A Methodology for Dynamic Driving Task safety evaluation: from scenario development to criteria definition

23rd/Sep/2020

Lead of Japanese AD Safety Assurance project
(JAMA, SIP-adus, SAKURA)

Satoshi Taniguchi

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)

Perception

External Environment

Camera

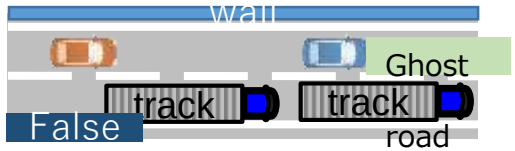
ex. Low signal from a target in the darkness

LiDAR

ex. Low reflection caused by dark color of a target

Radar

ex. ,ghost from multiple reflection



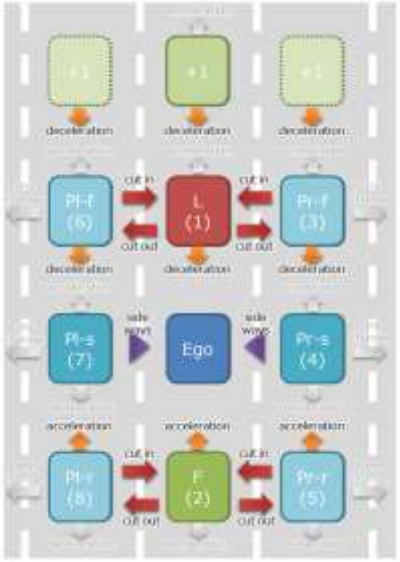
Fusion

Judgement

Traffic Participants' Position

Planning

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

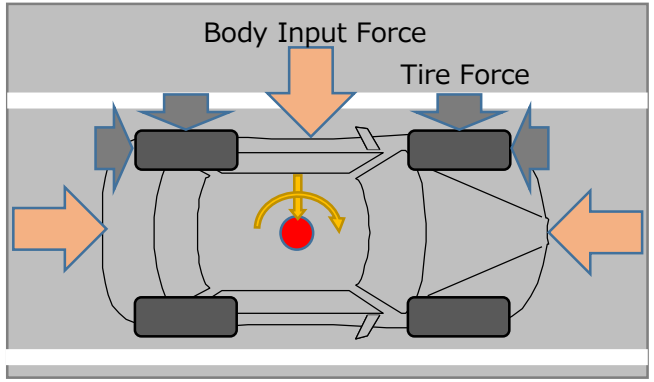


