Combining Simulation and Driving Scenarios Analytics for Safe Automated Driving

Bernard Dion
CTO – ANSYS Systems

DSC 2019
Strasbourg – September 5th, 2019

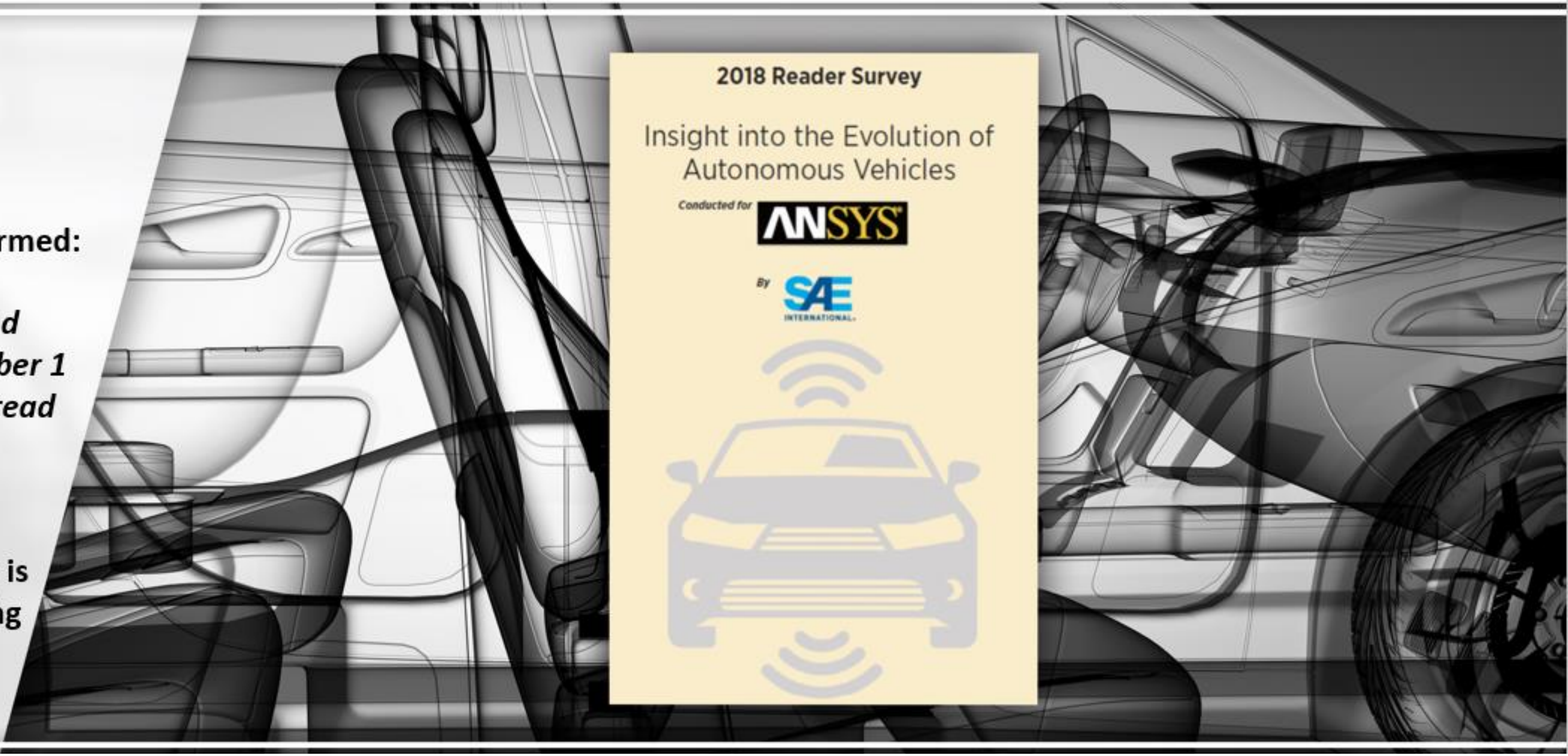
Demonstrating Safety is the Critical Engineering Challenge

Exclusive research by ANSYS and SAE

The SAE Automotive Industry Survey Confirmed:

"Public Confidence and Adoption" is the number 1 barrier to the widespread adoption of fully autonomous vehicles

Demonstrating Safety is the Critical Engineering Challenge



2018 Reader Survey

Insight into the Evolution of Autonomous Vehicles

Conducted for ANSYS

By SAE INTERNATIONAL

We need to address all key elements of autonomous vehicles through simulation

Sensors

Human-Machine Interfaces

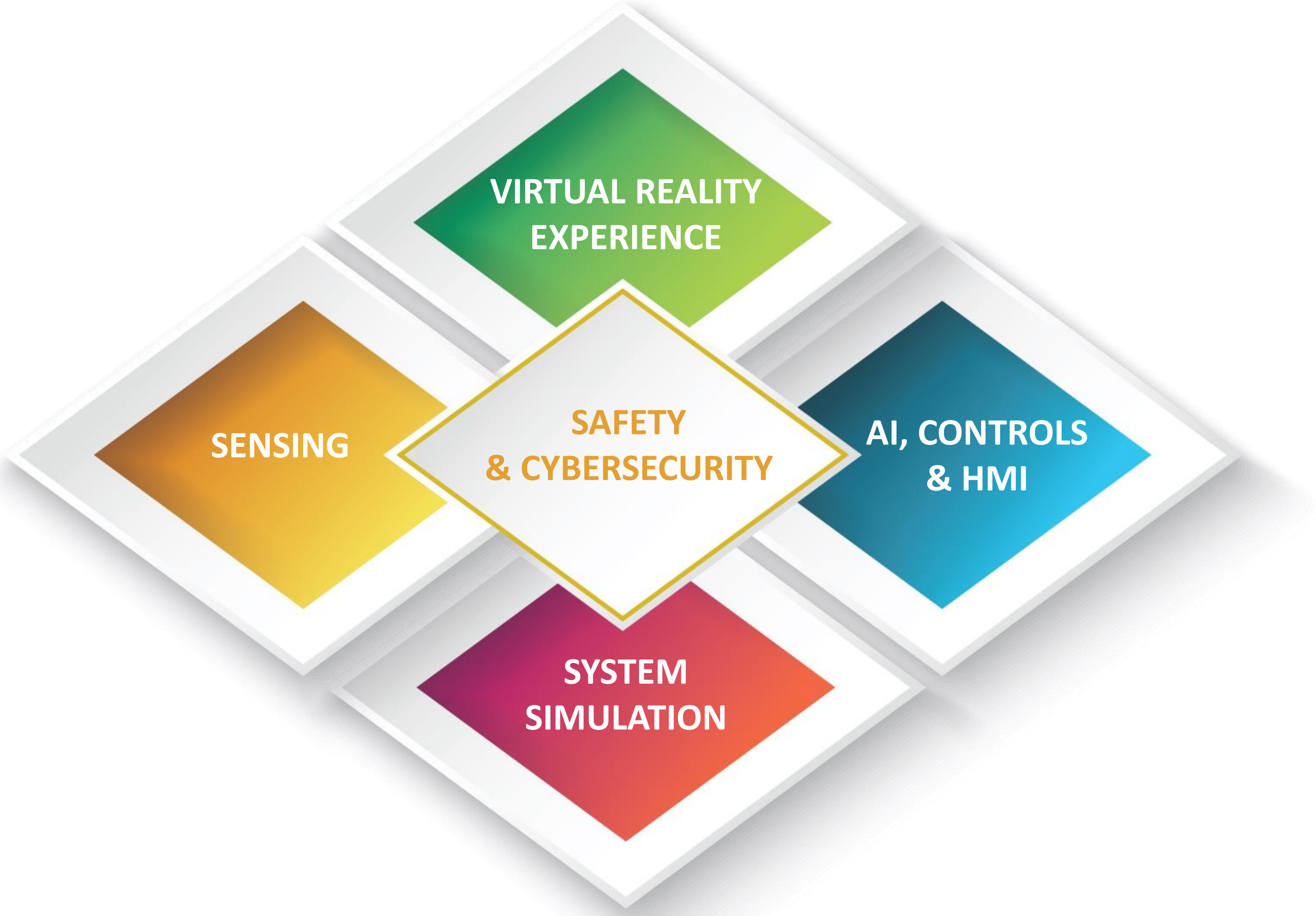
Automated Driving Software

Control Software

Computing Platform

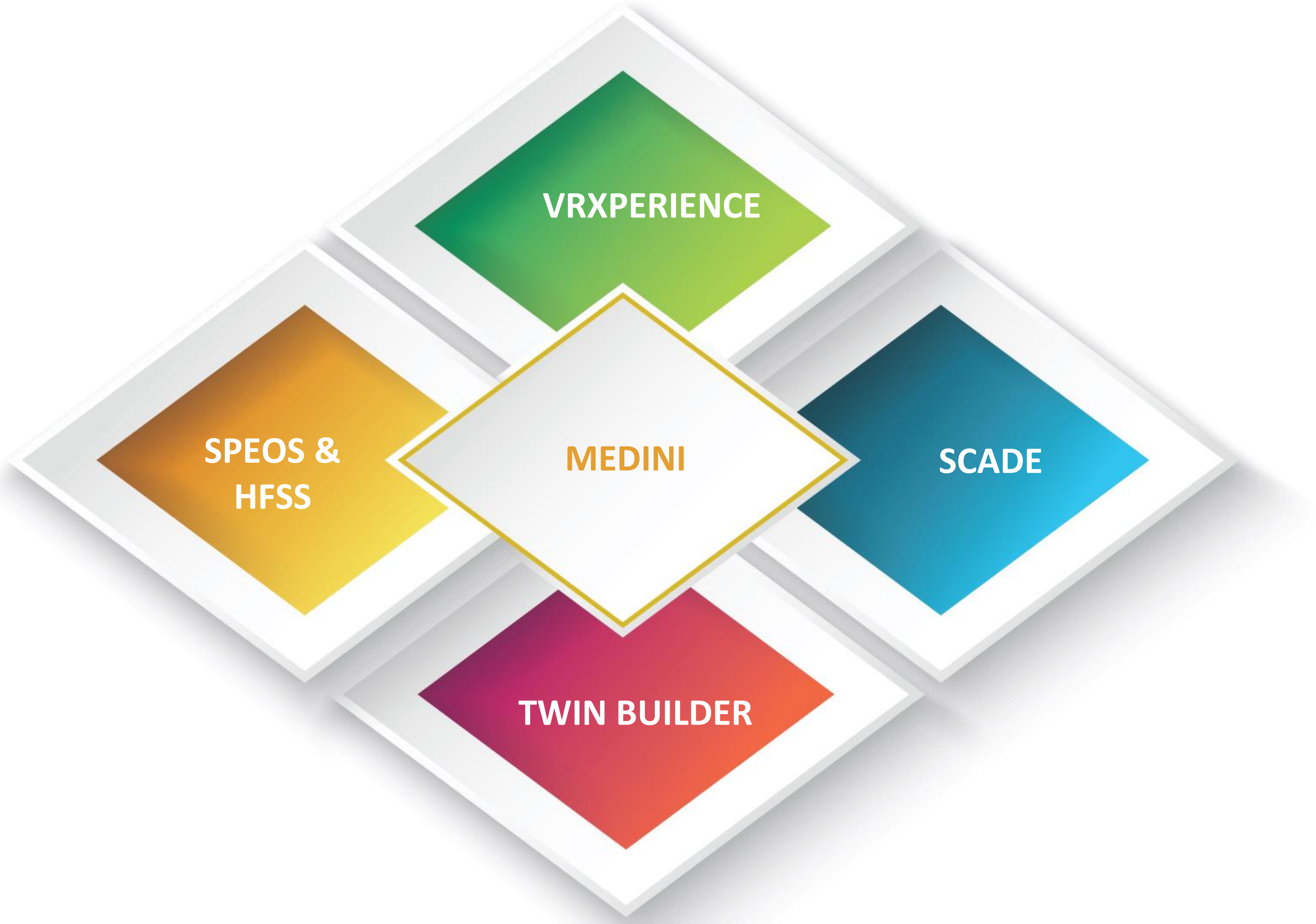
Vehicle Platform

Digital Safety Solutions for Autonomous Vehicles



SIMULATION PROCESS AND DATA MANAGEMENT

ANSYS Autonomy



MINERVA and OPTISLANG

1 Functional Safety & Cybersecurity Analysis

2 Sensors

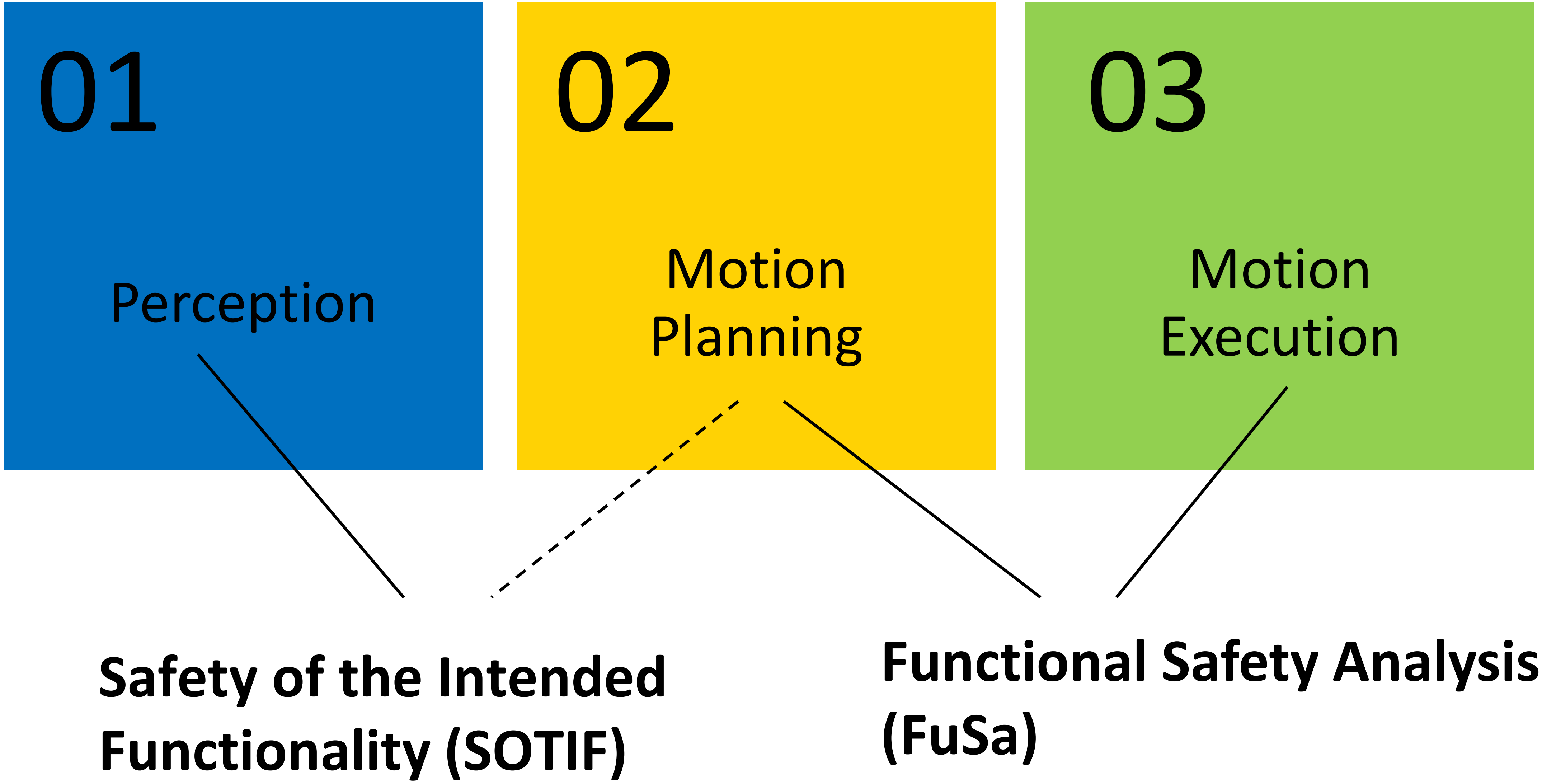
3 Closed-Loop Simulation

4 Control Software

5 Automated Driving Software

6 Vehicle Platform

Safety of AV Systems



01

Perception

02

Motion Planning

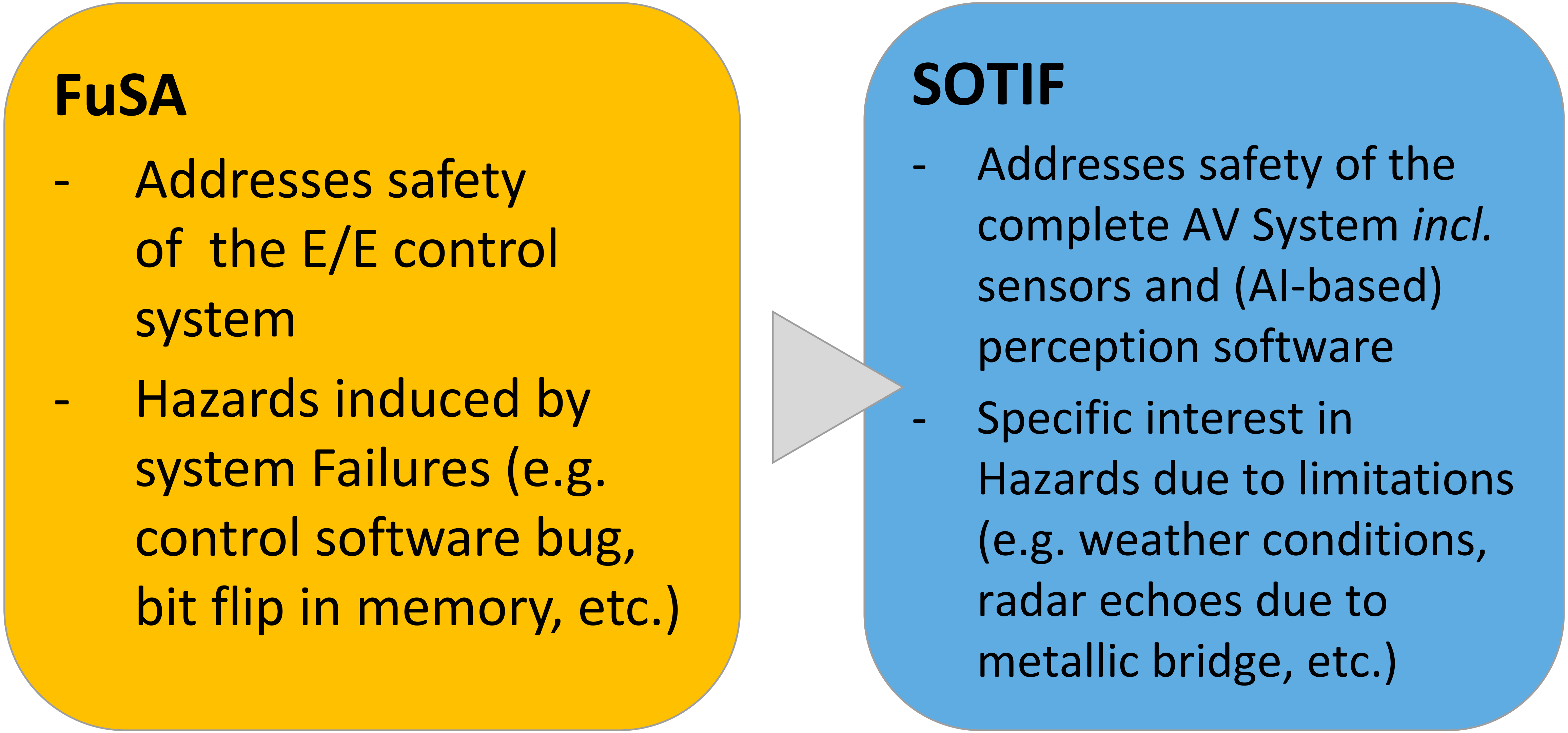
03

Motion Execution

Safety of the Intended Functionality (SOTIF)

