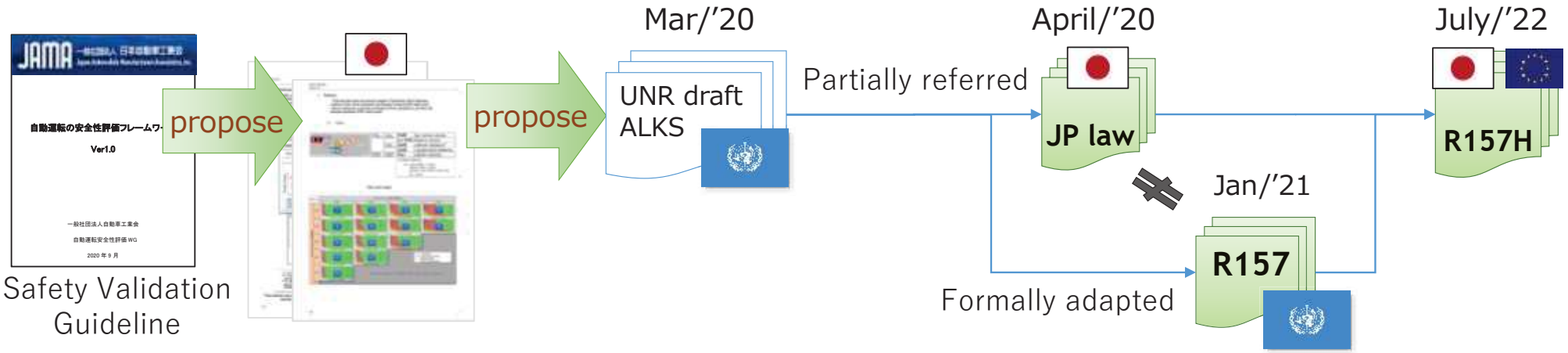
SIP adus SAKURA
Safety Assurance Breakout Workshop

Satoshi Taniguchi

12th/Nov/2020

UN regulation for Lv3 low seed on highway

✓ UN regulation for Lv3 low speed lane keep on highway was established as R157 in March/'20.



ALKS Highlights

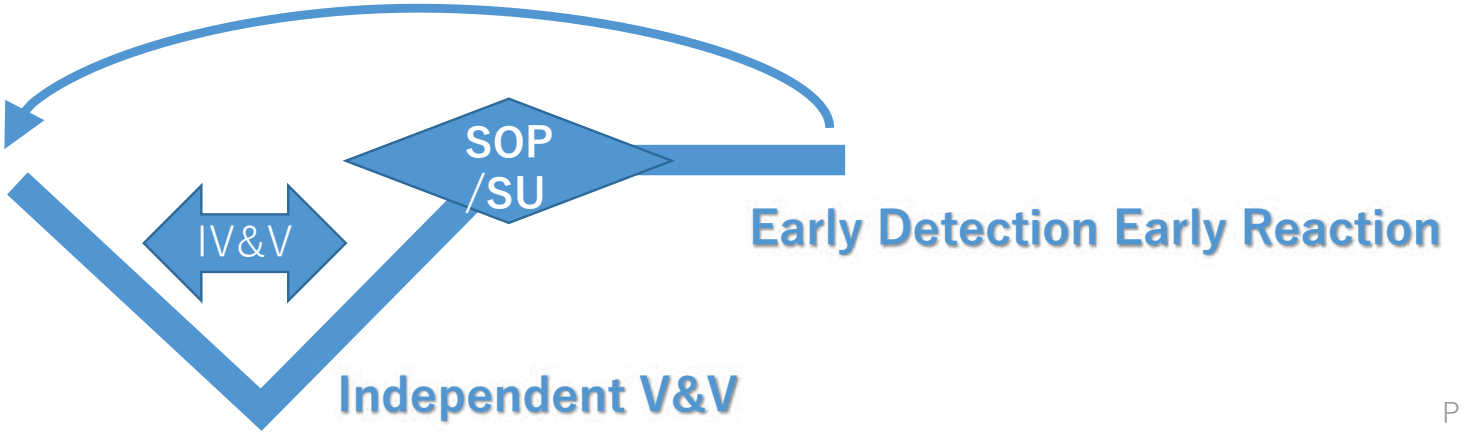
【 Performance Criteria 】

■ AD shall avoid accident which competent and careful human driver can avoid.

≦

【 Process Requirement 】

■ Safety Management System



UN regulation next step

✓ Lv4 MaaS, and Lv3 Highway Chauffeur is just started to be discussed after R157.

Lv3 low speed lane keep

are added to ALKS member for next step

Lv3 Highway Chauffeur

Lv4 MaaS

AD safety assurance regulation and standard rand scape

✓ Many initiatives on safety case standard because of audit business chance.
✓ Less collaboration on safety validation methodology.

Regulation

WP29(Vehicle Type Approval)

GRVA(Automated Driving):Post ALKS

FRAV
(Functional Requirement)

VMAD
(Validation Methodology)

refer ?

? US Government is less aggressive about national regulation

CalSTA
NEW YORK Department of Transportation

- State laws
- Demonstrations

NHTSA

- "AV 2.0" guidance
- "AV TEST" initiative
- Research Grant

refer ?

