foretellix
verifying autonomous systems

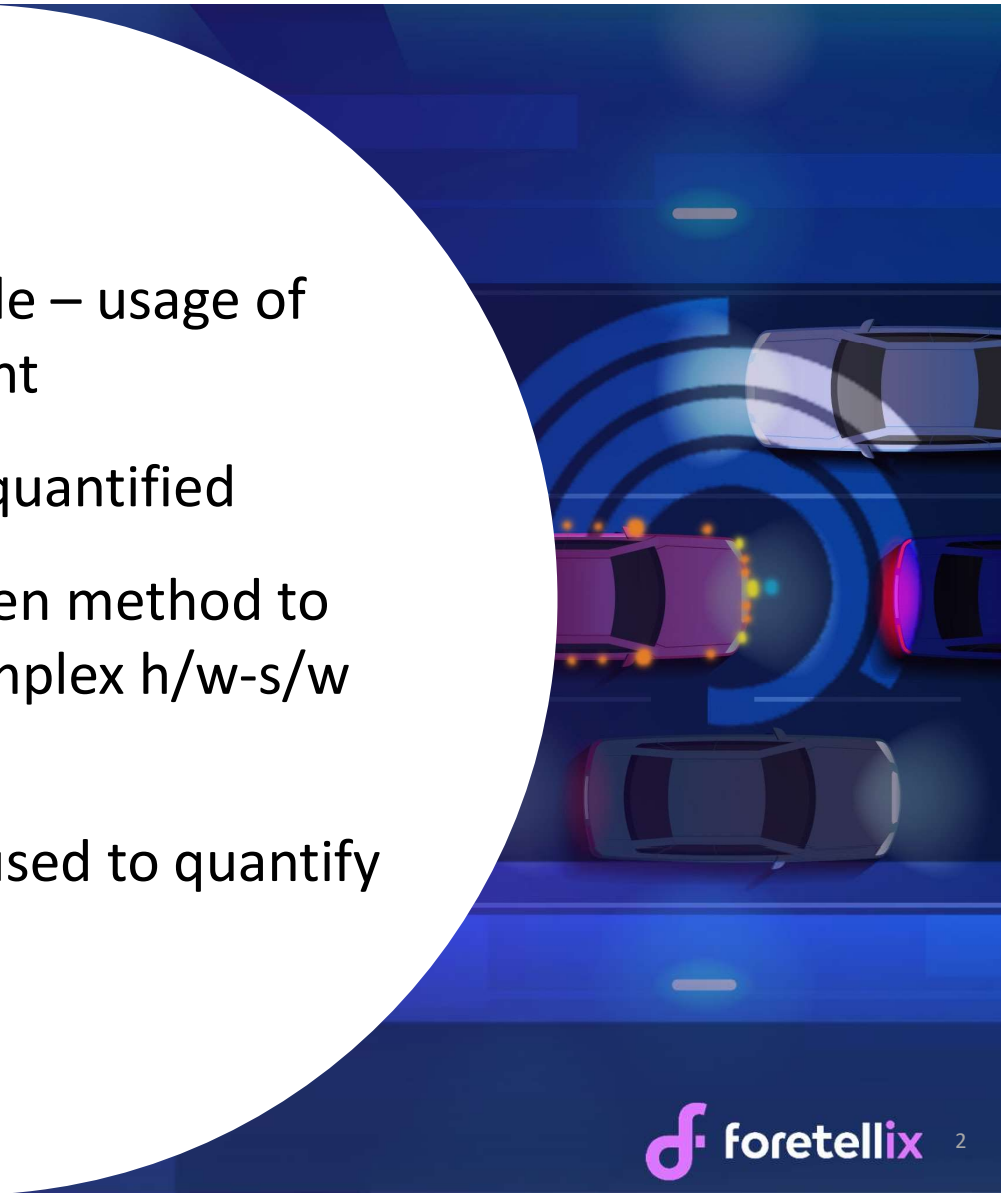
Measurable Safety – A Metric Driven Approach for Safety Assessment And Rating of AVs

CDV – Coverage Driven verification

Gil Amid
Foretellix Ltd

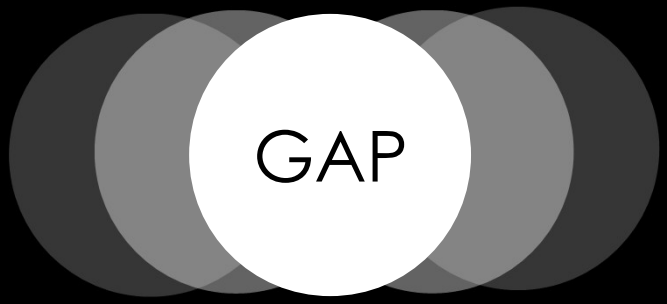
Key Messages

- AV/ADS Safety needs to be quantifiable – usage of miles and disengagement is insufficient
- AV/ADS Safety can be measured and quantified
- Coverage Driven Verification is a proven method to measure and quantify maturity of complex h/w-s/w systems
- Coverage metrics can and should be used to quantify AV/ADS safety



Safe?

- How do I 'Cover' 100s of Millions of Scenarios?
- How do I Find the Edge Cases?
- No Standards In Place
- No Rating system in place



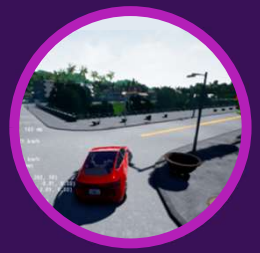
What to demand for certification?

What can be tested ?

What data can be used ?

What is "safe enough" ?

What is the required minimum ?


Simulation


X-in-the-Loop


Test Tracks


Test Driving

foretellix
verifying autonomous systems

Foretellix's Mission

Measurable Safety of Autonomous Vehicles and ADAS

Quantity
of Miles

Physically or Virtually Logging Miles and Associated Disengagements and/or Failure Rates

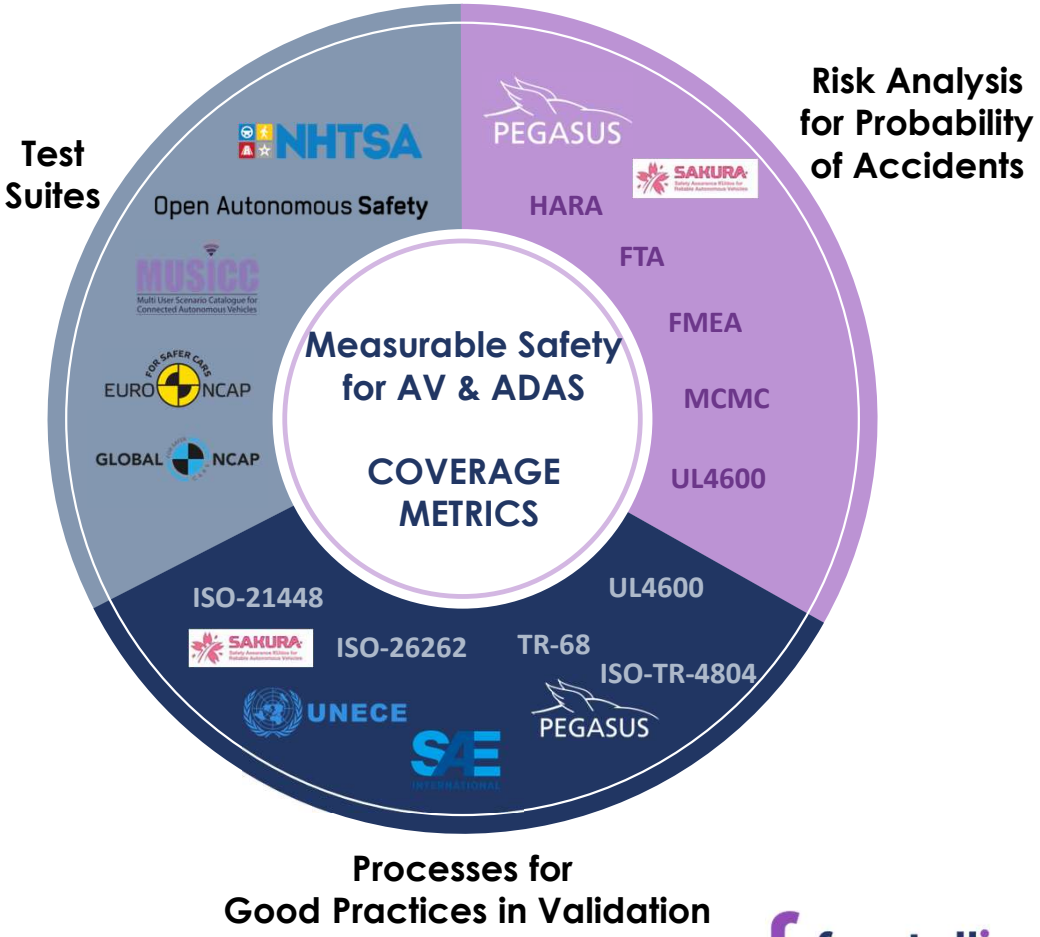
Quality
of Coverage & Performance

Successfully Exercising the Scenarios Critical for AV Safety and Extracting the Metrics to Prove It