Functional Safety Analysis (FuSa)

FuSa *vs.* SOTIF



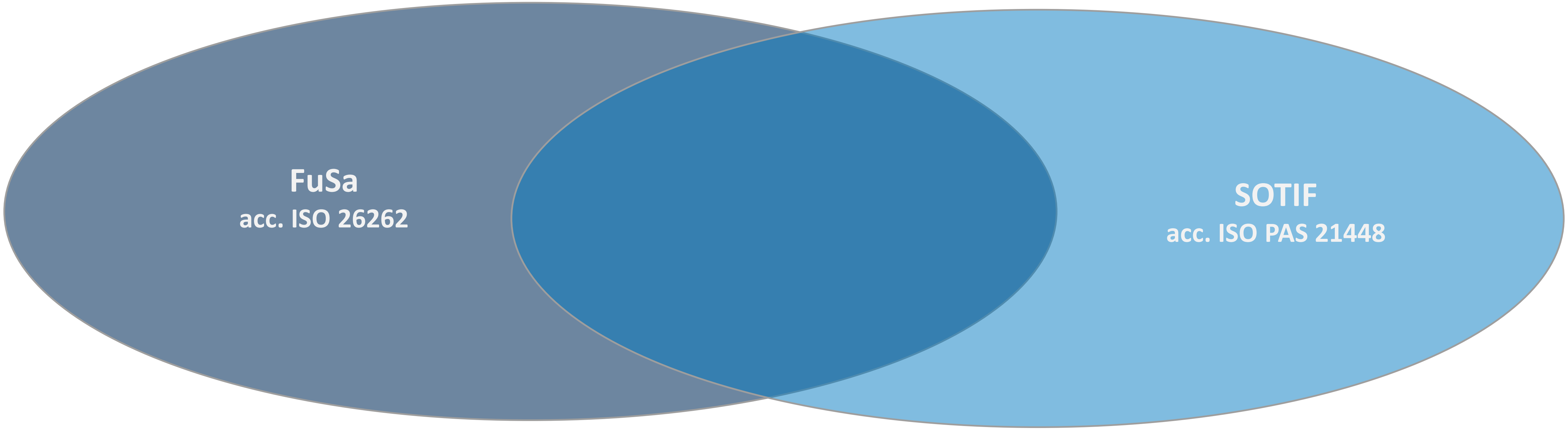
FuSA

- Addresses safety of the E/E control system
- Hazards induced by system Failures (e.g. control software bug, bit flip in memory, etc.)

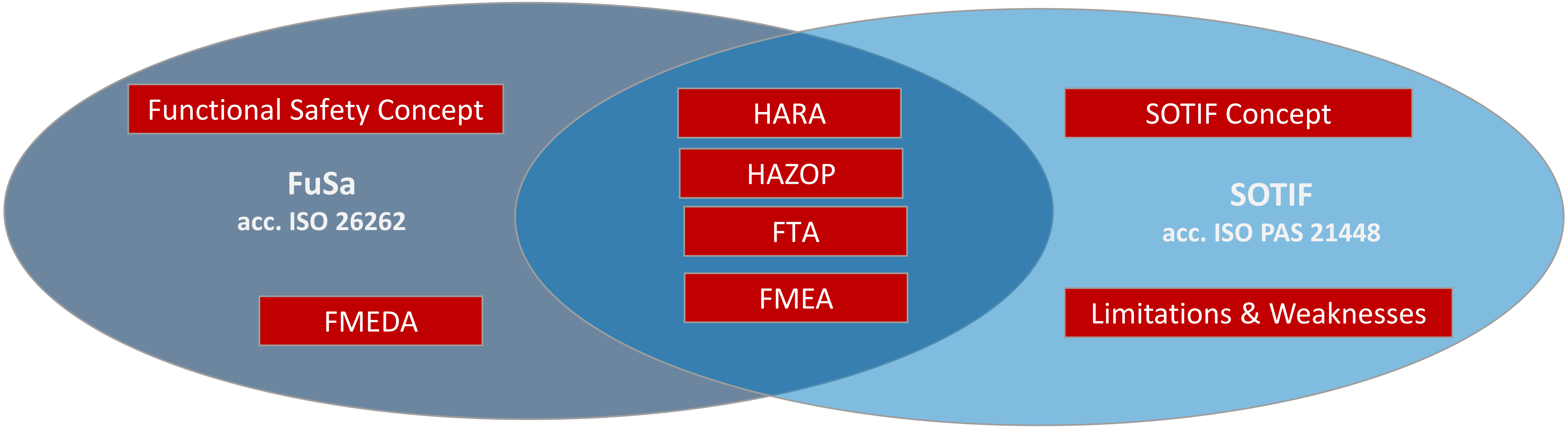
SOTIF

- Addresses safety of the complete AV System *incl.* sensors and (AI-based) perception software
- Specific interest in Hazards due to limitations (e.g. weather conditions, radar echoes due to metallic bridge, etc.)

FuSa acc. ISO 26262 *vs.* SOTIF acc. ISO 21448



Methods in the FuSa and SOTIF Processes



Functional Safety Concept

FuSa
acc. ISO 26262

FMEDA

HARA

HAZOP

FTA

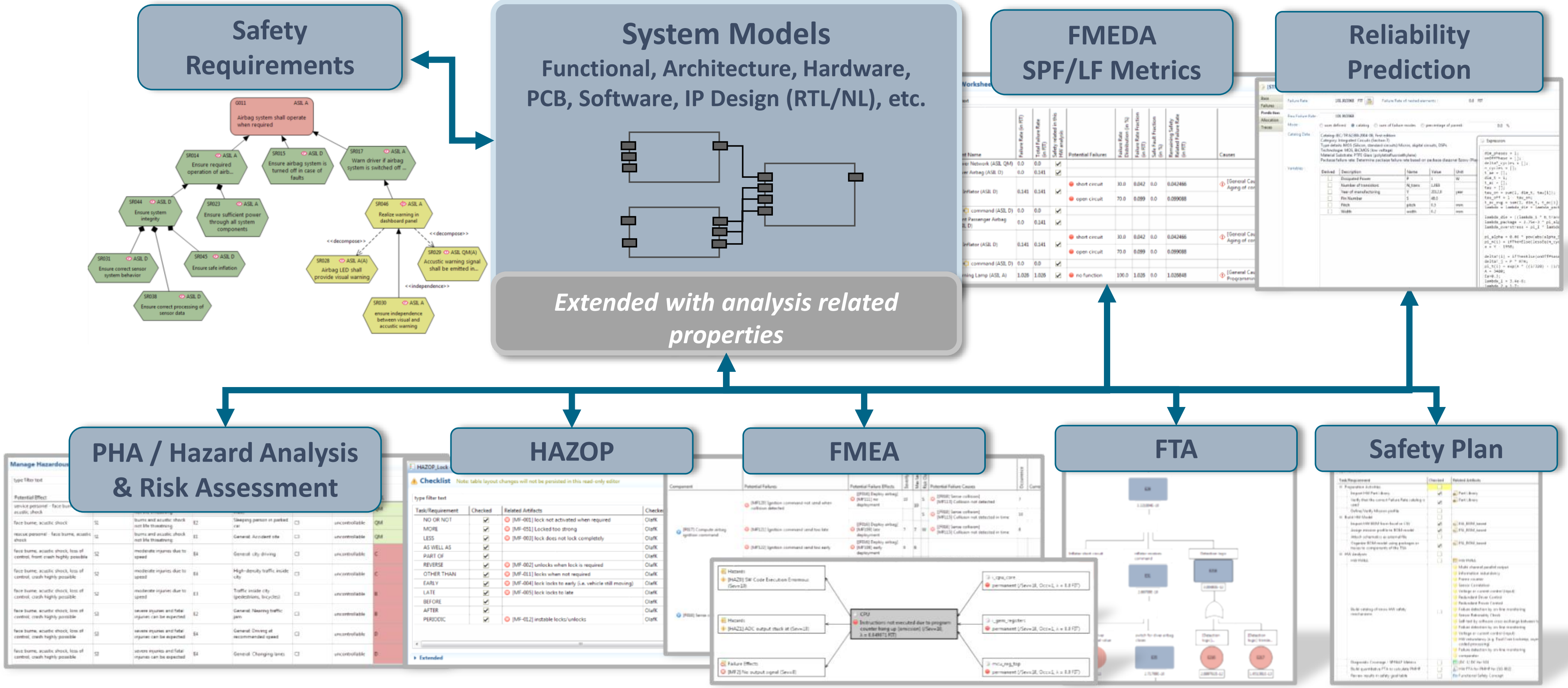
FMEA

SOTIF Concept

SOTIF
acc. ISO PAS 21448

Limitations & Weaknesses

ANSYS provides a model-based, system-oriented solution for functional safety analysis (FuSa)



Safety Requirements

System Models

Functional, Architecture, Hardware, PCB, Software, IP Design (RTL/NL), etc.

Extended with analysis related properties

FMEDA SPF/LF Metrics

Reliability Prediction

PHA / Hazard Analysis & Risk Assessment

HAZOP

FMEA

FTA

Safety Plan

G011 ASIL A Airbag system shall operate when required
SR014 ASIL A Ensure required operation of airb...
SR015 ASIL D Ensure airbag system is turned off in case of faults
SR017 ASIL A Warn driver if airbag system is switched off ...
SR044 ASIL D Ensure system integrity
SR023 ASIL A Ensure sufficient power through all system components
SR046 ASIL A Realize warning in dashboard panel
SR031 ASIL D Ensure correct sensor system behavior
SR045 ASIL D Ensure safe inflation
SR028 ASIL A(A) Airbag LED shall provide visual warning
SR029 ASIL QM(A) Accustic warning signal shall be emitted in...
SR038 ASIL D Ensure correct processing of sensor data
SR030 ASIL A ensure independence between visual and accustic warning
<<decompose>>
<<independence>>
Manage Hazardous
HAZOP_Lock
Checklist
NO OR NOT
MORE
LESS
AS WELL AS
PART OF
REVERSE
OTHER THAN
EARLY
LATE
BEFORE
AFTER
PERIODIC
Extended
CPU
Worksheet

Traceability

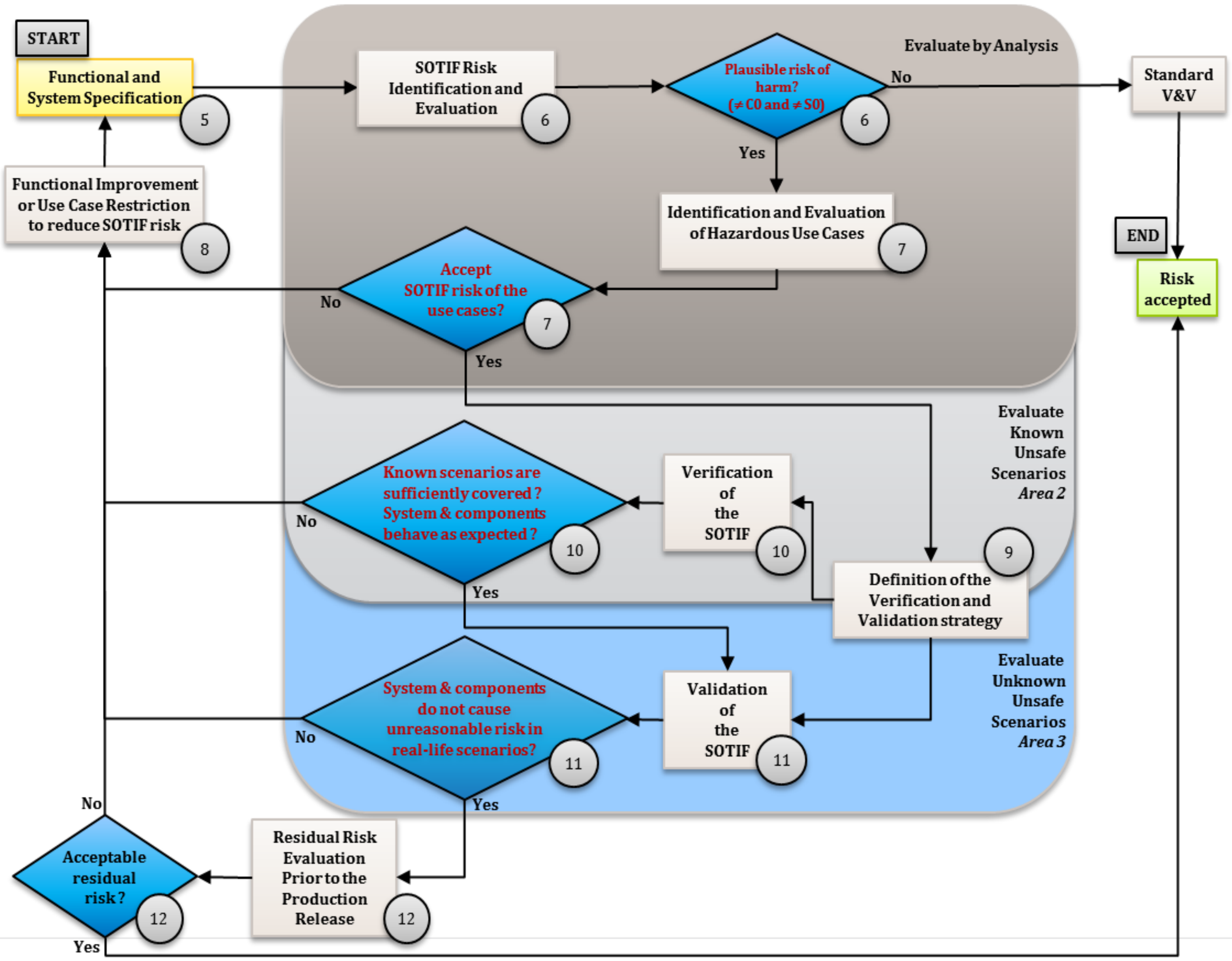
Checklists

CMS Integration

Compare & Merge

Task Management

ANSYS extends medini to implement the ISO PAS 21448 (SOTIF) iterative process model



START

Functional and System Specification 5

SOTIF Risk Identification and Evaluation 6

Evaluate by Analysis

Plausible risk of harm? (≠ C0 and ≠ S0) 6

No

Standard V&V

Yes

Identification and Evaluation of Hazardous Use Cases 7

END

Risk accepted

Functional Improvement or Use Case Restriction to reduce SOTIF risk 8

Accept SOTIF risk of the use cases? 7

No

Yes

Evaluate Known Unsafe Scenarios *Area 2*

Known scenarios are sufficiently covered ? System & components behave as expected ? 10

No

Verification of the SOTIF 10

9

Definition of the Verification and Validation strategy

Yes

Evaluate Unknown Unsafe Scenarios *Area 3*

System & components do not cause unreasonable risk in real-life scenarios? 11

No

Validation of the SOTIF 11

Yes

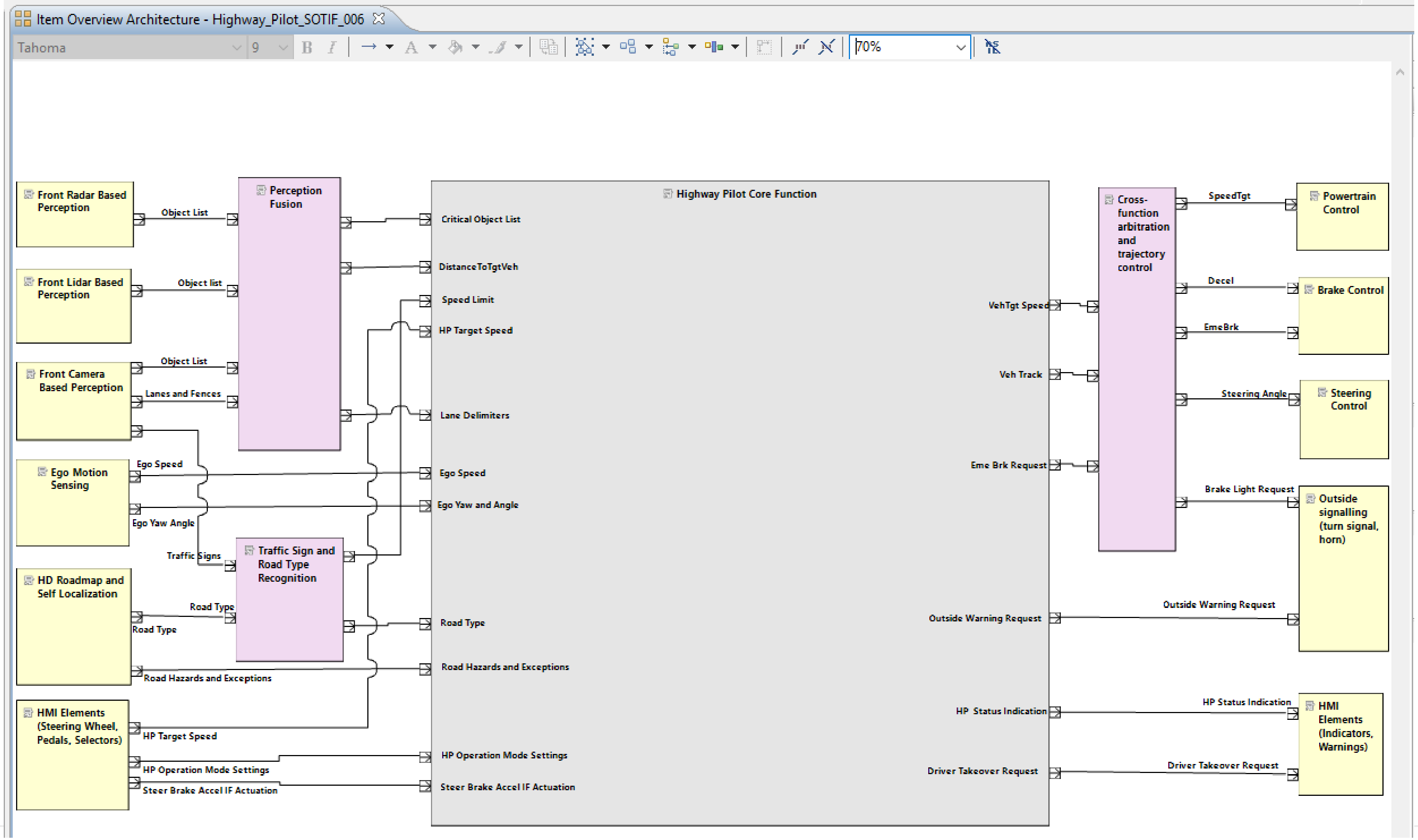
No

Acceptable residual risk ? 12

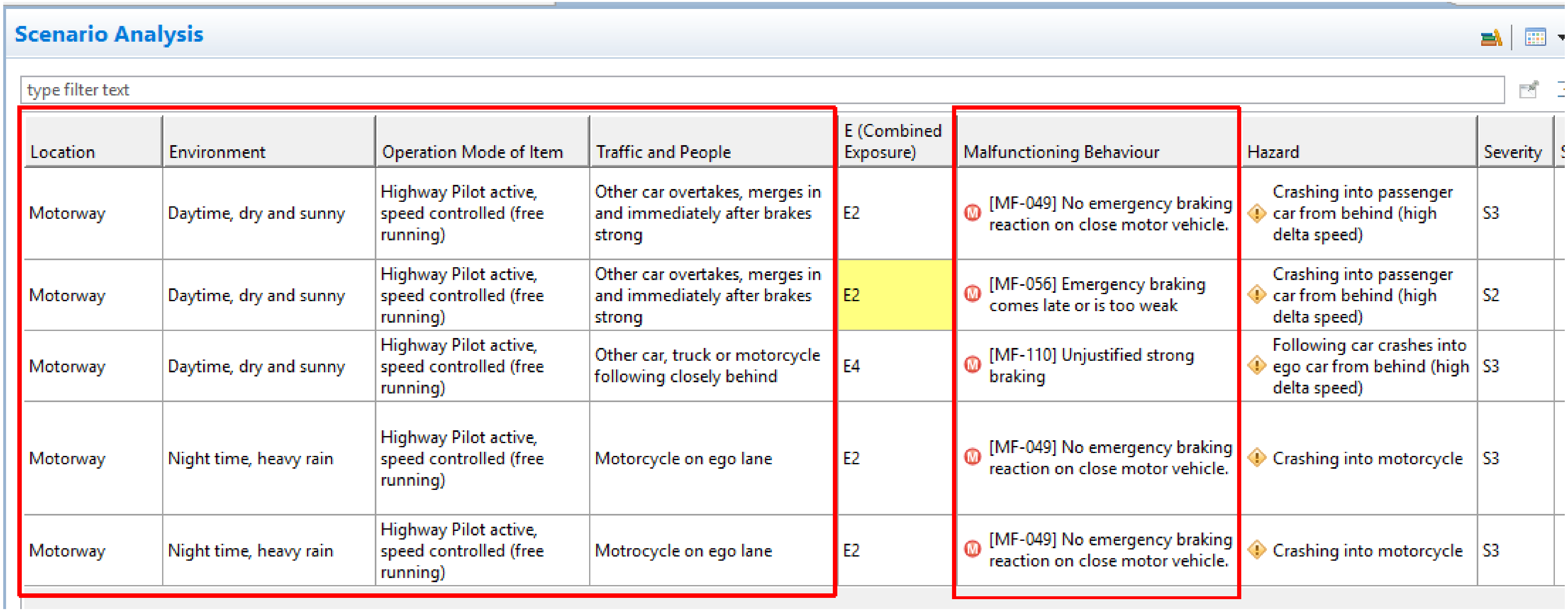
Residual Risk Evaluation Prior to the Production Release 12