Standard

ISO International Organization for Standardization

ISO34502 | DTR4804 | ISO21448

IEEE P2846

intel

Safety Validation Guideline

Safety Case Guideline

PSDO

JAMA

SAE ITC Automated Vehicle Safety Consortium

Input to SAE J-docs

Safety Assurance Guideline

SAE INTERNATIONAL

ORAD

MoU(June/'20)

UL

EDGE CASE RESEARCH

ANSI/UL4600
(Safety Case)

Japanese collaboration on safety validation methodology

✓ In order to achieve both sufficient test coverage and practicality a safety validation platform which comprise a scenario database and a virtual testing environment needs to be established.

DIVP SIP Cabinet Office

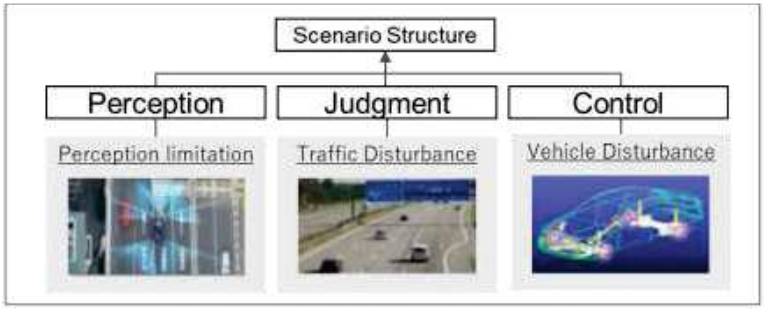
DIVP™ Objectives

- *Open Standard Interface*
- *Reference platform with reasonable verification level*
- *Environment & Sensor paired models based approach*

SAKURA METI

SAKURA Objectives

- *Standardized engineering process*
- *Scenario based safety assurance methodology*
- *Scenario database*



Regulations for level 3 systems on highways

Regulation
Safety criteria & Test requirements
Regulation

ISO34502 Engineering framework and scenario based approach

Standard
Test Scenario Derivation Process
Standard

OpenDRIVE, OpenSCENARIO, ···

ASAM
Technical Standard
Specification of driving maneuvers and test scenarios
Technical Standard

Japan White Paper on AD safety assurance

STRATEGY JAMA

RESEARCH STANDARDIZATION

DIVP SAKURA

Background and top level safety requirement

Background (UN157)

United Nations ECE/TRANS/WP.29/2020/81

Economic and Social Council

Distr.: General
6 April 2020

Original: English

Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System

Economic Commission for Europe

Inland Transport Committee

World Forum for Harmonization of Vehicle Regulations

181st session
Geneva, 23-25 June 2020
Item 4.12.6. of the provisional agenda
1958 Agreement:
Consideration of proposals for new UN Regulations submitted by the Working Parties subsidiary to the World Forum

[System Safety] the automated vehicle should be **free of unreasonable** safety risks to the driver and other road users.

[Safety Vision] automated vehicle systems, under their operational domain (OD), **shall not cause any** traffic accidents resulting in injury or death that are **reasonably foreseeable and preventable**.

Top level Safety Requirement

AD systems **free of unreasonable** safety risks

Safety evaluation methodology

Top level Safety Requirement

AD systems **free of** **unreasonable** safety risks

Safety evaluation methodology

Does the AD system **cover all** **reasonable** safety risks?

Our proposal:

① Physics Principles based scenario approach + **② Safety requirements based on reasonable foreseeability and preventability**

Safety evaluation methodology

Top level Safety Requirement

AD systems **free of** **unreasonable** safety risks

Safety evaluation methodology

Does the AD system **cover all** **reasonable** safety risks?

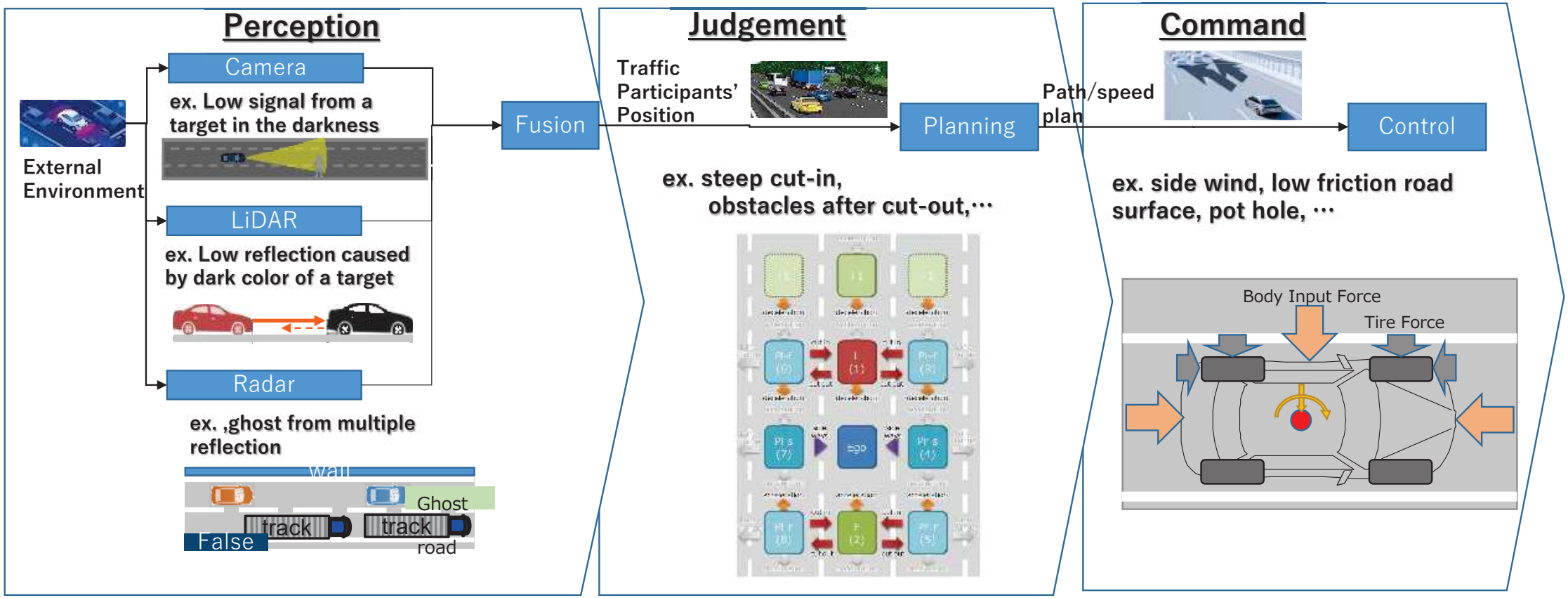
Our proposal:

