MODULE 4:
STANDARDS/TECHNICAL REFERENCE FOR AUTONOMOUS VEHICLES

Nicholas Ho
Institute of System Science, NUS

Contents

1. Brief Introduction to Standards

2. Sharing and elaboration on selected standards topics (e.g. SAE-J3016, TR-68-1/2/3/4)

3. Pop Quiz

Introduction to Technical Standards

- **Definition:** Standards are **published documents that establish specifications and procedures designed to ensure the reliability** of the materials, products, methods, and/or services people use every day. Standards address a range of issues, including but not limited to various protocols that help **ensure product functionality and compatibility, facilitate interoperability and support consumer safety and public health**
- **Examples** of well-known technical standards: ISO, SAE, IATF, GSMA, IEC, NIST, TR

Importance of Technical Standards

A basis for mutual understanding

A basis for the introduction of new technologies and innovations

Ensure compatibility

Facilitate communication, measurement, commerce and manufacturing

Speeds time-to-market

Enable companies to comply with relevant laws and regulations

Facilitate business interaction

Ensure interoperability

SHARING AND ELABORATION ON SELECTED STANDARDS TOPICS (E.G. SAE-J3016, TR-68)

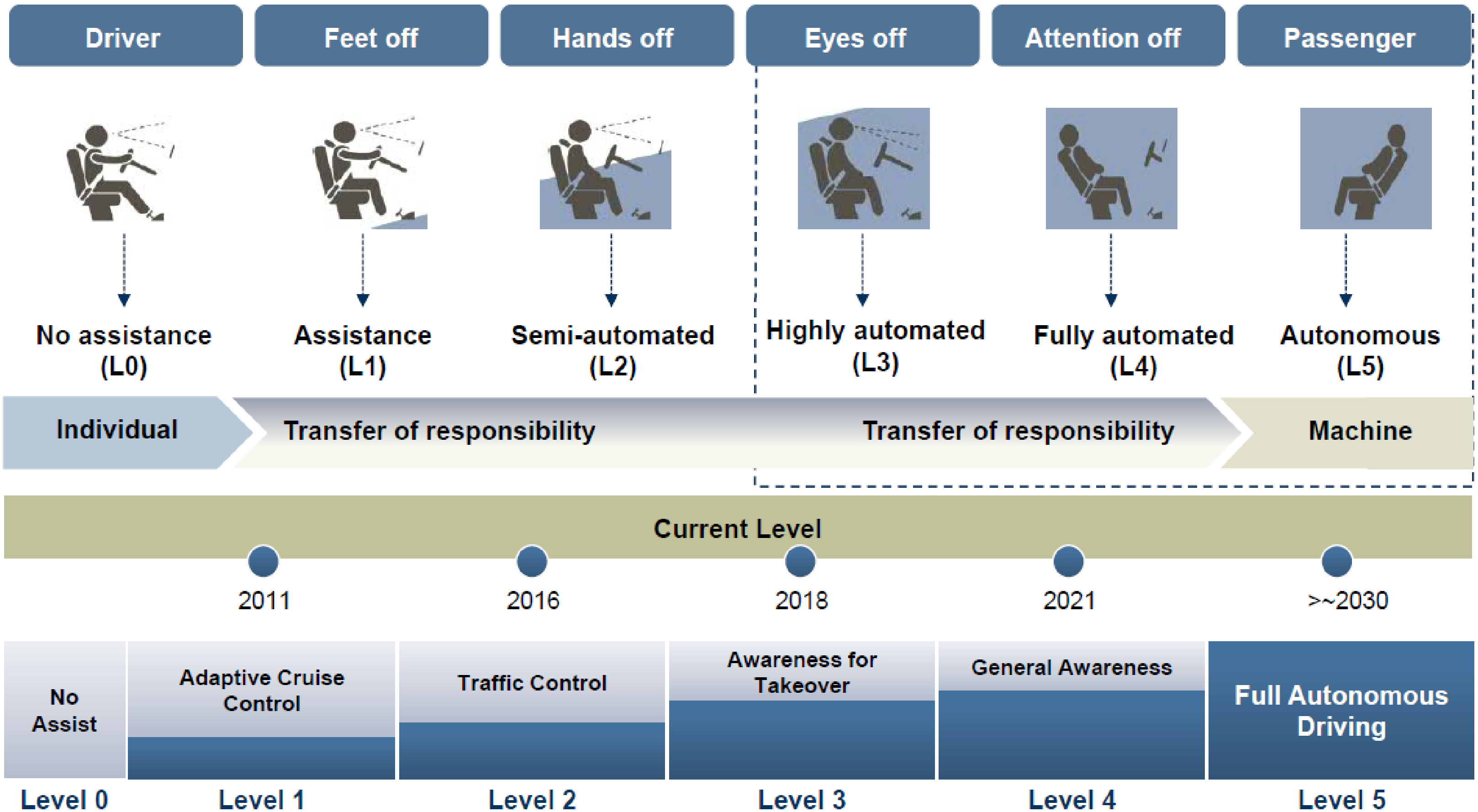
1. SAE INTERNATIONAL – J3016

Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

Practice J3016

- Freely available via SAE website
- **Provides a classification** (Level 0 to Level 5) describing the full range of levels of driving automation in on-road motor vehicles and includes **functional definitions for advanced levels of driving automation and related terms and definitions**
- <u>**Does not provide specifications**</u> for and <u>**does not impose requirements**</u> on driving automation systems

The 5 Levels of Autonomous Driving



Source: BMW Group

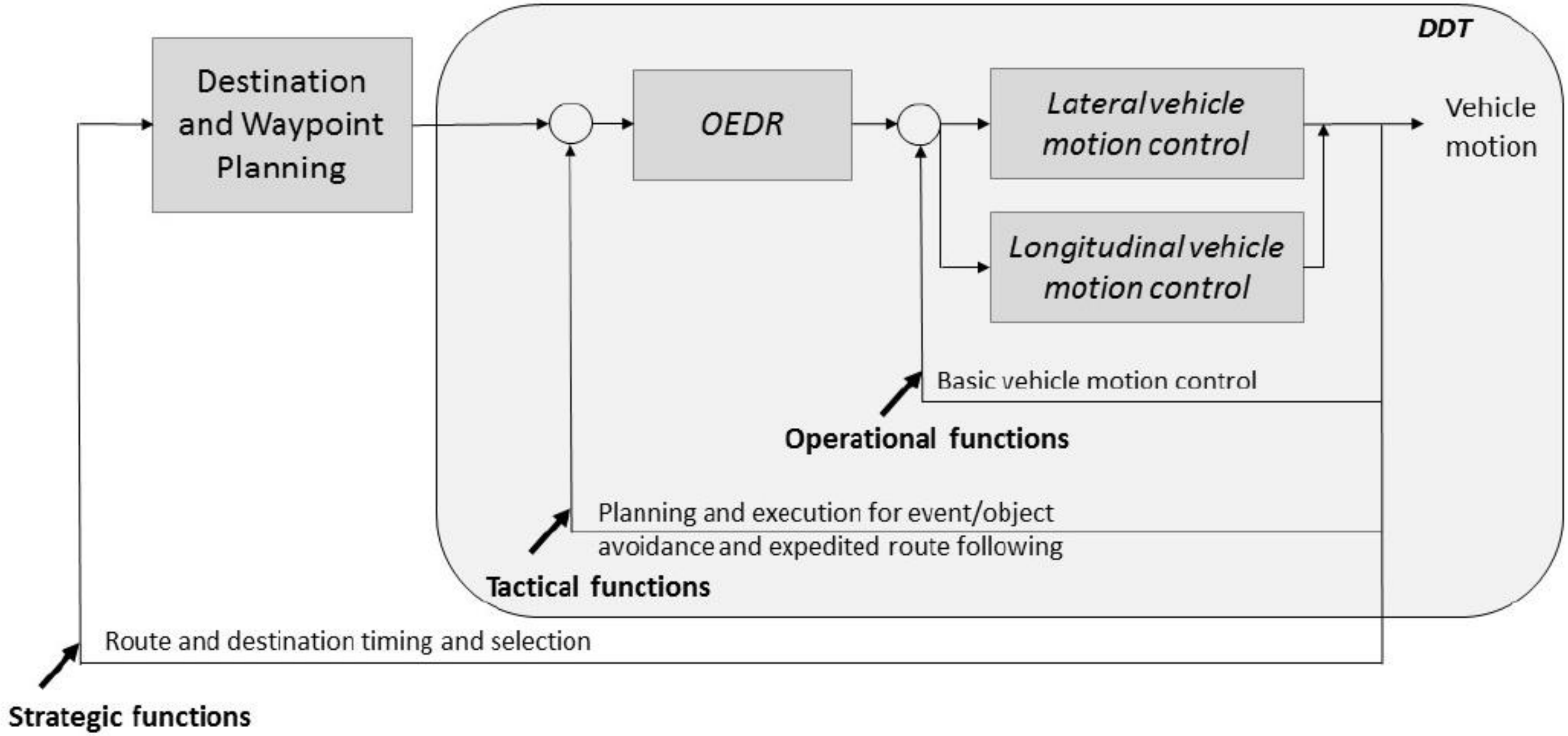
Dynamic Driving Task (DDT)

- Includes **all real-time operational and tactical functions** required to operate a vehicle in on-road traffic, **excluding the strategic functions** such as trip scheduling and selection of destinations and waypoints, and including without limitation:
  1. Lateral vehicle motion control via **steering** (operational)
  2. Longitudinal vehicle motion control via **acceleration and deceleration** (operational)
  3. **Monitoring** the driving environment via object and event detection, **recognition, classification, and response preparation** (operational and tactical)
  4. **Object and event response execution** (operational and tactical)
  5. **Maneuver planning** (tactical)
  6. **Enhancing conspicuity** via lighting, signaling and gesturing, etc. (tactical)

Dynamic Driving Task (DDT)

Schematic (not a control diagram) view of driving task showing DDT portion

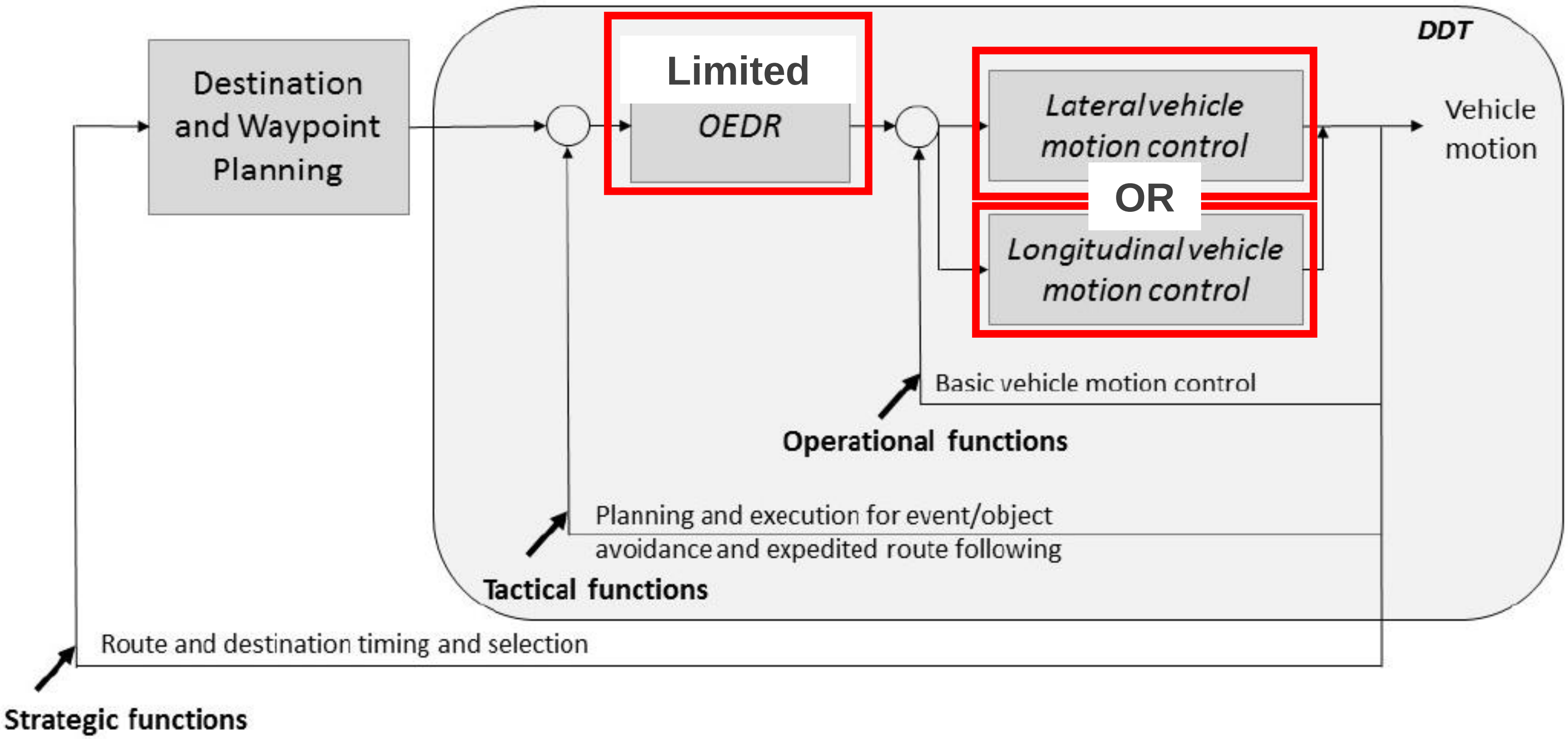
OEDR = object and event detection, recognition, classification, and response



Graphics from SAE International J3016

Dynamic Driving Task (DDT)

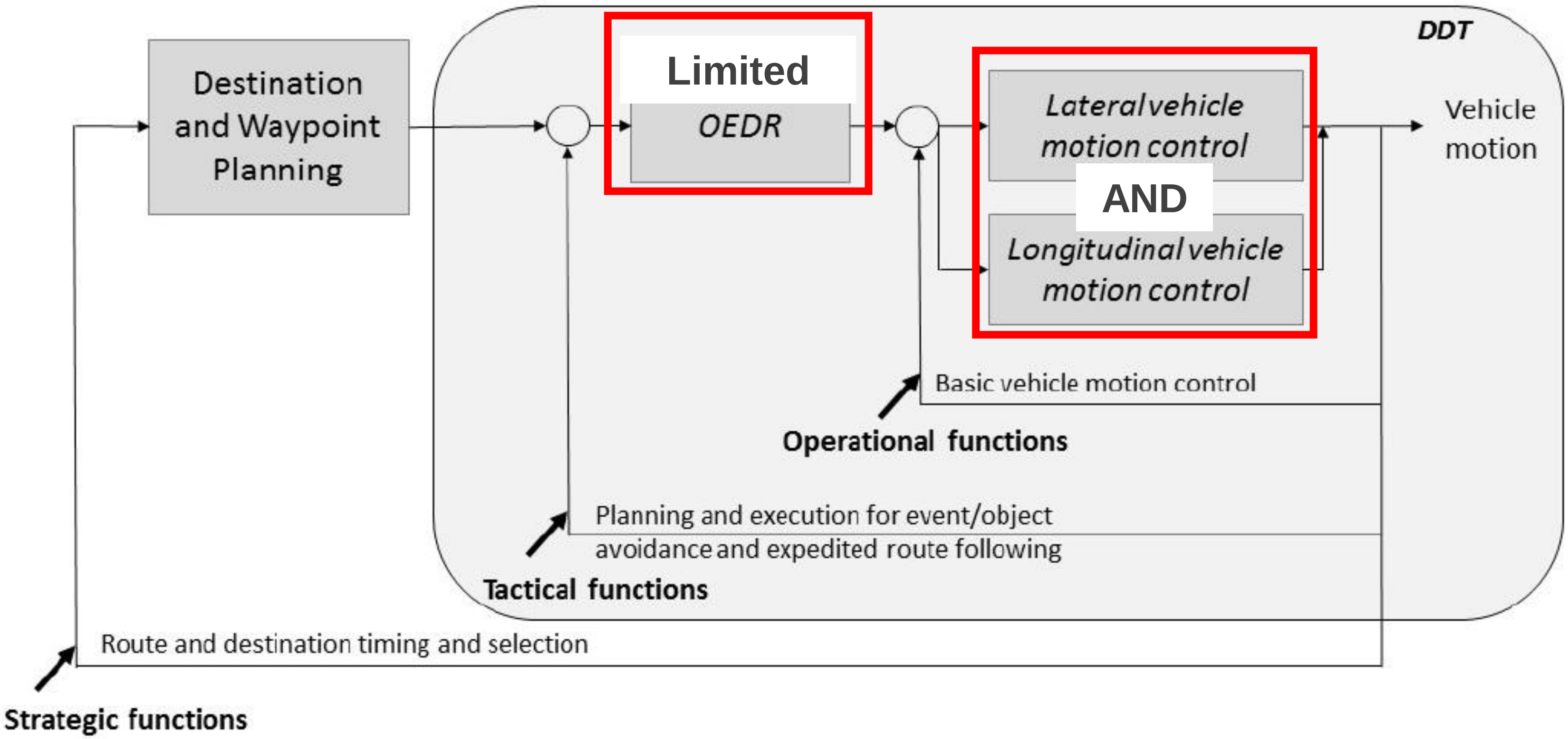
For Level 1



Graphics from SAE International J3016

Dynamic Driving Task (DDT)