Yes

Architecture Modeling is common for FuSa and SOTIF: Highway Autopilot example


Item Overview Architecture - Highway_Pilot_SOTIF_006
Tahoma
9
70%
Front Radar Based Perception
Object List
Front Lidar Based Perception
Object list
Front Camera Based Perception
Object List
Lanes and Fences
Ego Motion Sensing
Ego Speed
Ego Yaw Angle
Traffic Signs
HD Roadmap and Self Localization
Road Type
Road Type
Road Hazards and Exceptions
HMI Elements (Steering Wheel, Pedals, Selectors)
HP Target Speed
HP Operation Mode Settings
Steer Brake Accel IF Actuation
Perception Fusion
Traffic Sign and Road Type Recognition
Highway Pilot Core Function
Critical Object List
DistanceToTgtVeh
Speed Limit
HP Target Speed
Lane Delimiters
Ego Speed
Ego Yaw and Angle
Road Type
Road Hazards and Exceptions
HP Operation Mode Settings
Steer Brake Accel IF Actuation
VehTgt Speed
Veh Track
Eme Brk Request
Outside Warning Request
HP Status Indication
Driver Takeover Request
Cross-function arbitration and trajectory control
SpeedTgt
Decel
EmeBrk
Steering Angle
Brake Light Request
Outside Warning Request
HP Status Indication
Driver Takeover Request
Powertrain Control
Brake Control
Steering Control
Outside signalling (turn signal, horn)
HMI Elements (Indicators, Warnings)

SOTIF Hazard Analysis and Risk Assessment (HARA): Establishing functions and malfunctions for the Highway Autopilot example

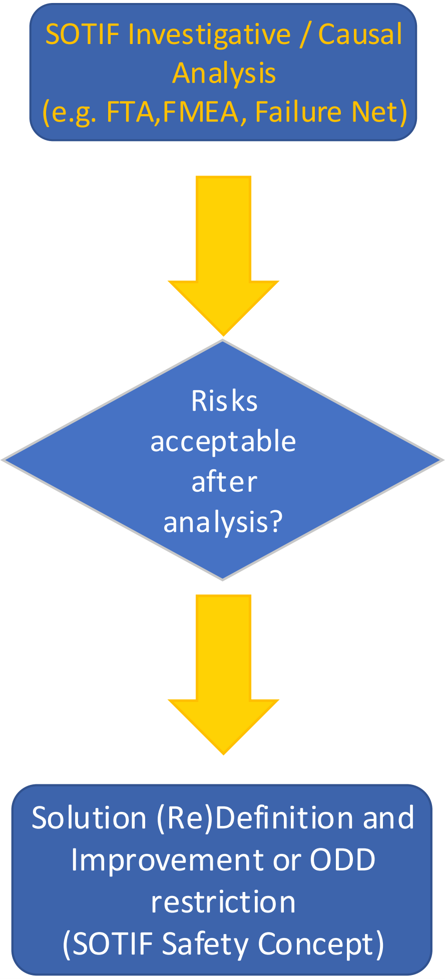


Scenario Analysis

type filter text

Location	Environment	Operation Mode of Item	Traffic and People	E (Combined Exposure)	Malfunctioning Behaviour	Hazard	Severity	S
Motorway	Daytime, dry and sunny	Highway Pilot active, speed controlled (free running)	Other car overtakes, merges in and immediately after brakes strong	E2	[MF-049] No emergency braking reaction on close motor vehicle.	Crashing into passenger car from behind (high delta speed)	S3	
Motorway	Daytime, dry and sunny	Highway Pilot active, speed controlled (free running)	Other car overtakes, merges in and immediately after brakes strong	E2	[MF-056] Emergency braking comes late or is too weak	Crashing into passenger car from behind (high delta speed)	S2	
Motorway	Daytime, dry and sunny	Highway Pilot active, speed controlled (free running)	Other car, truck or motorcycle following closely behind	E4	[MF-110] Unjustified strong braking	Following car crashes into ego car from behind (high delta speed)	S3	
Motorway	Night time, heavy rain	Highway Pilot active, speed controlled (free running)	Motorcycle on ego lane	E2	[MF-049] No emergency braking reaction on close motor vehicle.	Crashing into motorcycle	S3	
Motorway	Night time, heavy rain	Highway Pilot active, speed controlled (free running)	Motrocycle on ego lane	E2	[MF-049] No emergency braking reaction on close motor vehicle.	Crashing into motorcycle	S3	

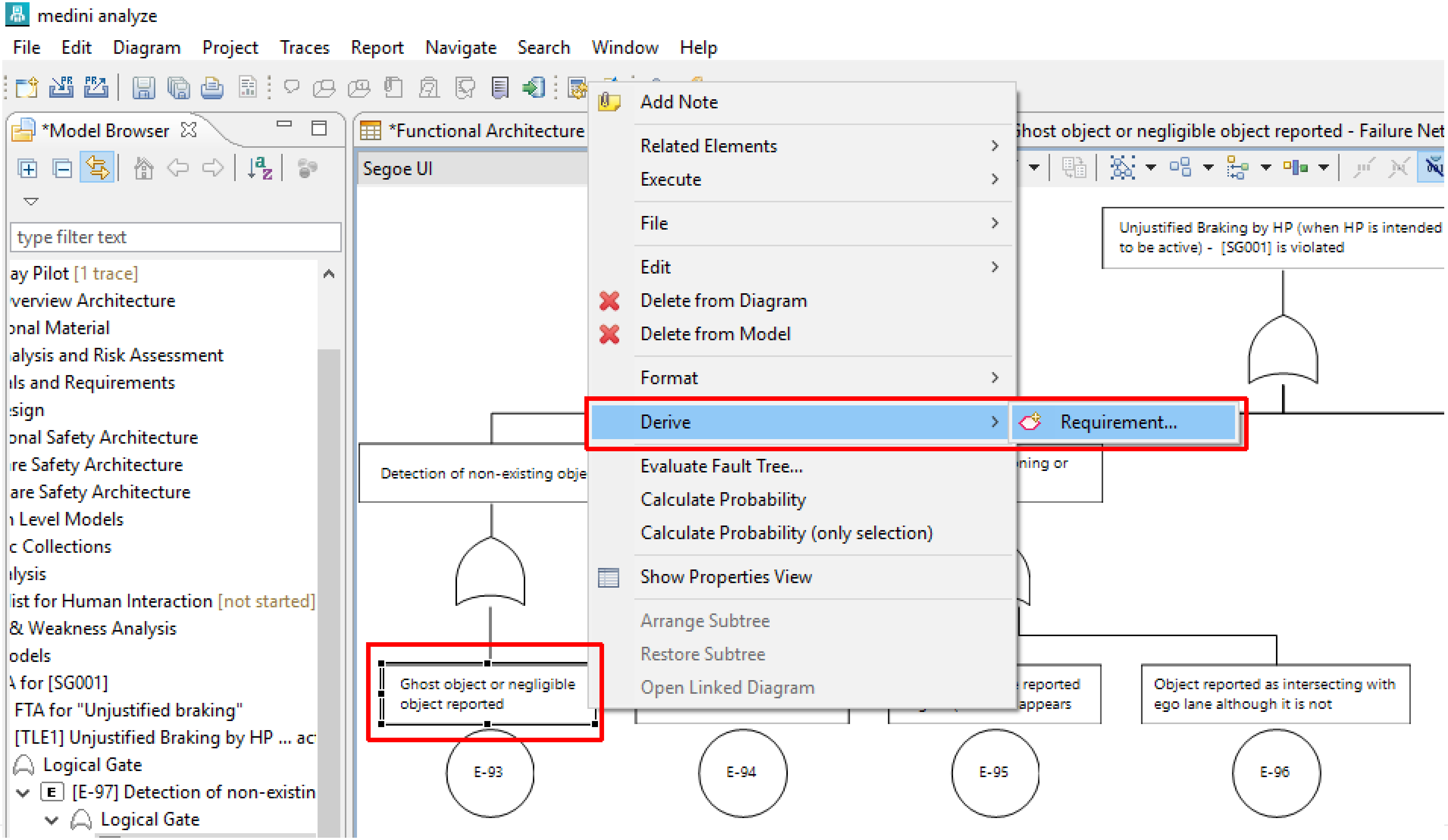
Iterative Improvement of Highway Autopilot until Remaining Risk is Acceptable



SOTIF Investigative / Causal Analysis (e.g. FTA,FMEA, Failure Net)

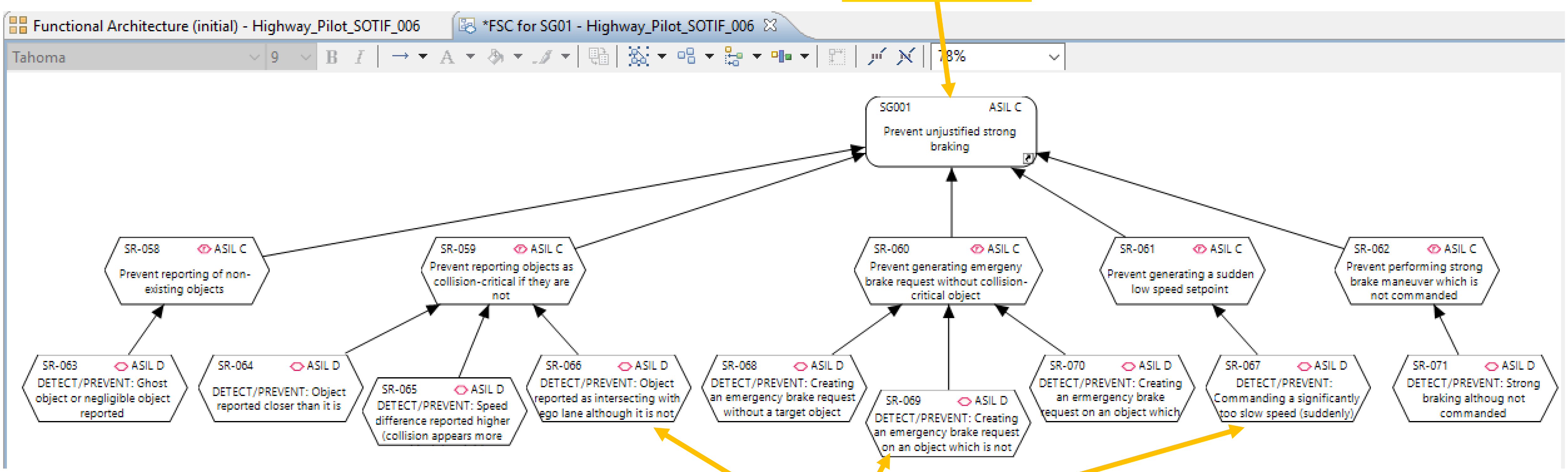
Risks acceptable after analysis?

Solution (Re)Definition and Improvement or ODD restriction (SOTIF Safety Concept)



Safety Concept is improved – Requirements are refined

Safety Goal
(from HARA)


Functional Architecture (initial) - Highway_Pilot_SOTIF_006
*FSC for SG01 - Highway_Pilot_SOTIF_006
Tahoma
9
B
I
78%

SG001 ASIL C
Prevent unjustified strong braking

SR-058 ASIL C
Prevent reporting of non-existing objects

SR-059 ASIL C
Prevent reporting objects as collision-critical if they are not

SR-060 ASIL C
Prevent generating emergeny brake request without collision-critical object

SR-061 ASIL C
Prevent generating a sudden low speed setpoint

SR-062 ASIL C
Prevent performing strong brake maneuver which is not commanded

SR-063 ASIL D
DETECT/PREVENT: Ghost object or negligible object reported

SR-064 ASIL D
DETECT/PREVENT: Object reported closer than it is

SR-065 ASIL D
DETECT/PREVENT: Speed difference reported higher (collision appears more

SR-066 ASIL D
DETECT/PREVENT: Object reported as intersecting with ego lane although it is not

SR-068 ASIL D
DETECT/PREVENT: Creating an emergency brake request without a target object

SR-069 ASIL D
DETECT/PREVENT: Creating an emergency brake request on an object which is not

SR-070 ASIL D
DETECT/PREVENT: Creating an ermergency brake request on an object which

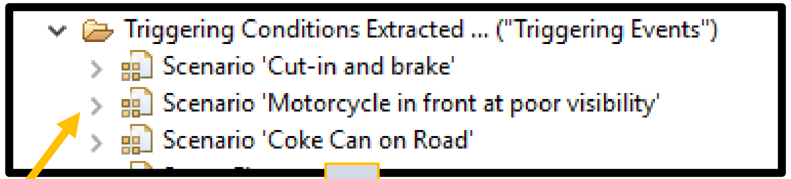
SR-067 ASIL D
DETECT/PREVENT: Commanding a significantly too slow speed (suddenly)

SR-071 ASIL D
DETECT/PREVENT: Strong braking althoug not commanded

Functional Requirements:
Initial iteration: imported from normal function development
Following iteration (system improvement): derived from safety analysis (e.g. FTA events)

SOTIF Triggering Conditions Analysis:
Building in medini Scenarios to be simulated in VRXPERIENCE

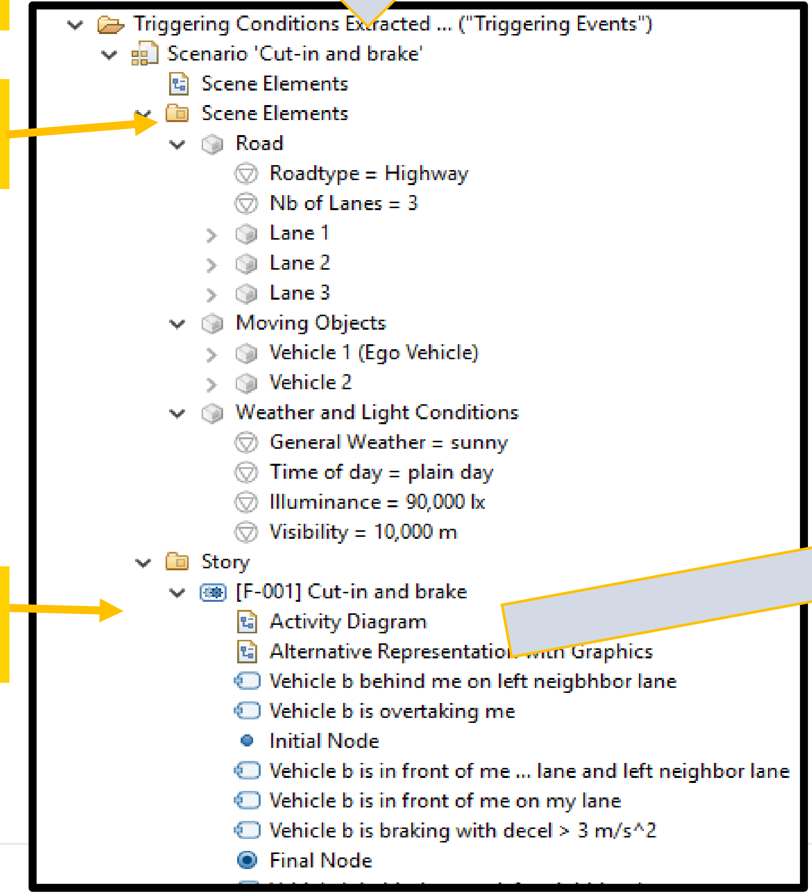
Import/Export to OpenSCENARIO standard under preparation



- Triggering Conditions Extracted ... ("Triggering Events")
  - Scenario 'Cut-in and brake'
  - Scenario 'Motorcycle in front at poor visibility'
  - Scenario 'Coke Can on Road'