① Physics Principles based scenario approach

+

② Safety requirements based on reasonable foreseeability and preventability

Decomposition of dynamic driving tasks (DDT)



- Dynamic driving tasks can be decomposed into subtasks involving Perception, Judgement and Command processes.
- Each of these sub functions are associated with specific physics principles.

Scenarios that account for safety-relevant root causes for DDT

Perception Scenario

ex.

Camera

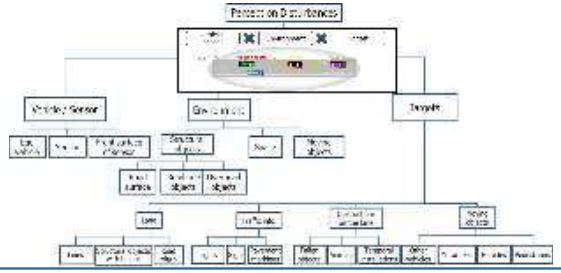
Low signal from a target in the darkness

Lidar

. Low reflection caused by dark color of a target

Radar

ghost from multiple reflection

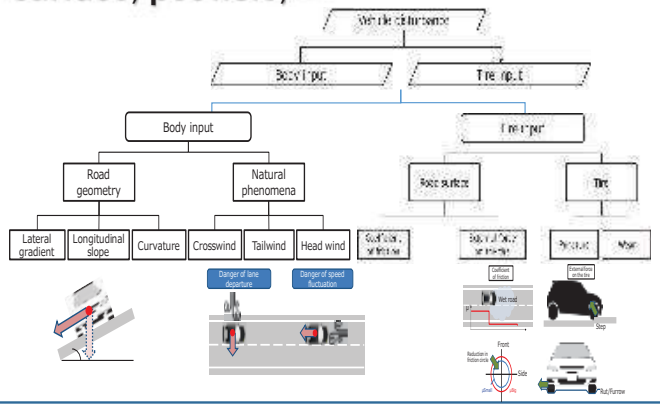


Traffic Disturbance Scenario

ex. steep cut-in,
obstacles after cut-out,…

Vehicle Stability Disturbance Scenario

ex. side wind, low friction road surface, pot hole, …



- By logically structuralizing scenarios in accordance with the **physics principles** of the AD system, it is possible to provide a holistic coverage of **all the safety-relevant root causes** for given dynamic driving tasks.
- We apply this rationale to develop three scenario categories: perception (perception disturbance scenario), judgement (traffic disturbance scenario) and command (vehicle stability disturbance scenario).

Safety evaluation methodology

Top level Safety Requirement

AD systems **free of** **unreasonable** safety risks

Safety evaluation methodology

Does the AD system **cover all** **reasonable** safety risks?

Our proposal:

① Physics Principles based scenario approach

+

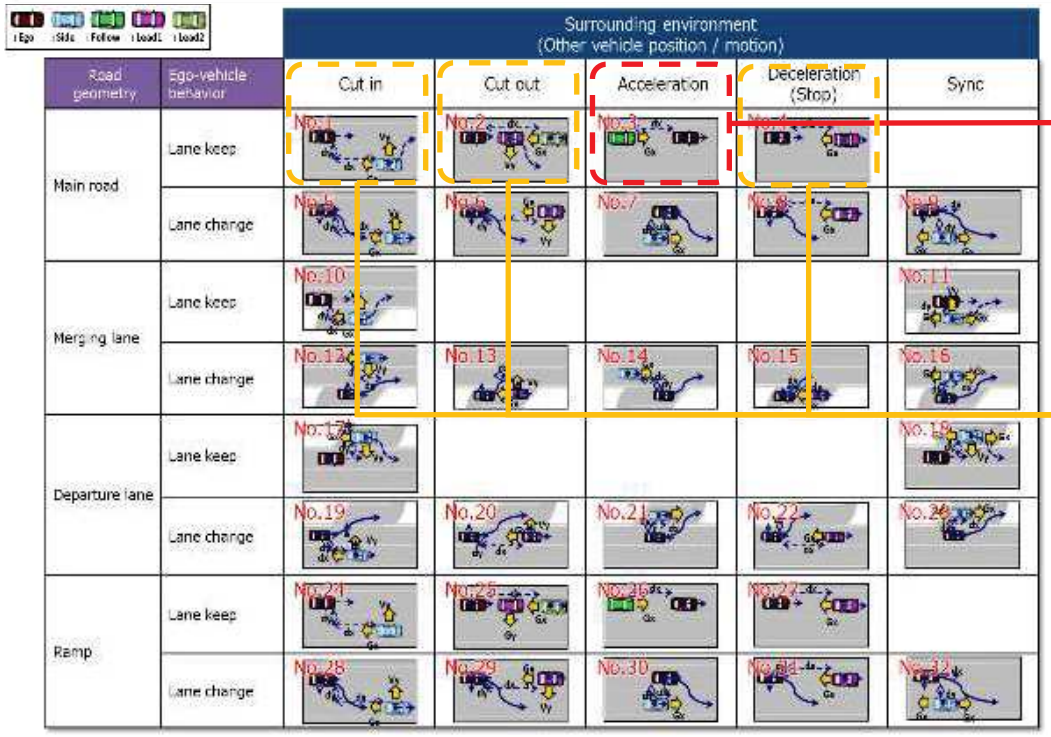
② Safety requirements based on reasonable foreseeability and preventability