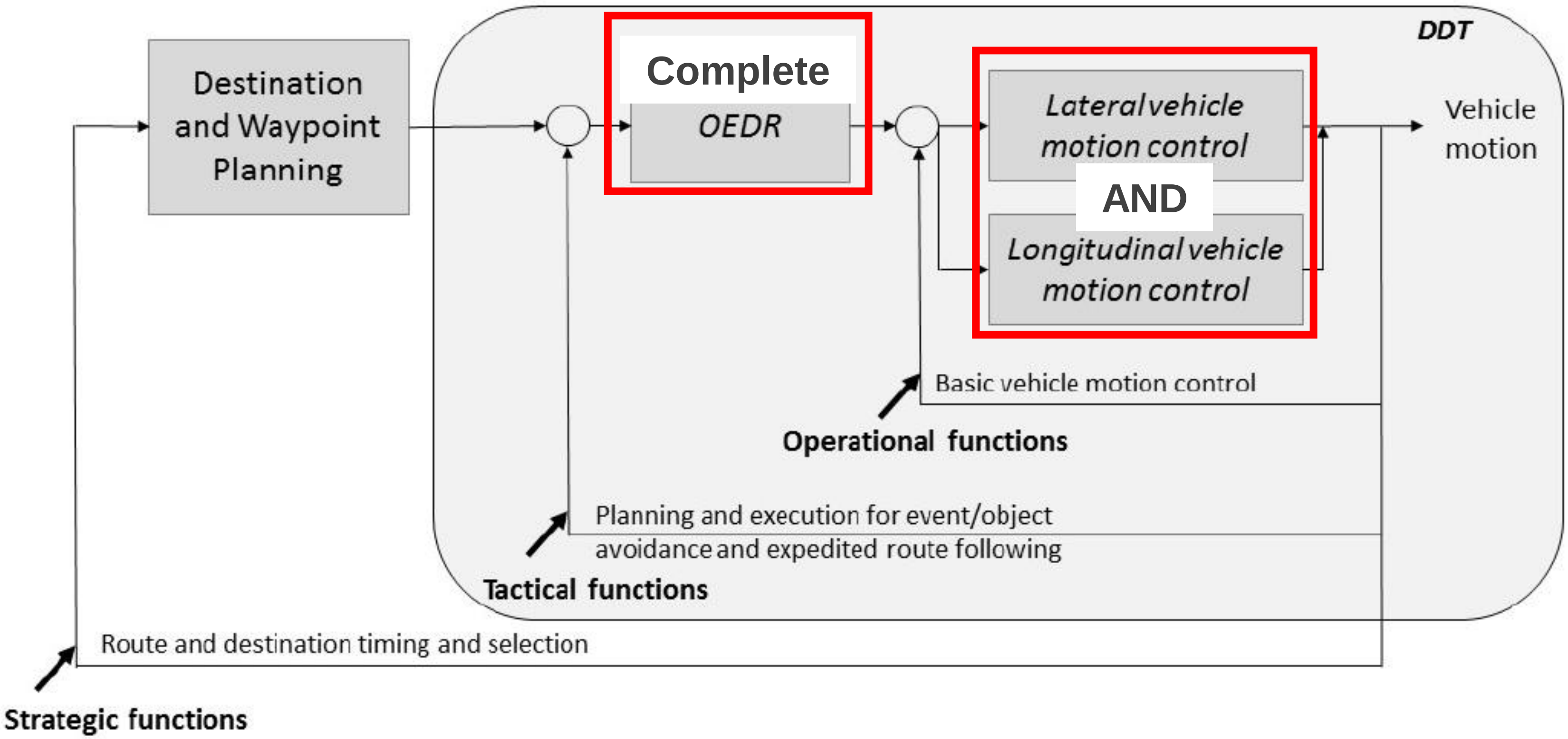
For Level 2



Graphics from SAE International J3016

Dynamic Driving Task (DDT)

For Levels 3-5



Graphics from SAE International J3016

Driving vs DDT

	Driving	**DDT**
Types of effort involved	Strategic, Tactical, and Operational	Tactical and Operational only

- Driving entails a variety of decisions and actions, which may or may not involve a vehicle being in motion, or even being in an active lane of traffic
- Strategic effort involves trip planning, such as deciding whether, when and where to go, how to travel, best routes to take, etc
- **DDT is a subset of driving**

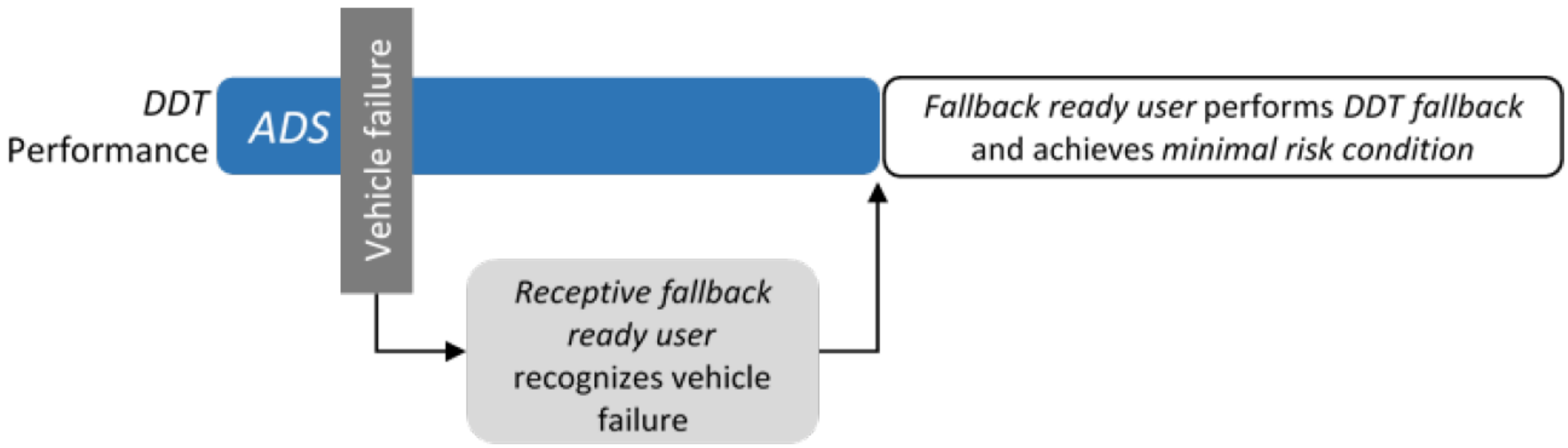
DDT Fallback

- Define as the **response by the user to either perform the DDT or achieve a minimal risk condition after occurrence of a DDT performance-relevant system failure(s) or upon operational design domain (ODD) exit, or the response by an ADS to achieve minimal risk condition (MRC)**, given the same circumstances
  - **ODD** is defined as **operating conditions under which a given driving automation system or feature thereof is specifically designed to function**, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics
  - **MRC** is defined as **a condition to which a *user* or an *ADS* may bring a *vehicle* after performing the *DDT fallback*** in order to **reduce the risk of a crash when a given *trip* cannot or should not be completed**

DDT Fallback; E.g.

1. **A level 1 adaptive cruise control (ACC) feature** experiences a system failure that causes the feature to stop performing its intended function. The human driver performs the DDT fallback by resuming performance of the complete DDT
2. **A level 3 ADS (Automated Driving System) feature** that performs the entire DDT during traffic jams on freeways is not able to do so when it encounters a crash scene and therefore issues a request to intervene to the DDT fallback-ready user. S/he responds by taking over performance of the entire DDT in order to maneuver around the crash scene (Note that in this example, a minimal risk condition is not needed or achieved)
3. **A level 4 ADS-dedicated vehicle (ADS-DV)** that performs the entire DDT within a geo-fenced city center experiences a DDT performance-relevant system failure. In response, the ADS-DV performs the DDT fallback by turning on the hazard flashers, maneuvering the vehicle to the road shoulder and parking it, before automatically summoning emergency assistance (Note that in this example, the ADS-DV automatically achieves a minimal risk condition)

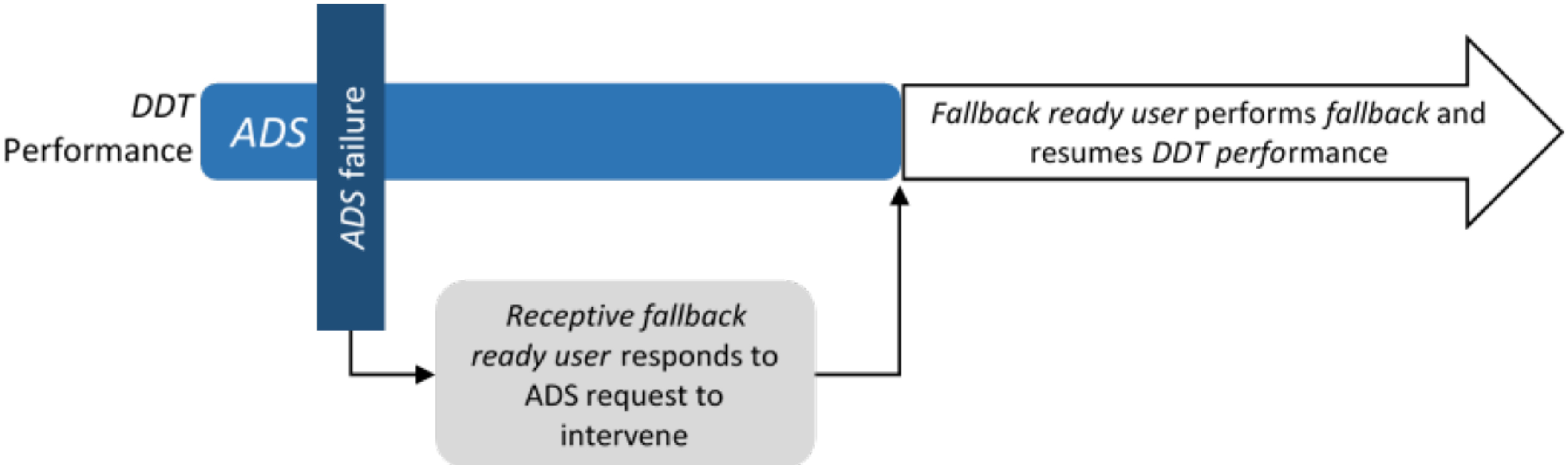
DDT Fallback Illustrative Examples:



Sample use case sequence at **Level 3** showing *ADS* engaged and **occurrence of a *vehicle system failure*** that **prevents continued *DDT* performance**. *User* performs *fallback* and achieves ***a minimal risk condition***

Graphics from SAE International J3016

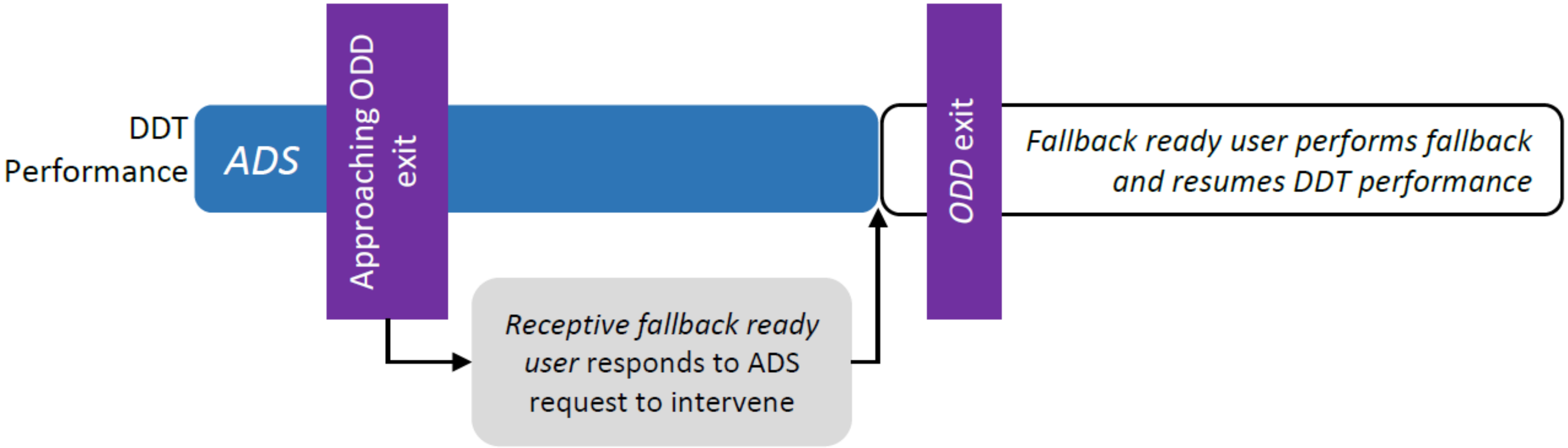
DDT Fallback Illustrative Examples:



Sample use case sequence at **Level 3** showing *ADS* engaged and **occurrence of an *ADS system failure*** that **<u>does not</u> prevent continued *DDT* performance**. *User* performs the *fallback* and **resumes *DDT* performance**

Graphics from SAE International J3016

DDT Fallback Illustrative Examples:



Sample use case sequence at **Level 3** showing *ADS* engaged and **occurrence of exiting the *ODD*** that **<u>does not</u> prevent continued *DDT* performance**. *User* performs the *fallback* and **resumes *DDT* performance**