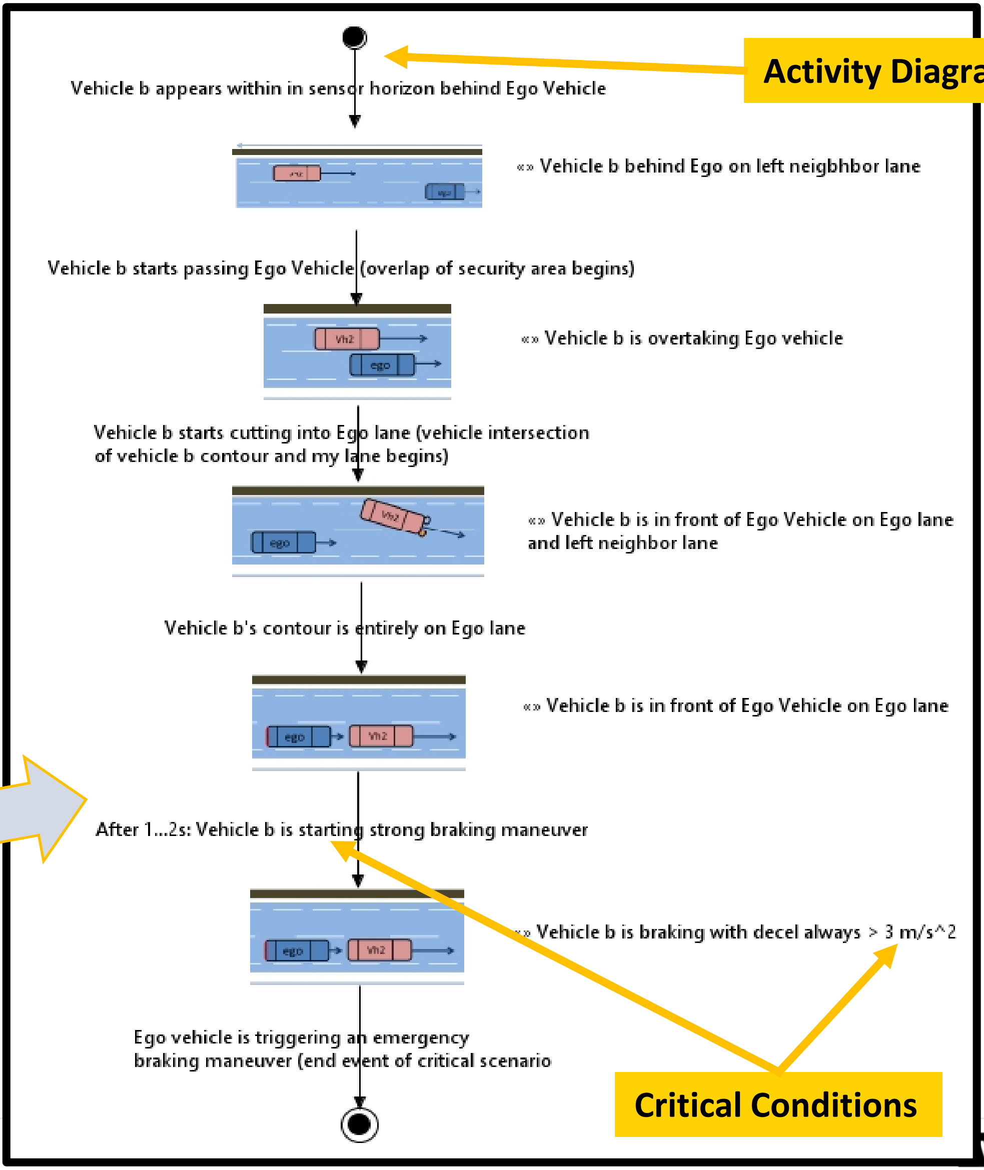
Scene Elements:
What is around

Story:
What is happening



- Triggering Conditions Extracted ... ("Triggering Events")
  - Scenario 'Cut-in and brake'
    - Scene Elements
    - Scene Elements
      - Road
        - Roadtype = Highway
        - Nb of Lanes = 3
        - Lane 1
        - Lane 2
        - Lane 3
      - Moving Objects
        - Vehicle 1 (Ego Vehicle)
        - Vehicle 2
      - Weather and Light Conditions
        - General Weather = sunny
        - Time of day = plain day
        - Illuminance = 90,000 lx
        - Visibility = 10,000 m
    - Story
      - [F-001] Cut-in and brake
        - Activity Diagram
        - Alternative Representation with Graphics
        - Vehicle b behind me on left neigbhbor lane
        - Vehicle b is overtaking me
        - Initial Node
        - Vehicle b is in front of me ... lane and left neighbor lane
        - Vehicle b is in front of me on my lane
        - Vehicle b is braking with decel > 3 m/s^2
        - Final Node

Activity Diagram



Vehicle b appears within in sensor horizon behind Ego Vehicle

«» Vehicle b behind Ego on left neigbhbor lane

Vehicle b starts passing Ego Vehicle (overlap of security area begins)

«» Vehicle b is overtaking Ego vehicle

Vehicle b starts cutting into Ego lane (vehicle intersection of vehicle b contour and my lane begins)

«» Vehicle b is in front of Ego Vehicle on Ego lane and left neighbor lane

Vehicle b's contour is entirely on Ego lane

«» Vehicle b is in front of Ego Vehicle on Ego lane

After 1...2s: Vehicle b is starting strong braking maneuver

«» Vehicle b is braking with decel always > 3 m/s^2

Ego vehicle is triggering an emergency braking maneuver (end event of critical scenario

Critical Conditions

Running SOTIF Driving Scenarios in VRXPERIENCE – Powered by AV Simulation SCANeR^{TM} Studio –

1. Functional Safety & Cybersecurity Analysis
2. Sensors
3. Closed-Loop Simulation
4. Control Software
5. Automated Driving Software
6. Vehicle Platform

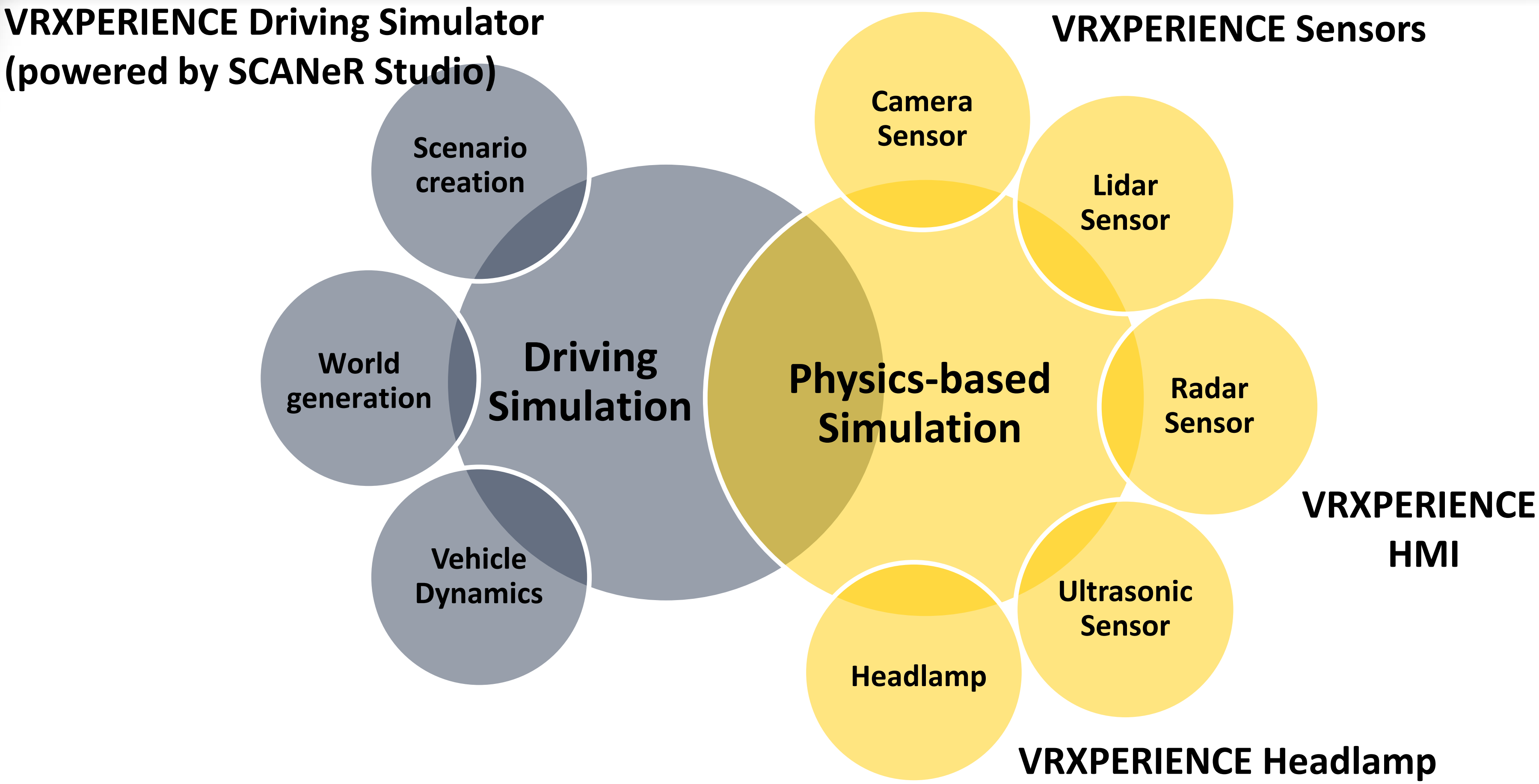
ANSYS AV open and customizable simulation environment

A comprehensive simulation software

Providing:

- ✓ Sensors & light models
- ✓ 3D world
- ✓ Scenarios
- ✓ Vehicle dynamics

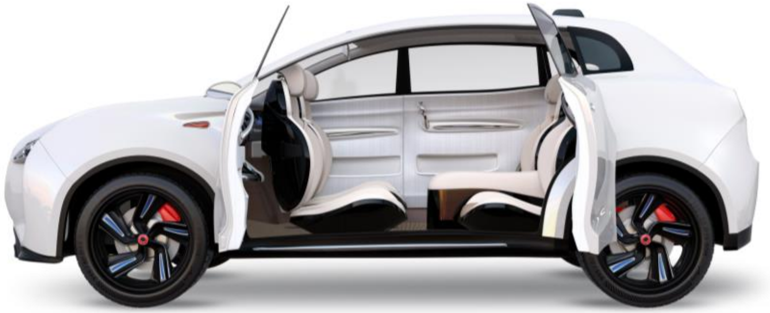
+ closed-loop platform
+ development tools



ANSYS addresses all key AV sensors

Radar

Camera



Lidar

Ultrasonic

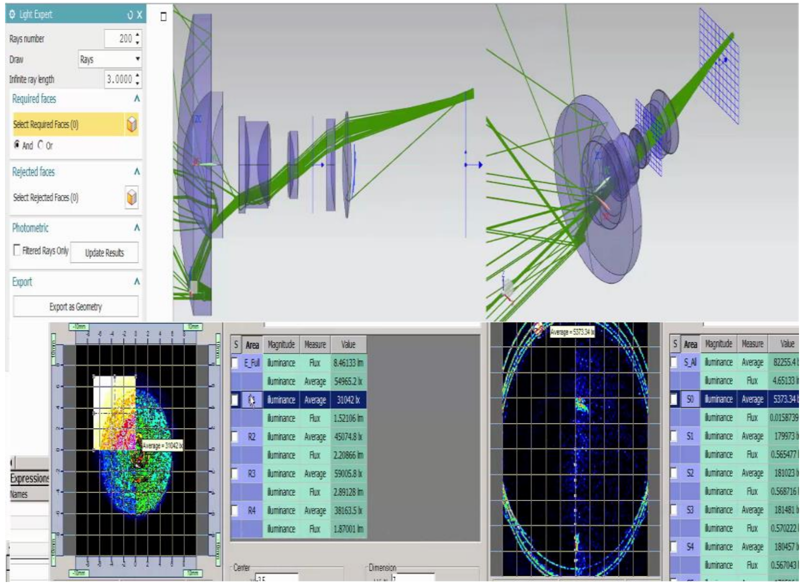
Three phases for each sensor

Component Development

Vehicle Integration

Scenario Simulation

Camera: Simulation from component design to full scenarios



Light Expert

Rays number: 200

Draw: Rays

Infinite ray length: 3.0000

Required faces

Select Required Faces (0)

● And ○ Or

Rejected faces

Select Rejected Faces (0)

Photometric

□ Filtered Rays Only

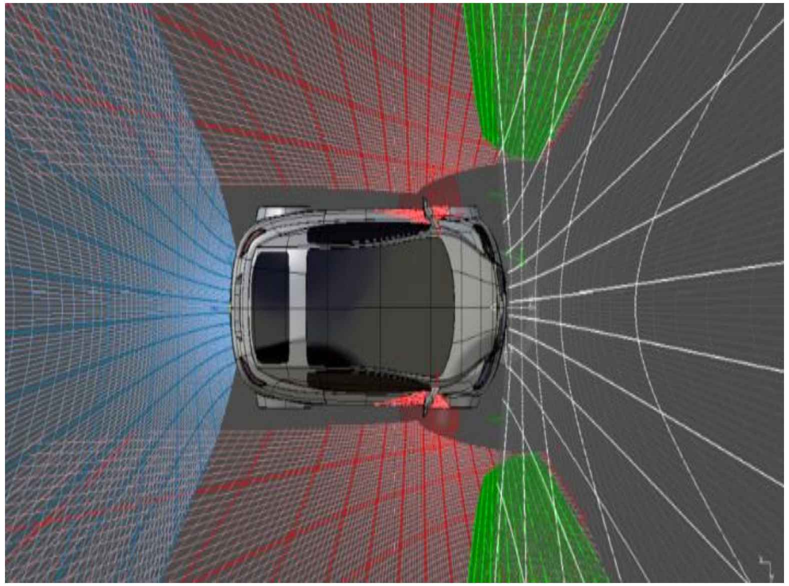
Update Results

Export

Export as Geometry

S	Area	Magnitude	Measure	Value
□	E_Full	Illuminance	Flux	8.46133 lm
		Illuminance	Average	54965.2 lx
□		Illuminance	Average	31042 lx
		Illuminance	Flux	1.52106 lm
□	R2	Illuminance	Average	45074.8 lx
		Illuminance	Flux	2.20866 lm
□	R3	Illuminance	Average	59005.8 lx
		Illuminance	Flux	2.89128 lm
□	R4	Illuminance	Average	38163.5 lx
		Illuminance	Flux	1.87001 lm

S	Area	Magnitude	Measure	Value
□	S_All	Illuminance	Average	82255.4
		Illuminance	Flux	4.65133
□	S0	Illuminance	Average	5373.34
		Illuminance	Flux	0.0158739
□	S1	Illuminance	Average	179973
		Illuminance	Flux	0.565477
□	S2	Illuminance	Average	181023
		Illuminance	Flux	0.568716
□	S3	Illuminance	Average	181481
		Illuminance	Flux	0.570222
□	S4	Illuminance	Average	180457
		Illuminance	Flux	0.567043



Component Development

Optical, Thermal, Structural

Design & Analysis

Vehicle Integration

Vision Performance Analysis

Position Optimization

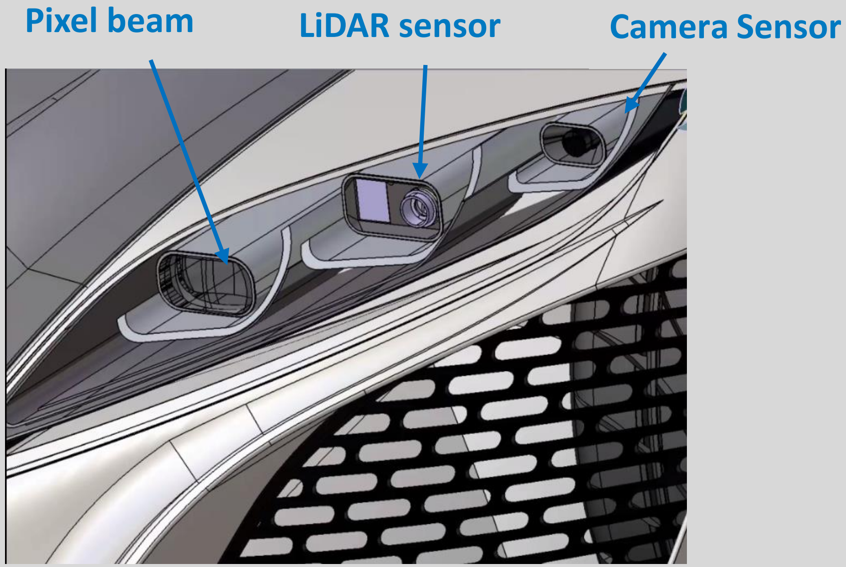
Scenario Simulation

Vision System

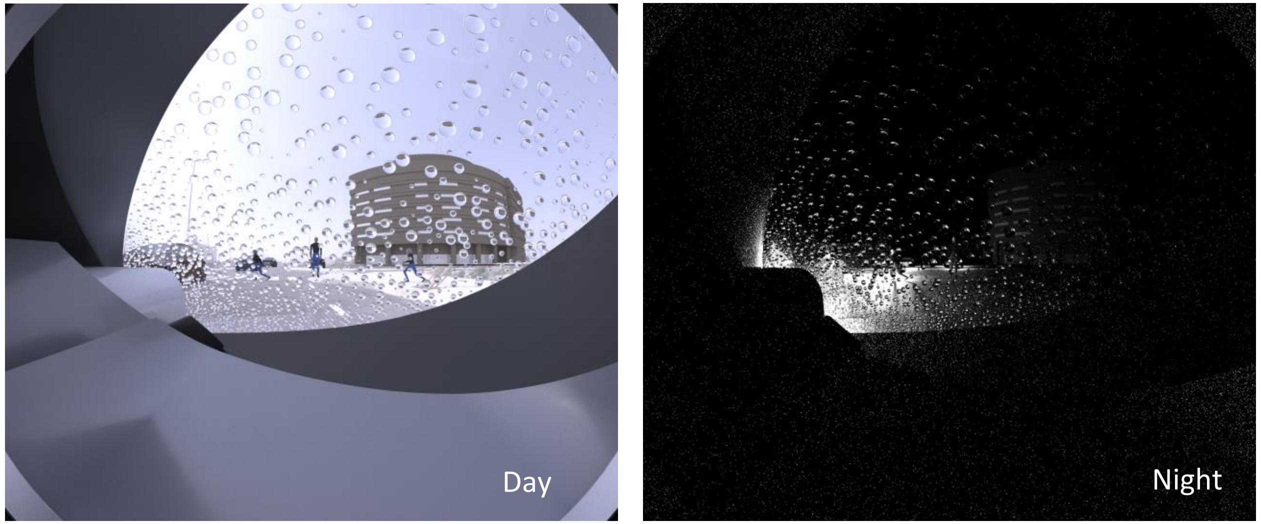
Test & Validation

Camera: Simulations in adverse weather conditions

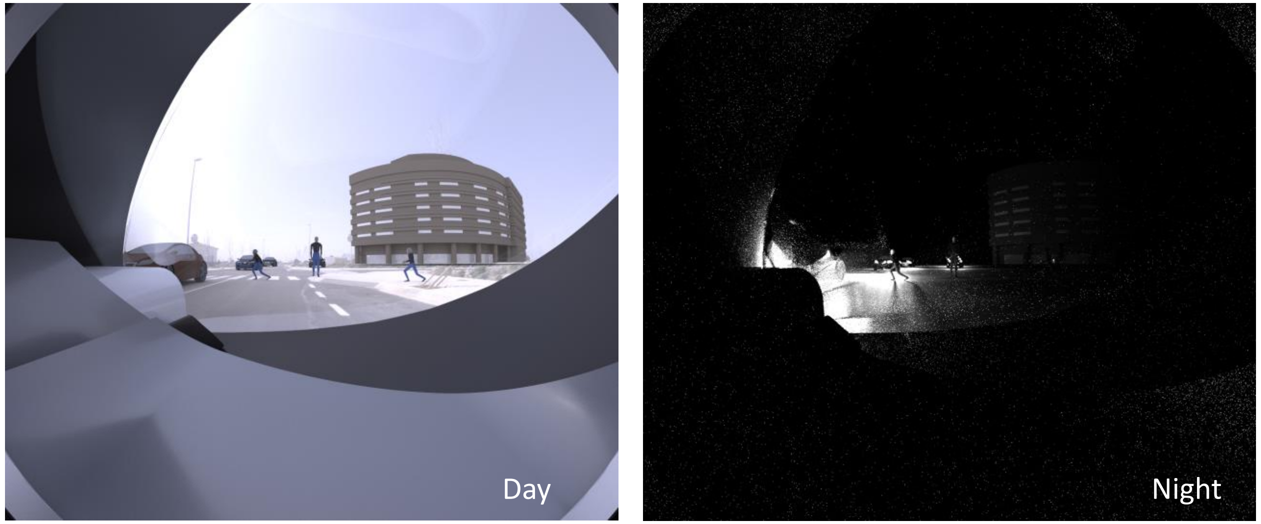
Simulations are performed using a headlamp model with an integrated camera and LiDAR sensor