Definition of Foreseeable and practical implementation of criteria

Reasonably foreseeable

= 1 Without ego- or other-vehicle drivers' extreme violation of traffic rules.

2 forecastable based on physics principles with a relevant exposure

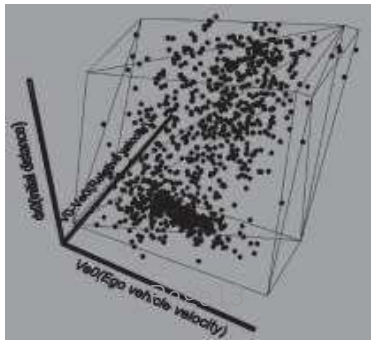


1

Rear end collision because of no brake of following vehicle

2

Dynamic parameter range of surrounding vehicle



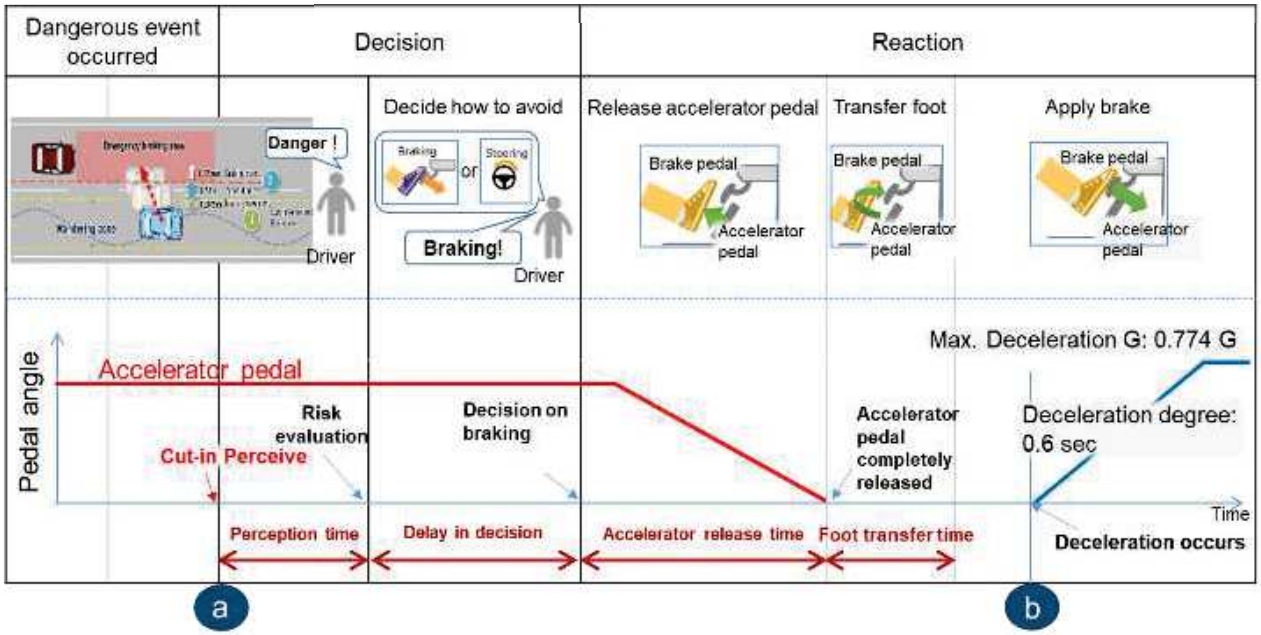
Definition of Preventable and practical implementation of criteria