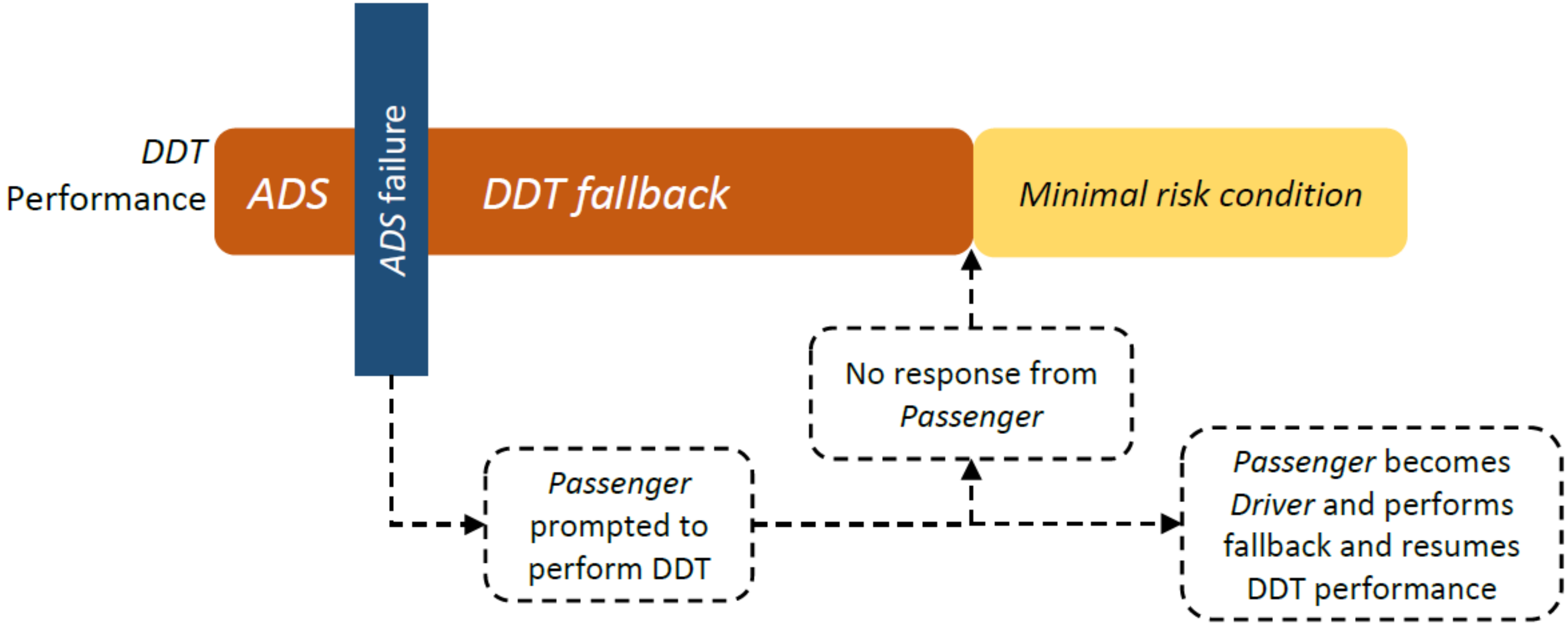
Graphics from SAE International J3016

DDT Fallback Illustrative Examples:

Sample use case sequence at **Level 4** showing *ADS* engaged and **occurrence of a *vehicle system failure*** that **prevents continued *DDT* performance.** *ADS* performs the *fallback* and **achieves a *minimal risk condition***

Graphics from SAE International J3016

DDT Fallback
Illustrative Examples:

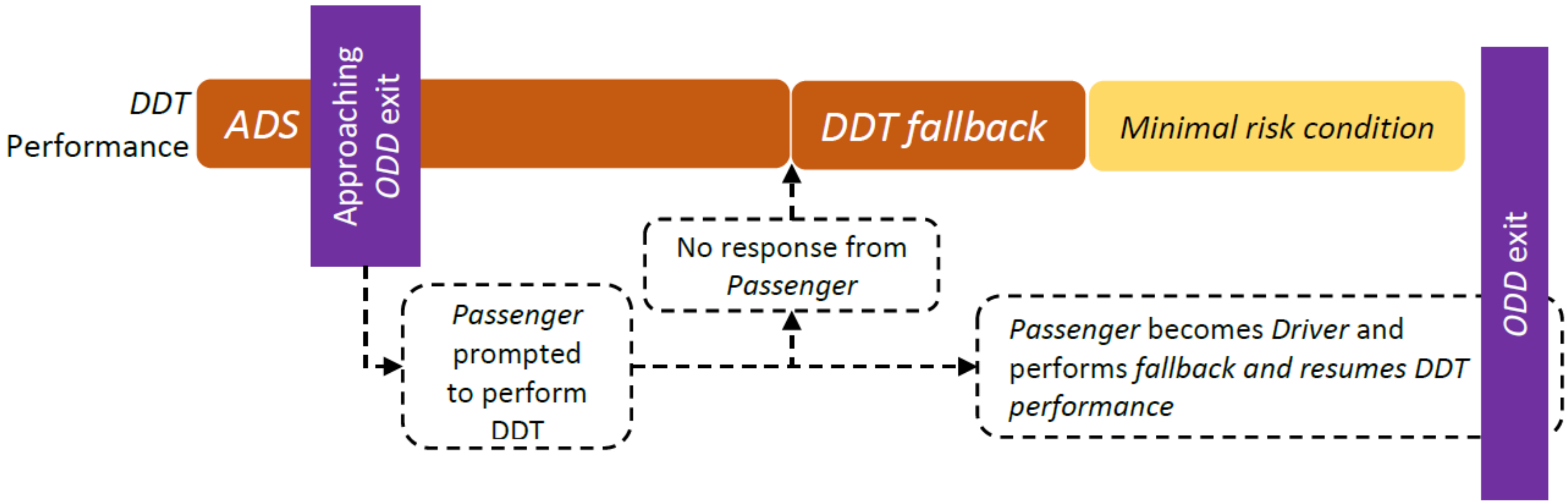


NOTE: Dotted lines represent optional conditions.

Sample use case sequence at **Level 4** showing *ADS* engaged and occurrence of **an *ADS* failure** that **<u>does not</u> prevent continued DDT performance by an available human *user***. The *ADS feature* may prompt a *passenger* seated in the driver's seat (if available) to resume DDT performance; if no driver's seat with *receptive passenger*, the *ADS* automatically achieves a *minimal risk condition*

Graphics from SAE International J3016

DDT Fallback Illustrative Examples:

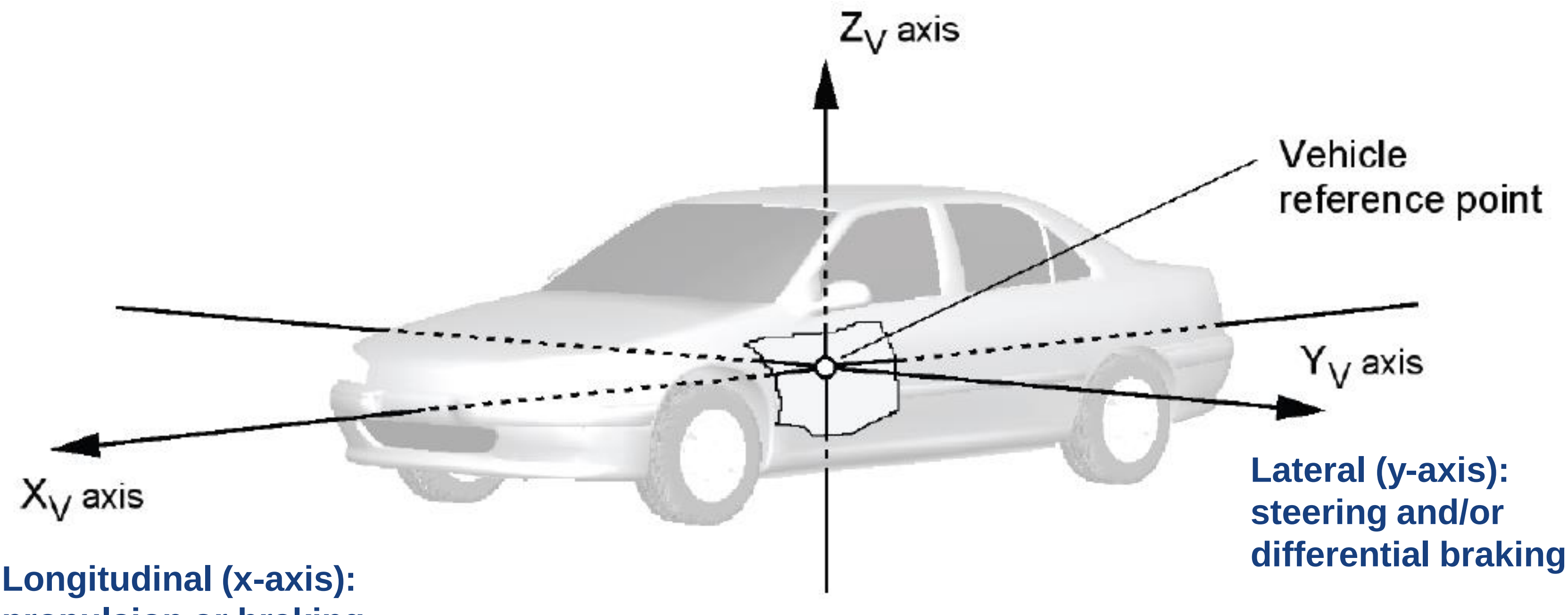


Use case sequence at **Level 4** showing *ADS* engaged with ***ODD* exit**, which **does not prevent continued *DDT* performance by an available human *user***. The *ADS feature* may prompt a *passenger* seated in the driver's seat (if available) to resume *DDT* performance; if no driver's seat with receptive *passenger*, the *ADS* automatically achieves a *minimal risk condition*

Graphics from SAE International J3016

Lateral and Longitudinal Vehicle Motion Control

Lateral & Longitudinal Vehicle Motion Control:
DDT subtask comprising the activities necessary for the real-time, *sustained* regulation of the **y-axis and x-axis** component of *vehicle* motion



Lateral (y-axis): steering and/or differential braking

Longitudinal (x-axis): propulsion or braking

A. VEHICLE AXIS SYSTEM – Z-UP

Graphics from SAE International J3016

Taxonomy of Driving Automation

Level	Name	Narrative definition	DDT: Sustained lateral and longitudinal vehicle motion control	DDT: OEDR	DDT fallback	ODD
Driver* performs part or all of the *DDT						
0	**No Driving Automation**	The performance by the *driver* of the entire *DDT*, even when enhanced by *active safety systems*.	*Driver*	*Driver*	*Driver*	n/a
1	**Driver Assistance**	The *sustained* and *ODD*-specific execution by a *driving automation system* of either the *lateral* or the *longitudinal vehicle motion control* subtask of the DDT (but not both simultaneously) with the expectation that the *driver* performs the remainder of the *DDT*.	*Driver* and *System*	*Driver*	*Driver*	Limited
2	**Partial Driving Automation**	The *sustained* and *ODD*-specific execution by a *driving automation system* of both the *lateral* and *longitudinal vehicle motion control* subtasks of the *DDT* with the expectation that the *driver* completes the *OEDR* subtask and *supervises* the *driving automation system*.	***System***	*Driver*	*Driver*	Limited
***ADS* (“*System*”) performs the entire *DDT* (while engaged)**						
3	**Conditional Driving Automation**	The *sustained* and *ODD*-specific performance by an *ADS* of the entire DDT with the expectation that the *DDT fallback-ready user* is *receptive* to *ADS*-issued *requests to intervene*, as well as to *DDT performance-relevant system failures* in other *vehicle* systems, and will respond appropriately.	*System*	***System***	*Fallback-ready user (becomes the driver during fallback)*	Limited
4	**High Driving Automation**	The *sustained* and *ODD*-specific performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	***System***	Limited
5	**Full Driving Automation**	The *sustained* and unconditional (i.e., not *ODD*-specific) performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	*System*	**Unlimited**

Summary of Driving Automation Levels

Note that: Level 5 “full driving automation” is the inverse analog of level 0 “no driving automation”

Graphics from SAE International J3016

Taxonomy of Driving Automation

Does the feature:

	Yes →	No
Perform the complete DDT and DDT fallback **without** ODD limitation?	Full Driving Automation **Level 5**	No
Perform the complete DDT and DDT fallback **within** a limited ODD?	High Driving Automation **Level 4**	No
Perform the complete DDT, but not DDT fallback, **within** a limited ODD?	Conditional Driving Automation **Level 3**	No
Perform **both** longitudinal and lateral vehicle motion control (on a sustained basis), but not complete OEDR?	Partial Driving Automation **Level 2**	No
Perform **either** longitudinal **or** lateral vehicle motion control (on a sustained basis), but not complete OEDR?	Driver Assistance **Level 1**	No
Perform none of the DDT or DDT fallback?	No Driving Automation **Level 0**	

Simplified logic flow diagram for assigning driving automation level to a feature

Graphics from SAE International J3016

Taxonomy of Driving Automation

	No *Driving Automation* 0	**Engaged Level of *Driving Automation*** 1	2	3	4	5
In-*vehicle user*	*Driver*			*DDT fallback-ready user*	*Passenger*	
Remote *User*	*Remote Driver*			*DDT fallback-ready user*	*Driverless operation dispatcher*	

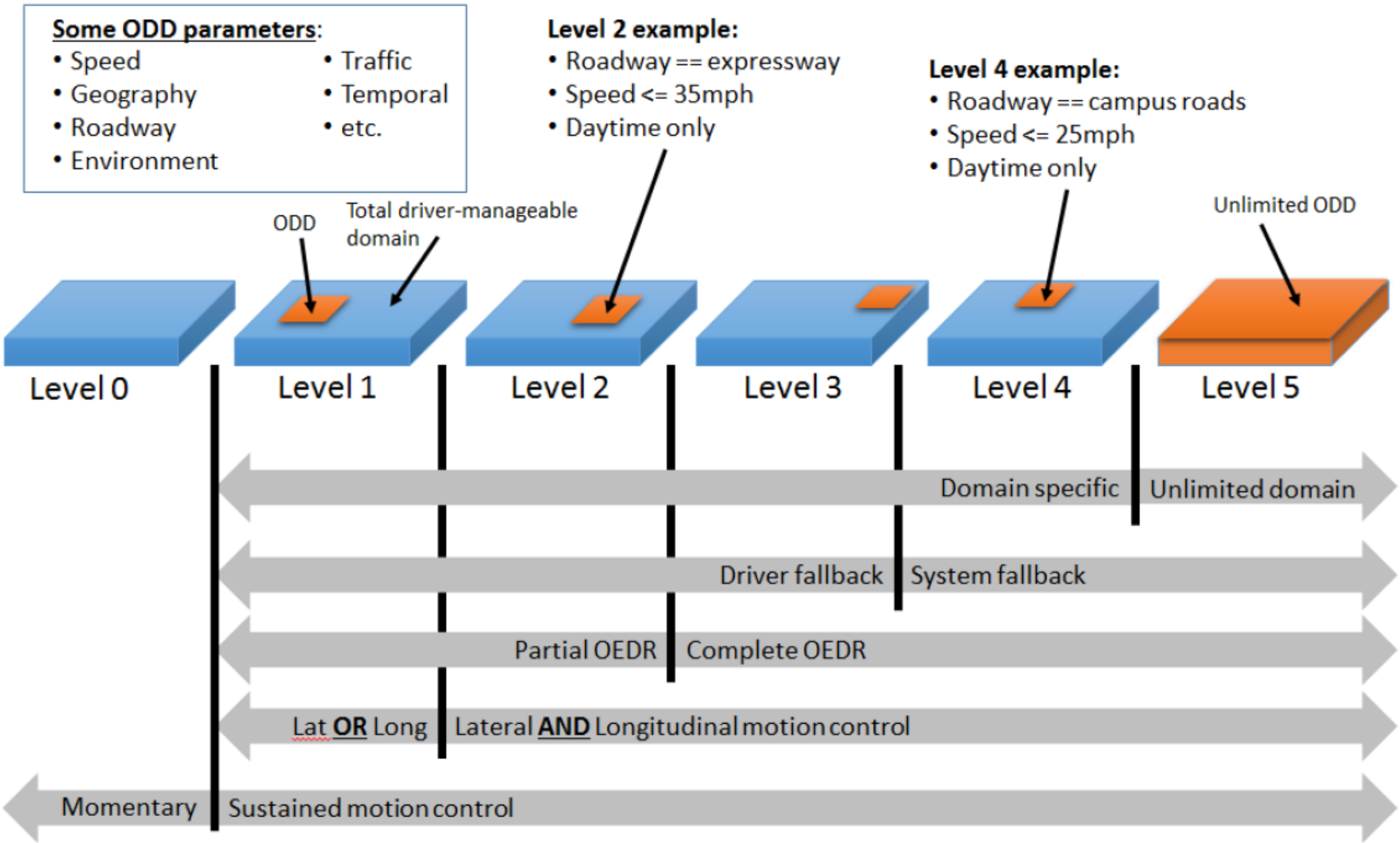
User roles while a driving automation system is engaged

Graphics from SAE International J3016

Taxonomy of Driving Automation; E.g.

- If the driving automation system performs the **sustained longitudinal and/or lateral vehicle motion control subtasks of the DDT**, the driver does not do so, although **s/he is expected to complete the DDT**. This division of roles corresponds to **levels 1 and 2**
- If the **driving automation system performs the entire DDT**, the user does not do so. However, if a DDT fallback-ready user is expected to take over the DDT when a DDT performance-relevant system failure occurs or when the driving automation system is about to leave its operational design domain (ODD), then that **user is expected to be receptive and able to resume DDT performance when alerted to the need to do so**. This division of roles corresponds to **level 3**
- Lastly, if **a driving automation system can perform the entire DDT and DDT fallback** either within a prescribed ODD or in all driver-manageable on-road driving situations (unlimited ODD), then any users present in the vehicle while the ADS is engaged are passengers. This division of roles corresponds to **levels 4 and 5**

Operational Design Domain (ODD); E.g.



