGA where integrator sets parameters and the set parameters which are ASIL are protected by a memory check
- Safe communication using Checksum / different CRCs can be configured / also Autosar compliant
- Flash check, ROM check
- Has very elaborated HDR function: enables your camera to create an image that captures all the range of contrast in a scene, from the depths of the shadows to the highlights of the brightest areas
- AEC Automatic Exposure control = shutter time diagnose
- Information: actually, the camera is ASILB(D) and there is a support of how to set the FPGA config in a diverse mode so that you can construct ASIL D with 2 overlapping cameras.

- 60 fps, means 16,6 ms per frame
- 45 fps, 25 ms per frame
- shutter time diagnose
- HDR balancing and image correction
- clock monitor
- state monitor
- short and open circuit
- safe state is XERR output by ASIL B
- memory protection

Safety-Related Properties (ISO 8800) to be assured

- AI Robustness → Model, System
- AI Generalization Capability → Model, System
- AI Reliability → Model, System
- AI Resilience → (Overall) System, Organization
- AI Controllability → (Overall) System, Organization
- AI Explainability → Process
- AI Predictability → Model, System
- AI Alignment → Process
- Justified Design Decisions → Process
- Maintainability → Organization, Process
- AI Bias and Fairness → Model, (Overall) System
- Distributional Shift over Time → (Overall) System

...more on what to be expected from AI-related Standards and Concepts et the EuroSPI Conference

Key Takeaways (1/2)

- Functional Safety critical Machine Learning (ML) Objectives (Targets) are **not covered** by the ISO 26262:2018
- SOTIF (ISO 21448:2021) **does not cover** securing the behavior of ML algorithms in vehicle (rather, it is about securing the behavior of deterministic algorithms to the changing outside world)
- Therefore, ML objectives have to be « **decomposed** » to
  - Objectives that the M-based models need to achieve through the a suitable training/validation process and data
  - Functional Safety Goals that can be achieved through fully deterministic design, analysis, and verification/validation methods of electronic hardware and software
  - Functional Safety Goals which address the safe computation of
    - the deterministic part of ML algorithms
    - the data sets that configure those algorithms (e.g. weights and biases of neural networks)
- Any decomposition path needs to be **uniquely assigned** to Functional Safety or ML Targets

Key Takeaways (2/2)

- In the Systems-of-Systems approach of the SDV, the identification of Vehicle-Level Safety Goals and Item-Level Technical Level Safety Requirements requirements requires an **iterative and combined** Top-Down and Bottumn-Up (starting from the SW-level) approach
- **Defect Diagnostics** are a **shared effort** between the sensors (which already have built-in diagnostic functions) and the Perception Item
- **Degradation strategies** in Perception Items used for ADAS require **sophistication** to avoid overly frequent control takeover by the human driver (which might be a safety risk in itself)

Thanks

Thank you for cooperating with ISCN.

1. ISCN is INTACS certified training provider for Automotive SPICE assessor courses
2. ISCN is certified by VDA to hold provisional and competent ASPICE assessor courses

3. ISCN moderates the German task force SOQRATES (https://soqrates.eurospi.net) since 2003 where >20 Tier 1 collaborate on ASPICE, Safety and Security.

4. ISCN organises the EuroSPI conference since 1994 where e.g. VW is organising a workshop community, and VW, Rheinmetall AG, EB, MAGNA, AVL held key notes. http://www.eurospi.net

5. EuroSPI certificates are issued by EuroSPI Certificates & Services GmbH (www.eurospi.net) in cooperation with DRIVES and the Automotive Skills Alliance (ASA). The ASA was founded by the EU Blueprint Project Drives and ALBATTS with support from the European Automobile Manufacturers' Association (ACEA). https://www.eurospi.net. ISCN is founding member.

Thanks

ISCN
www.iscn.com

Thank you for cooperating with EuroSPI Certificates GmbH.

1. Academy – Courses and Training Platform
2. Certification – Exam system and cerrificates
3. EuroSPI Conference Series
4. Assessment Tool – ISO 330xx based