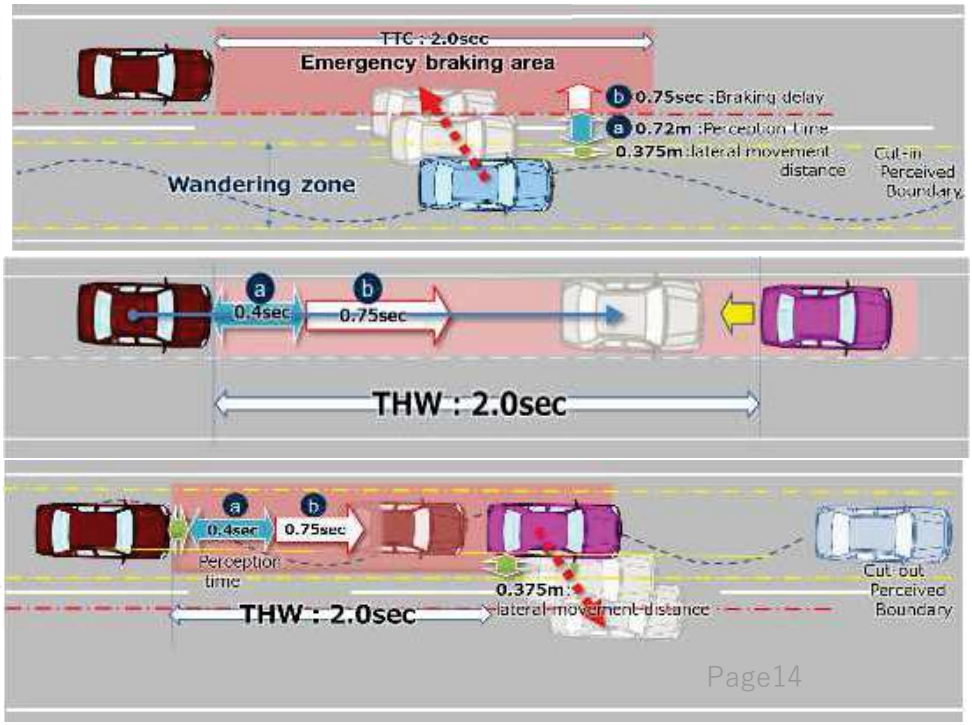
Preventable = Avoidable by a competent and careful human driver

? Does this criteria change depending on country due to different driving culture?

Should Not: sufficient capability of drivers is harmonized globally through international driver license.

Competent and careful human driver model for ALKS defined in UN157.

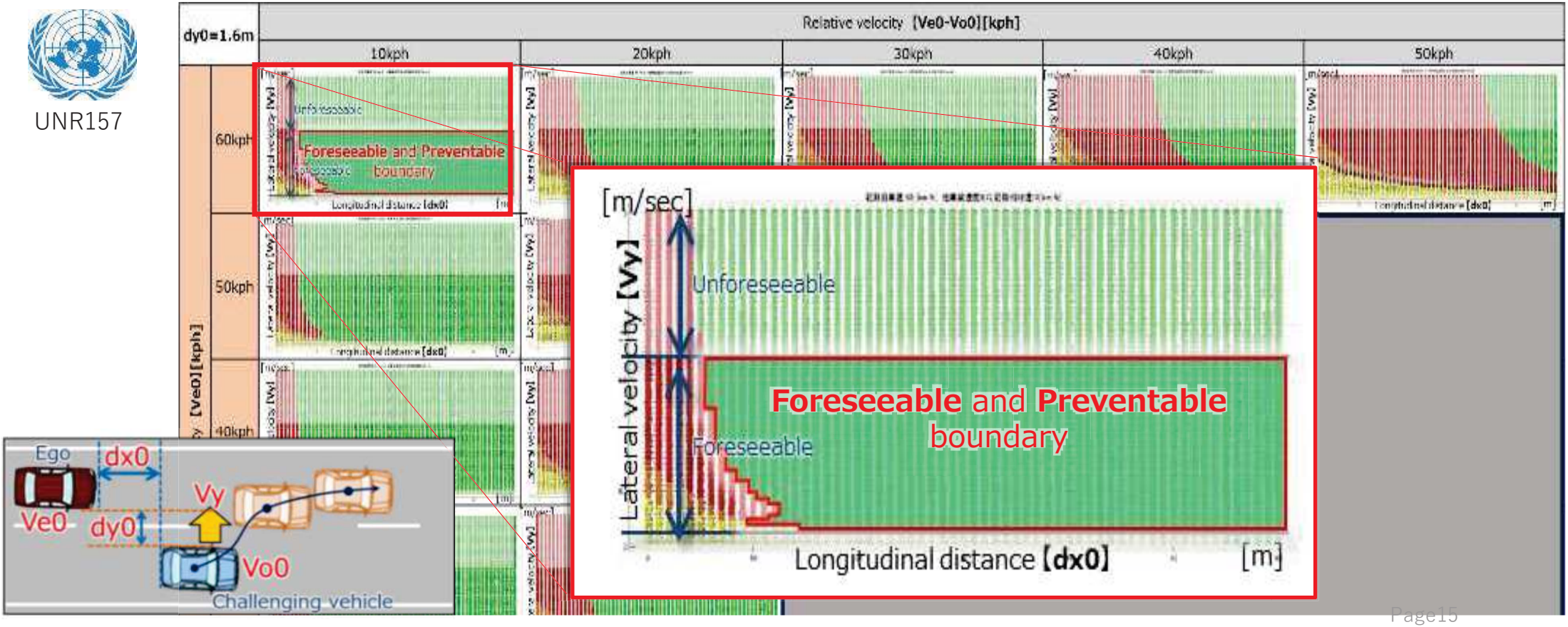




Foreseeable and Preventable Boundary

Preventable and foreseeable criteria is implemented into the ALKS regulation as quantitative pass fail boundary.

UNR157



Safety evaluation methodology

Top level Safety Requirement

AD systems **free of** **unreasonable** safety risks

Safety evaluation methodology

Does the AD system **cover all** **reasonable** safety risks?