Command

Path/speed plan

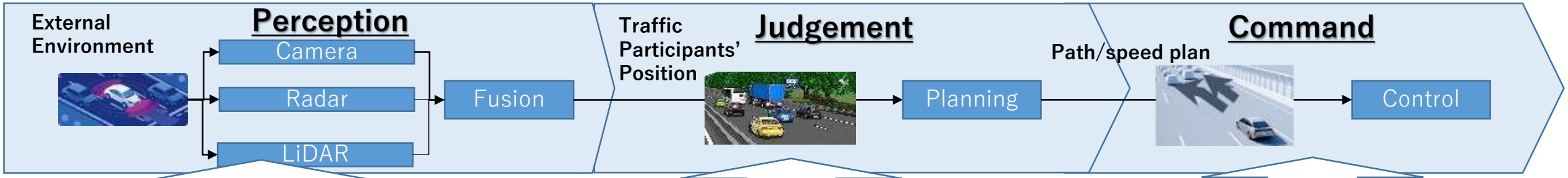
Control

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



- 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

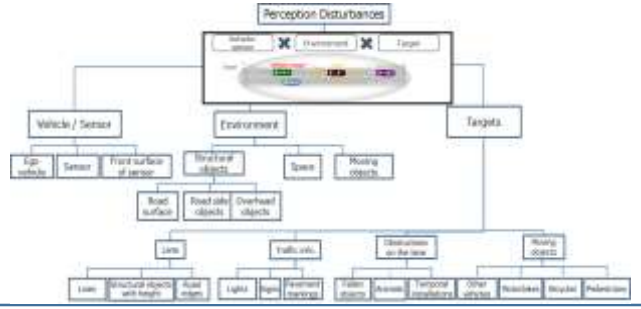


Perception Scenario

ex.
Camera
Low signal from a target in the darkness

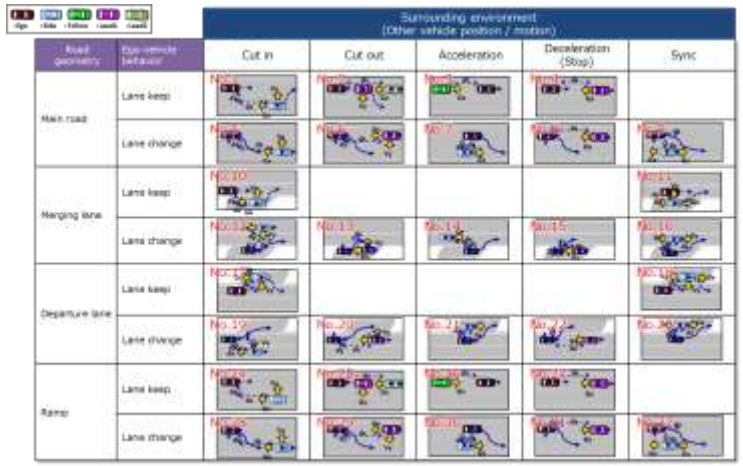
Lidar
. Low reflection caused by dark color of a target

Radar
ghost from multiple reflection



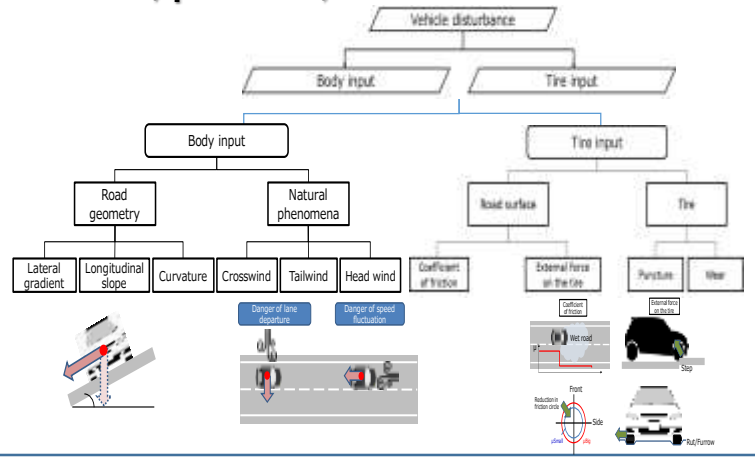
Traffic Disturbance Scenario

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**

\+

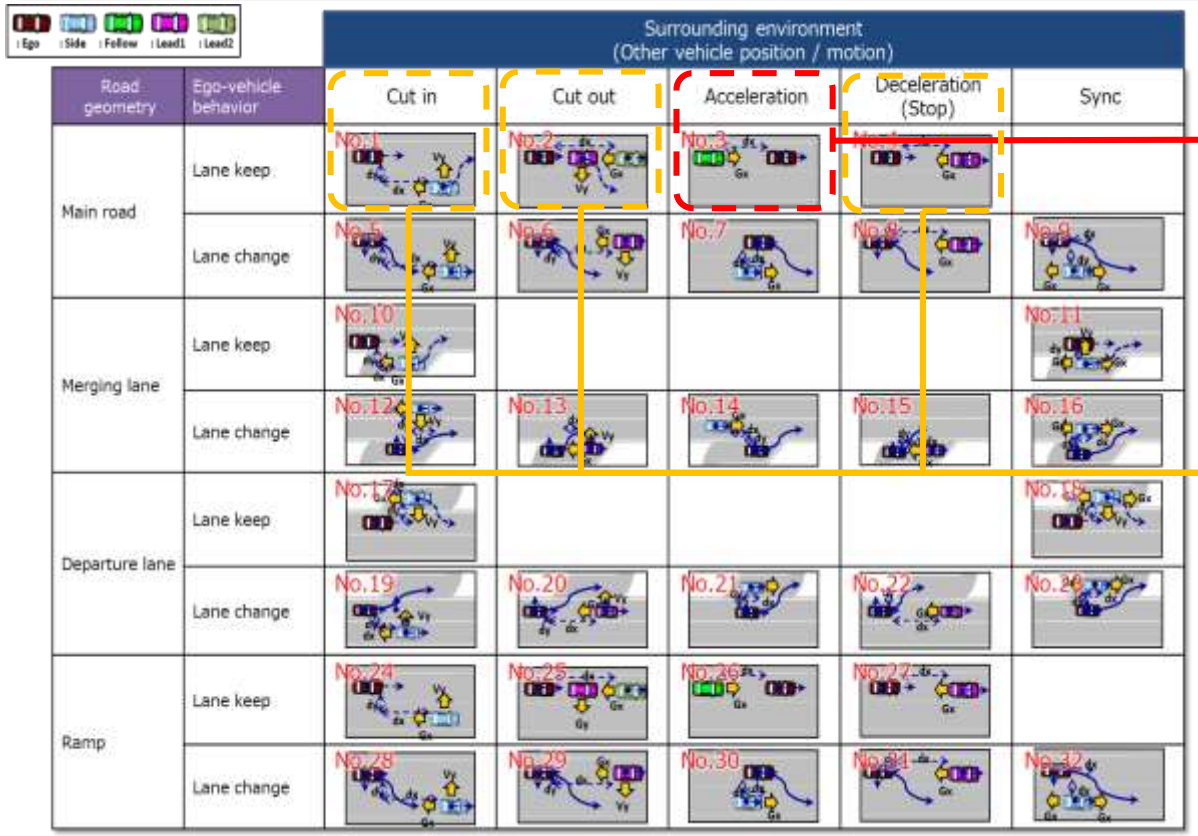
② **Safety requirements based on reasonable foreseeability and preventability**