foretellix
verifying autonomous systems

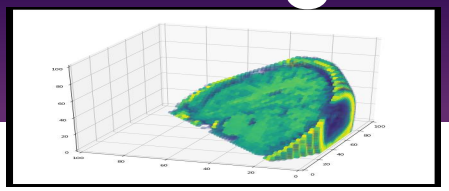
Building the AV Safety Argument

- Verification & validation coverage metrics are needed for enabling the body of evidence required for building the AV's safety case
- Coverage Metrics measure what actually happens and provides scenario coverage aggregation analytics & metrics
- Coverage metrics supports all existing and emerging safety standards & processes



foretellix

KPI/Measurement vs Coverage



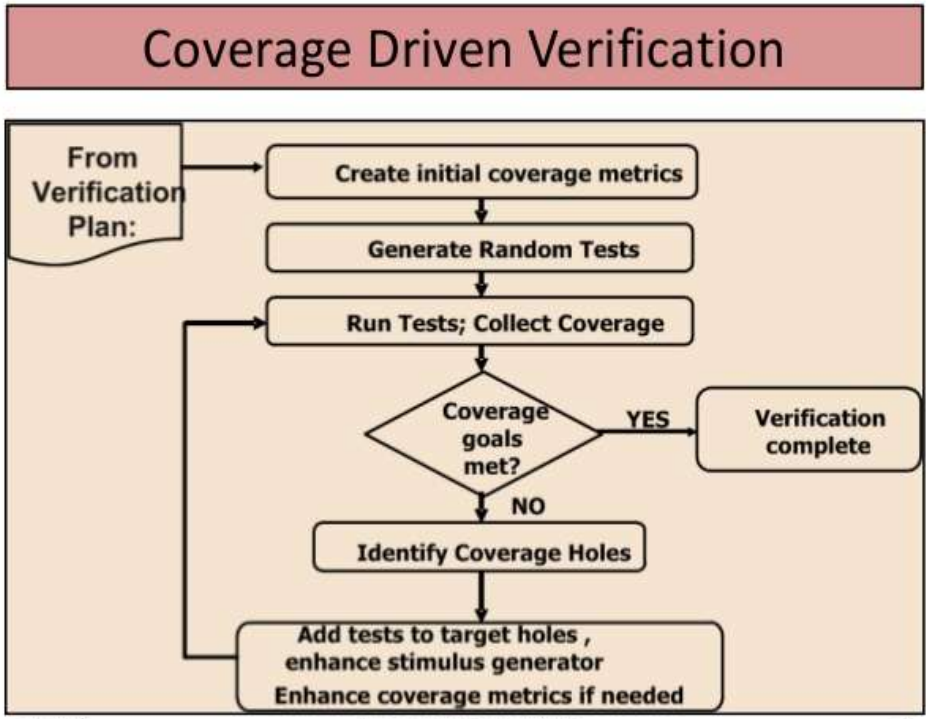
- How did the AV perform within a given ODD?
- KPI/Metrics specify the specific measurements to be analyzed, given specific test conditions /ODD. Usually – “simulation output”
- **Answering:**
  - In ODD X, How did the ego perform for all test variations in the context of “cut in” ? (aggregate of all specific measurement)
  - What was TTC, when the AV was driving at 55kph, and the other player deceleration was -3 m/s^2 ? Is it above my threshold ?

- What was actually tested, out of the possible space of testing values [per ODD]
- Coverage can be measured both on test input/settings ,as well on output/results of the tests. It can be measure on one ,two, or multiple dimensions
- **Answering:**
  - For “cut in” scenario, on a road with 2 lanes and only green cars, what % of the possible AV speeds between 50KPH and 100KPH did I test ?
  - What % of the TTC space between 0 and 3S was demonstrated during all tests ?

foretellix

Coverage Driven Verification

- The main method to verify complex VLSI/SOC designs: Microprocessors, GPUs, Network and cellular processors
- Method evolved in the early 90's
  - Intel's Pentium® floating point bug – ~$0.5B cost (1994)
- Main principles: Loop: Plan, test, measure and analyze metrics
- Goal is to maximize coverage
- Using Constrained Random Scenario/Test generation