Our proposal:

① Physics Principles based scenario approach + **② Safety requirements based on reasonable foreseeabilty and preventability**

From traffic disturbances to perception and stability disturbances

DDT Safety Risk

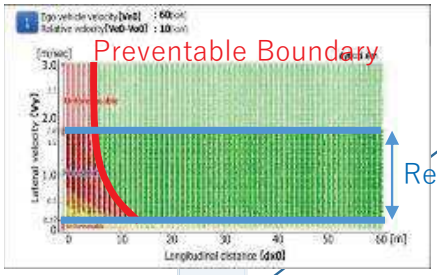
- **Collision with other traffic participants or obstacles**
- **Lane Departure**

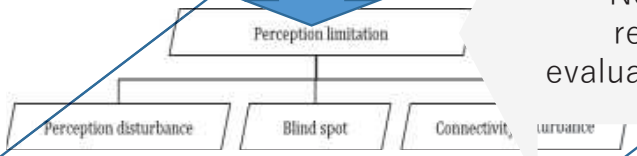
Traffic Disturbance Scenario

Safety Principle

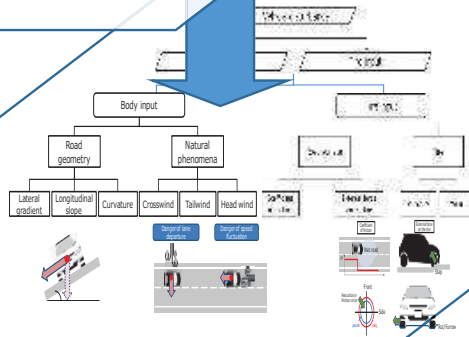
- ✓ Preventable
- ✓ Reasonably foreseeable

Reasonably Foreseeable and Preventable Boundary





No cause-effect relation: can be evaluated independently



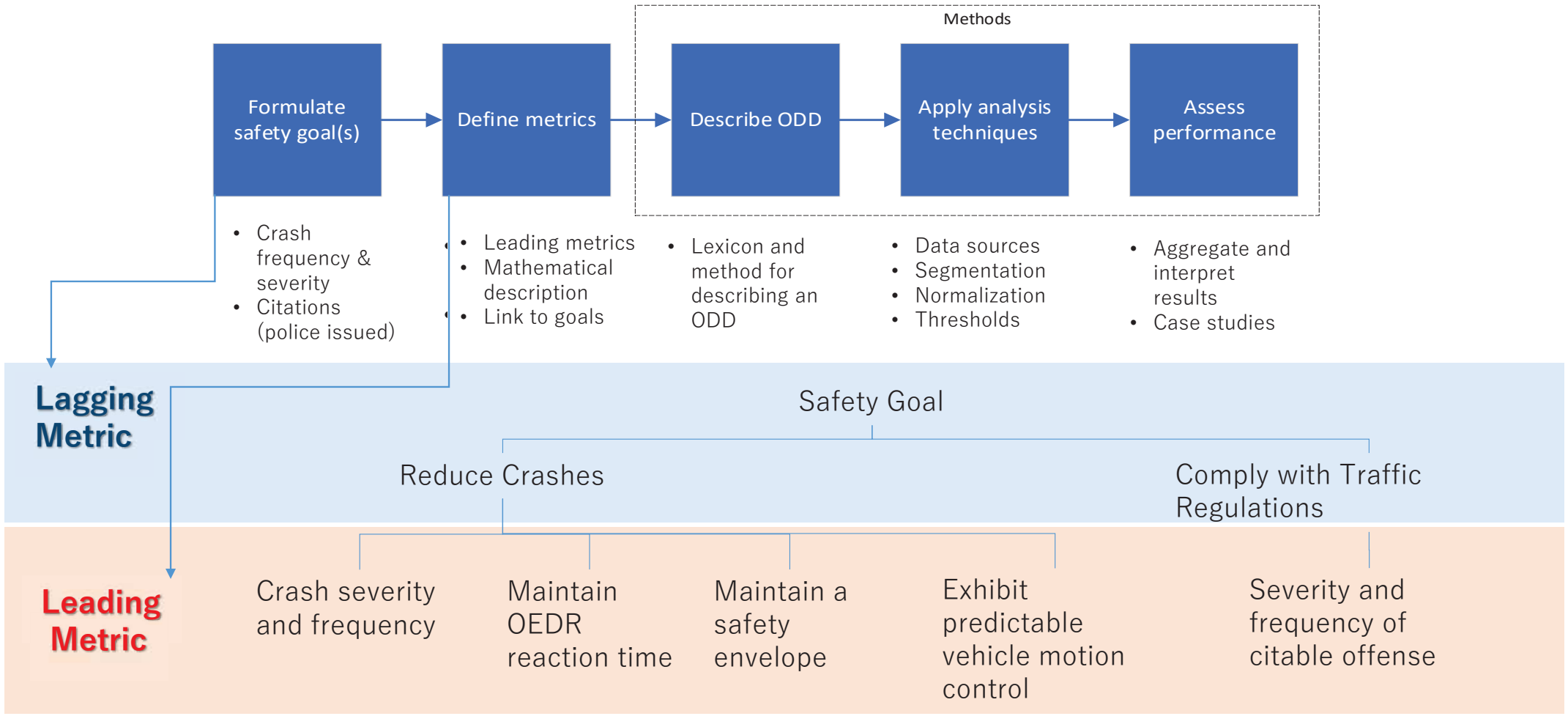
Avoid collision due to a perception disturbance within the pre-defined traffic disturbances

Avoid lane departure due to single or combined (worst case) reasonably foreseeable stability disturbances