Definition of Foreseeable and practical implementation of criteria

Reasonably foreseeable

= 1 ego- or other-vehicle drivers' extreme violation of traffic rules.

2 forecastable based on physics principles with a relevant exposure

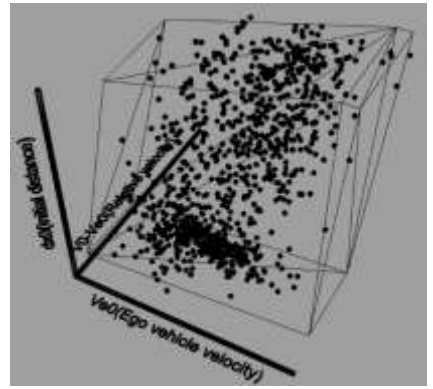


1

Rear end collision because of no brake of following vehicle

2

Dynamic parameter range of surrounding vehicle



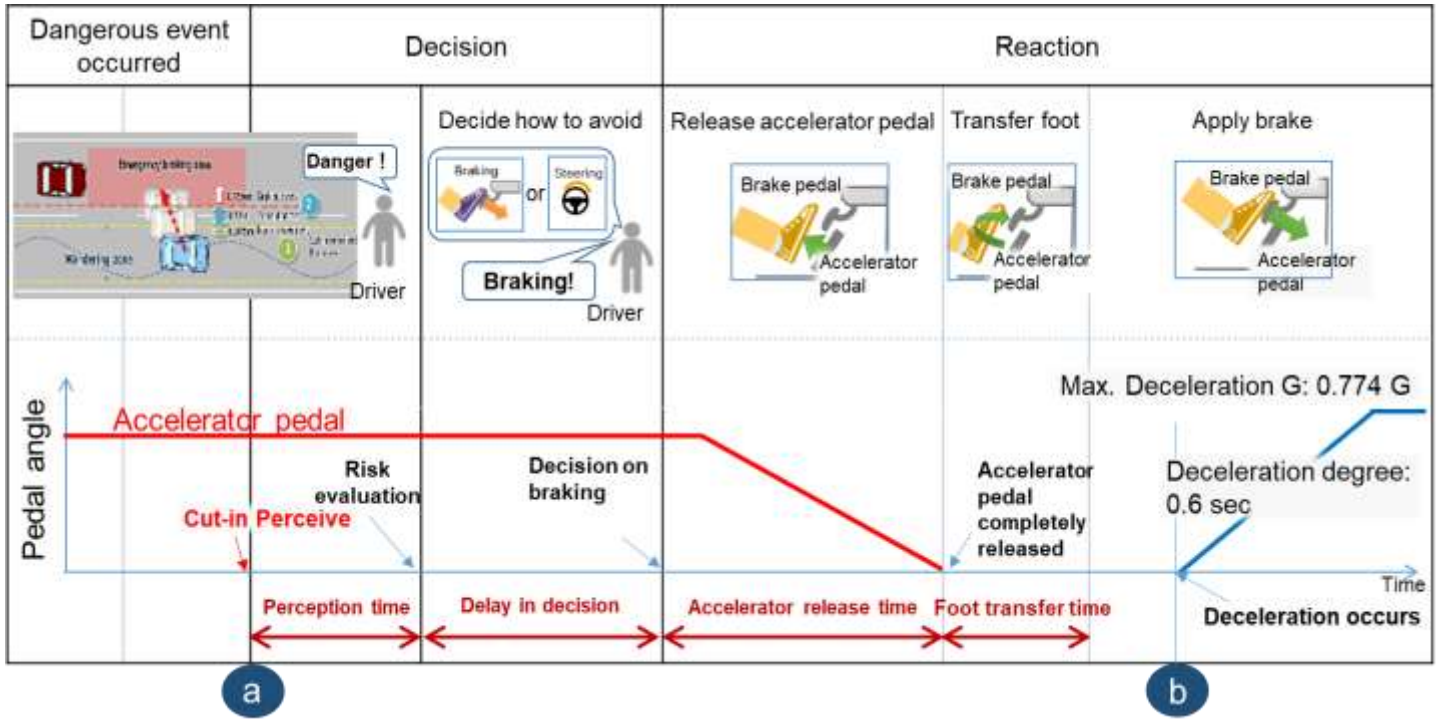
Definition of Preventable and practical implementation of criteria