foretellix

Putting it all together: Data Driven Measurable Safety

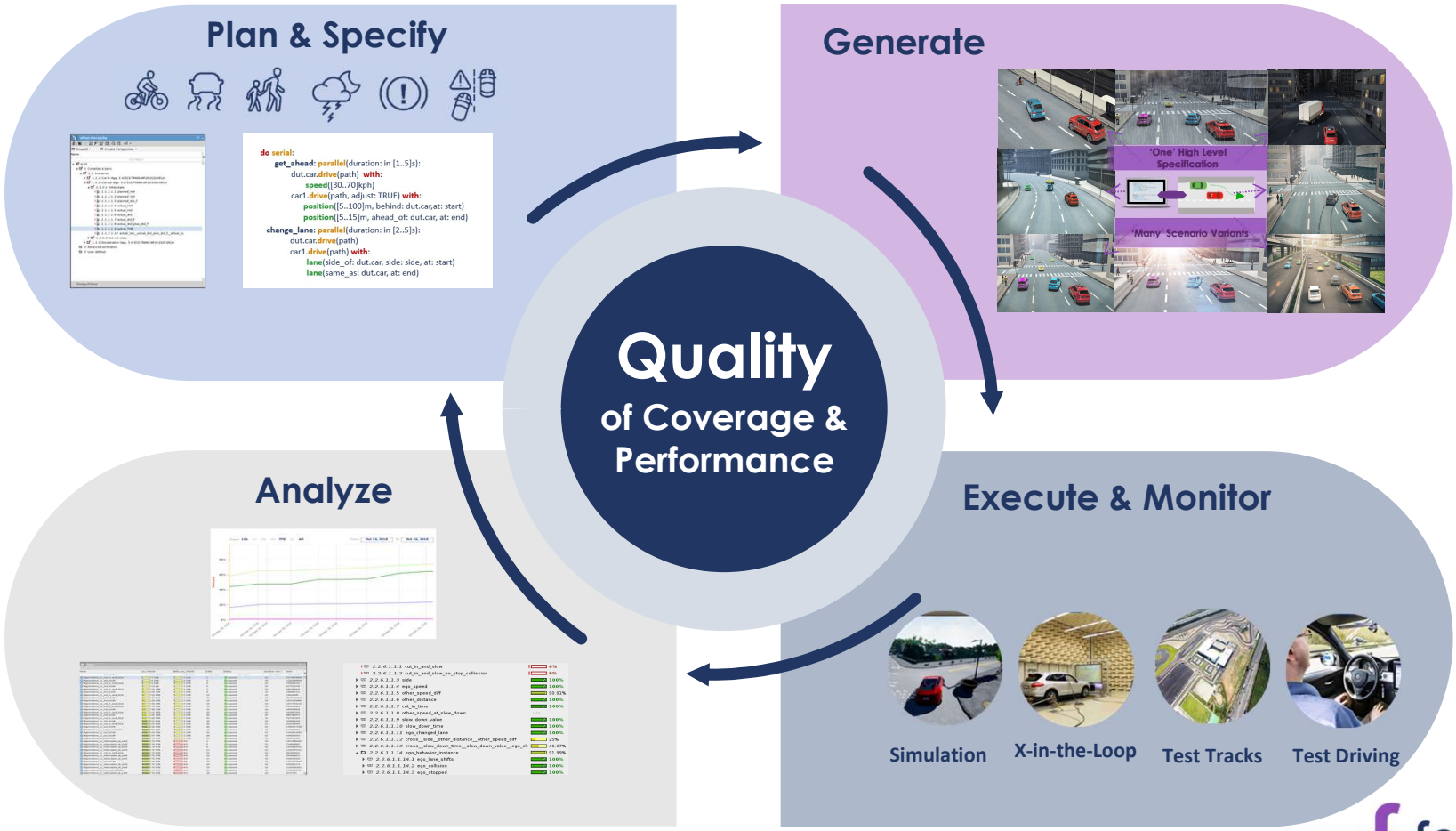
Quality of Coverage

Quantity of Miles

Simulation | X-in-the-Loop | Test Tracks | Test Driving

foretellix

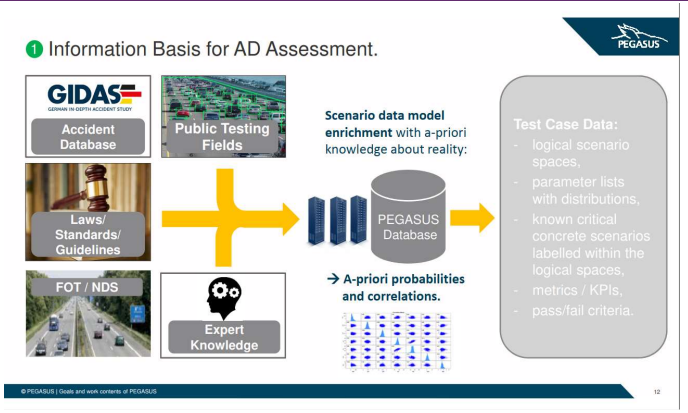
Coverage Driven Verification Methodology for Measurable Safety

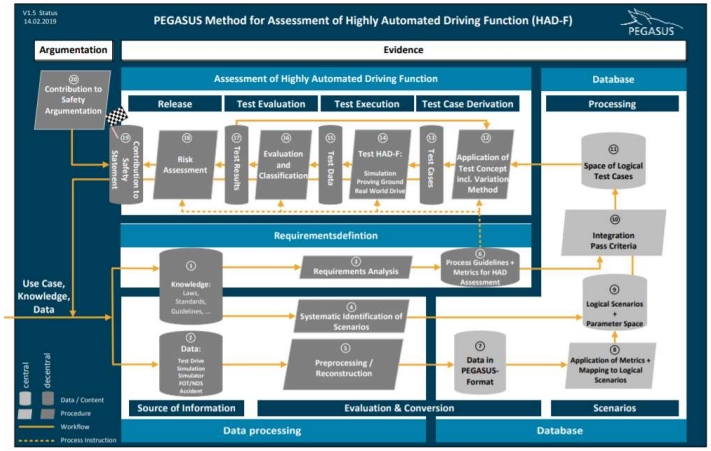


foretellix

CDV and PEGASUS method

- PEGAUS Method analyses extracted data and existing [historical] knowledge in order to create and define the required simulations space for AD assessment
- CDV complements and enhances the Pegasus approach:
  - CDV Adds the COVERAGE REQUIREMENTS as a data source for the decision process
  - Introduces constrained-random simulation generation to cover huge simulation and variation space
  - Provides methods to create unforeseeable scenarios

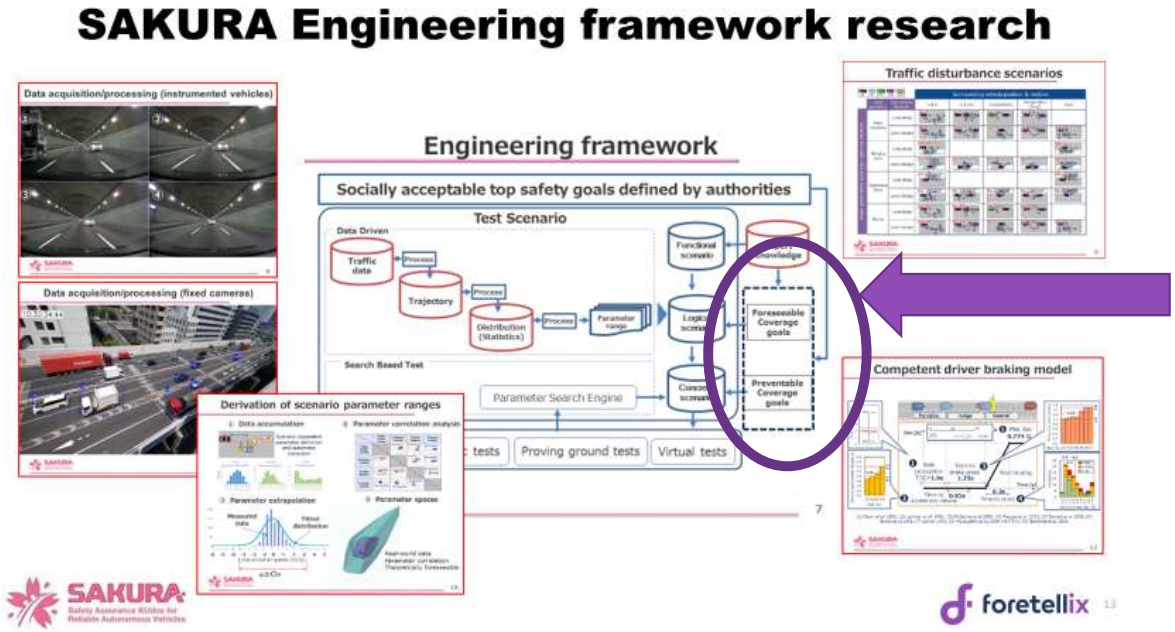




foretellix

CDV and SAKURA methods

- CDV fits with the overall framework developed in SAKURA project, and proposed to ISO and UNECE/VMAD.
- Coverage plans and goals are expert knowledge source for scenarios. Provides methods to create unforeseeable scenarios



Coverage Goals As Source of Scenarios

foretellix

The Building Blocks: Data Driven Measurable Safety

Scenario Libraries

Standard Templates
Standard ODDs,
Test Libraries and procedures

Metrics and rating analysis,
Standards and regulations:
Safety Ratings, Thresholds
Risks

foretify™

Quality of Coverage

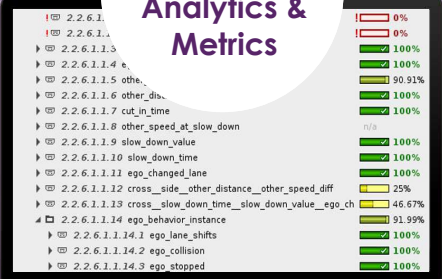
Quantity of Miles

Planning & Scenario Description using M-SDL

```
do serial:
    get_ahea
        dut.car.
            speed(|>
        car1.drive(path, adjust: TRUE) with:
            position([5..100]m, behind: dut.car,at: start)
            position([5..15]m, ahead_of: dut.car, at: end)
    change_lane: parallel(duration: in [2..5]s):
        dut.car.drive(path)
        car1.drive(path) with:
            lane(side_of: dut.car, side: side, at: start)
            lane(same_as: dut.car, at: end)
```

Generation of Scenario Variants

Coverage Aggregation Analytics & Metrics




Simulation


X-in-the-Loop


Test Tracks


Test Driving

foretellix

THANK YOU JAPAN FOR THE WIDE CONTRIBUTION IN ALL THESE DOMAINS

The Building blocks are forming….