Headlamp outer lens with water droplet build-up

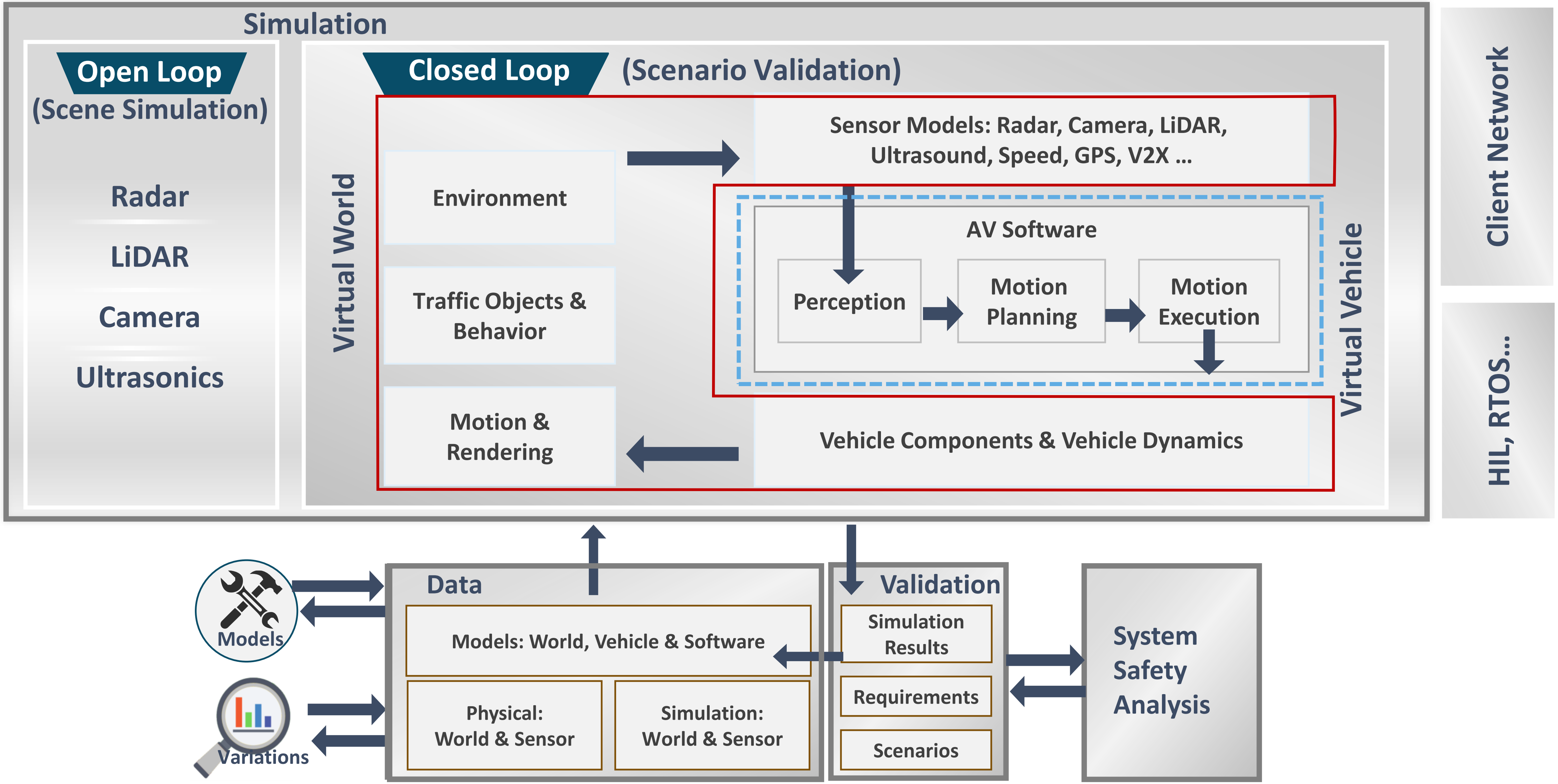


Headlamp outer lens with 3M hydrophobic film



1. Functional Safety & Cybersecurity Analysis
2. Sensors
3. **Closed-Loop Simulation**
4. Control Software
5. Automated Driving Software
6. Vehicle Platform

ANSYS AV open and customizable simulation environment



Simulation

Open Loop
(Scene Simulation)

Radar

LiDAR

Camera

Ultrasonics

Closed Loop (Scenario Validation)

Virtual World

Environment

Traffic Objects & Behavior

Motion & Rendering

Sensor Models: Radar, Camera, LiDAR, Ultrasound, Speed, GPS, V2X …

AV Software

Perception

Motion Planning

Motion Execution

Vehicle Components & Vehicle Dynamics

Virtual Vehicle

Client Network

HIL, RTOS…

Models

Variations

Data

Models: World, Vehicle & Software

Physical: World & Sensor

Simulation: World & Sensor

Validation

Simulation Results

Requirements

Scenarios

System Safety Analysis

3D world model & preparation

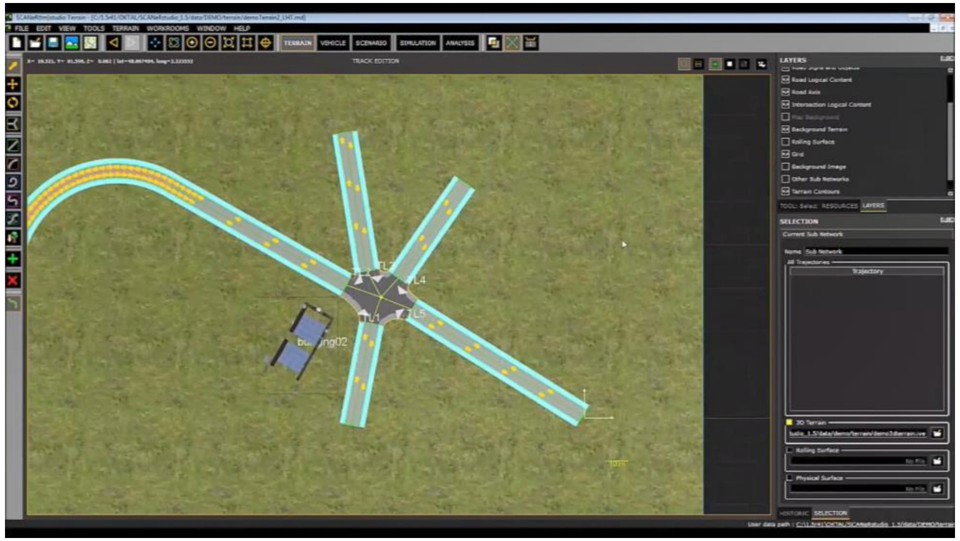
Support any process able to capture real world into simulation with very high fidelity road database and photorealism.

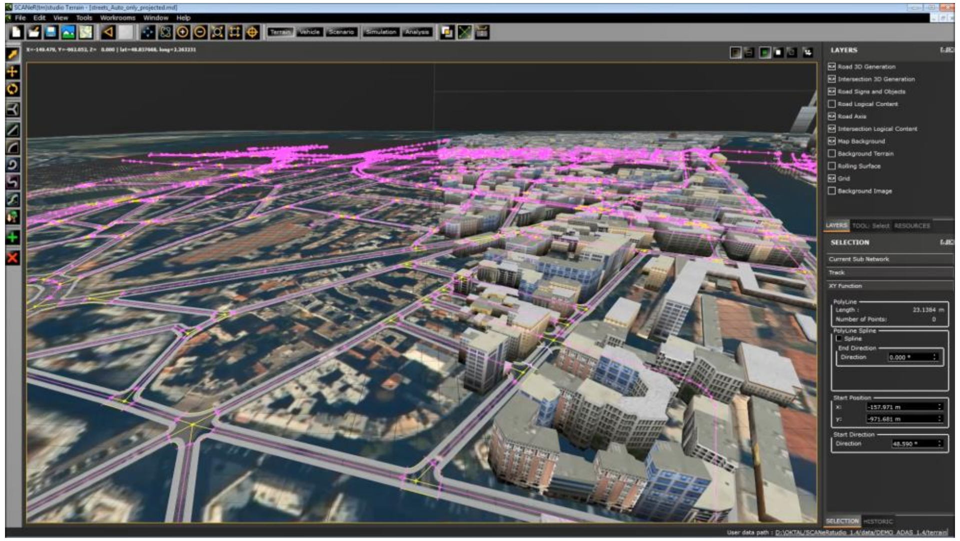
Key Features

- Ease the creation of 3D road environment
- openDrive compliant
- Import map data : OpenStreetMap, Here…
- Trim the world from libraries
- Set physics-based materials from libraries

Use case

- Create high fidelity 3D world model
- Automate 3D world model creation for quick and fast simulation test





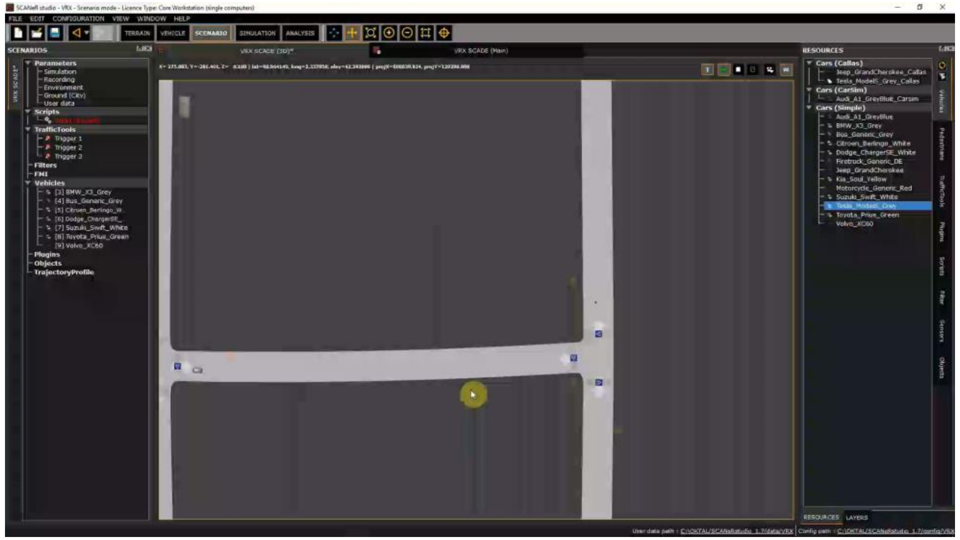
Scenario & Traffic

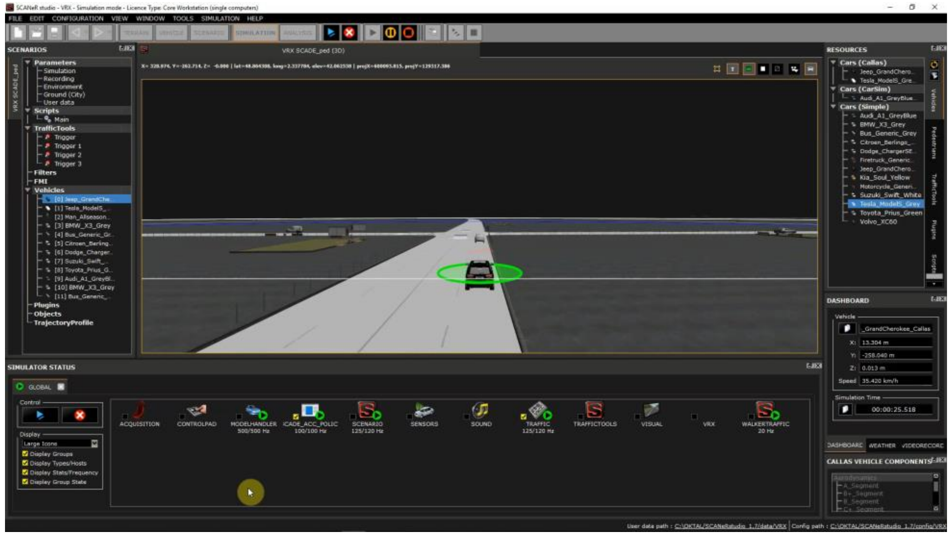
Key Features

- Bring ego car into a multi-agent simulated traffic model
- Traffic model based on AI able to generate any kind of traffic situations.
- Create scenario via script or GUI
- Automation of scenario from Test Plan.
- Large asset of car, trucks, motorbike, pedestrians, animals...

Use case

- Create dynamics driving scenario
- Create variability of scenario
- Automate scenario creation for massive simulation test





Sensors

Key Features

- Ideal or physics-based model of Camera, Radar, Lidar, Ultrasonic sensors

Use case

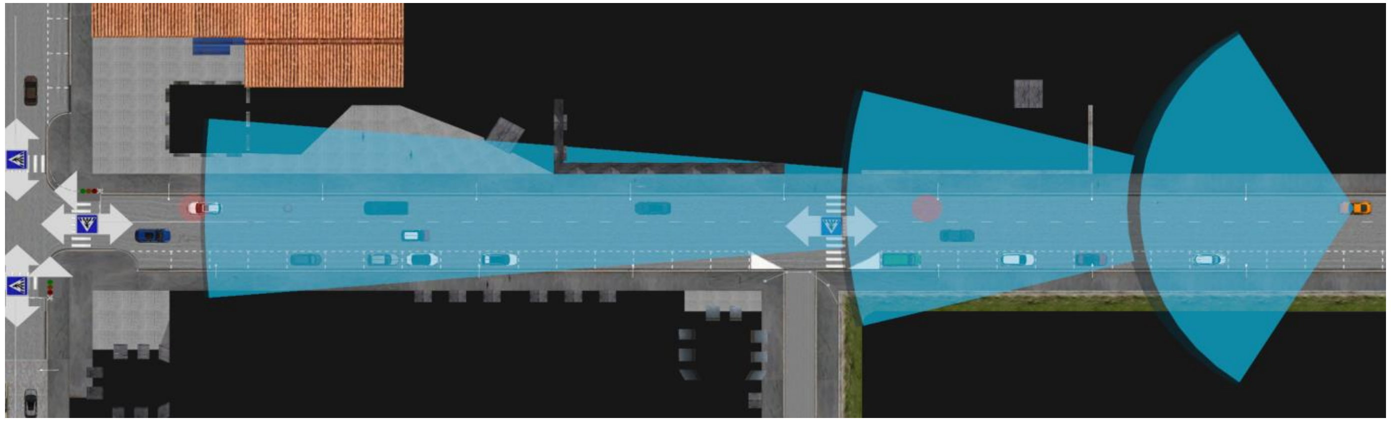
- Model the ideal or physics-based behavior of sensors

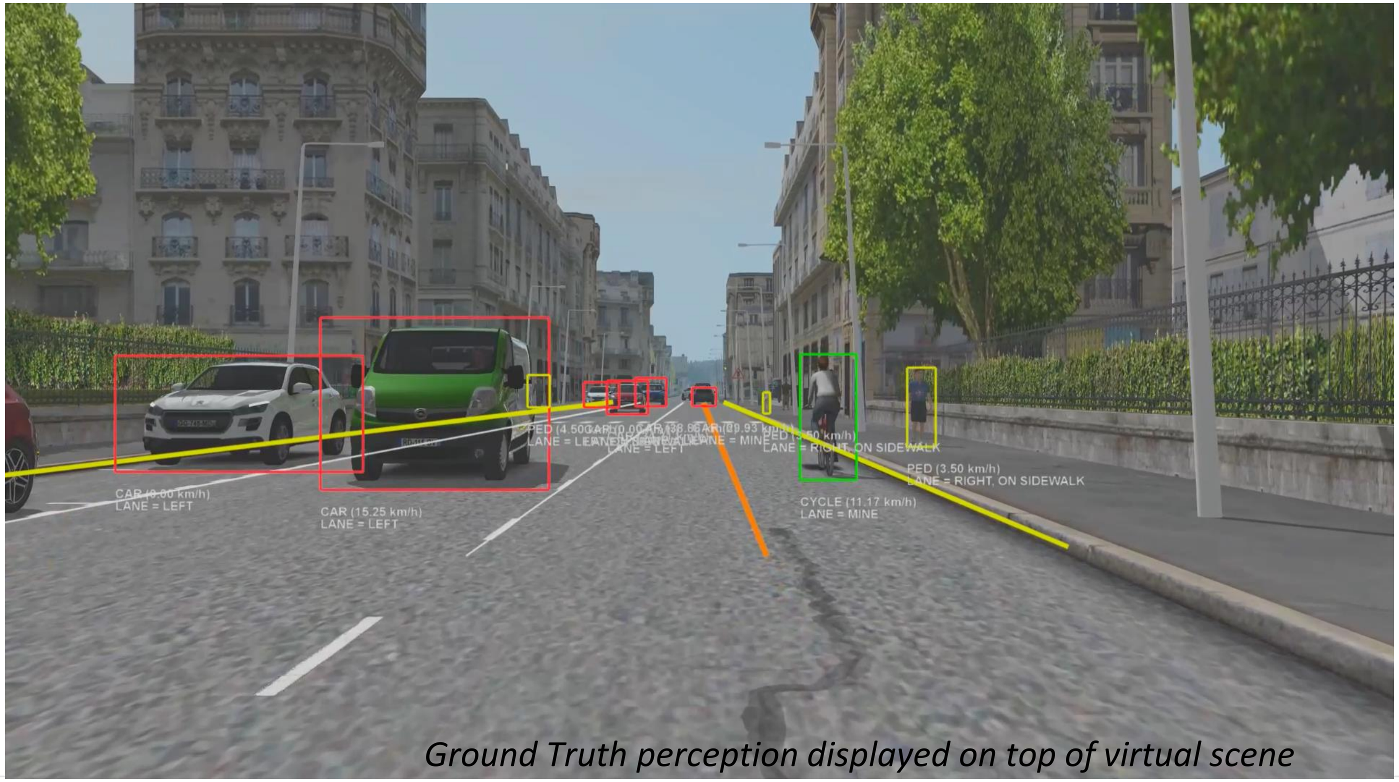
- Develop and test:
  - ○ perception, planning and control algorithm (physics-based)

  or

  - ○ planning and control isolated from perception (ideal)