ODD relative to driving automation levels

Graphics from SAE International J3016

Request to Intervene

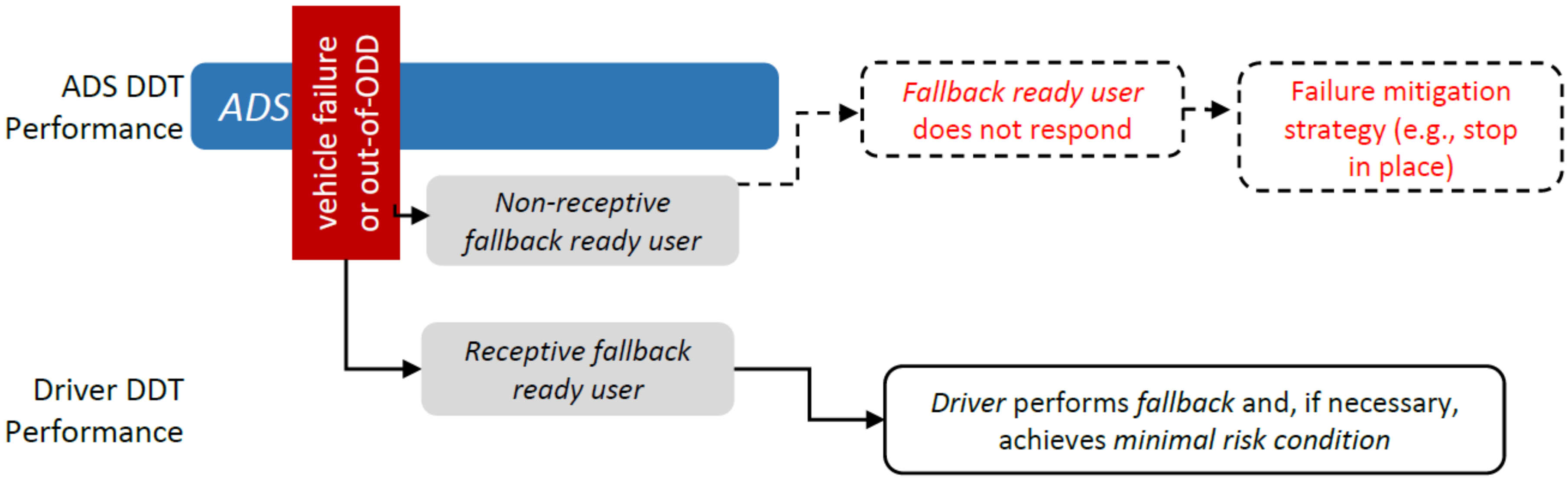
- The **situation where a system can no longer perform the DDT**, SAE J3016 indicates the system should issue a "*request to intervene*"; defined as:
  - "**Notification by an *ADS* to a *fallback-ready user* indicating that s/he should promptly perform the *DDT fallback*,** which may entail resuming **manual *operation*** of the *vehicle* (i.e., becoming a *driver* again), or achieving **a *minimal risk condition*** if the *vehicle* is not drivable."

- **Example:** "A level 3 ADS experiences a DDT performance-relevant system failure in one of its radar sensors, which prevents it from reliably detecting objects in the vehicle's pathway. The **ADS responds by issuing a request to intervene to the DDT fallback-ready user**. The ADS continues to perform the DDT, while reducing vehicle speed, for several seconds to allow time for the DDT fallback-ready user to resume operation of the vehicle in an orderly manner."

Failure Mitigation Strategy (FMS)

- **FMS:** "**strategy designed to bring the vehicle to a controlled stop wherever the vehicle happens to be**, if the driver fails to supervise the feature's performance (level 2), or if the fallback-ready user fails to perform the fallback when prompted (level 3)."
  - **E.g.** if the fallback-ready user of a level 3 traffic jam feature **fails to respond to a request to intervene after traffic clears (an out-of-ODD condition)**, the vehicle may have a failure mitigation strategy designed to **bring the vehicle to a controlled stop in its present lane of travel and turn on the hazard lamps**
- FMS is **different from minimal risk condition achievement and is not part of the fallback function** assigned to a level 4 or 5 ADS, because it **occurs after the ADS has disengaged or been incapacitated by a rare, catastrophic event**
  - **E.g. loss of backup power** after initial power failure **or incapacitation of the *ADS's* computing capability**, which **render it incapable of performing the *fallback*** and achieving a *minimal risk condition*

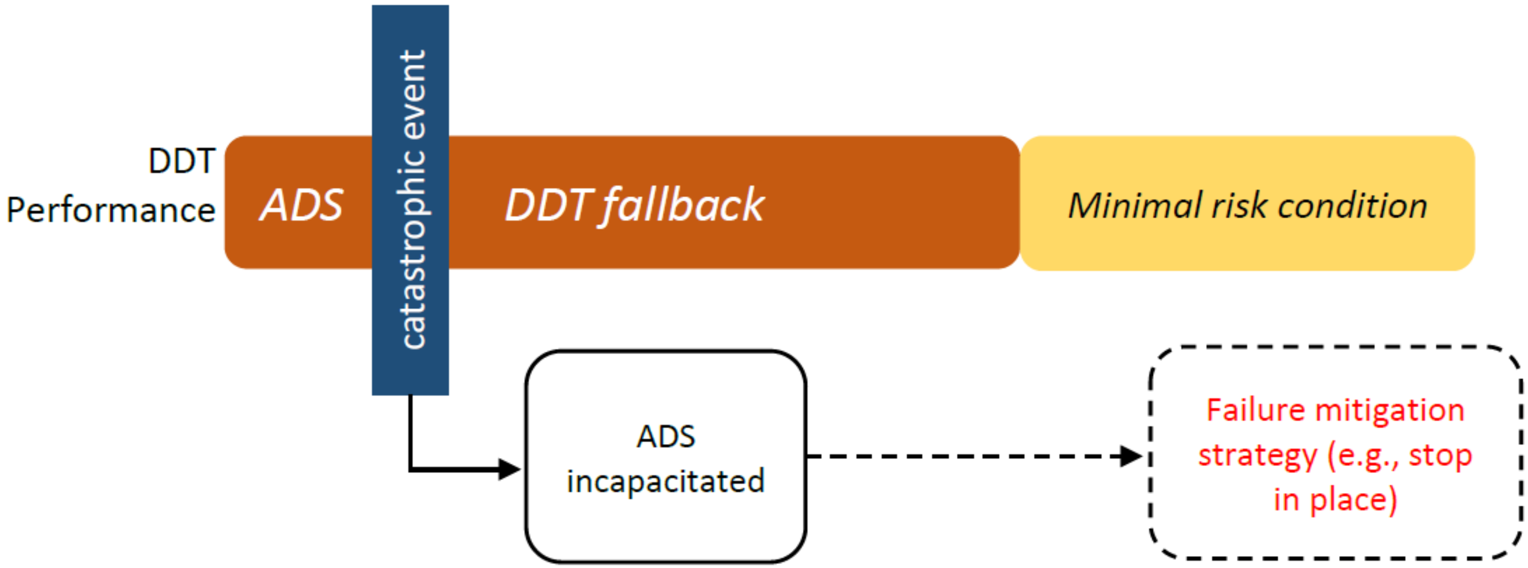
DDT Fallback vs Failure Mitigation Strategy (FMS)



Use case sequence for a **Level 3** feature showing ADS engaged, **occurrence of a failure or out-of-ODD condition**, and the fallback-ready user performing the **fallback, or**, if the fallback-ready user fails to do so, **a failure mitigation strategy**, such as stop-in-lane (Note: Dotted lines represent failure mitigation strategy)

Graphics from SAE International J3016

DDT Fallback vs Failure Mitigation Strategy (FMS)



Use case sequence at **Level 4** showing ADS engaged and will perform DDT fallback and achieve minimal risk condition as per normal. However, **in the event of a catastrophic event (e.g. complete power failure)**, the system will **adopt a FMS**. (Note: Dotted lines represent failure mitigation strategy)

Graphics from SAE International J3016

Practical Use of SAE J3016 in Europe

AdaptIVe (Automated driving applications and technologies for Intelligent Vehicles) Project

- **Co-funded by the European Commission** as part of the Seventh Framework Programme with €14.3 million **supported by the European Council for Automotive R&D, EUCAR**
- **29 partners from 8 countries – France, Germany, Greece, Italy, Spain, Sweden, The Netherlands, United Kingdom; including 11 original equipment manufacturers, 4 suppliers, 11 research institutes and universities, and 3 small/medium enterprises**
- Objectives include human factors issues, evaluation methods, and legal aspects
- Deliverable D2.1 - System Classification and Glossary
  - Describes harmonization of levels between BASt, VDA, and SAE
  - **Applies these harmonized levels and SAE J3016 supporting terms**

Practical Use of SAE J3016 in US

CAMP AVR (Crash Avoidance Metrics Partnership Automated Vehicle Research) Project

- **Cooperative Research Agreement with NHTSA** (i.e. National Highway Traffic Safety Administration)
- **Consortium members: Ford Motor Company, General Motors, Nissan, Mercedes-Benz, Toyota, and Volkswagen Group of America**
- Objectives included: functional descriptions of automation levels, list of potential driving automation features, level-specific safety principles, potential objective test methods for evaluating driving automation systems
- CAMP AVR Consortium **incorporated the SAE J3016 levels and supporting terms and embellished upon them**
- Final report has been submitted to NHTSA

2. SINGAPORE STANDARDS COUNCIL – TR-68-1/2/3

Disclaimer:

The materials on the following slides are adapted from TR-68-1/2/3 documents, and are included for educational and informational purposes. Singapore Standards Council (SSC) still reserves the right to the content used. It must not be reproduced, copied or communicated to any third party. It is strictly not for advisory or distribution purposes. NUS-ISS accepts no liability or responsibility whatsoever for the content in these slides, in respect of any use of or reliance upon these slides by any other party.

TR-68 Part 1: Basic Behaviour

Purpose of TR-68-1 (Basic Behaviour):

- **Describes required AV basic driving behaviours**
  - ➢ DDT and behavior controlled by the ADS of an AV
  - ➢ Conduct of AV driving
  - ➢ Road signs, markings and traffic signals interpretation
- **Definitions adapted from SAE J3016_2018**
- **Applicable to the following parties:**

  a) AV-related companies (i.e. developers/operators, manufacturers, suppliers)

  b) Relevant govt organizations (e.g. LTA, TP)

  c) Vehicle testing, inspection and certification organizations (e.g. VICOM, STA)

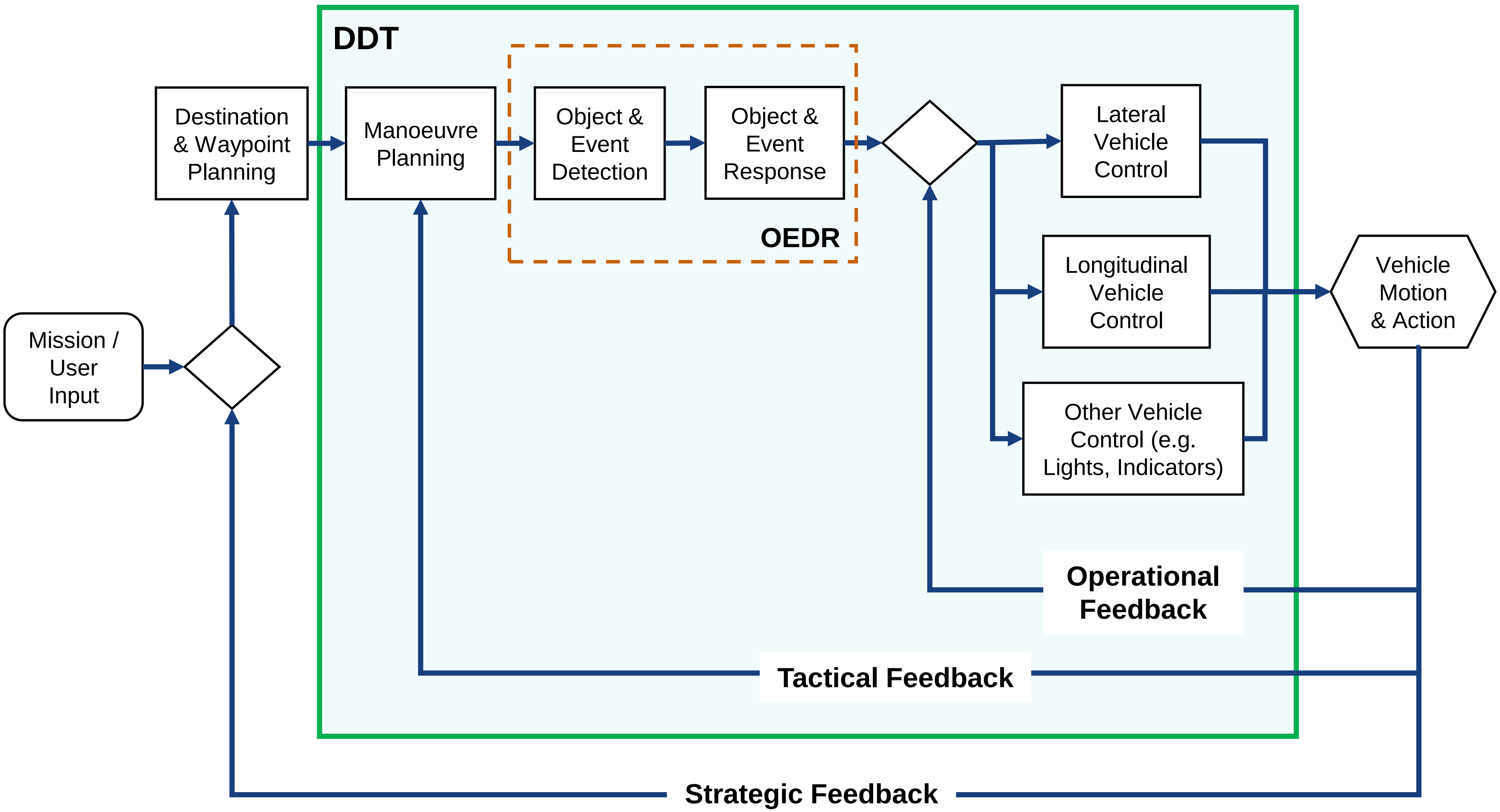
  d) Motor insurance companies

  e) Service and data providers (e.g. SingTel, Starhub)

Content adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

DDT Process Flow Chart (TR-68 Version):



Content and Graphics adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

Assumptions made for TR-68-1:

a) **AVs will be deployed on existing infrastructure** (i.e. public roads with current traffic facilities) together with other non-autonomous vehicles (i.e. Level 0 and 1), pedestrians, bicycles and PMDs

b) **Current driving rules and regulations will apply to all AVs** (e.g. road traffic rules, Highway Code, traffic facilities)

c) **No on-board human operator will be involved in the AV operations**; this TR does not consider the human-AV interface

d) **AVs are expected to only depend on on-vehicle systems to provide safe operation**. In other words, if any critical events occur (e.g. malfunctions, power loss, cyberattacks), the AVs cannot rely on any off-vehicle systems (e.g. wireless communications) to execute safety measures

e) **The responsibility for ensuring a safe vehicle deployment will be bore by the AV developer/operator**. This includes validation and verification of the AV and other relevant systems

Content adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

Filtering Rules Applicable to AV Driving Behaviour:

Input = BTD + FTD → Is item a rule?

Is item a rule? — **No** → **Item not a rule END**

Is item a rule? — **Yes** → Is rule specific to human driving?

Is rule specific to human driving? — **Yes** → **Rule not applicable to AVs END**

Is rule specific to human driving? — **No** → Does rule relate to DDT?