UNECE/GRVA – New Assessment and Test Methods:
Scenario Catalogue

Testing Methods

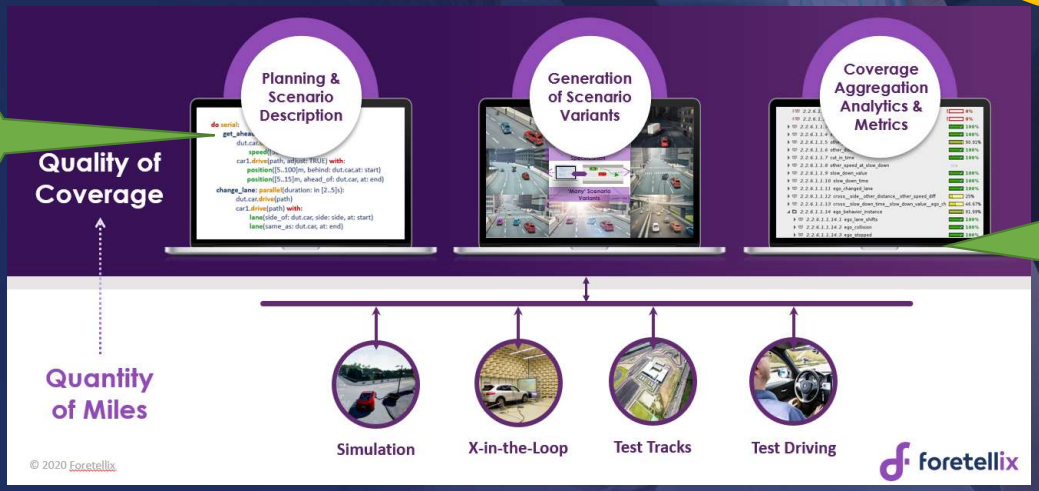
Regulatory Thresholds
UNECE, ISO, SAE

Scenario Libraries

Standard Templates
Standard ODDs,
Test Libraries and procedures

Metrics and rating analysis,
Standards and regulations:
Safety Ratings, Thresholds
Risks

ASAM
OpenSCENARIO
2.0



Foretellix's
coverage analysis.

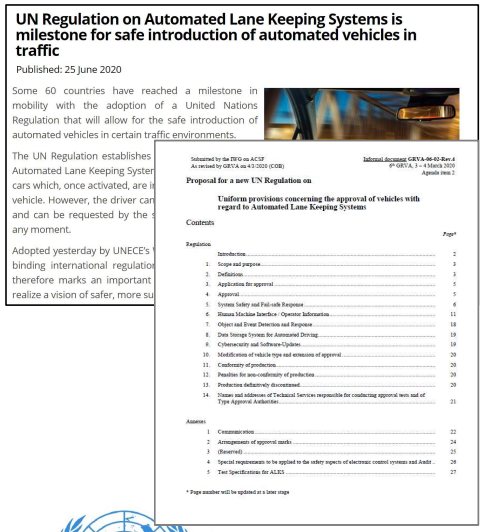
foretellix

A Pragmatic Example:

Applying CDV to Verify Regulatory Compliance – ALKS regulation.

ALKS UNECE Regulation is Approved. (UN Reg. 157)

- ALKS - Automated Lane Keeping System. The system controls the lateral and longitudinal movement of the vehicle for extended periods without further driver command
- This UNECE Regulation is the **first ever level 3 ADS regulation**
  - Approved on 24th of June 2020 and will be in force on January 2021
- ALKS's ODD
  - Roads where pedestrians and cyclists are prohibited
  - A physical separation exists and divides the traffic moving in opposite directions
  - The operational speed is limited to 60 km/h maximum.
- The regulation specifies guidance for 3 critical scenarios for testing and simulation (in addition to other testing requirements) – Specific contribution from Japan


UN Regulation on Automated Lane Keeping Systems is milestone for safe introduction of automated vehicles in traffic

Published: 25 June 2020

Some 60 countries have reached a milestone in mobility with the adoption of a United Nations Regulation that will allow for the safe introduction of automated vehicles in certain traffic environments.

The UN Regulation establishes ... Automated Lane Keeping Syster... cars which, once activated, are i... vehicle. However, the driver car... and can be requested by the ... any moment.

Adopted yesterday by UNECE's ... binding international regulatio... therefore marks an important ... realize a vision of safer, more su...

Proposal for a new UN Regulation on

Uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems

Contents

Page*

Regulation

1. Introduction ... 2
2. Scope and purpose ... 3
3. Definitions ... 3
4. Application for approval ... 5
5. Approval ... 5
6. System Safety and Fail-safe Response ... 6
7. Human Machine Interface / Operator Information ... 11
8. Object and Event Detection and Response ... 18
9. Data Storage System for Automated Driving ... 19
10. Cybersecurity and Software Updates ... 19
11. Modification of vehicle type and extension of approval ... 20
12. Conformity of production ... 20
13. Penalties for non-conformity of production ... 20
14. Production definitively discontinued ... 20
15. Names and addresses of Technical Services responsible for conducting approval tests and of Type Approval Authorities ... 21

Annexes

1 Communication ... 22
2 Arrangements of approval marks ... 24
3 (Reserved) ... 25
4 Special requirements to be applied to the safety aspects of electronic control systems and Audit ... 26
5 Test Specifications for ALKS ... 27

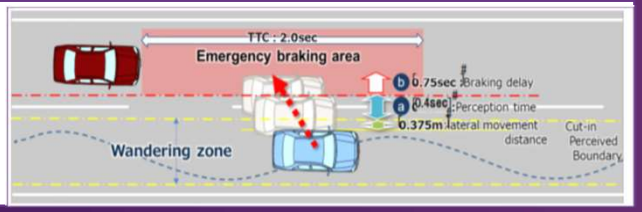
* Page number will be updated at a later stage

UNECE

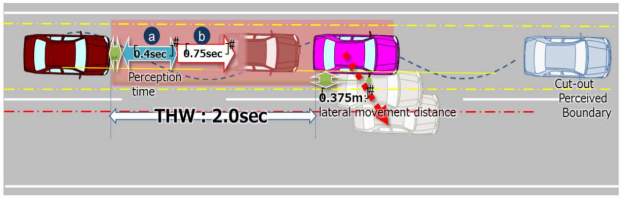
foretellix

ALKS Scenarios

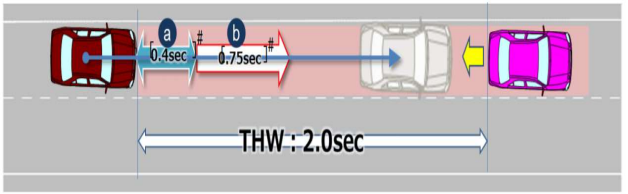
Cut-in - A car cuts-in to the ego's lane (in front of the ego)



Cut-out - A leading car cuts out in front of the ego



Deceleration - A leading car in front of the ego decelerates



foretellix

Cut Out - Terminology and Notations

Initial Velocity

Ve0 = Ego vehicle

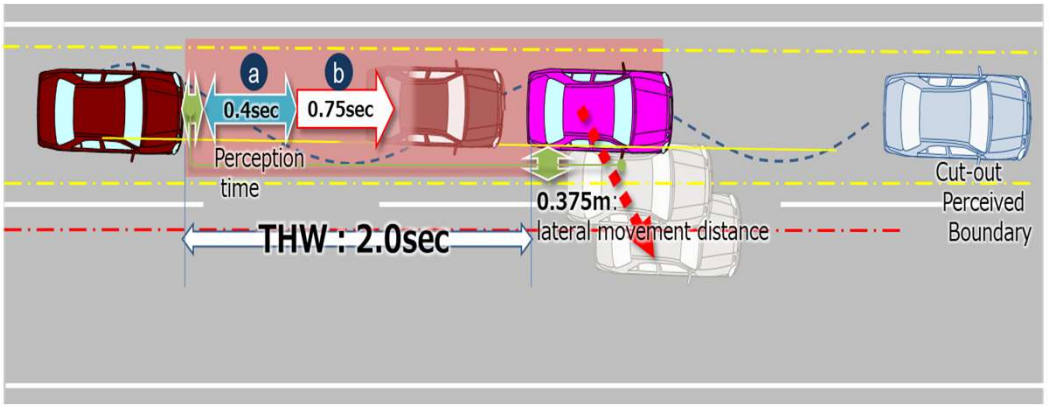
Vo0 = Leading vehicle in lane or in adjacent lane