Perception Scenario

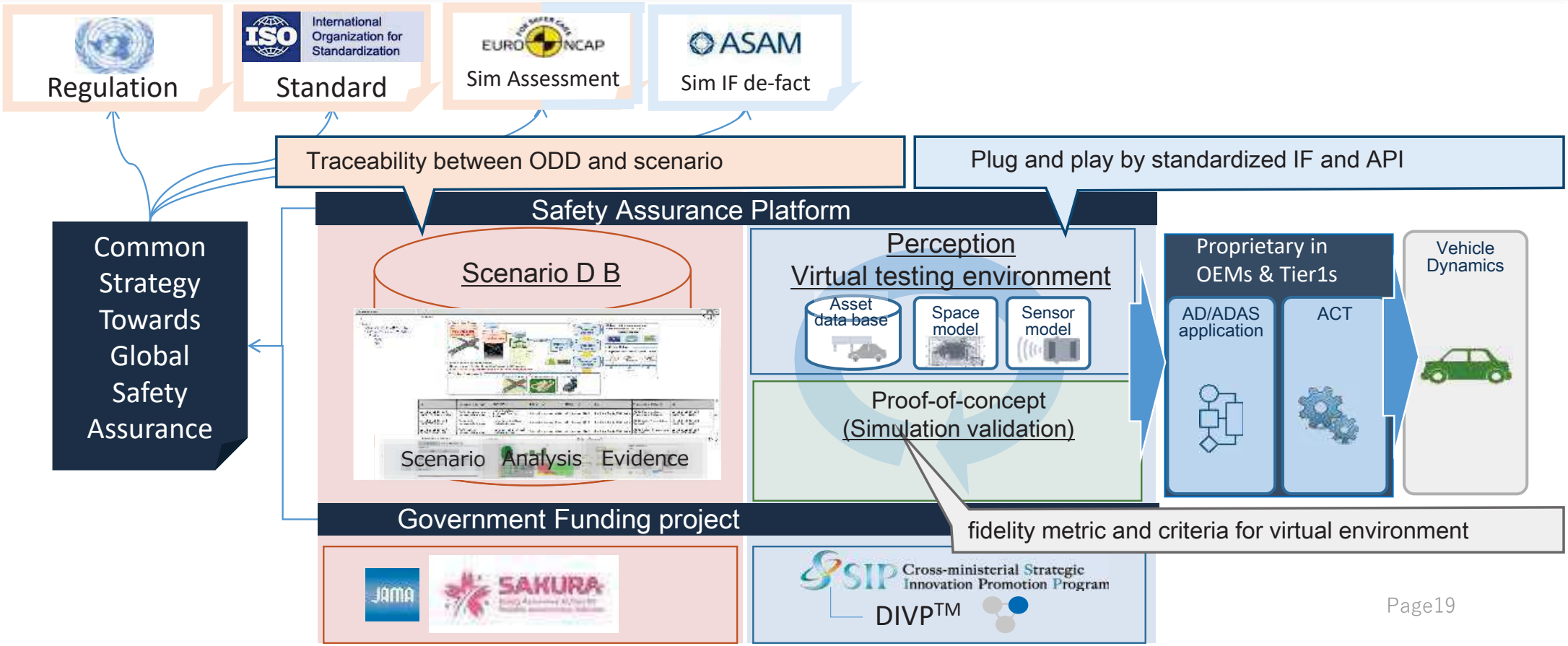
Vehicle Stability Scenario

Safety Evaluation Process

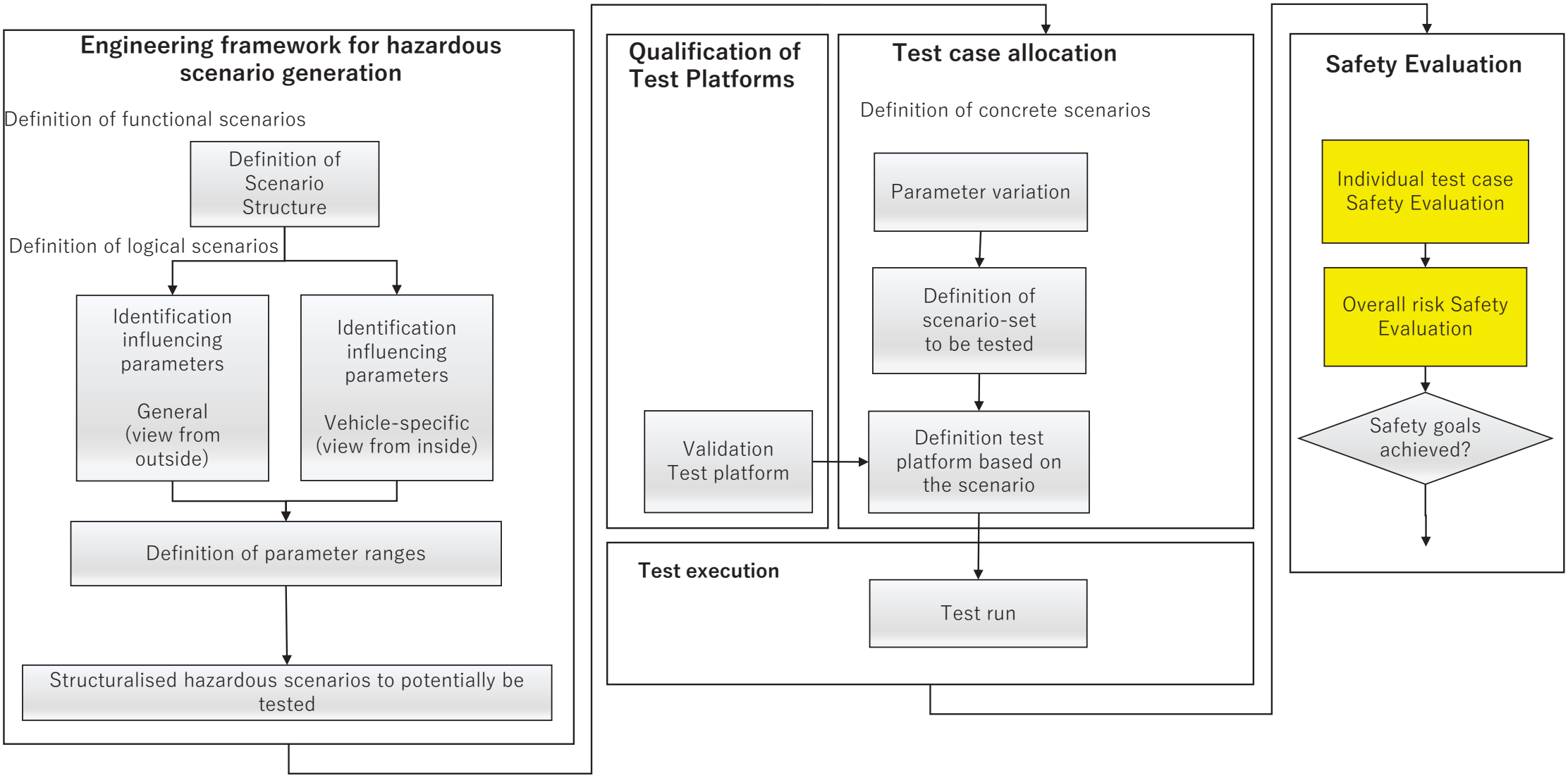


Safety Validation Platform

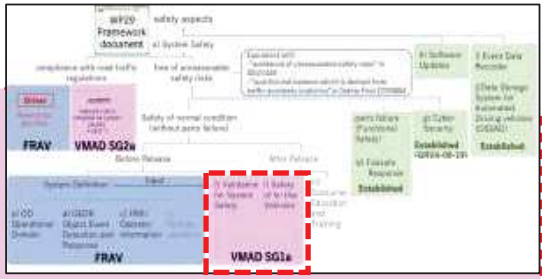
- ✓ In order to achieve both sufficient test coverage and practicality a safety validation platform which comprise a scenario database and a virtual testing environment needs to be established.
- ✓ Open innovation for both scenario databases and virtual testing environments need to be driven by collaborative activity to define the corresponding requirements.

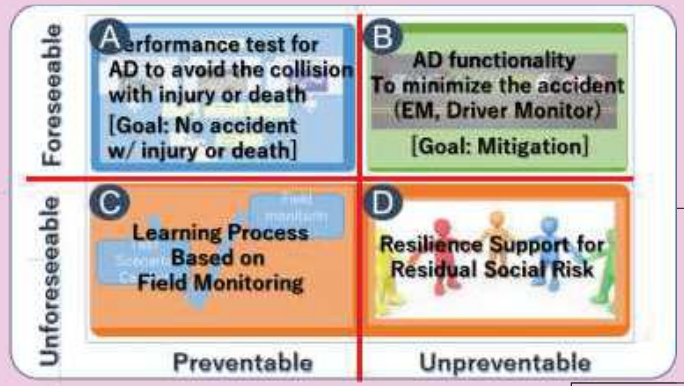


Scenario Based Engineering Process



Safety Argumentation Structure (Normal Condition)





Safety of normal condition

Before release

D After release

- Accident Monitoring and Feedback

Dynamic Driving Task ← Input — System Definition

Safety Operation by human

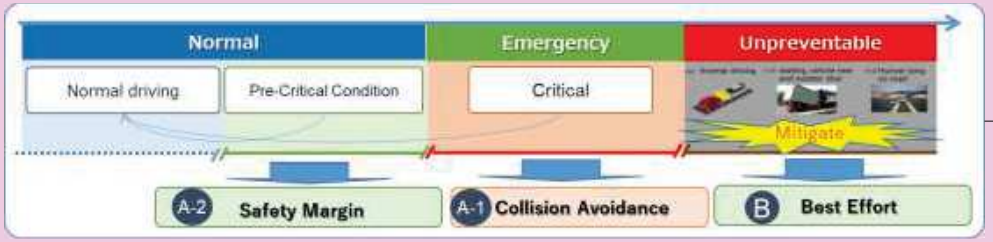
- Misuse Analysis

ODD boundary

within ODD

Goal; (WP29 Frame Work Document)
Within ODD reasonably foreseeable and preventable crashes that result in injury or death shall be avoided

Goal;
Better than competent and careful human driver within reasonable foreseeable scenario



Reasonably Foreseeable

NO(unforeseeable) → C Accident Monitoring

YES

Preventable

NO(Unpreventable) → B Collisional Test

- Best effort
- Passive safety performance

YES

preventable

A Edge Case Test

Pre-Critical Condition

- safety margin

Critical Condition

Evaluation Scenario

1.Traffic 2.Perception 3.Vehicle

Environment

Multi Pillar Approach

Physical Principal Based Scenario Based Testing

Summary

Safety Principle

Audit Pillar

Safety by Design

Documentation structure in accordance with
-ISO21447 SOTIF
-ISO26262 Functional Safety, etc

Testing Pillar

Safety by V&V

Scenario base approach
- ISO TC22/SC33/WG9

Testing Environment

Real-traffic tests

Proving ground tests

Virtual tests

Our safety validation methodology proposal:

① Physics Principles based scenario approach + ② Safety requirements based on reasonable foreseeability and preventability

Willing to collaborate with research, industry, standardization and regulatory institutions, towards joint efforts to ensure a safe automated driving global society