Does rule relate to DDT? — **No** → **Rule not applicable to TR-68-1 END**

Does rule relate to DDT? — **Yes** → **The rule is applicable END**

Not all items in the BTD and FTD are rules; some are general information, which are not applicable

E.g. rules that target undesirable human emotions/actions (like road rage, drink drive, tailgating, reckless overtaking), rules that describes how humans perform physical actions (like checking blind spots, turning the steering wheel)

E.g. Journey planning before driving, opening vehicle doors without endangering anyone

BTD = Singapore’s Basic Theory of Driving
FTD = Singapore’s Final Theory of Driving

Content and Graphics adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

What happens if AV faces dilemmas (common in current driving situations)? Examples of dilemmas:

- Preventing harm
- Maintaining traffic movements
- Conflicting rules (e.g. various driving rules result in different required actions to a given situation)

Two Directives for Automated Driving to resolve dilemmas:

A. **Prime Directive: To ensure safety**
   - Able to violate driving rules to avoid any harmful events

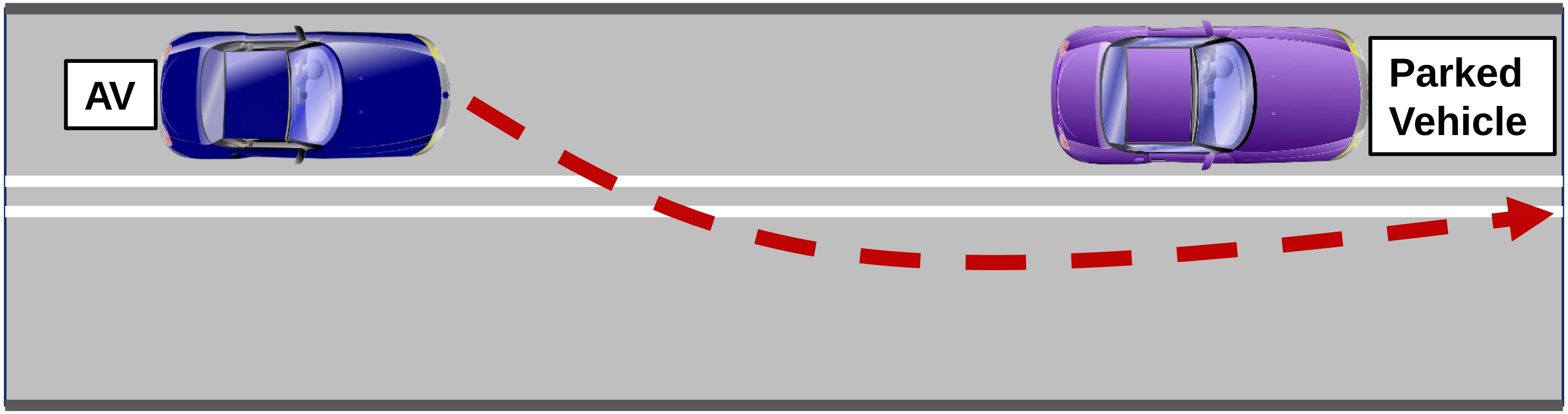
B. **Secondary Directive: To ensure free movement of traffic**
   - Able to violate driving rules if not doing so will lead to unnecessary traffic obstruction, provided if Rule A still applies (i.e. no unreasonable safety risks taken)

Content adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

Examples of Application of Directives for Automated Driving to resolve dilemmas; E.g. 1:

- Violate driving rules by crossing the double white line to overtake an illegally parked car in order to ensure free movement of traffic.
- Prime directive still applies; no foreseen danger inflicted if action is carried out

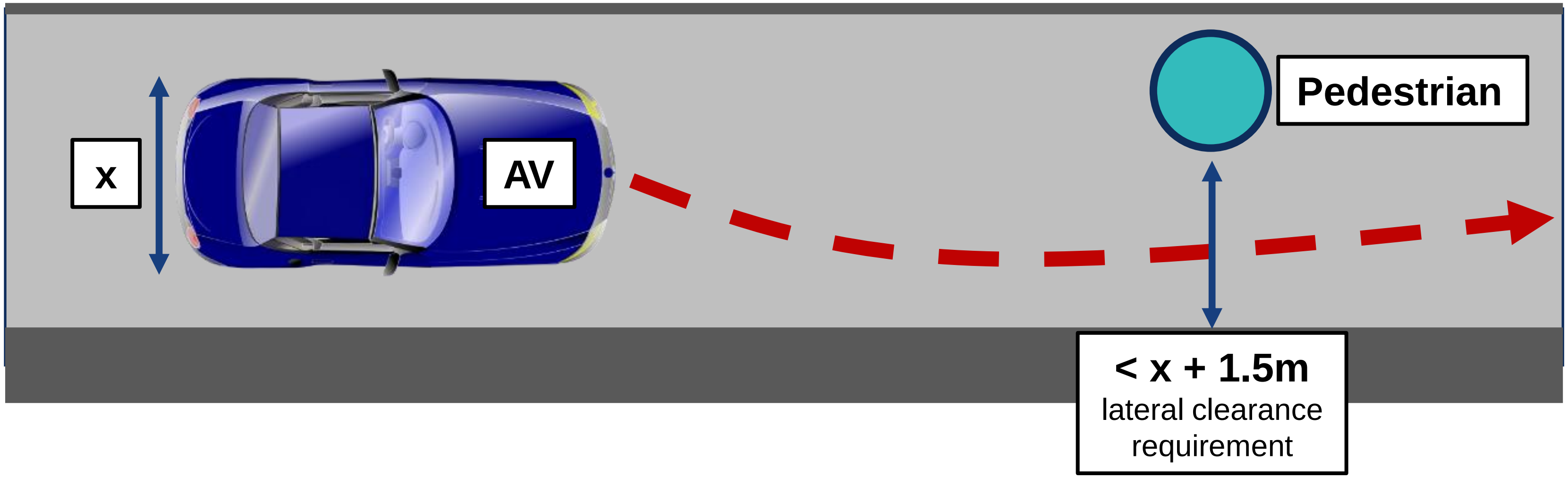


Content and Graphics adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

Examples of Application of Directives for Automated Driving to resolve dilemmas; E.g. 2:

- Violating a rule pertaining to lateral clearance requirement; able to proceed as long as physical clearance is sufficient. This ensure free movement of traffic
- Prime directive still applies; no foreseen danger inflicted if action is carried out

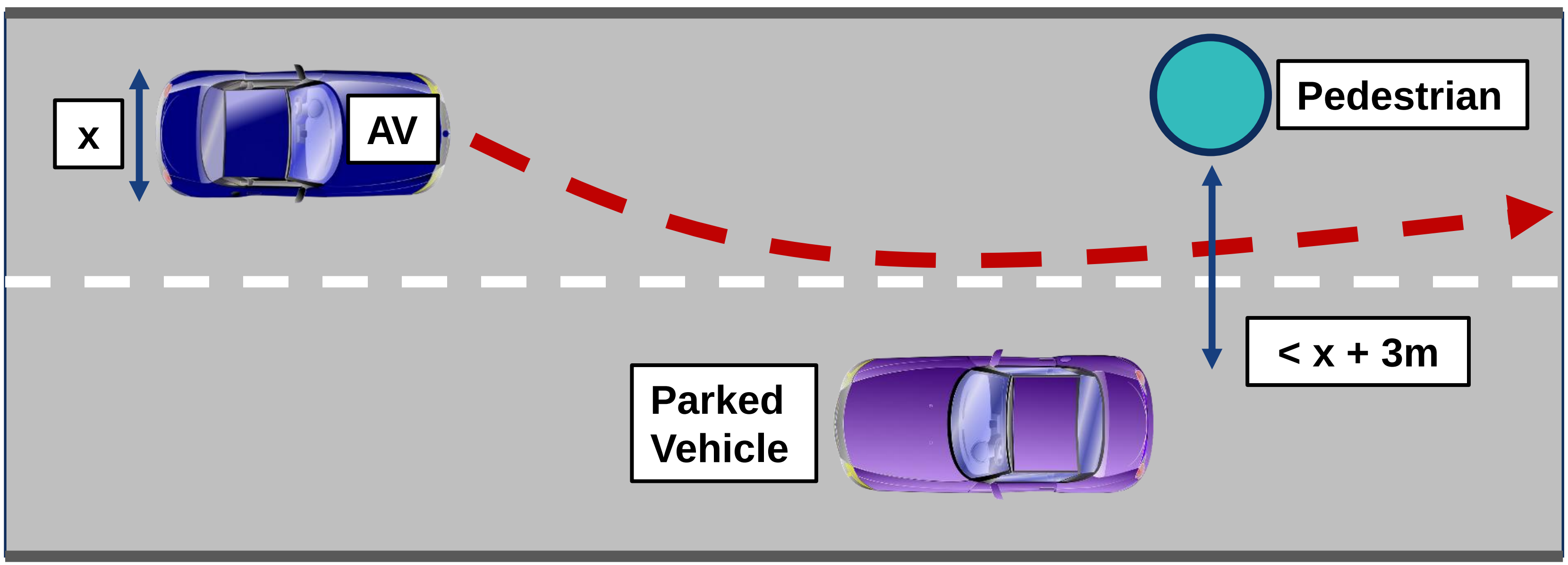


Content and Graphics adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

Examples of Application of Directives for Automated Driving to resolve dilemmas; E.g. 3:

- **If violating rules are necessary, it must be done minimally**
- Violating more lateral clearance toward one actor (e.g. parked car) and less toward a more vulnerable actor (e.g. pedestrian)
- Prime directive still applies; no foreseen danger inflicted if action is carried out



Content and Graphics adapted from TR-68-1

TR-68 Part 1: Basic Behaviour

Conduct of DDT by AVs Pertaining to the Interpretation of rules:

- **Hand signals** – AVs must be able to detect and recognize hand signals by humans (e.g. police officers, other road users, construction/school traffic facilitators) and respond accordingly
- **Vehicles on Emergency Calls** – Able to detect and respond to such vehicles (i.e. ambulances, police cars)
- **Use of Mapping and Adherence to Traffic Signs and Road Markings** – All relevant traffic signs and road markings can be found in the BTD

Content adapted from TR-68-1

TR-68 Part 2: Safety

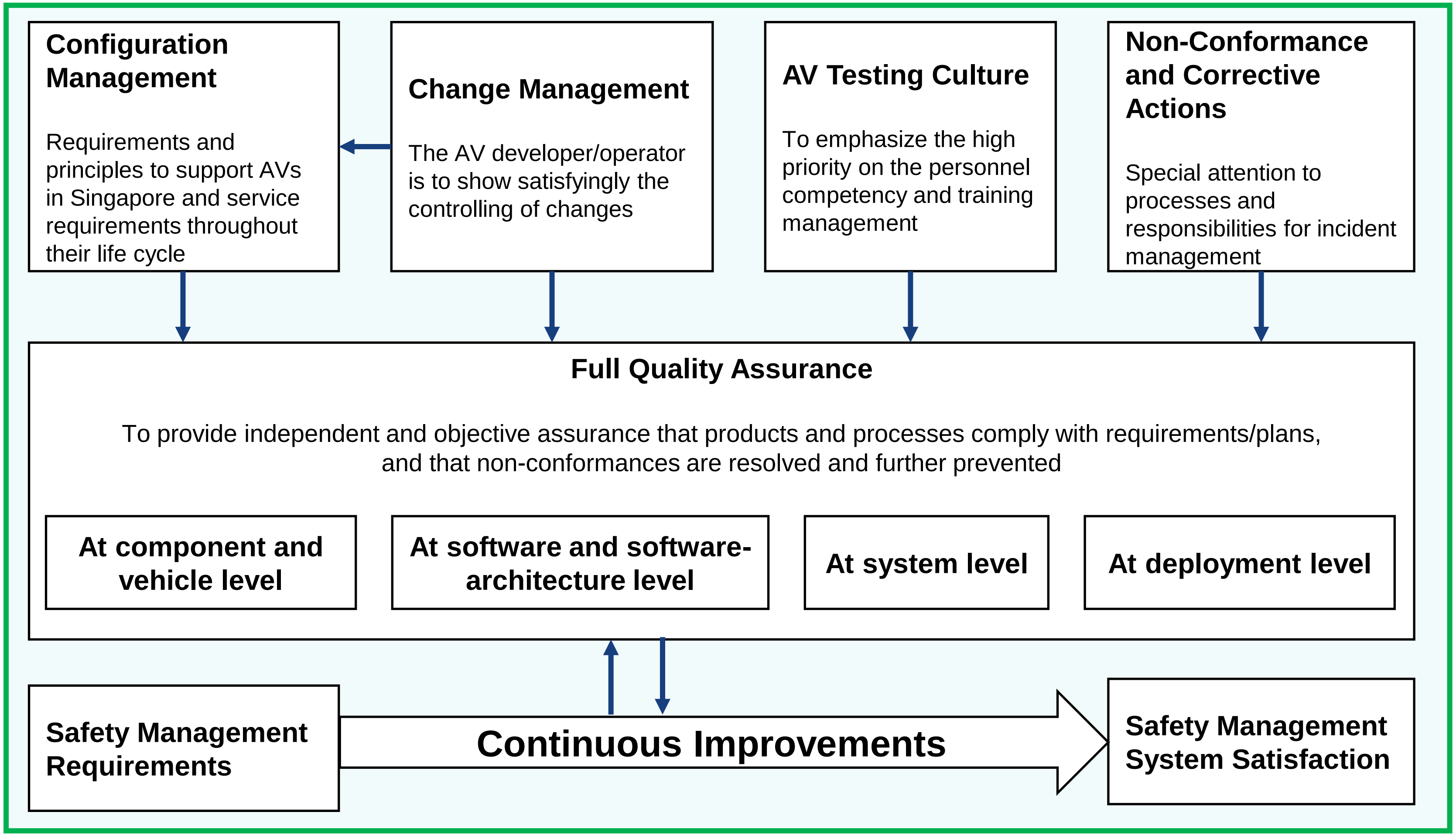
Purpose of TR-68-2 (Safety):

- **Describes a set of minimal safety requirements to be met by AV developers, manufacturers and/or operators**
- **Focuses on Quality and Safety Management Systems**
- **Applicable to the following parties:**
  a) AV developers/operators
  b) Relevant govt organizations (e.g. LTA, TP)
  c) Vehicle testing, inspection and certification organizations (e.g. VICOM, STA)
  d) Engineering and consulting companies (e.g. ST Engineering)

Content adapted from TR-68-2

TR-68 Part 2: Safety

Quality Management System Overview



Content and Graphics adapted from TR-68-2

TR-68 Part 2: Safety

Safety Management System Overview

AV & Sg Operations

"What does the AV do?"

AV functions, manoeuvres, platform integration, services and interactions

"Where does the AV operate?"

Use cases, traffic, scenarios, weather, geography, road types, infrastructure

Hazard Analysis & Risk Assessment

"What can happen?"

Assessment of the negative impacts of failures and malfunctions of the AV system during operational

"How bad is that?"

Rating of identified hazards to measure risk/severity/criticality pertaining to likelihood/exposure

Risk Mitigation Strategy

"Addressing identified risks in AV?"

Safety measures in AV design for prevention/mitigation of identified hazards, appropriate for its risk level

"Restricting operations?"

Operational restrictions to mitigate or prevent identified hazards without an AV design measure in place

System Safety & SOTIF

"Does the AV do the right thing?"

Assessment of whether what the AV does is safe, ethical and expected

"How good must the AV be?"

Determination of performance metrics for AV system components

Application & Implementation

"Software updates safe?"

Ensure software changes are properly managed and validated

"Safety-related applications"

Requirements for AV suppliers and integrators

Validation

"Validating what?"

Test cases drafted to cover all of the AV functions and manoeuvres in the Sg operational domain, with the safety mitigations/preventions in place

"Validating how?"