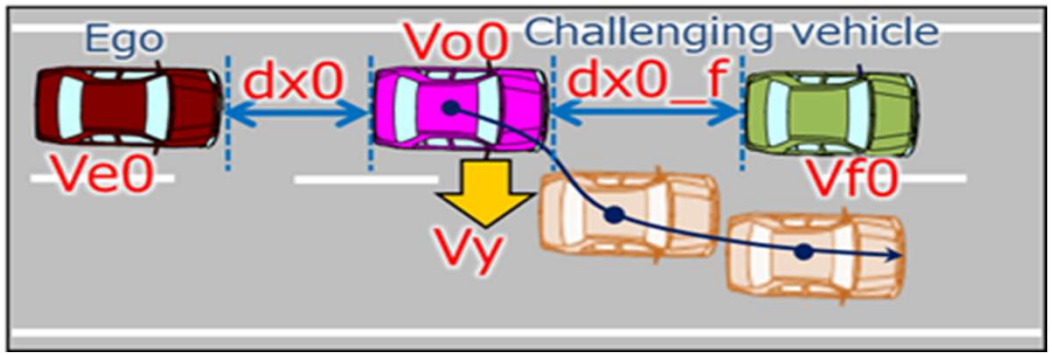
Vf0 = Vehicle in front of leading vehicle in lane

Initial Distance

dx0 = Distance in Longitudinal direction between the front end of the ego vehicle and the rear end of the leading vehicle

dx0_f = Distance in longitudinal direction between front end of leading vehicle and rear end of vehicle in front of leading vehicle

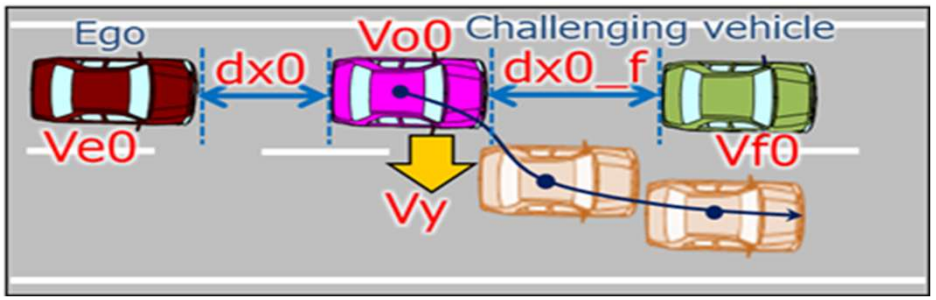




Vy =Leading vehicle lateral velocity

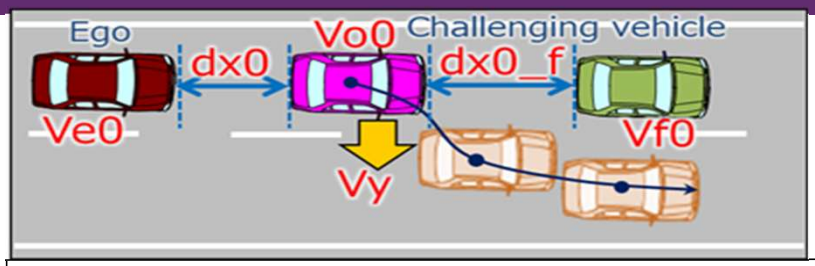
M-SDL Cut Out Scenario Implementation

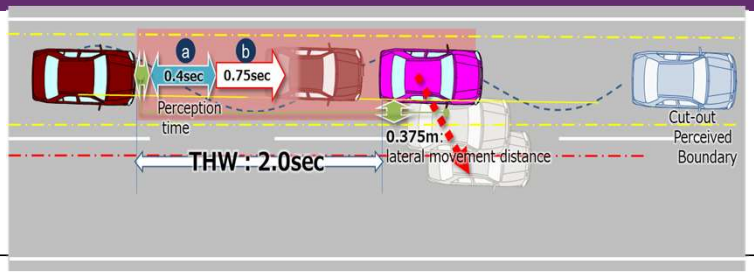
```
do serial():

    dut_speed_up: parallel( duration: [6..10]second):
        dut.car.drive(path: path) with:
            ego_mode(alk)
        other_car.drive(path: path, adjust: false)
        in_front_car.drive(path:path)

    lead: parallel(duration: [1..3]second):
        dut.car.drive(path: path) with:
            ego_mode(alk)
        other_car.drive(path: path, adjust: false) with:
            lane(same_as: dut.car)
            position(time: [THW..THW], ahead_of: dut.car, at:end)
            speed([0..0]kph, faster_than: dut.car, at: end )
        in_front_car.drive(path: path, adjust: false) with:
            lane(same_as: other_car)
            speed([0..0]kph)
            position([dxo_f+in_front_car.length ,ahead_of:other_car, at:end )

    cut_out: parallel(duration: [1..4]second):
        dut.car.drive(path: path)
        other_car.drive(path: path, adjust: false) with:
            change_lane()
        in_front_car.drive(path: path, adjust: false) with:
            keep_lane()
            speed(speed: [0..0]kph)
```



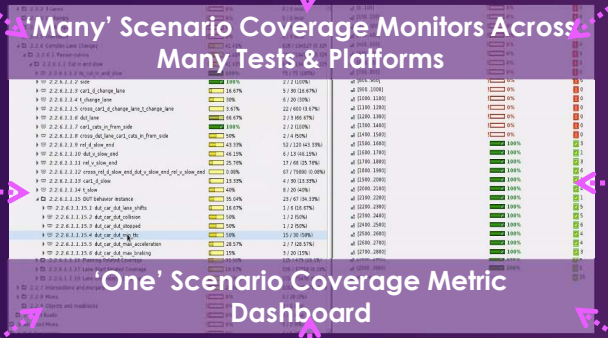
foretellix

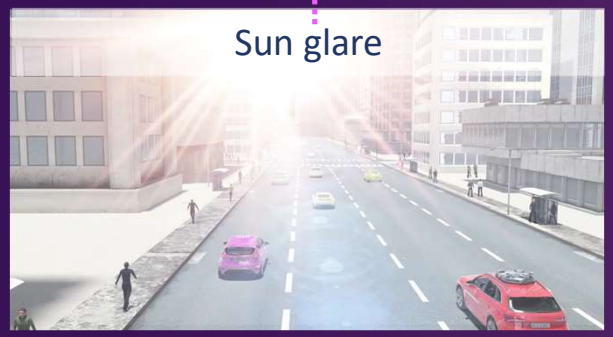
Cut Out- Coverage and Measurements Definitions






```
!actual_ttc := sample(get_min_ttc(),@cut_out.end) with:
  cover(it,unit:ms,every: 100,range:[0..3000],text:"Minimal time to collision for ego car")

!actual_Ve0 := sample(dut.car.state.speed,@lead.end) with:
  cover(it,unit:kph,range:[0..60],every:10,text:"Actual velocity of ego at cut out start (can go up to 60kph by spec)")


!actual_Vy := sample(other_car.state.avg_lateral_speed,@cut_out.end) with:
     cover(it,unit:kph,range:[1..10],every:1,text:"Actual lateral speed of the cutting out car")

!actual_THW := sample(actual_dx0/actual_Ve0,@lead.end) with:
    cover(it, unit:millisecond, range:[0..5000], every:500, text : "Actual THW when cut-out car starts cutting-out")
```





foretellix
verifying autonomous systems

vPlan Hierarchy

ALKS

Ex	UNR	Name	Overall Average Grade	Overall Covered
		(no filter)	(no filter)	(no filter)
		ALKS	48.29%	191 / 1644 (11.62%)
		1 Compliance basic	48.29%	191 / 1644 (11.62%)
		1.1 Scenarios	48.29%	191 / 1644 (11.62%)
		1.1.1 Cut In (App. 3 of ECE-TRANS-WP29-2020-081e)	54.23%	46 / 167 (27.54%)
		1.1.2 Cut out (App. 3 of ECE-TRANS-WP29-2020-081e)	51.71%	88 / 653 (13.48%)
		1.1.2.1 Initial state	62.87%	80 / 614 (13.03%)
		1.1.2.1.1 planned_Ve0	100%	6 / 6 (100%)
		1.1.2.1.2 planned_Vo0	100%	6 / 6 (100%)
		1.1.2.1.3 planned_dxo_f	100%	10 / 10 (100%)
		1.1.2.1.4 actual_Ve0	66.67%	4 / 6 (66.67%)
		1.1.2.1.5 actual_Vo0	16.67%	1 / 6 (16.67%)
		1.1.2.1.6 actual_dx0	40%	4 / 10 (40%)
		1.1.2.1.7 actual_dx0_f	90%	9 / 10 (90%)
		1.1.2.1.8 actual_dx0_plus_dx0_f	70%	7 / 10 (70%)
		1.1.2.1.9 actual_THW	40%	4 / 10 (40%)
		1.1.2.1.10 actual_Ve0__actual_dx0_plus_dx0_f_	5.37%	29 / 540 (5.37%)
		1.1.2.2 Cut out state	40.56%	8 / 39 (20.51%)
		1.1.3 Deceleration (App. 3 of ECE-TRANS-WP29-2020-0	38.92%	57 / 824 (6.92%)
		2 Advanced verification	n/a	0 / 0 (n/a)
		3 User defined	n/a	0 / 0 (n/a)