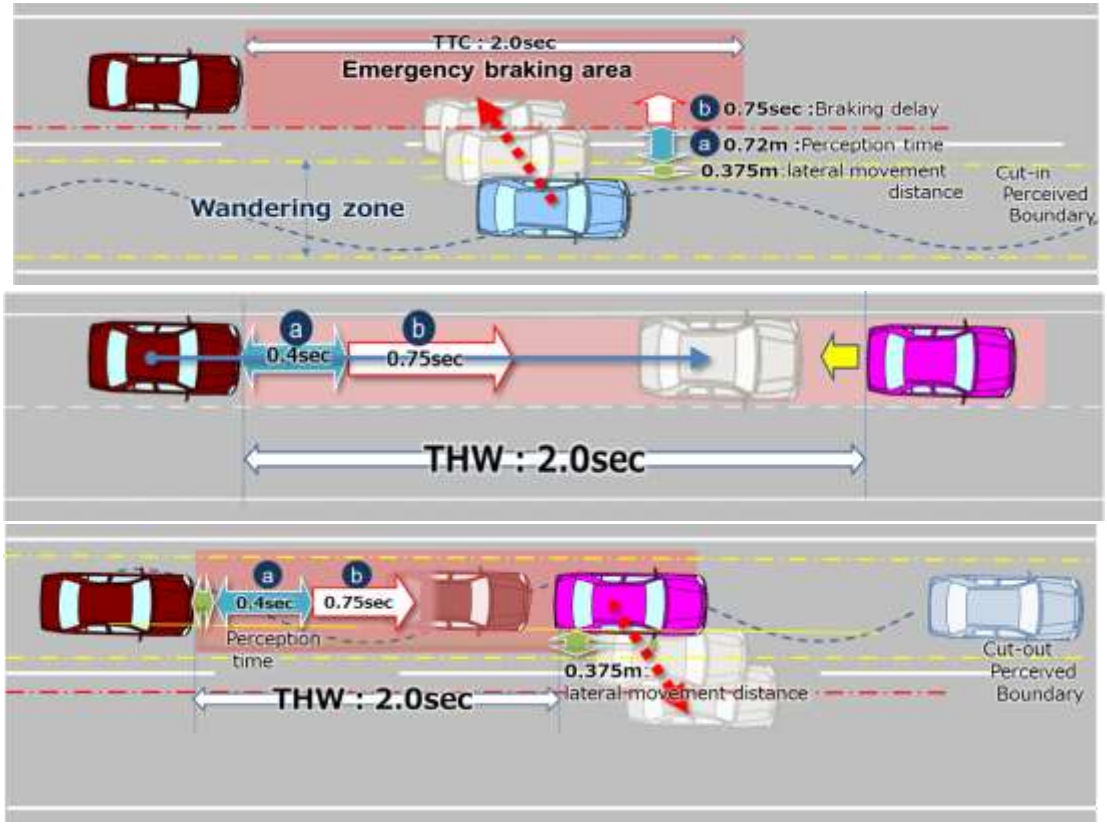
Preventable = Avoidable by a competent and careful human driver

? 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.