- Test ADAS feature robustness

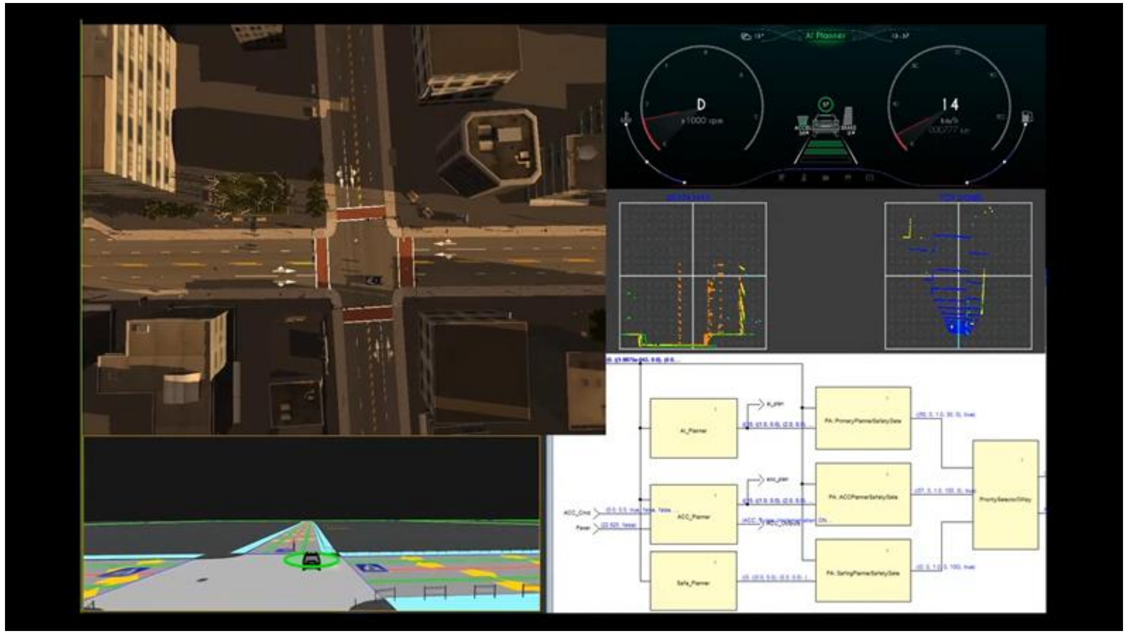


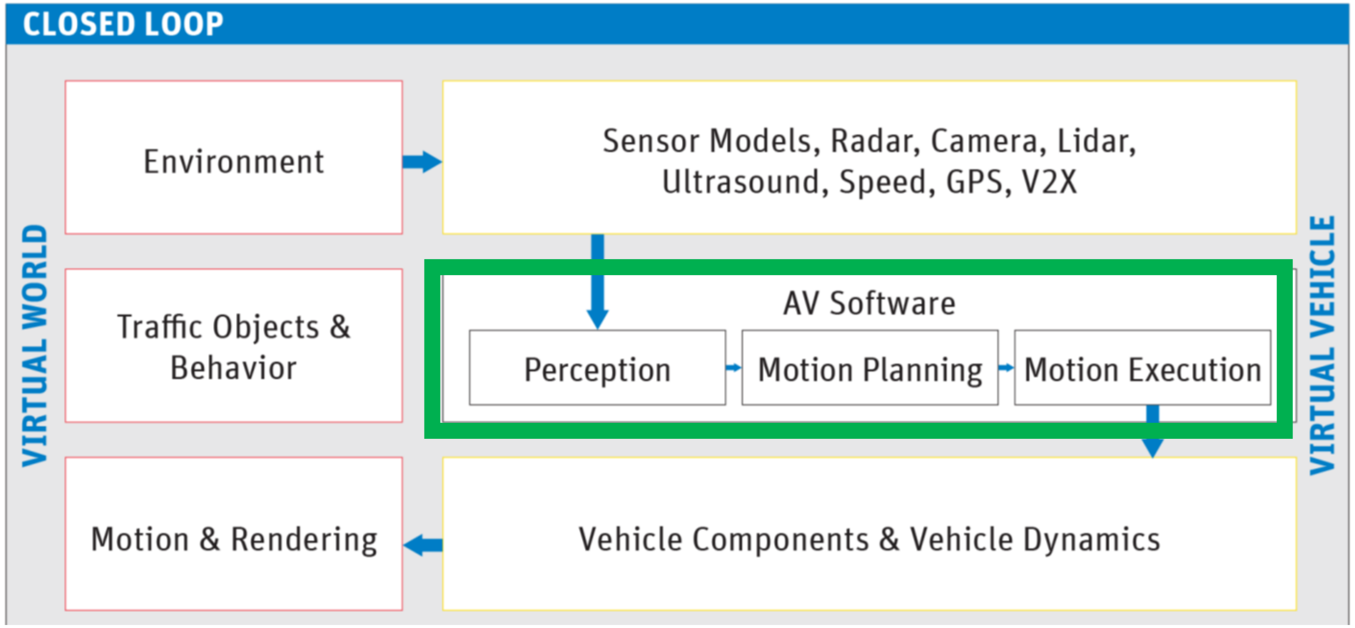


Ground Truth perception displayed on top of virtual scene

Closed-loop simulation of full AV stack (Software-in-the-loop)

- Physics-based sensor models allow testing of full AV software stack
- Run real-time asynchronous or externally synchronized simulation
- Distribute computing and rendering node on several CPU or GPU
- Massive simulation on HPC





CLOSED LOOP
VIRTUAL WORLD
Environment
Traffic Objects & Behavior
Motion & Rendering
Sensor Models, Radar, Camera, Lidar, Ultrasound, Speed, GPS, V2X
AV Software
Perception
Motion Planning
Motion Execution
Vehicle Components & Vehicle Dynamics
VIRTUAL VEHICLE

Scenario Re-Creation from Real-World Driving

Demo Case:
Left turn
in Pittsburgh

Powered by Edge Case Research

EDGE CASE RESEARCH
MAKING AUTONOMY SAFER

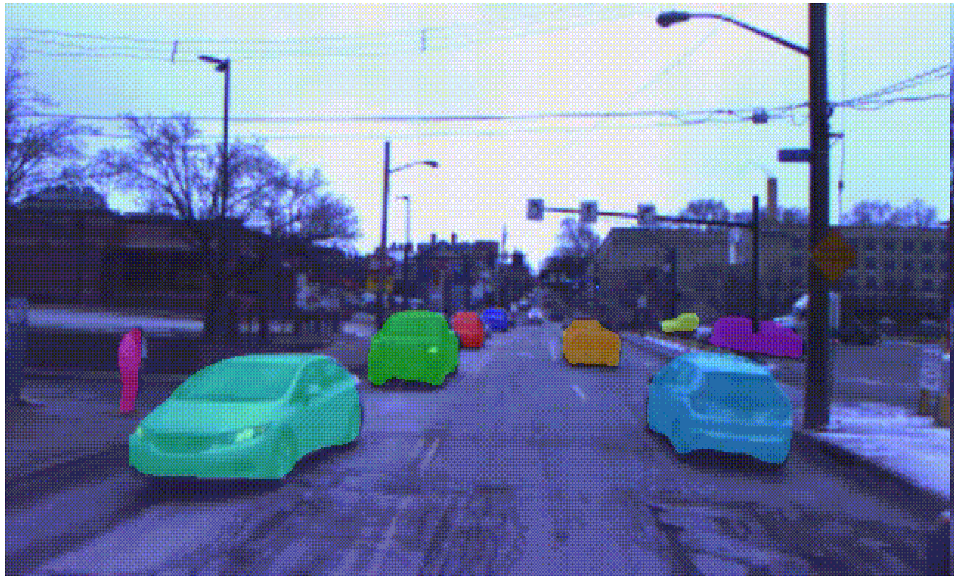
Tracking Moving Object to Re-Create Scenario

Convolutional Neural Network (CNN)

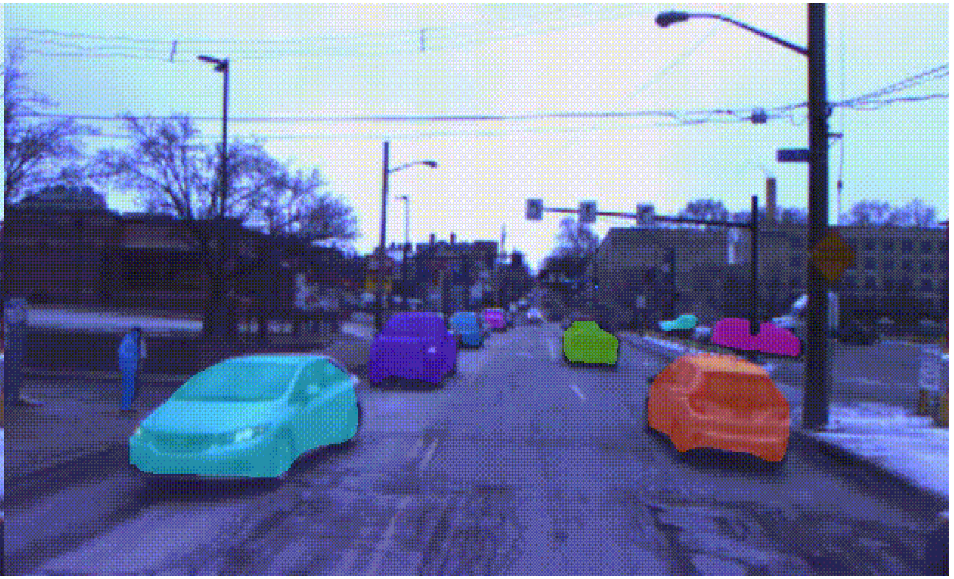
- Detects objects frame by frame

Visual object associator

- Performs object association

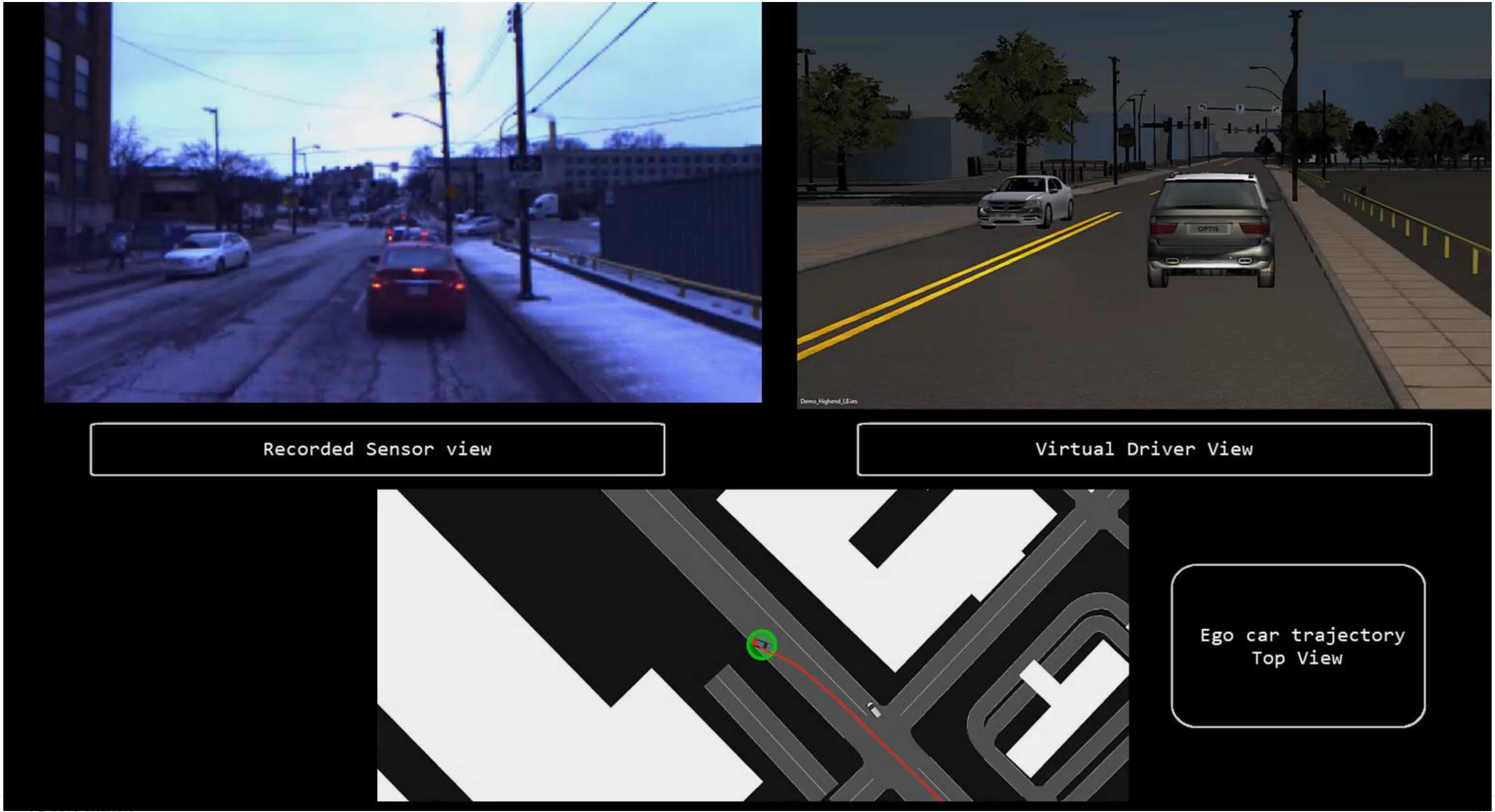


Before object associator



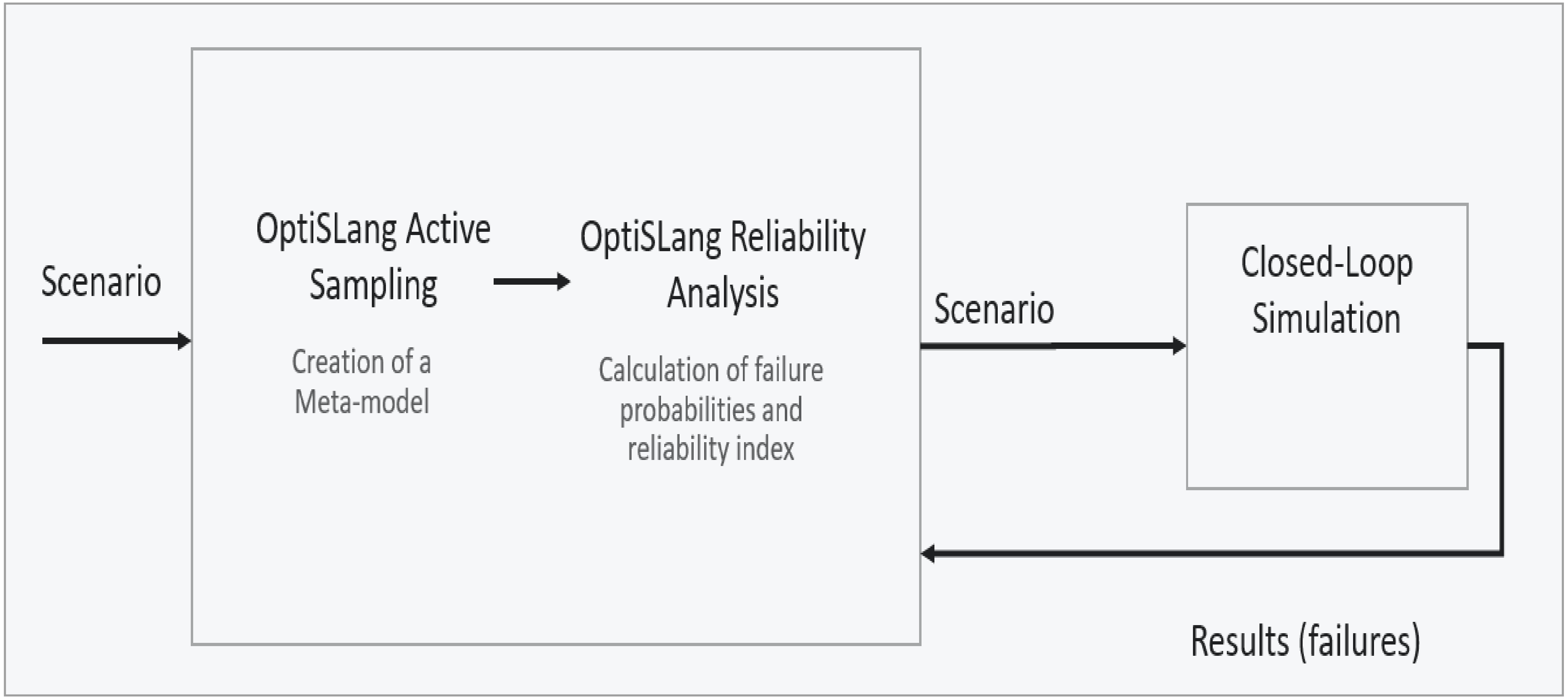
After object associator

Scenario Re-Creation: Left turn in Pittsburgh

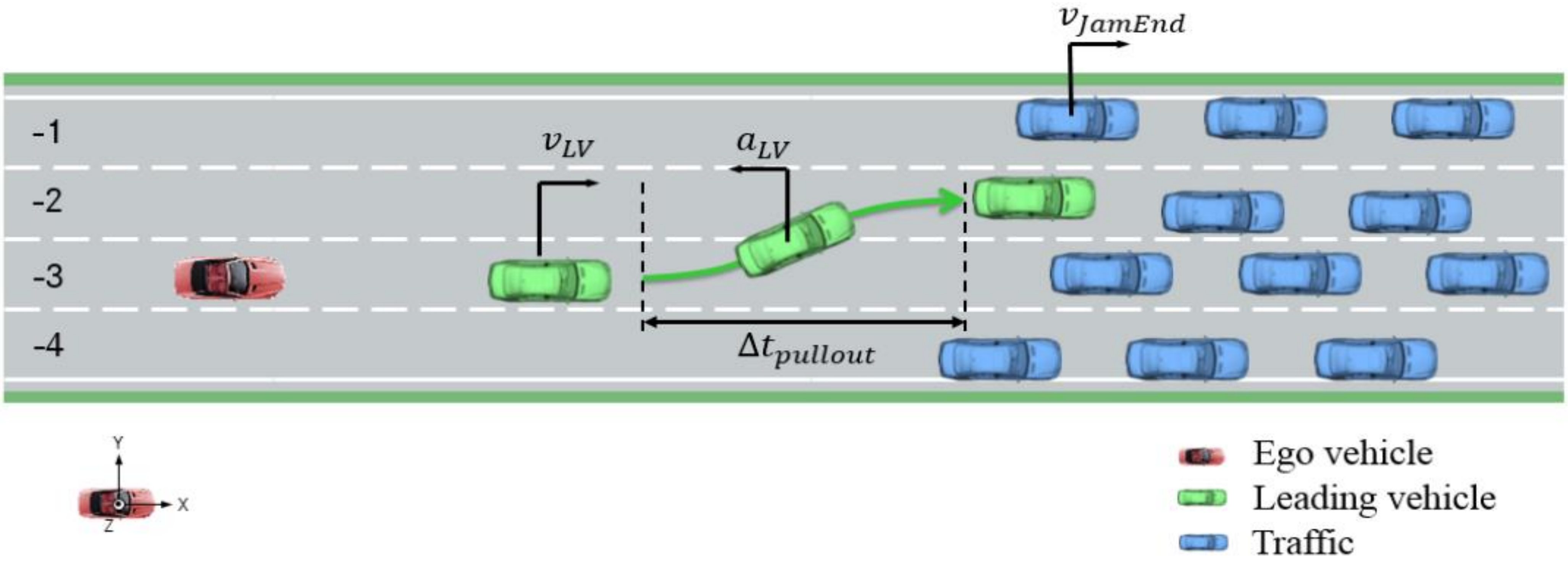


Scenario Variation using ANSYS optiSLang (Dynardo optiSLang®)

The goal is to perform robustness and reliability analysis for <u>parameterized driving scenarios</u> in a way that is much more efficient than Monto-Carlo Simulation.