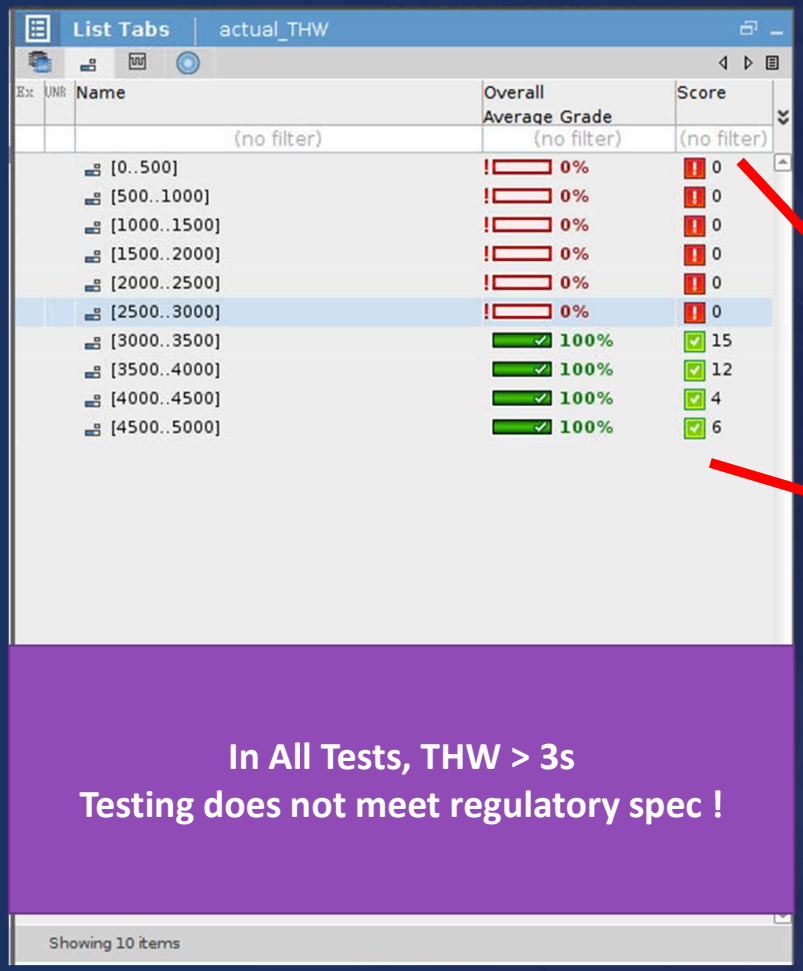
Showing 20 items

Productivity

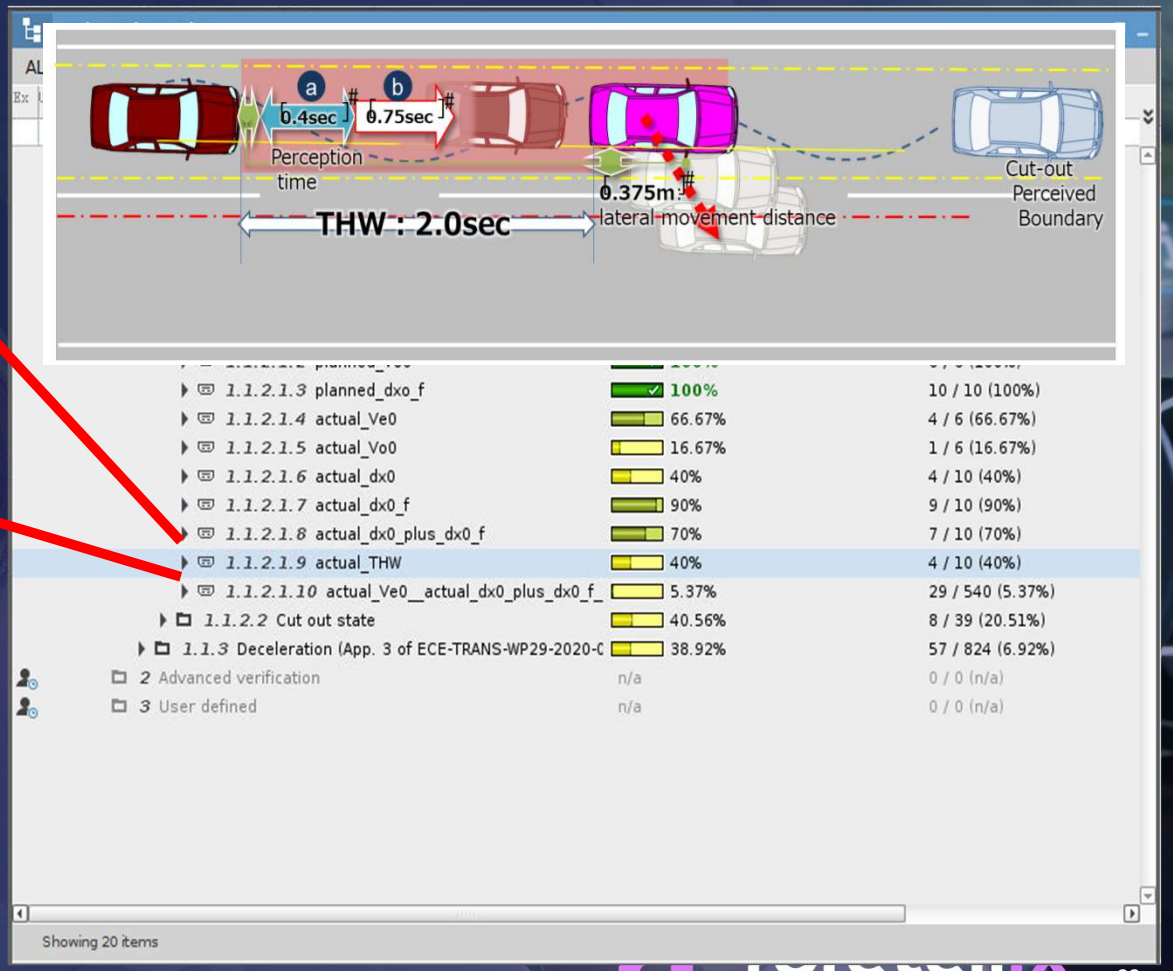
Portability

foretellix
verifying autonomous systems

THW COVERAGE/TESTING HOLE



In All Tests, THW > 3s
Testing does not meet regulatory spec !