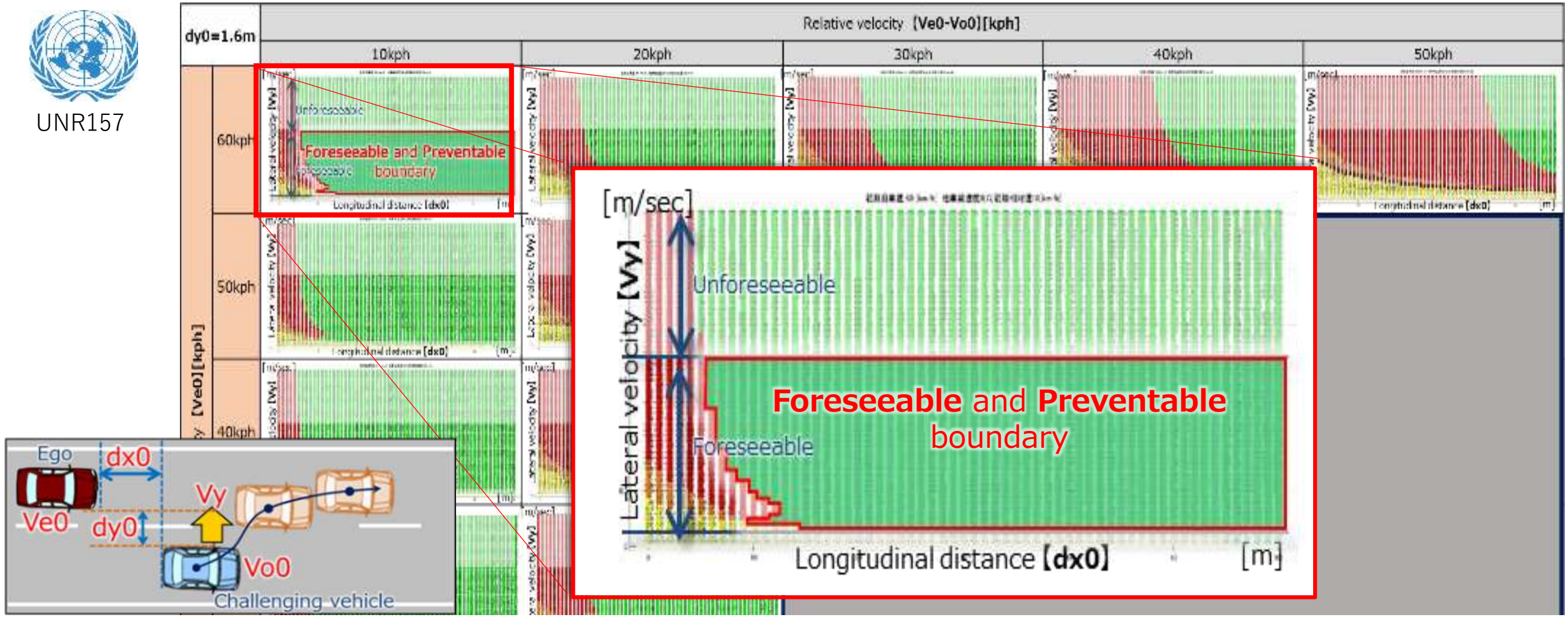




Foreseeable and Preventable Boundary

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

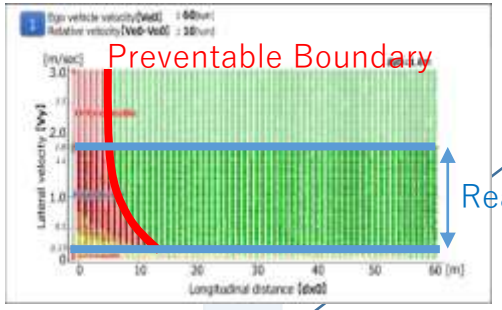
- **Collision with other traffic participants or obstacles**
- **Lane Departure**