Scenario
OptiSLang Active Sampling
Creation of a Meta-model
OptiSLang Reliability Analysis
Calculation of failure probabilities and reliability index
Scenario
Closed-Loop Simulation
Results (failures)

Example of Scenario Variations (Jam-End, 9 parameters)



	Number of samples	Failure probability	Coeff. of variation	Reliability index
Limit TTC = 0.4				
MCS	39.420.000	$2.54{*}10^{-6}$	10.0%	4.56
AS	16.000	$2.81{*}10^{-6}$	9.1%	4.54
ISPUD+FORM	7.000+5.500	$2.31{*}10^{-6}$	9.5%	4.58

28,500 simulation runs using optiSLang

vs.

39.420.000 using Monte-Carlo simulation

1 Functional Safety & Cybersecurity Analysis

2 Sensors

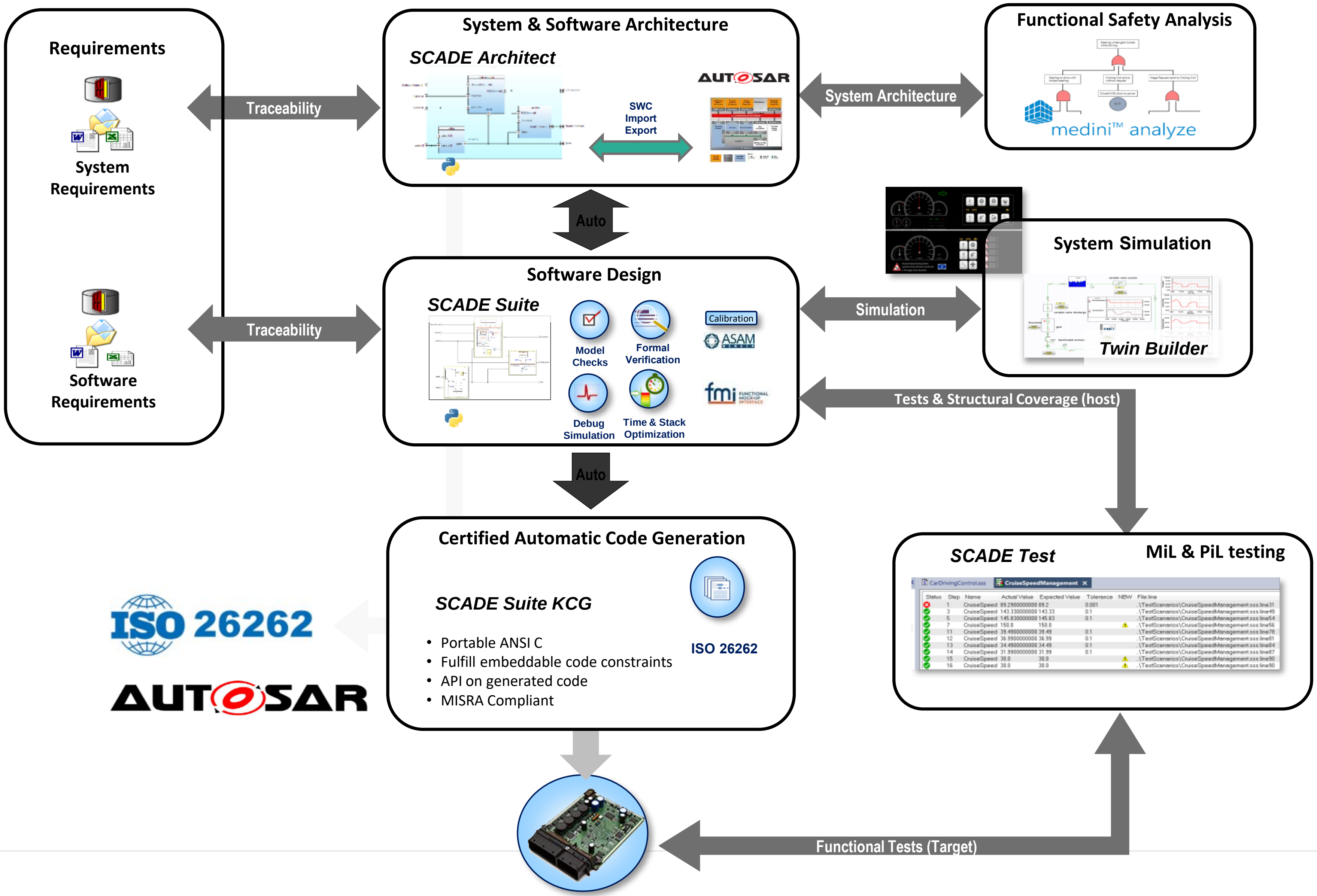
3 Closed-Loop Simulation

4 Control Software

5 Automated Driving Software

6 Vehicle Platform

ANSYS SCADE provides a model-based software development flow with ISO 26262 certified code generation and AUTOSAR compliance



Requirements

System Requirements

Software Requirements

Traceability

Traceability

System & Software Architecture

SCADE Architect

SWC Import Export

AUTOSAR

System Architecture

Functional Safety Analysis

medini™ analyze

Auto

Software Design

SCADE Suite

Model Checks

Formal Verification

Debug Simulation

Time & Stack Optimization

Calibration

ASAM

fmi

Simulation

System Simulation

Twin Builder

Tests & Structural Coverage (host)

Auto

Certified Automatic Code Generation

SCADE Suite KCG

- Portable ANSI C
- Fulfill embeddable code constraints
- API on generated code
- MISRA Compliant

ISO 26262

ISO 26262

AUTOSAR

SCADE Test

MiL & PiL testing

CarDrivingControl.sss | CruiseSpeedManagement

Status	Step	Name	Actual Value	Expected Value	Tolerance	NBW	File:line
✗	1	CruiseSpeed	89.2900000000	89.2	0.001		..\TestScenarios\CruiseSpeedManagement.sss:line31
✓	3	CruiseSpeed	143.330000000	143.33	0.1		..\TestScenarios\CruiseSpeedManagement.sss:line49
✓	5	CruiseSpeed	145.830000000	145.83	0.1		..\TestScenarios\CruiseSpeedManagement.sss:line54
✓	7	CruiseSpeed	150.0	150.0		⚠	..\TestScenarios\CruiseSpeedManagement.sss:line56
✓	11	CruiseSpeed	39.4900000000	39.49	0.1		..\TestScenarios\CruiseSpeedManagement.sss:line78
✓	12	CruiseSpeed	36.9900000000	36.99	0.1		..\TestScenarios\CruiseSpeedManagement.sss:line81
✓	13	CruiseSpeed	34.4900000000	34.49	0.1		..\TestScenarios\CruiseSpeedManagement.sss:line84
✓	14	CruiseSpeed	31.9900000000	31.99	0.1		..\TestScenarios\CruiseSpeedManagement.sss:line87
✓	15	CruiseSpeed	30.0	30.0		⚠	..\TestScenarios\CruiseSpeedManagement.sss:line90
✓	16	CruiseSpeed	30.0	30.0		⚠	..\TestScenarios\CruiseSpeedManagement.sss:line90

Functional Tests (Target)

1 Functional Safety & Cybersecurity Analysis

2 Sensors

3 Closed-Loop Simulation

4 Control Software

5 **Automated Driving Software**

6 Vehicle Platform

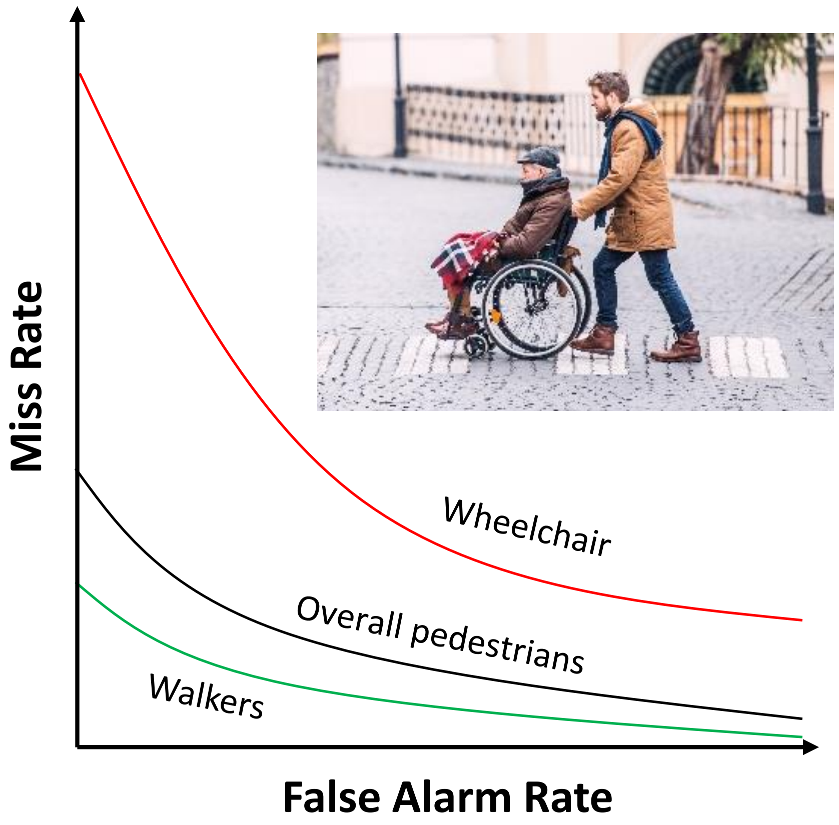
5 Automated Driving Software

5.1 Perception testing (Open Loop)

5.2 Perception testing (Closed Loop)

5.3 Planning

Why are edge cases a problem?



Perhaps your autonomy can detect 999 out of every 1,000 images with pedestrians that walk on two legs.

But what if it only detected 700 out of every 1,000 images with pedestrians that use wheelchairs?

P (accident | wheelchair) should be the same as
P (accident | walker)

So we need to find all the edge cases!

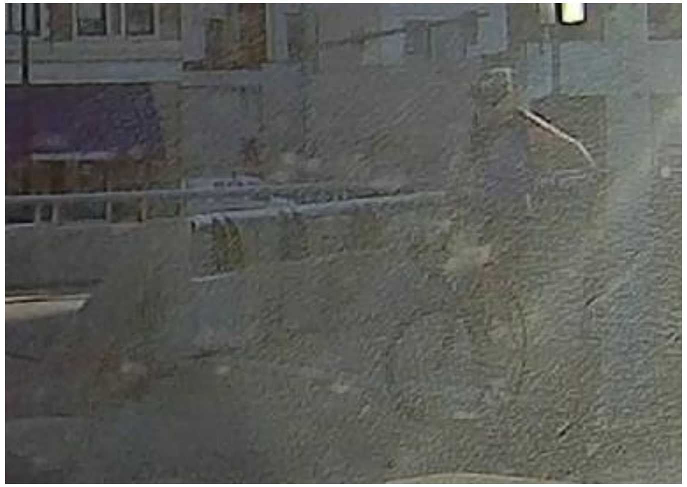
The pedestrian in a wheelchair is an edge case, i.e. a condition that unknowingly poses safety risks.

Edge cases can be caused by…

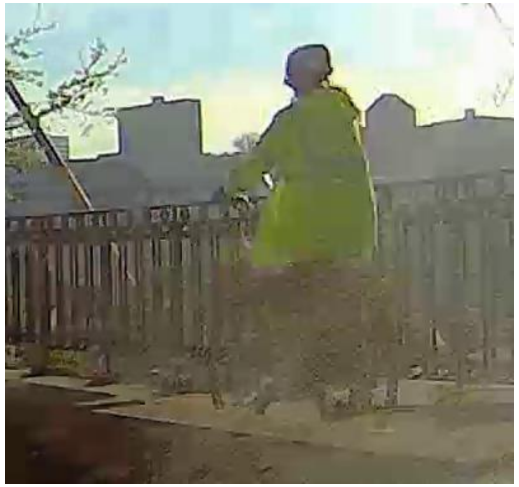
- **Weather conditions (snow, rain, wildfire)**
- **Lighting conditions (glare, night, high beams)**
- **Infrastructure (fences, reflective surfaces, statues)**
- **Types of road users (wheelchairs, people in costumes)**
- **Incomplete training of machine learning systems!**

Just because you handle one edge case safely doesn't mean you'll handle the next one safely, too!

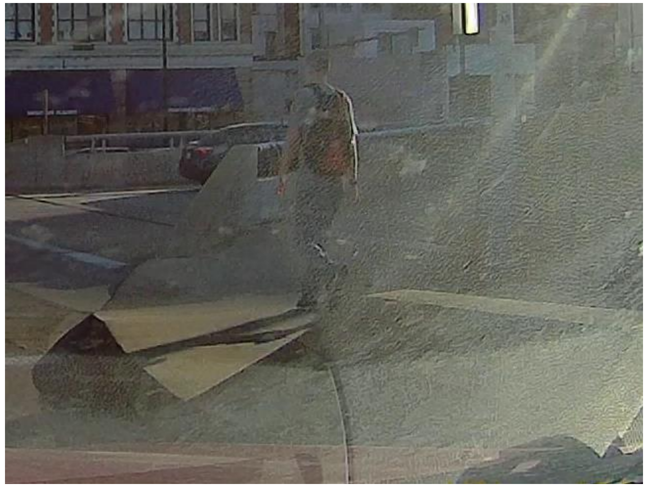
and identify the root causes of these edge cases



{ “**sun glare**”, “guardrail” }



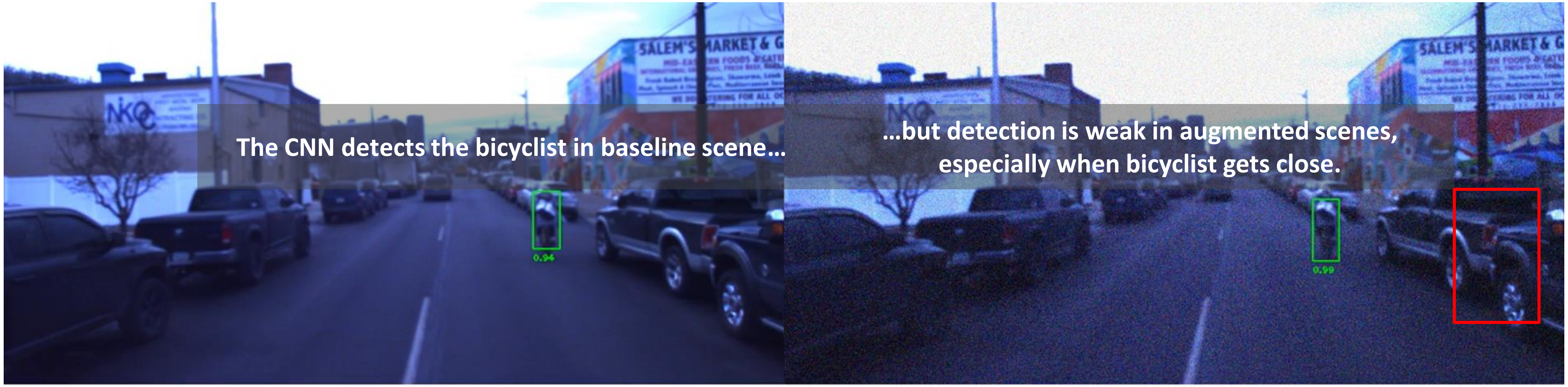
{ “**sun glare**”, “fence”, “high-visibility vest” }



{ “**sun glare**”, “guardrail” }

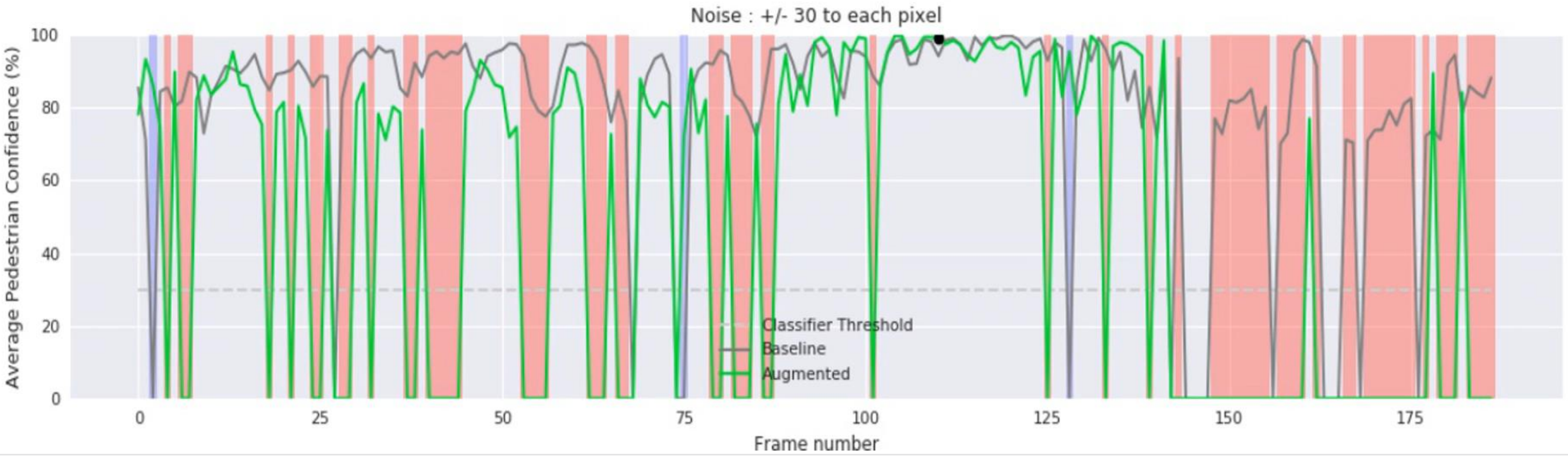
Root causes (“triggering conditions” per SOTIF) can be hypothesized, validated, mitigated, and verified.

SCADE Vision (Powered by Edge Case research) filters through huge data sets to identify real-world edge cases and safety risks



The CNN detects the bicyclist in baseline scene…

…but detection is weak in augmented scenes, especially when bicyclist gets close.