Execution of test cases using virtual validation (i.e. simulation), closed road testing, public road testing for reliability and accuracy

SOTIF = Safety of the Intended Functionality

Content and Graphics adapted from TR-68-2

TR-68 Part 2: Safety

Other Considerations in TR-68-2

a) Human Machine Interface (HMI) within safety systems

- **AVs of L4/5** (in SAE terms) should **exclude safety roles for humans**
- **Assume as though there are no human occupants in AVs for use cases relevant to TR, as passengers are occupied with non-driving activities**
- Hence, **necessary for a remote takeover to be possible without involving the passengers pertaining to safety measures**

b) Artificial Intelligence (AI) within safety systems

- The application of AI has the potential to enhance safety. However……
- **Explicitly prohibit usage of AI during AV operations to influence the system safety and for other intended safety functions**
- Usage of AI **allowed during development and testing phases** as long as it does not compromise the safety aspect of the AV (e.g. collecting and transferring data from AV to a test platform located outside the AV. This test platform utilizes AI to optimize the AV performance)
- Usage of AI **allowed in non-safety related parts of the system**; functional independence necessary

Content adapted from TR-68-2

TR-68 Part 3: Security

Purpose of TR-68-3 (Cybersecurity):

- **TR for enhanced cybersecurity framework for AVs**
  - Sg does not manufacture vehicles; dependent on AV developer/operator for security-by-design processes
  - Independent approach required to ensure foolproof cybersecurity (i.e. conducting cybersecurity assessment of AVs before deploying them on the roads)
- **2 tiers of cybersecurity safeguards:**

  A. Cybersecurity Principles

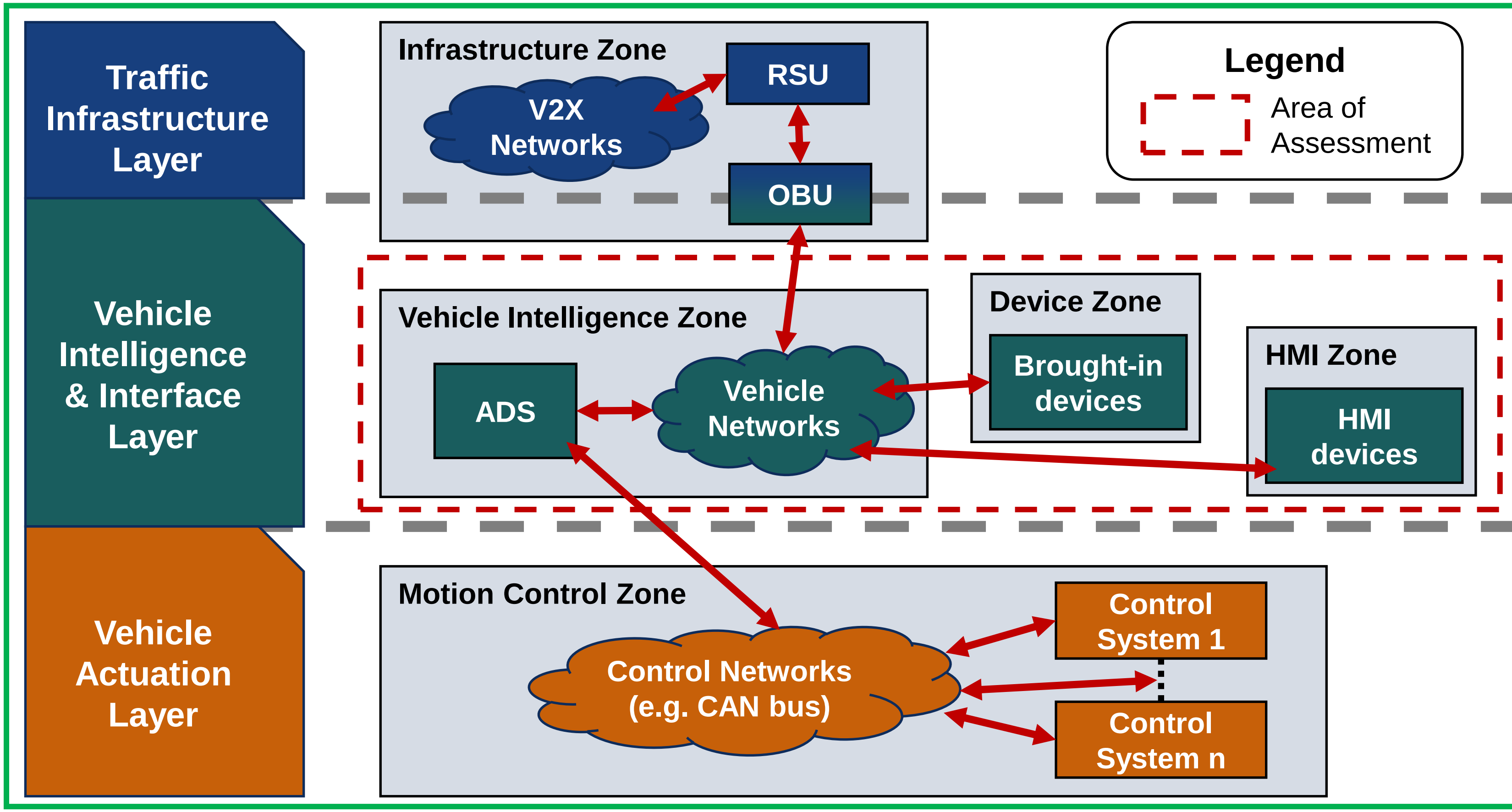
  B. Cybersecurity Assessment Framework

Content adapted from TR-68-3

TR-68 Part 3: Security

AV Security Zone

(includes area of assessment covered in this TR)



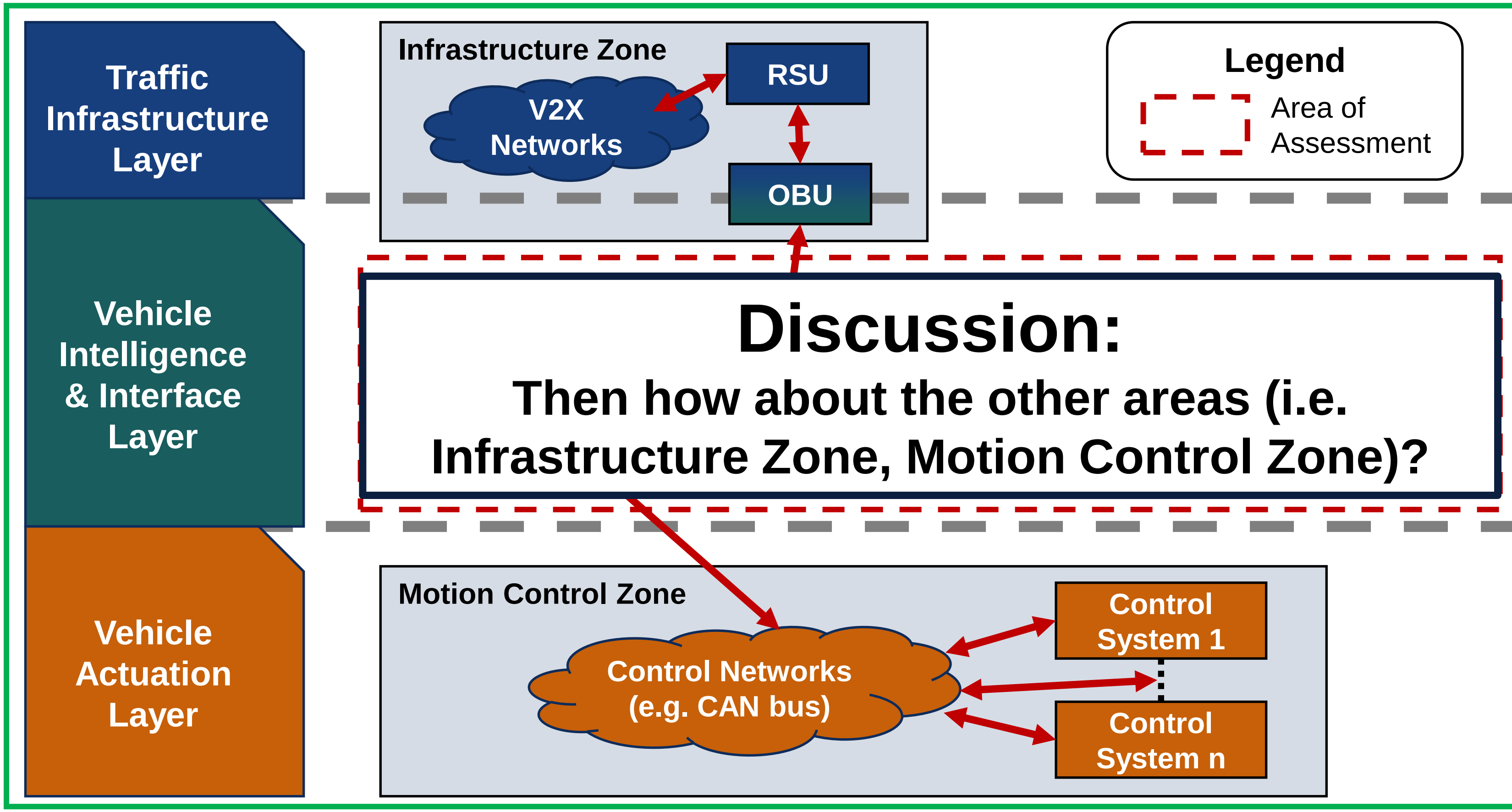
RSU = roadside units, OBU = On-Board Unit,
V2X = Vehicle to everything, ADS = Automated Driving System,
CAN = Controller Area Network

Content and Graphics adapted from TR-68-3

TR-68 Part 3: Security

AV Security Zone

(includes area of assessment covered in this TR)



RSU = roadside units, OBU = On-Board Unit,
V2X = Vehicle to everything, ADS = Automated Driving System,
CAN = Controller Area Network

Content and Graphics adapted from TR-68-3

Cybersecurity Key Principles:

Security-by-design	Defence-in-depth	Continuous Operational Management & Oversight	Resiliency
- Cybersecurity considered **from early development stages** and integrated into the design - Security practices should be **built on established standards and proven methods** - **Evaluated and certified products** must be used at all times - **Design safeguards must be considered** to account for potentially untrusted components	- **Apply a holistic approach for security on the system architecture**; this ensures a more complete and comprehensive protection - **E.g.** compartmentalisation, multi-layered defence, multifactor authentication, multitier access control - **Do not rely on security by obscurity as a solution** (i.e. design/implementation secrecy)	- Cybersecurity operations cycle includes: **Prevent/Predict** (threat anticipation), **Detect** (threat discovery), **Respond** (mitigation and containment measures), and **Recover** **- Protection must be proactive; not static** **- Mandatory continuous security updates and vulnerability management**	- Cybersecurity attack is a **matter of when** - Hence, **AV operations must be resilient to cybersecurity attacks** - About **ensuring the preparedness and readiness of cybersecurity** - **E.g.** periodic design review, penetration test, consequence management

Content adapted from TR-68-3

TR-68 Part 3: Security

Cybersecurity Assessment Framework:

AV System

↓

System Review

TRA	Threat Mgmt	SAO	Intended Use

↓

Threat Risk Analysis

Threat Analysis	Threat Classification	Risk Assessment

↓

Cybersecurity Testing

Vulnerability Analysis	Fuzz Testing	Attack Simulation

↓

Report

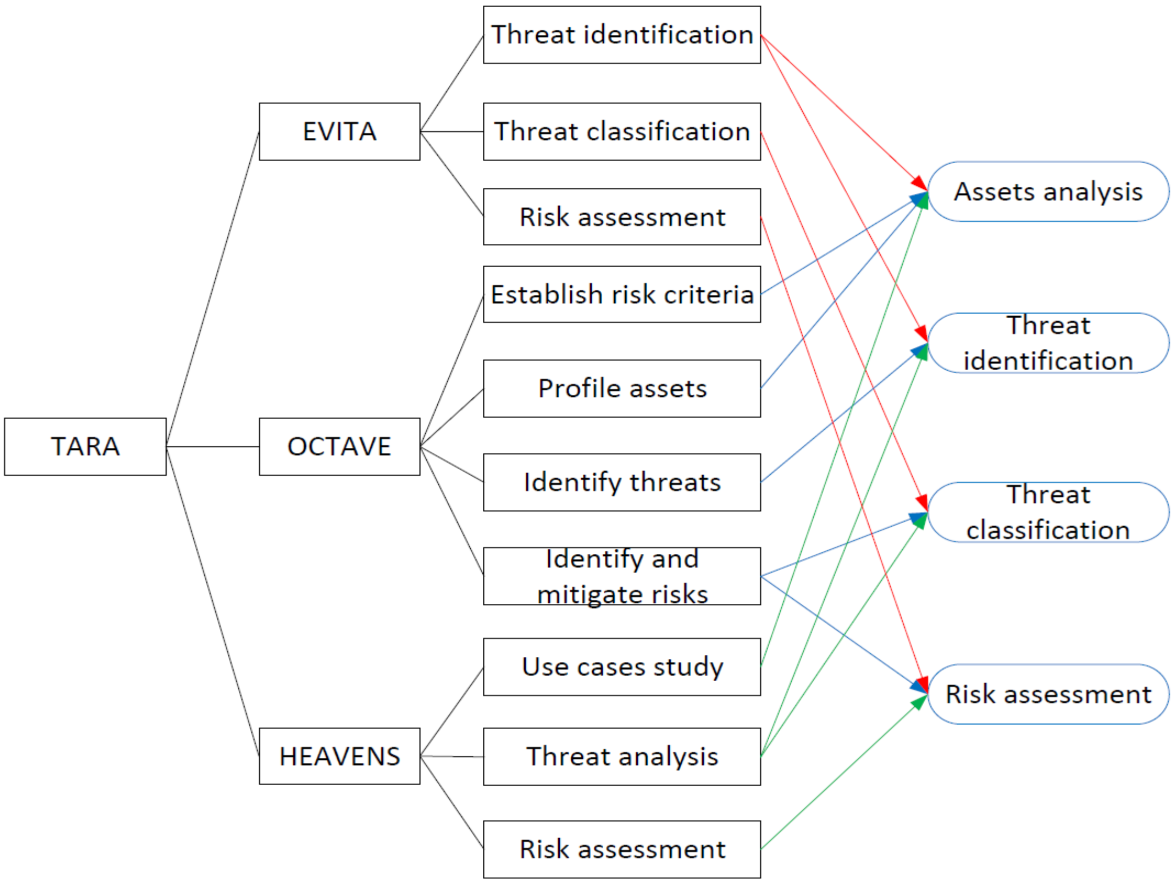
Results	Evaluated Risks	Recommendations

TRA = Threat Risk Assessment
SAO = System Architecture Overview

Content adapted from TR-68-3

TR-68 Part 3: Security

Various Methods for TARA:

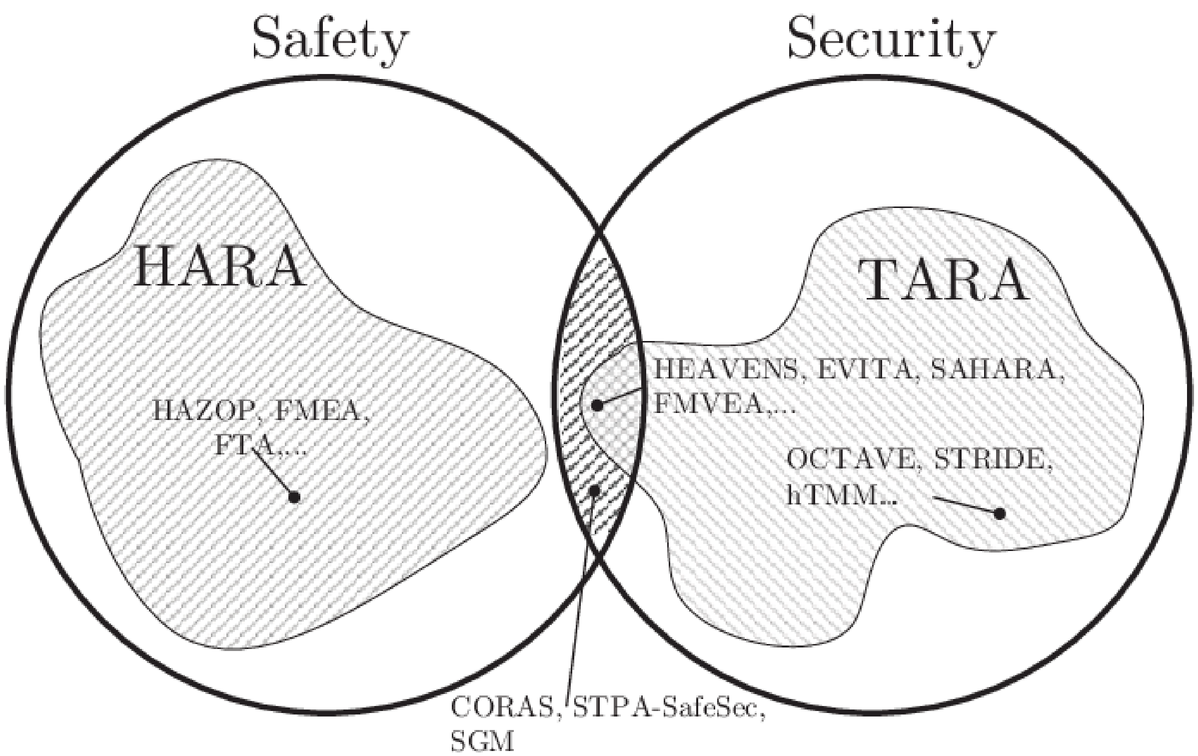


Graphics from *On the Alignment of Safety and Security for Autonomous Vehicles* by Cui, et al.