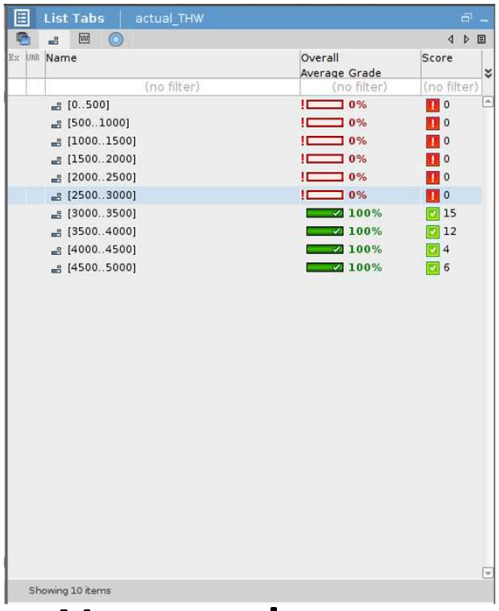


verifying autonomous systems

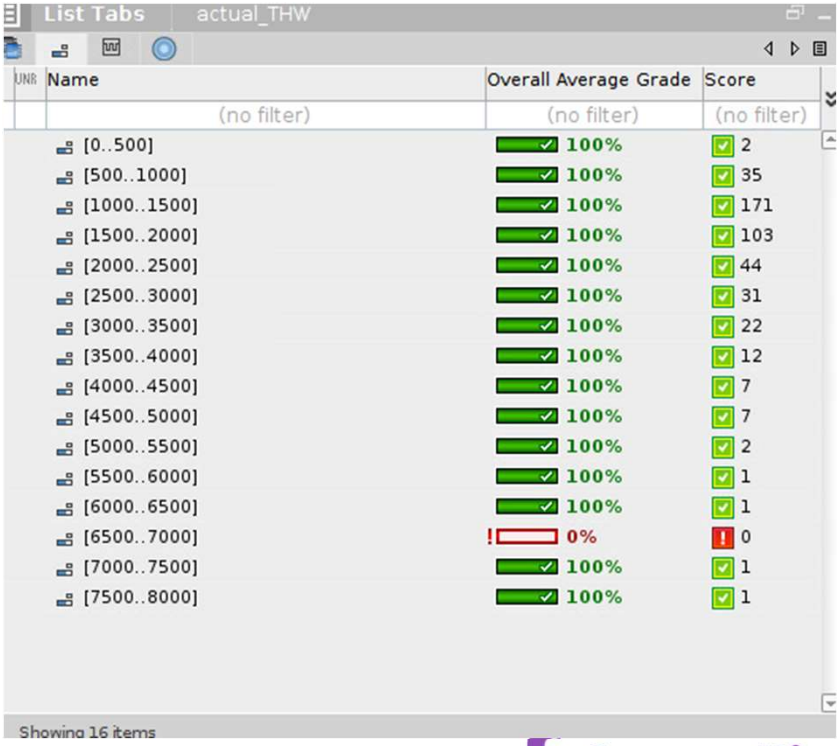
Re-tuning EGO Parameters: THW issue solved

- Re-tuning solved the issue

Before



After



Very good coverage of all risky areas , and regulatory spec.

foretellix

The Building Blocks: Data Driven Measurable Safety

Scenario Libraries

Standard Templates
Standard ODDs,
Test Libraries and procedures

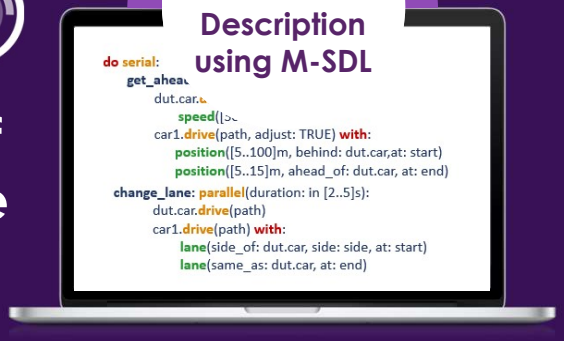
Metrics and rating analysis,
Standards and regulations:
Safety Ratings, Thresholds
Risks

foretify™

Quality of Coverage

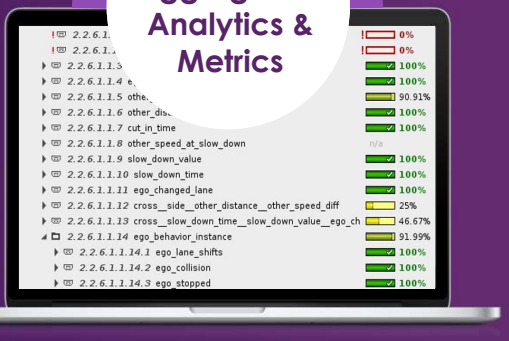
Quantity of Miles

Planning & Scenario Description using M-SDL



Generation of Scenario Variants

Coverage Aggregation Analytics & Metrics




Simulation


X-in-the-Loop


Test Tracks


Test Driving

foretellix

Summary: Measurable Safety – Coverage Metrics

- **Usage of Coverage Metrics Supplies:**
  - **Goals for testing**
  - **Threshold of quality and safe behaviors**
  - **Relative comparison between AVs**

- With Coverage Driven Verification AND Using standard templates, standard testing libraries and ODDs – you have a complete, **measurable**, certification system