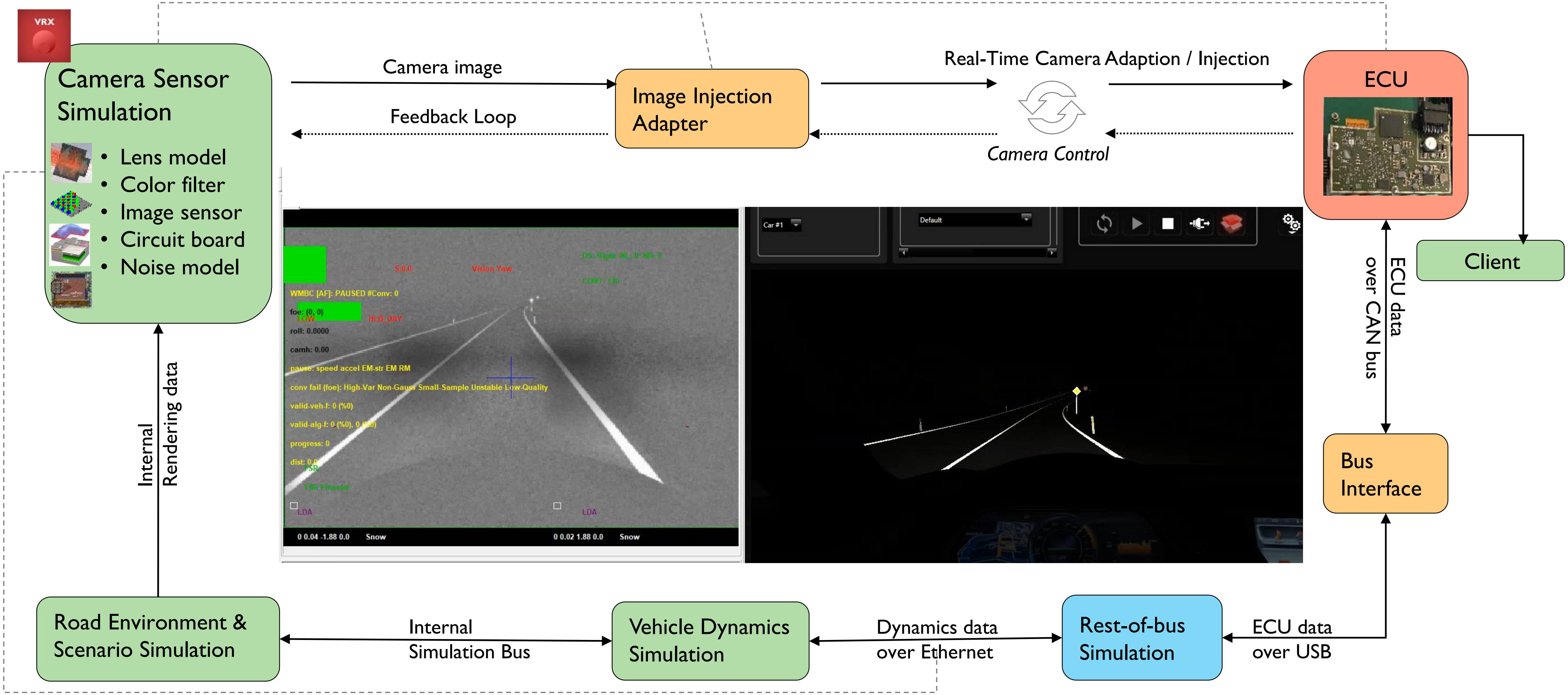
5 Automated Driving Software

5.1 Perception testing (Open Loop)

5.2 Perception testing (Closed Loop)

5.3 Planning

Perception testing (HiL Simulation/Closed loop)



Camera Sensor Simulation

- Lens model
- Color filter
- Image sensor
- Circuit board
- Noise model

Camera image

Feedback Loop

Image Injection Adapter

Real-Time Camera Adaption / Injection

Camera Control

ECU

Client

ECU data over CAN bus

Bus Interface

Internal Rendering data

Road Environment & Scenario Simulation

Internal Simulation Bus

Vehicle Dynamics Simulation

Dynamics data over Ethernet

Rest-of-bus Simulation

ECU data over USB

```
S:0.0          Vision Yaw
WMBC [AF]: PAUSED #Conv: 0
foe: (0, 0)
LOW            HLB_DAY
roll: 0.0000
camh: 0.00
pause: speed accel EM-str EM RM
conv fail (foe): High-Var Non-Gauss Small-Sample Unstable Low-Quality
valid-veh-f: 0 (%0)
valid-alg-f: 0 (%0), 0 (%0)
progress: 0
dist: 0.0
□ LDA                                   □ LDA
0 0.04 -1.88 0.0     Snow               0 0.02 1.88 0.0     Snow
```

5 Automated Driving Software

5.1 Perception testing (Open Loop)

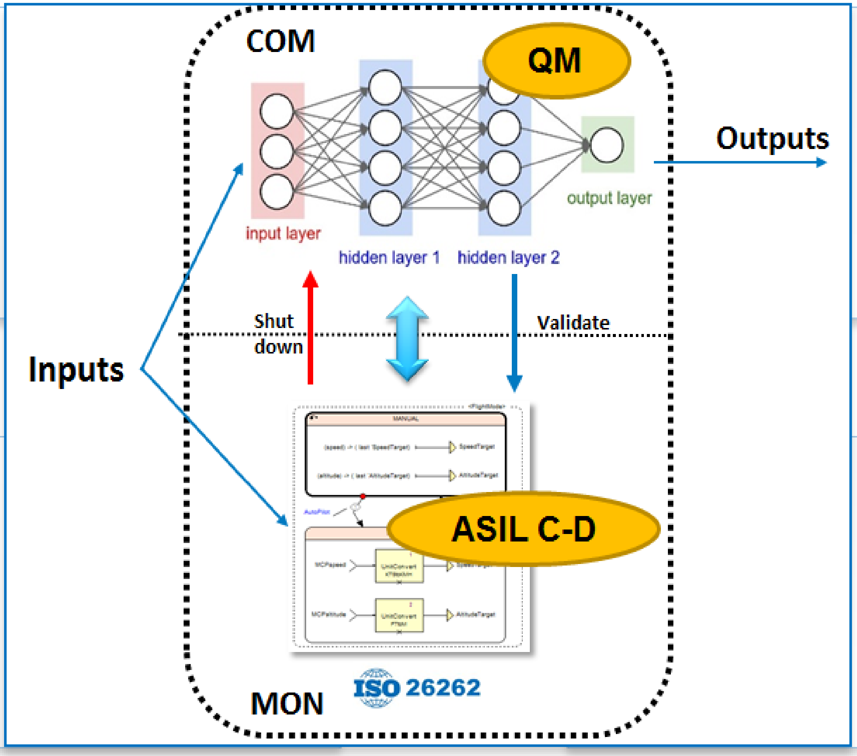
5.2 Perception testing (Closed Loop)

5.3 Planning

Safe Software Architecture for Integrating Neural Networks

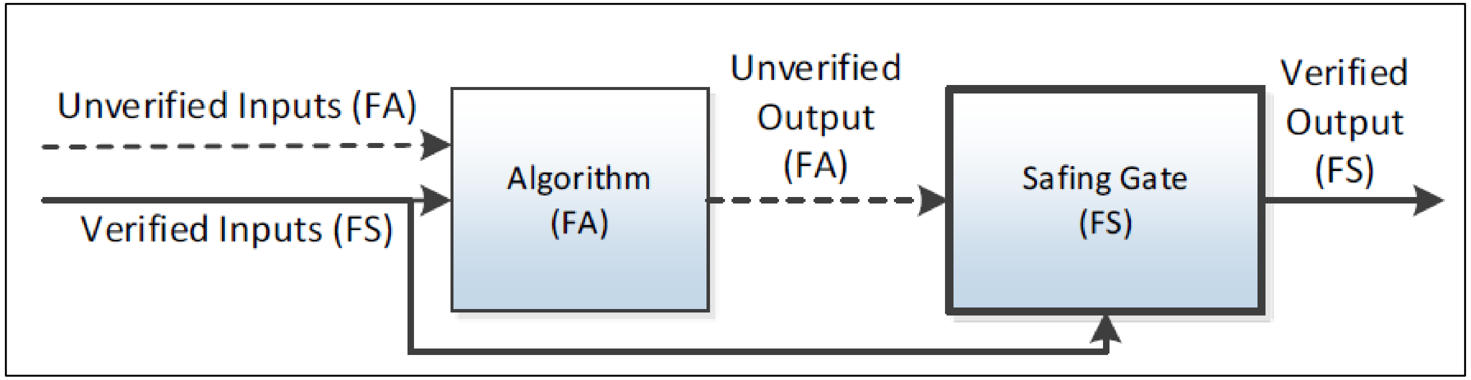
A COM-MON (Command and Monitor) architecture is used when using neural nets

Safety is allocated to the monitor. The monitor is developed using MBSE, safety analyses, certified code generation



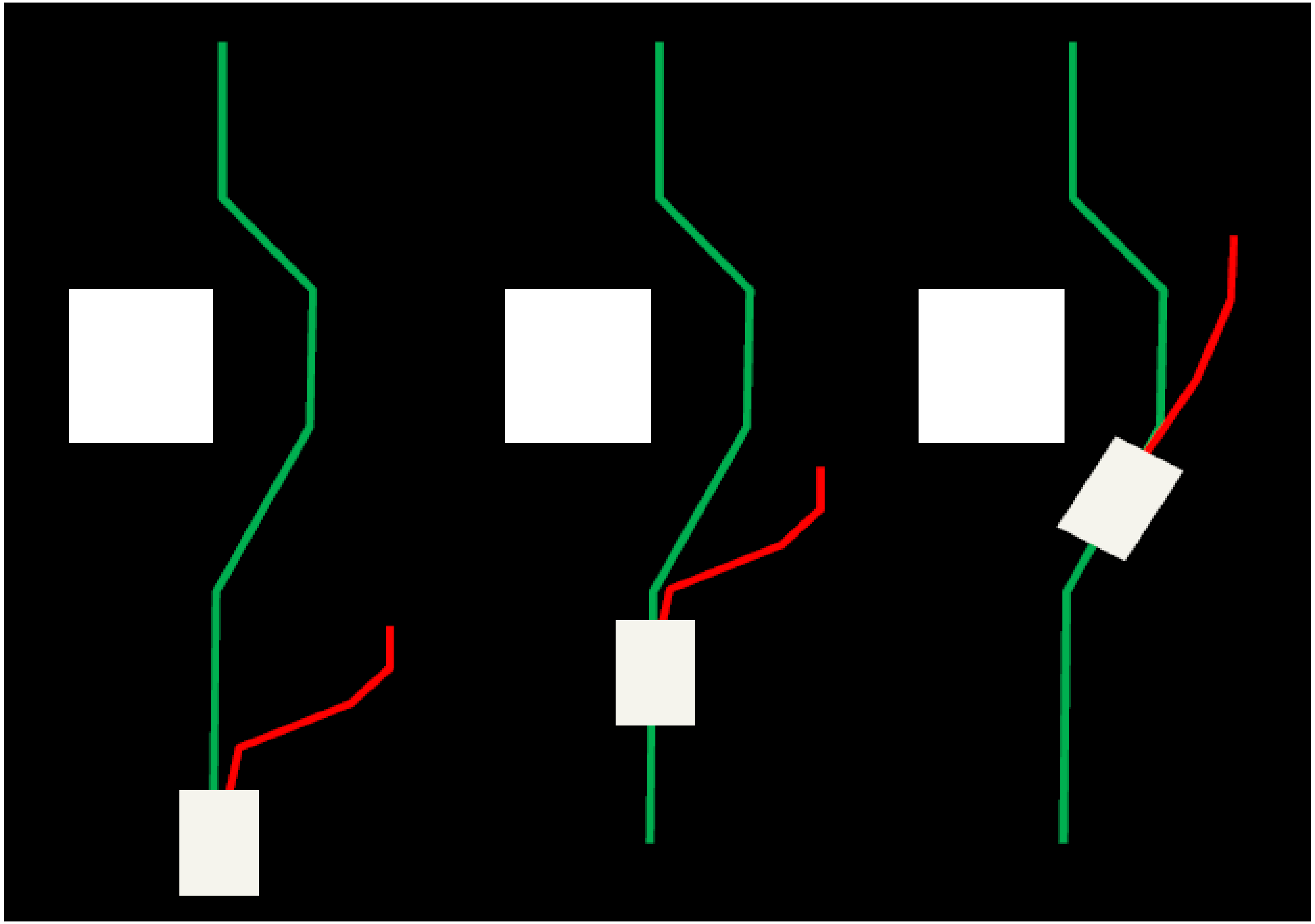
The “DOER” Algorithm can fail arbitrarily (FA) meaning that it can do wrong things in the worst possible way

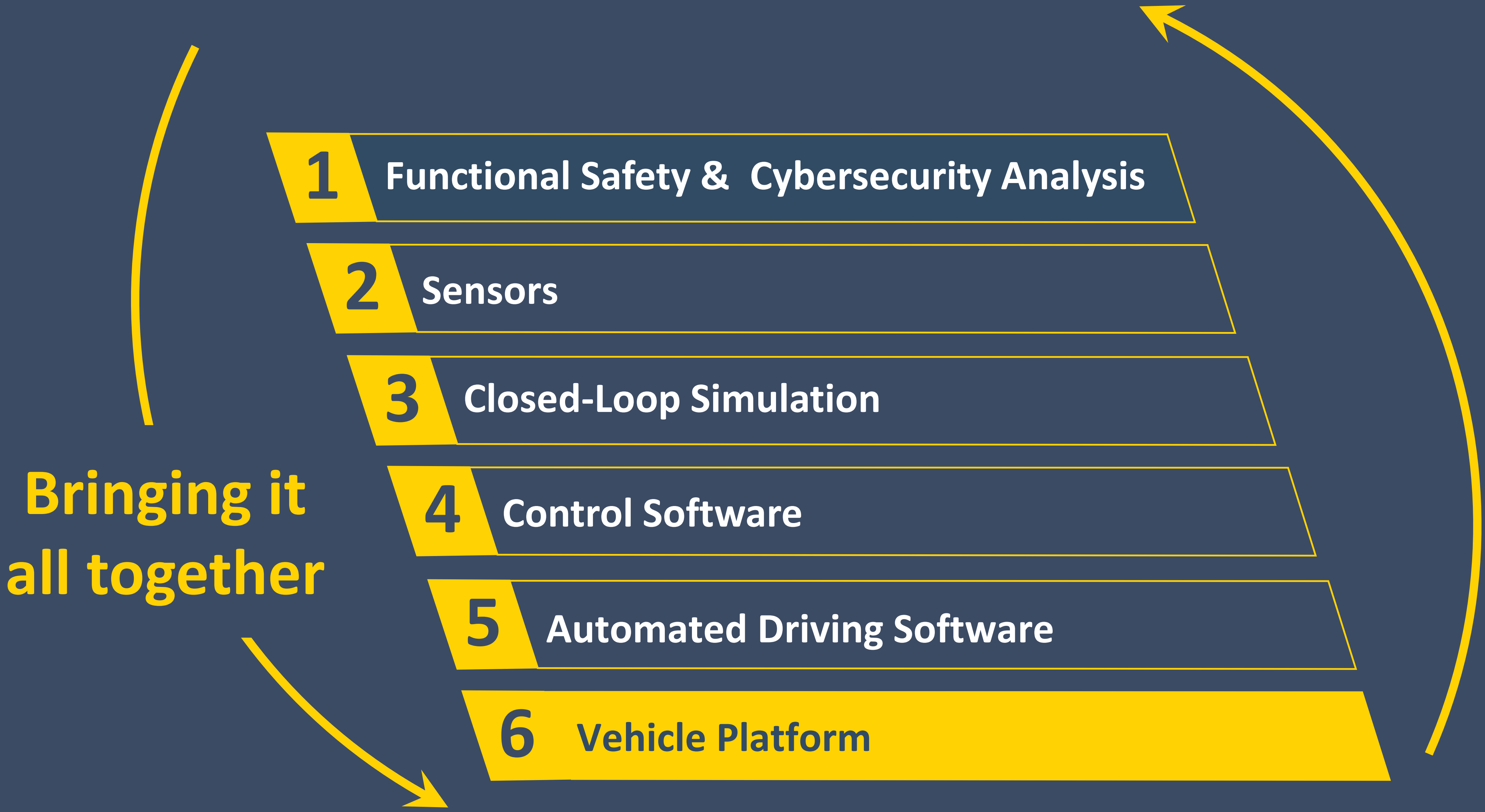
The Safing Gate (the “CHECKER”) turns the Algorithm into a fail silent (FS) component, only producing correct data or shutting down



Source: Carnegie Mellon University

Example of Primary and Safing Missions for a Planner





Bringing it all together

1 Functional Safety & Cybersecurity Analysis

2 Sensors

3 Closed-Loop Simulation

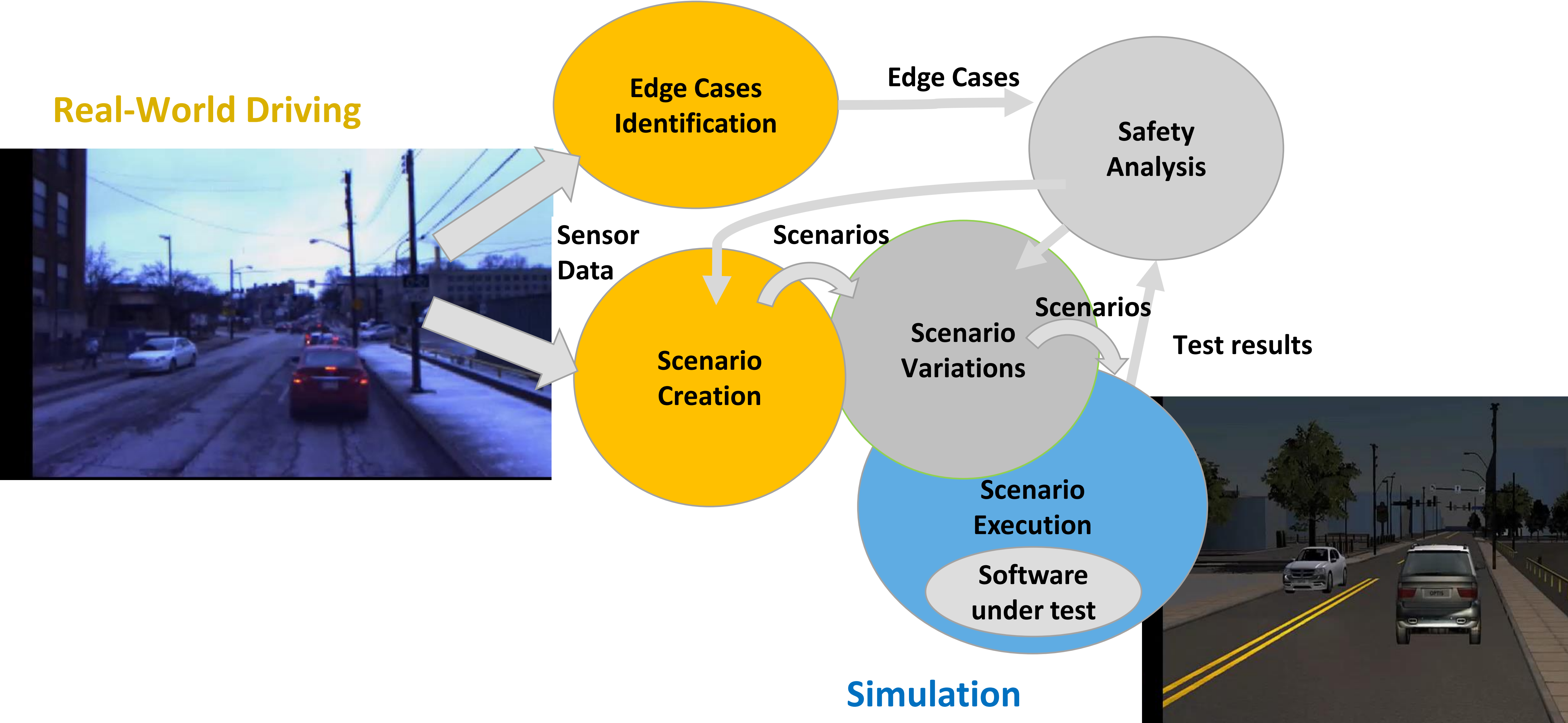
4 Control Software

5 Automated Driving Software

6 Vehicle Platform

Summary

Summary: Connecting Real-Real World Driving and Simulation to Achieve Safety of Autonomous Driving



Thank you!