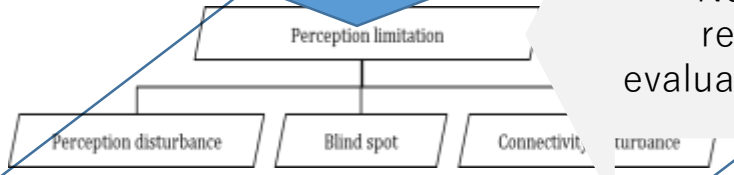
Traffic Disturbance Scenario

Safety Principle

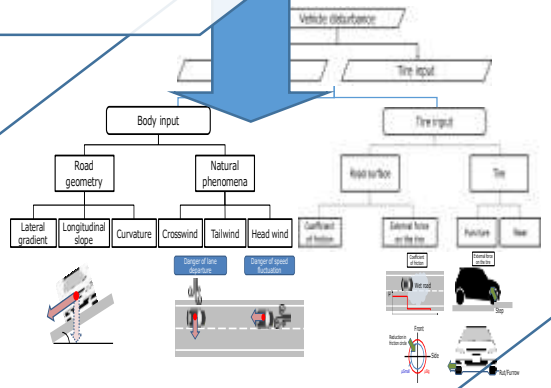
- ✓ Preventable
- ✓ Reasonably foreseeable

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

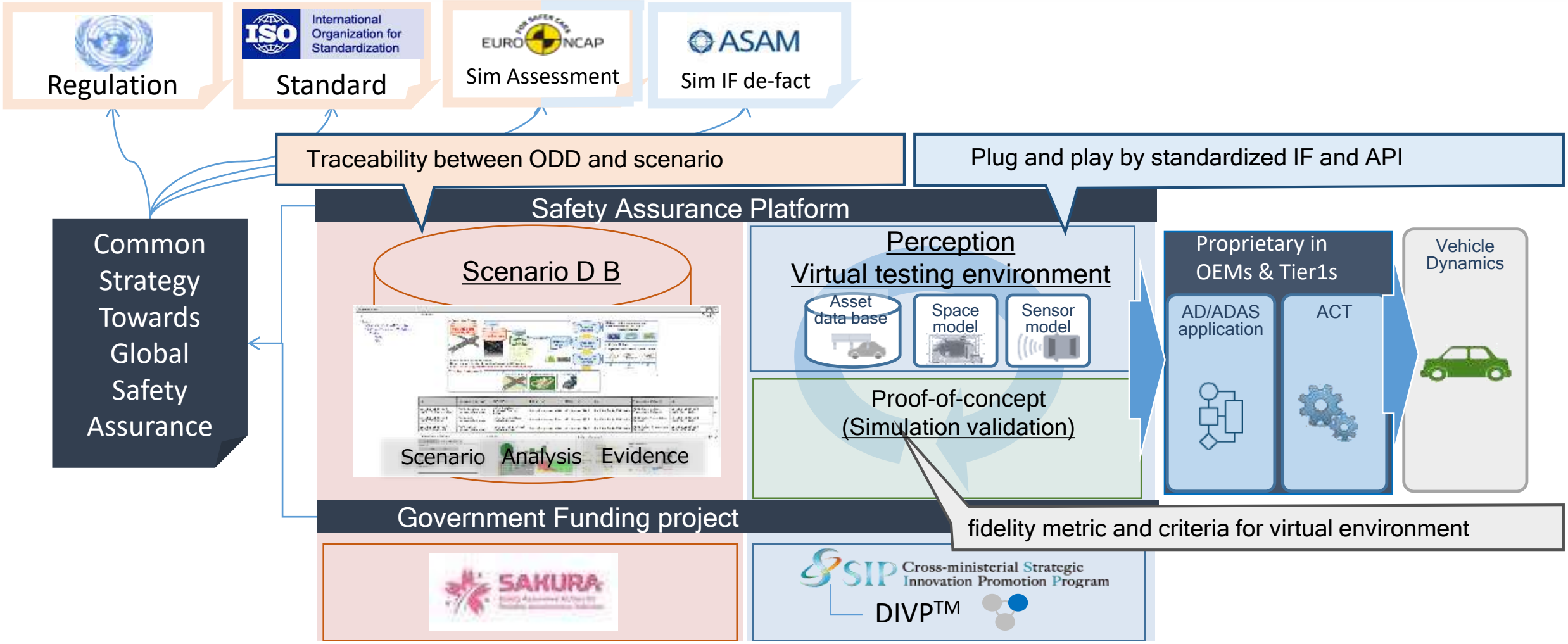
Avoid lane departure due to single or combined (worst case) reasonably foreseeable stability disturbances

Perception Scenario

Vehicle Stability Scenario

Safety 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.



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

Thank you for your attention

Questions?

satoshi_taniguchi_ad@mail.toyota.co.jp