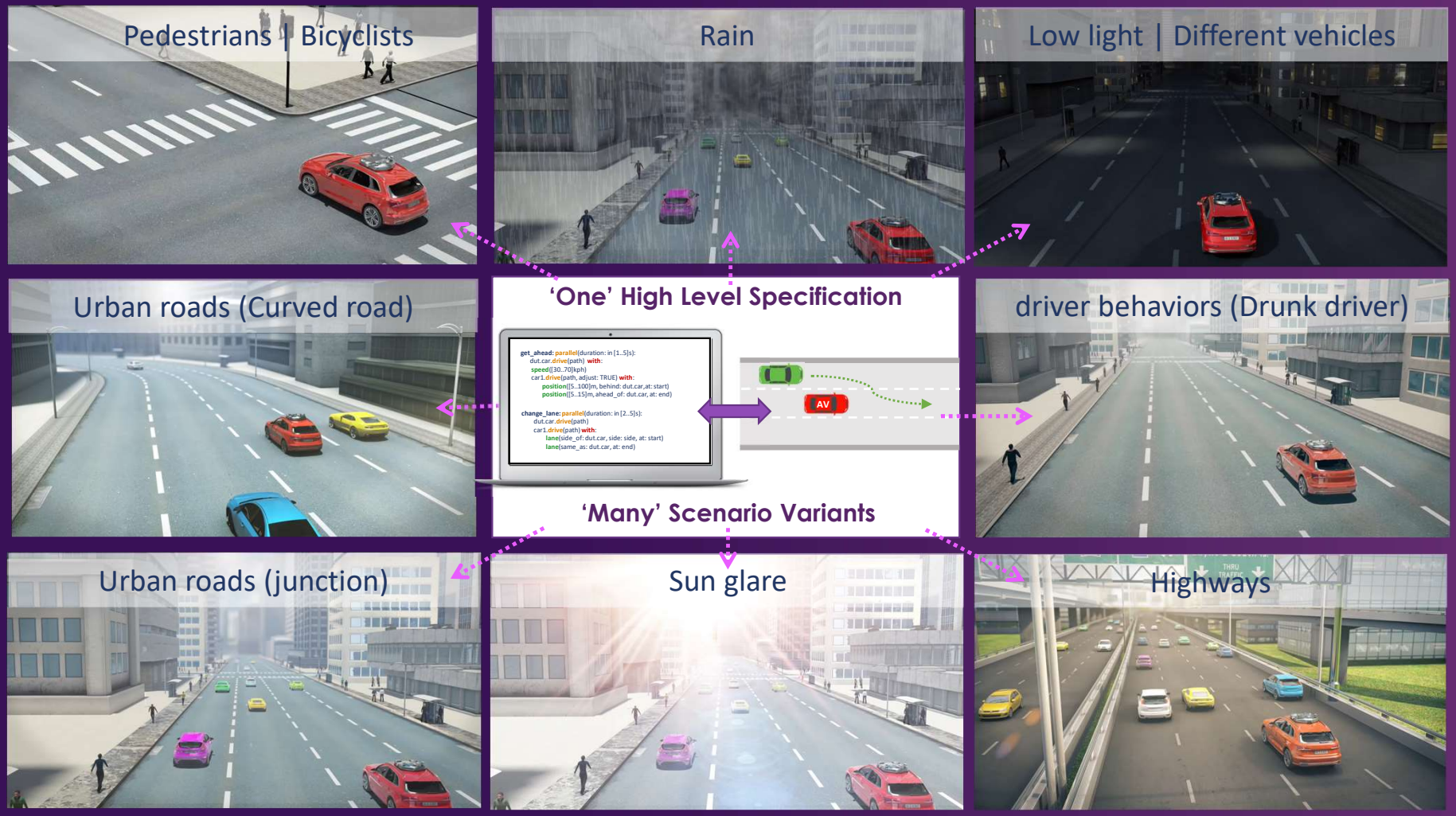
25

For More Information

www.Foretellix.com
info@foretellix.com
blog.foretellix.com

foretellix
verifying autonomous systems

Backup Slides



Portability Across Testing Platforms & ODDs

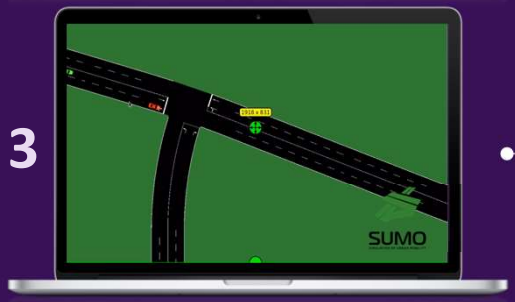
Portability

Example Simulators & ODDs

ODD 1

ODD 2

ODD 3



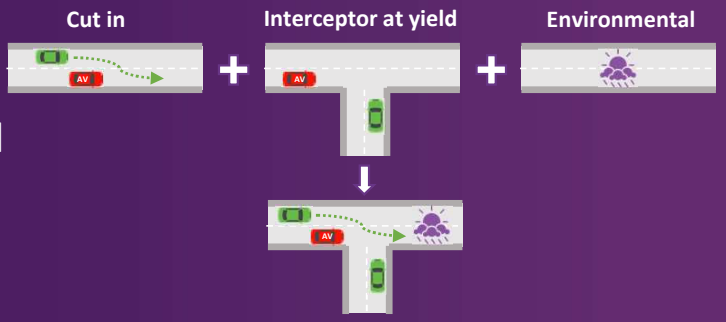
Simulation | X-in-the-Loop | Test Tracks | Test Driving

foretellix
verifying autonomous systems

Mixing Scenarios

Provability Productivity

- Create many meaningful scenarios and extend your coverage by mixing and overlaying different scenarios
- Create Combinations of Combinations of edge cases and scenarios a human cannot think about
- Create more powerful & reusable scenario libraries



metamoto®

metamoto®

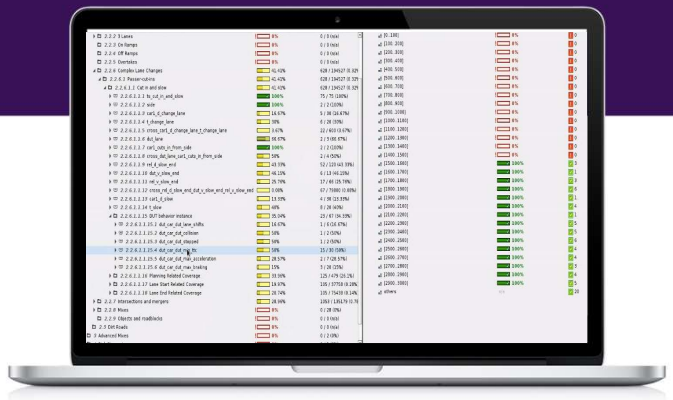
metamoto®

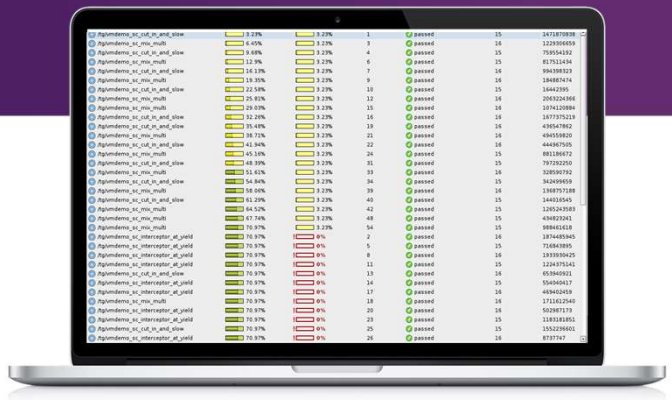
foretellix

Provability Productivity

Coverage Aggregation Analytics & Metrics

- Independently monitor for scenarios and parameter coverage
- Measure what actually happens
- Automatically optimize based on coverage and KPIs



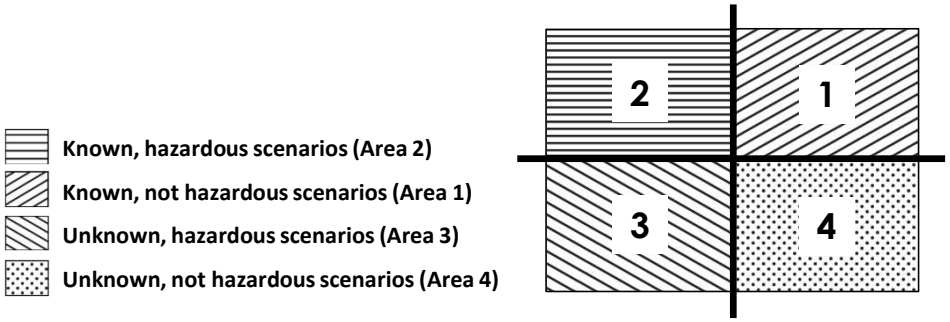


foretellix

Safety Of The Intended Functionality (SOTIF)

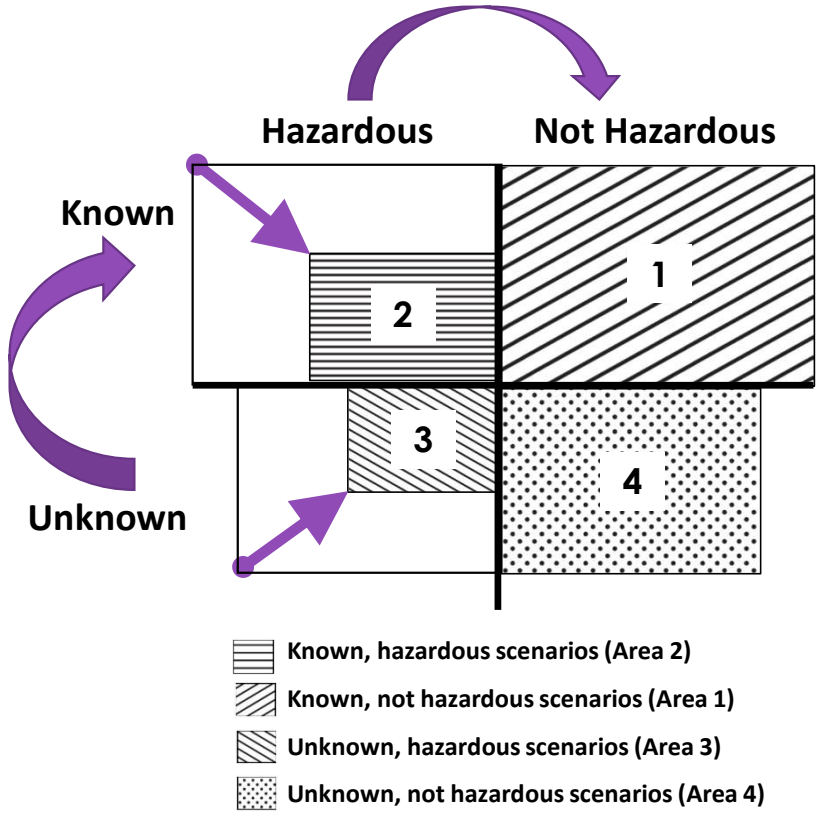
"Absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons"

- SOTIF (ISO 21448) is dealing with Safety of Autonomous Systems, and provides guidance on design, verification, and validation measures
- SOTIF breaks down the possible scenario space to 4 categories
- "The ultimate goal is to evaluate the safety in **area 2 and area 3** and to provide an argument that these areas are **sufficiently small and the resulting residual risk is acceptable"**



foretify™ – The Full SOTIF Flow

- Foretify™ is an automation and analysis tool, implementing the Coverage Driven Verification methodology
- Foretify™ provides a systematic approach to reduce both area 2 and area 3
- Foretify™ supports the SOTIF process, intended for reaching acceptable levels of risk



foretellix
verifying autonomous systems

For More Information

www.Foretellix.com
info@foretellix.com
blog.foretellix.com

foretellix
verifying autonomous systems