TARA = Threat Analysis & Risk Assessment, OCTAVE = Operationally Critical Threat, Asset, and Vulnerability Evaluation, EVITA = E-safety Vehicle Intrusion proTected Applications, HEAVENS = HEAling Vulnerabilities to Enhance Software Security and Safety

TR-68 Part 3: Security

Classification of HARA (for Safety) and TARA (for Security) methods:



Graphics from *Enhancement of Automotive Penetration Testing with Threat Analyses Results* by Dürrwang, et al.

TR-68 Part 4: Vehicular data types and formats

Purpose of TR-68-4 (Data):

- **TR for standardized services and data exchange formats for AVs**
  - Emphasizes a common communication protocol for data exchange
  - Aims to facilitate efficiency in communication processes that involve multiple parties, enabling interoperability among parties in an AV ecosystem
  - Only relevant to Lvl 4 and 5 AVs in mixed-use traffic and on public roads
- **Applicable to the following parties:**
  a) AV developers/operators
  b) Vehicle testing, inspection and certification organizations (e.g. VICOM, STA)

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Key Specifications; Defines vehicular data types & formats for:

- Automated driving data recording
- Safe and effective use of AV data
- Dynamic content management (e.g. HD maps, traffic info)
- Accident investigation and claim disputes
- V2X (Vehicle-to-Everything) communication for safety and efficiency

Exclusions:

- Over-the-air software updates
- AV fleet management systems
- Interfaces between AVs and human operators/drivers
- Data privacy and ownership concerns

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

TR-68-4 adopts the following assumptions:

1. **Deployment Environment:** AVs will operate on public roads with mixed traffic, including interaction with various road users (e.g. other vehicles, pedestrians, bicycles).
2. **Regulatory Stability:** No changes to existing traffic rules, road signs, or signals to accommodate AVs.
3. **No Human Operator:** AVs will operate without an in-vehicle fallback human operator; the TR does not address AV-human operator interfaces.
4. **Independence from Off-Vehicle Systems**: AVs must operate safely without reliance on external systems (e.g. cloud-based services, remote operation centres, V2X network). If external communication is disrupted, AVs should still function safely.
5. **Developer/Operator Responsibility:** AV developers and operators are responsible for safe deployment, validation, and verification of AV systems, not transferring safety responsibilities to assessors.
6. **Electronic Identification:** AVs must be identifiable electronically.
7. **Programming Flexibility:** The TR does not specify a programming language for data exchange; parties can choose their preferred language.

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

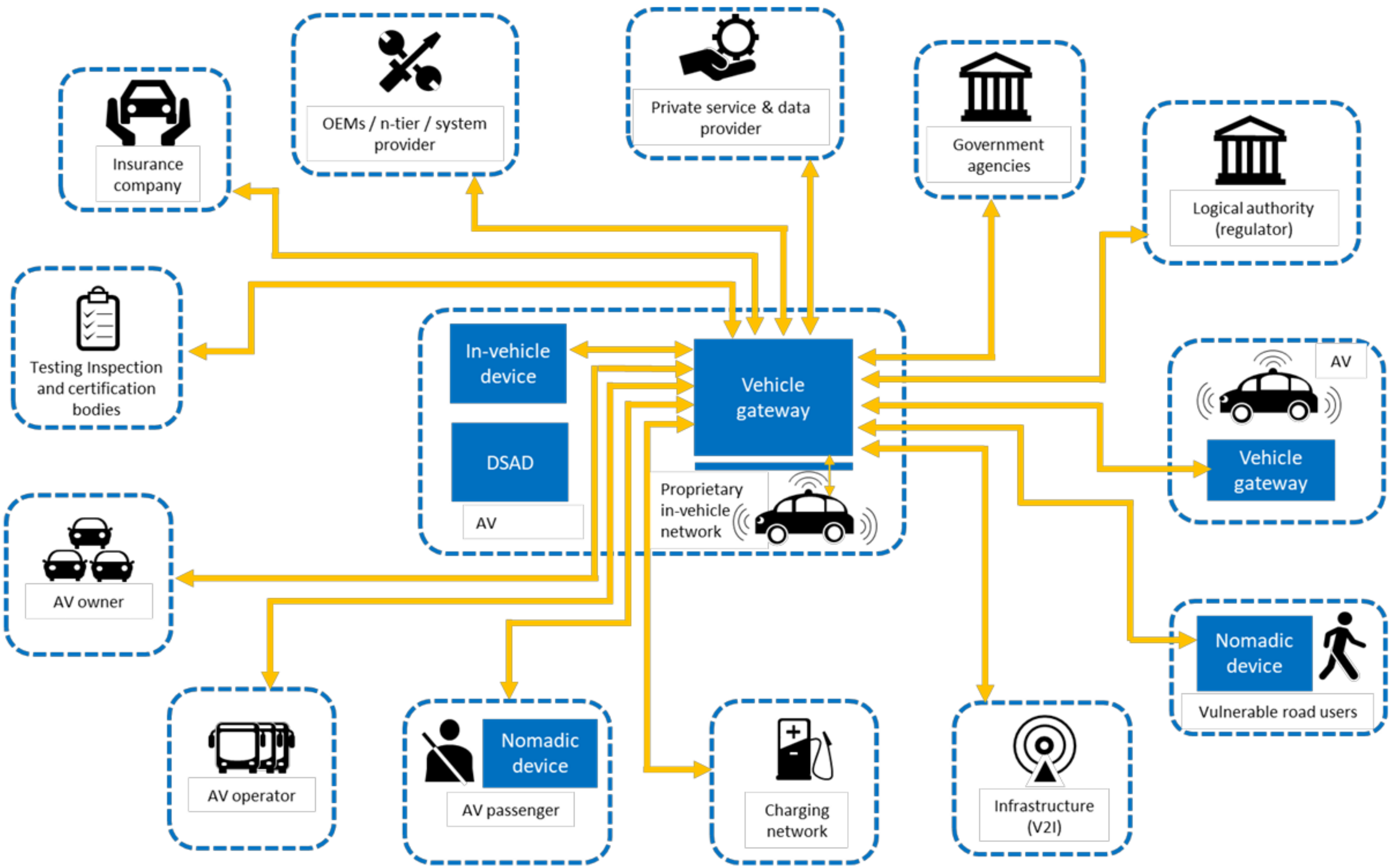


Figure 1 – An AV ecosystem

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

AV Ecosystem:

- This framework helps define the data sets required for different use cases and supports the safe and efficient operation of AVs in a connected environment.
- Includes various stakeholders interacting with Autonomous Vehicles (AVs) through a vehicle gateway, which manages communication between the AV and external entities.
- **Key components and interactions**
  - **Vehicle Gateway:** Central communication hub within the AV that connects in-vehicle devices, sensors, actuators, and the AV operating system with external entities.
  - **In-Vehicle Devices and DSSAD:** Devices within the AV, including the Data Storage System for Automated Driving (DSSAD), that gather and exchange data.
  - **External Interactions:** AVs interact with other AVs, infrastructure equipment, nomadic devices (brought into the vehicle by users), and servers that provide or consume data.
  - **Stakeholders:** Include OEMs, system providers, private service and data provider, government agencies, regulatory bodies, insurance companies, AV operators, AV owners/passengers, and vulnerable road users. These entities are involved in various use cases and data exchanges.

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Examples of use cases

1. Sharing of Sensor Data with Local Authorities

- **Goal:** Ensure safety and reliability by sharing sensor data with authorities for certification, monitoring, and investigation.
- **Data Classes:** AVInfo, AV (Navigation, Perception, Controls, Monitoring)
- **Data Flow:** Data sharing

2. AV to AV Data Sharing for Enhanced Navigation Safety

- **Goal:** Improve navigation safety by allowing AVs to share data and communicate with each other.
- **Data Classes:** AV (Navigation, Perception)
- **Data Flow:** Data exchange and/or data sharing

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Examples of use cases (Cont)

3. AV Data to Private Service and Data Providers and vice versa

- **Goal:** Enhance road safety and efficiency by sharing real-time data with private service and data providers to update environmental changes.
- **Data Classes:** AV (Navigation, Perception, Controls, Monitoring), Infrastructure (Static, Dynamic)
- **Data Flow:** Data exchange and/or data sharing

4. AV to Driver/Passenger Data Sharing

- **Goal:** Communicate critical information to passengers using in-vehicle or handheld devices. E.g. AV making an unexpected stop or terminating a service.
- **Data Classes:** AV (Navigation, Perception)
- **Data Flow:** Data sharing

5. AV to OEM/System Provider

- **Goal:** Facilitate servicing, repair, and preventive maintenance through communication between AV and manufacturers.
- **Data Classes:** AVInfo, AV (Perception, Controls, Monitoring)
- **Data Flow:** Data exchange and/or data sharing

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Examples of use cases (Cont)

6. AV Sending/Receiving Data to/from Road Infrastructure

- **Goal:** Enhance safety and efficiency by sharing data with road infrastructure (e.g. traffic lights, smart signs) for better navigation and maneuvering.
- **Data Classes:** AV (Navigation, Perception, Monitoring), Infrastructure (Static, Dynamic)
- **Data Flow:** Data exchange and/or data sharing

7. AV Exchanging Priority Information with Traffic Control Infrastructure [focuses on priority vehicles!]

- **Goal:** Support priority vehicles by exchanging data to ensure safe navigation.
- **Data Classes:** AV (Navigation, Perception, Monitoring), Infrastructure (Static, Dynamic)
- **Data Flow:** Data sharing and/or data exchange

8. AV Exchanging Data with Vulnerable Road Users

- **Goal:** Improve safety by sharing situational data (e.g. location, intention) with vulnerable road users to avoid accidents, and vice versa.
- **Data Classes:** AV (Navigation, Perception)
- **Data Flow:** Data sharing and/or data exchange

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Examples of use cases (Cont)

9. AV Data Exchange During Medical/Safety Emergencies

- **Goal:** Release emergency alerts through AV monitoring systems.
- **Data Classes:** AV (Monitoring)
- **Data Flow:** Data sharing and/or data exchange

10. AV Data Sharing with Insurance Companies

- **Goal:** Provide data about vehicle performance and health status for insurance assessment purposes in event of claims or incidents.
- **Data Classes:** AVInfo, AV (Navigation, Perception, Monitoring, Controls), Infrastructure (Dynamic, Static)
- **Data Flow:** Data sharing

11. Government Agencies Providing Information to AVs

- **Goal:** Facilitate AV operations by providing transport-related data (from government agencies) to AV operators [www.mytransport.sg]
- **Data Classes:** Infrastructure (Static, Dynamic)
- **Data Flow:** Data sharing

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Examples of use cases (Cont)

12. Stations Exchanging Information with AVs for Service Provisioning Purposes

- **Goal:** Optimize AV charging and service provisioning by sharing information with charging networks. E.g. physical location, operational availability, efficiency and type of charging stations
- **Data Classes:** AVInfo, AV (Navigation, Perception, Monitoring, Controls), Infrastructure (Dynamic, Static)
- **Data Flow:** Data sharing and/or data exchange

13. AV Exchanging Data with Transit Stops for operational needs

- **Goal:** Enhance operational efficiency for AV buses and taxis by interacting with transit stops and commuters waiting there. E.g. transit stops can broadcast to nearby AVs their status, the demand for a specific service, etc
- **Data Classes:** AVInfo, AV (Navigation), Infrastructure (Static)
- **Data Flow:** Data sharing and/or data exchange

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

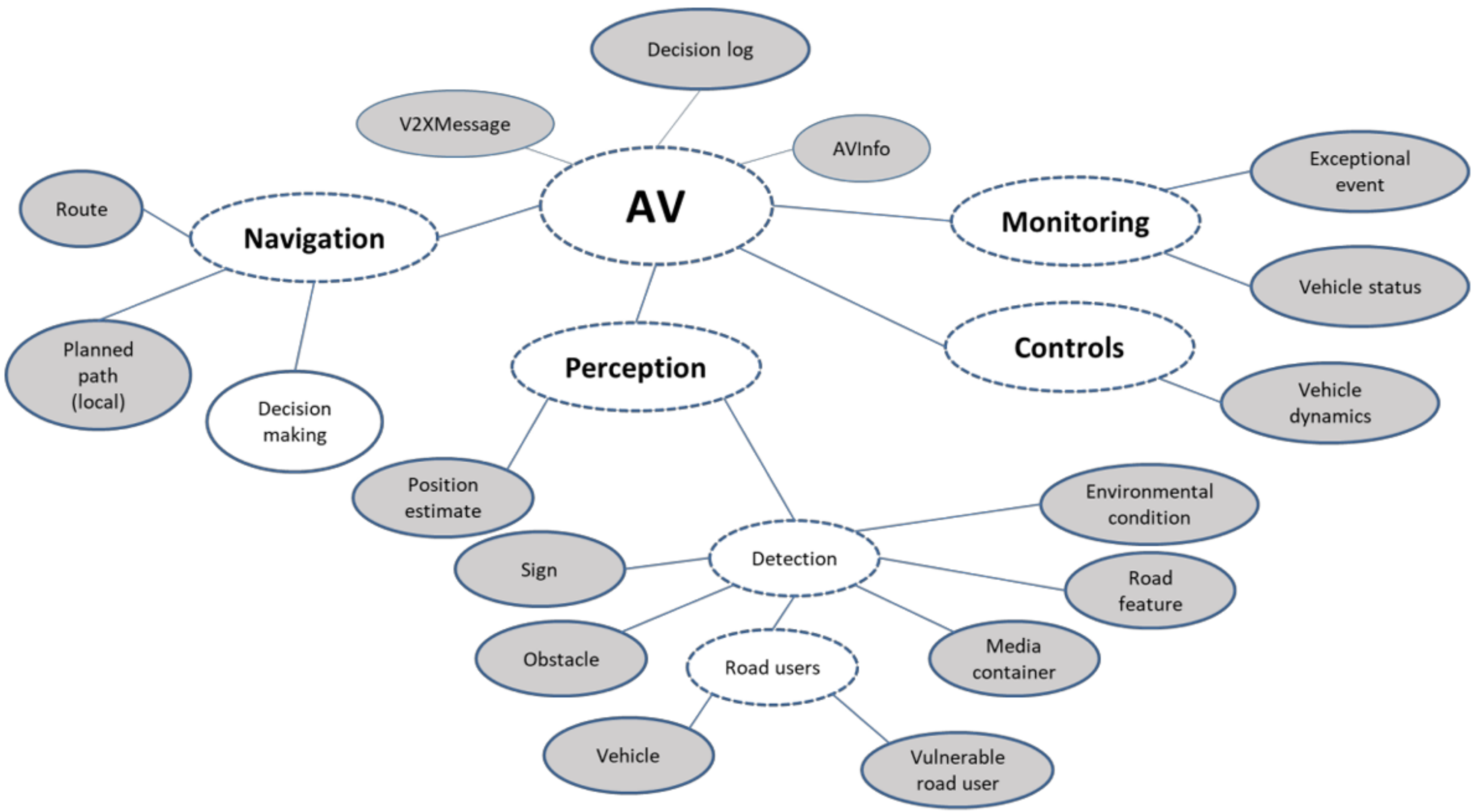


Figure 2 – Class relationship diagram for AVs

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Class Relationship Diagram for AVs; Illustrates the key components and their interrelationships within an AV system; main modules:

1. **Navigation Module:**
   - Responsible for local/global path planning and decision-making.
   - **Interacts with perception module** to perceive the surroundings and **commands the control module** to carry out mission activities.

2. **Perception Module:**
   - **Gathers, interprets, and fuses external data from sensors and external infrastructure system** to localize the AV and make sense of its surroundings; the sensed data is fused with a prior digital map to build a real-time representation of the surroundings.
   - Detects traffic signs, obstacles, road users, road features (e.g. lanes, arrows) and environmental and weather conditions.

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

3. **Control Module:**
    - Related to the advanced system **that coordinates chassis control systems to optimize safety, comfort, and fuel efficiency.**
    - The vehicle dynamics class is linked to the control module; provides info on the dynamic states, e.g. speeds, accelerations, actuator values, etc
4. **Monitoring Module:**
    - Collects, fuses and interprets **internal sensor data relating to the AV's health and vehicle status.**
    - Reports faults of the vehicle subsystem, or component failures via the exceptional event class.
5. **AVInfo Class:**
    - Provides **static information about the AV, including capabilities and dimensions.**

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

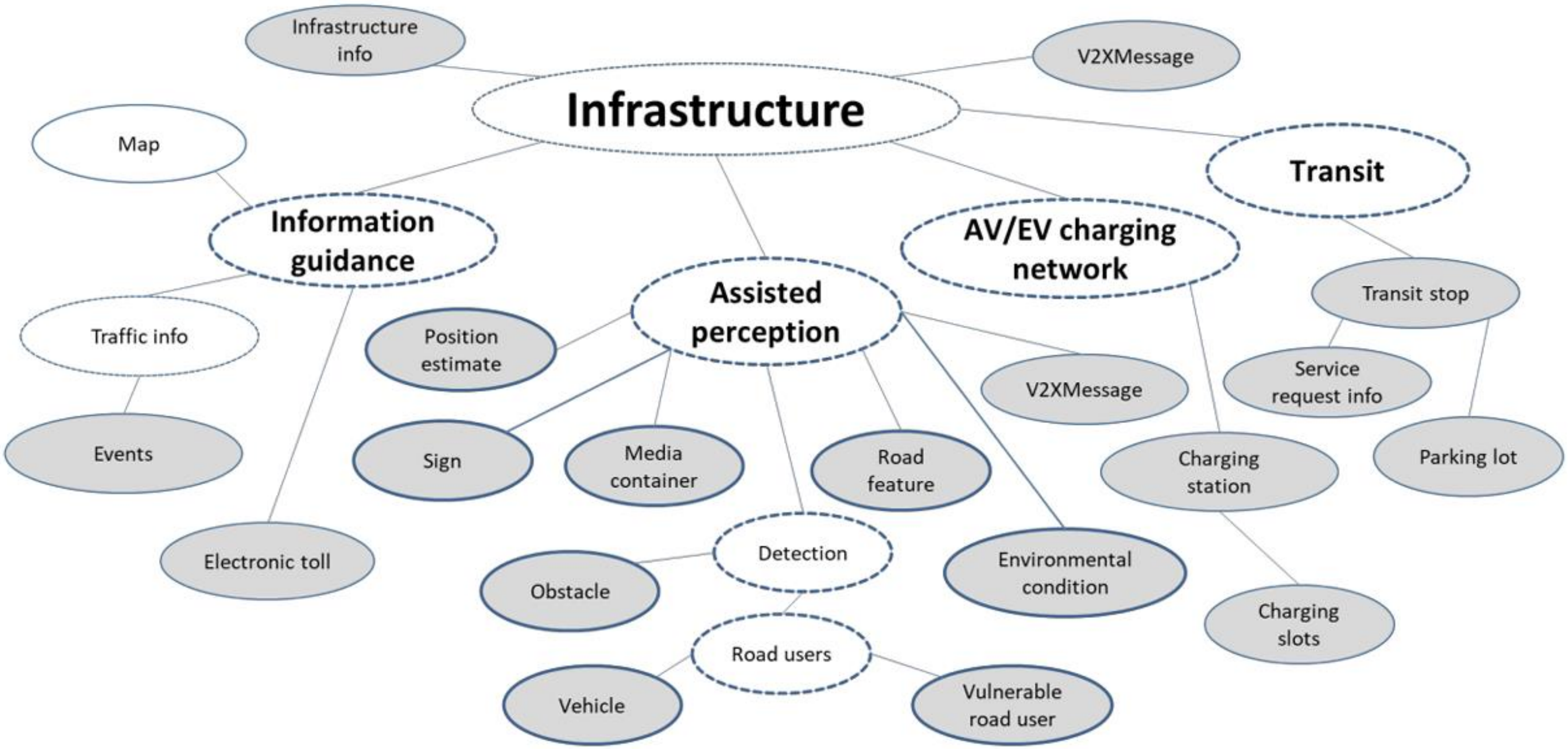


Figure 3 – Class relationship diagram for infrastructure

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Class Relationship Diagram for Infrastructure; Outlines the key data components and their interactions with AVs; infrastructure data can be broadly categorized into the following 4 main areas:

1. **Information Guidance:**
   - Provides **global data to assist AVs in decision-making**, such as **maps, traffic information, events, and electronic toll details.**
   - Critical for navigation and strategic planning within AV systems.
2. **Assisted Perception:**
   - Contains **data related to environmental perception, including road features, obstacles, road users, and vehicle detection.**
   - Supports AVs in understanding their surroundings through sensor data processing and roadside devices like traffic lights.

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

3. AV/EV Charging Network:

- Focuses on **data classes relevant to EV and AV charging infrastructure**, such as **charging stations, slots, and service request information**.
- Facilitates energy management and operational planning for AVs.

4. Transit:

- Covers **data related to transit stops, parking lots, and service requests**, providing **operational information crucial for AV integration with public transport systems.**

The V2XMessage class represents the data exchange and communication between AVs and infrastructure, leveraging standards like SAE J2735 for traffic light data and ISO 14819-2 or SAE J2540 for traffic information.

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

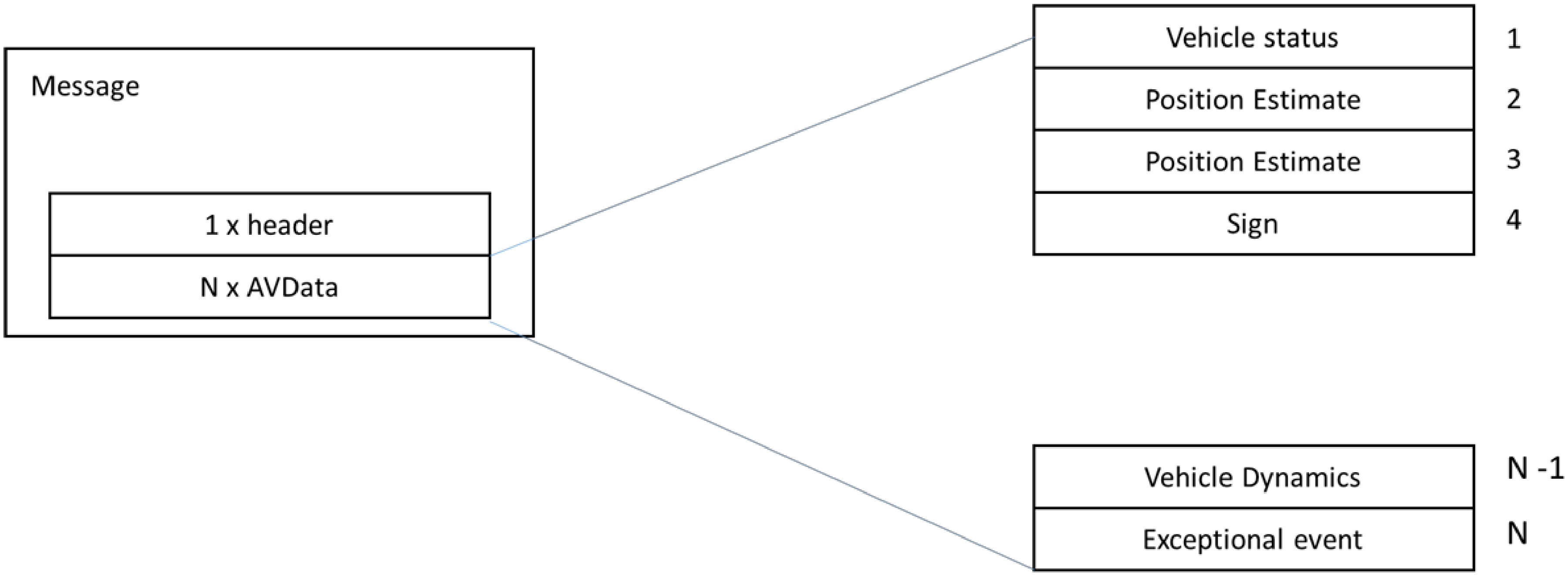


Figure 5 – General message structure

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Data Message Format:

- Designed to efficiently communicate data within the AV ecosystem, considering bandwidth constraints and storage limitations.
- The message structure is layered to ensure flexible and compact data transmission:

  1. **Message Structure:**
     - Header: Each message starts with a header containing essential information such as location and timestamp.
     - AVData Frames: Following the header, a configurable number of AVData frames (N x AVData) are included, representing different AV sub-system data.
  2. **Encoding Layers:**
     - Data Elements: The smallest unit of information, forming the building blocks of a data frame.
     - Data Frames: Collections of data elements and potentially other sub-data frames, representing more complex structures.

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

3. Flexibility and Efficiency:

- The design allows multiple data frames of the same type, such as position estimates from different sensors, to be encoded within a single message.
- This approach helps manage bandwidth and storage resources, optimizing data transmission across various communication channels.

4. Contextual Information:

- Messages are tagged with essential contextual data to support various AV operations, ensuring that each message is relevant and actionable within the AV ecosystem.

Content adapted from TR-68-4

POP QUIZ

POP Quiz at Kahoot!

- Go to www.kahoot.it or download the Kahoot! App
- Key in the given Game PIN on the screen
- Answer the questions as instructed on screen

End of Module 4

THANK YOU for your kind attention!

APPENDIX FOR TR-68-4 (DATA FRAMES)

TR-68 Part 4: Vehicular data types and formats

Data Elements in Data Frame for VulnerableRoadUser:

Item	Data element	Description	Mandatory	Element type	Unit	Precision	Values/range	Notes
1	timeStampUTC	Timestamp for this collected data in the following format YYYYMMDDHH[MM[SS[.fff]]]Z.	Yes	UTCTime		1ms		
2	sensorType	The technology used to detect and/or communicate with the VRU.	No	IA5String				
3	vruObjectType	Classification of the VRU object.	No	VRUTypeEnum				
4	detectedObjectID	ID assigned by the AV's sensor/Infrastructure sensor.	No	Integer				
5	positionOffset_m	Position offset from the vehicle/Infrastructure.	No	PositionOffset	Metre	0.01	[-1000;1000]	
6	movingVector_mps	Velocity of the object; axis need to be defined (e.g. aligned to latitude, longitude, etc.)	No	Vector3D	Metre/second	0.001	[-300;300]	
7	objectSize_m	Size of the detected object.	No	VectorSize3D	Metre	0.01	[-10;10]	
8	objectSizeAccuracy_m	Accuracy provided by the sensor.	No	VectorAccuracy3D	Percentage	0.001	[0;100]	
9	mediaID	ID used to tag a media content.	No	Integer				

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Data Elements in Data Frame for Detected Vehicles Collected by the Perception Module:

Item	Data element	Description	Mandatory	Element type	Unit	Precision	Values/range	Notes
1	timeStampUTC	Timestamp for this collected data in the following format YYYYMMDDHH[MM[SS[.fff]]]Z.	Yes	UTCTime		1ms		
2	sensorType	The sensor technology used to detect and/or communicate with the vehicle.	No	IA5String				
3	vehObjectType	Classification of the vehicle object	No	VehTypeEnum				
4	detectedObjectID	ID assigned by the AV's sensor/infrastructure sensor.	No	Integer				
5	positionOffset_m	Position offset from the vehicle/ infrastructure.	No	PositionOffset	Metre	0.01	[-1000;1000]	
6	movingVector_mps	Velocity of the object; axis need to be defined (e.g. aligned to latitude, longitude, etc.)	No	Vector3D	Metre/second	0.001	[-300;300]	
7	objectSize_m	Size of the detected object.	No	VectorSize3D	Metre	0.01	[-10;10]	
8	objectSizeAccuracy_m	Accuracy provided by the sensor.	No	VectorAccuracy3D	Percentage	0.001	[0;100]	
9	mediaID	ID used to tag a media content.	No	Integer				

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Data Elements in Data Frame for AutonomousVehicleInfo:

Item	Data element	Description	Mandatory	Element type	Unit	Precision	Values/range	Notes
1	timeStampUTC	Timestamp for this collected data in the following format YYYYMMDDHH[MM[SS[.fff]]] Z.	Yes	UTCTime		1ms		
2	proprietaryInfo	Is used to send non-standardized data elements from AV to infra or vice versa. This could be proprietary information related to an OEM.	No	KeyValuePairString				
3	avSoftwareName	To define software name to main AV.	No	IA5String				
4	avSoftwareVersion	To define software version to main AV.	No	IA5String				
5	vehicleID	Unique ID to identify a vehicle	Yes	IA5String				
6	vehicleClassType	For describing the vehicle class type.	No	VehClassTypeEnum				
7	vehicleFunctionalType	Defines the functional use of the vehicle.	No	VehFunctionalTypeEnum				
8	vehicleReferencePointDeltaAboveGround_m	Vertical reference point of the vehicle which is defined by the OEM. Used for datum of the vehicle.	No	Real	Metre	0.001	[0;20]	
9	vehicleReferencePointDeltaFromFront_m	Longitudinal reference point of the vehicle which is defined by the OEM. Used for datum of the vehicle.	No	Real	Metre	0.001	[0;20]	
10	vehicleReferencePointDeltaFromLeft_m	Lateral reference point of the vehicle which is defined by the OEM. Used for datum of the vehicle.	No	Real	Metre	0.001	[0;20]	
11	vehicleLength_m	Length of the vehicle.	No	Real	Metre	0.001	[0;100]	
12	vehicleWidth_m	Width of the vehicle.	No	Real	Metre	0.001	[0;100]	

Content adapted from TR-68-4

TR-68 Part 4: Vehicular data types and formats

Data Elements in Data Frame for AutonomousVehicleInfo (Cont):

Item	Data element	Description	Mandatory	Element type	Unit	Precision	Values/range	Notes
13	vehicleHeight_m	Height of the vehicle.	No	Real	Metre	0.001	[0;100]	
14	primaryFuelType	Main fuel type used for this vehicle.	No	FuelTypeEnum				
15	primaryFuelTankVolume	Corresponding volume of the fuel tank depending on the type of fuel used. The volume indicated is the max capacity.	No	Real	Depending on fuel type; can be specified as volume (l), mass (kg), or energy (Ah)	0.01	[0;1000]	
16	primaryFuelTypeVolumeOthers	Corresponding measurement of the fuel tank if undefined fuel type is used. To specify the measurement and value using a key-value string. The volume indicated is the max capacity.	No	KeyValuePairString				
17	secondaryFuelType	Main fuel type used for this vehicle.	No	Real	Depending on fuel type, can be specified as volume (l), mass (kg), or energy (Ah).	0.01	[0;1000]	
18	secondaryFuelTankVolume	Corresponding volume of the fuel tank depending on the type of fuel used. The volume indicated is the max capacity.	No	Real	Depending on fuel type; can be specified as volume (l), mass (kg), or energy (Ah).	0.01	[0;1000]	
19	secondaryFuelTankVolumeOthers	Corresponding measurement of the fuel tank if undefined fuel type is used. To specify the measurement and value using a key-value string. The volume indicated is the max capacity.	No	KeyValuePairString				
20	vehicleCapabilityLevel	For defining the level of driving automation based on SAE defined “levels”.	No	CapabilityLevelEnum				

Content adapted from TR-68-4