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)
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)

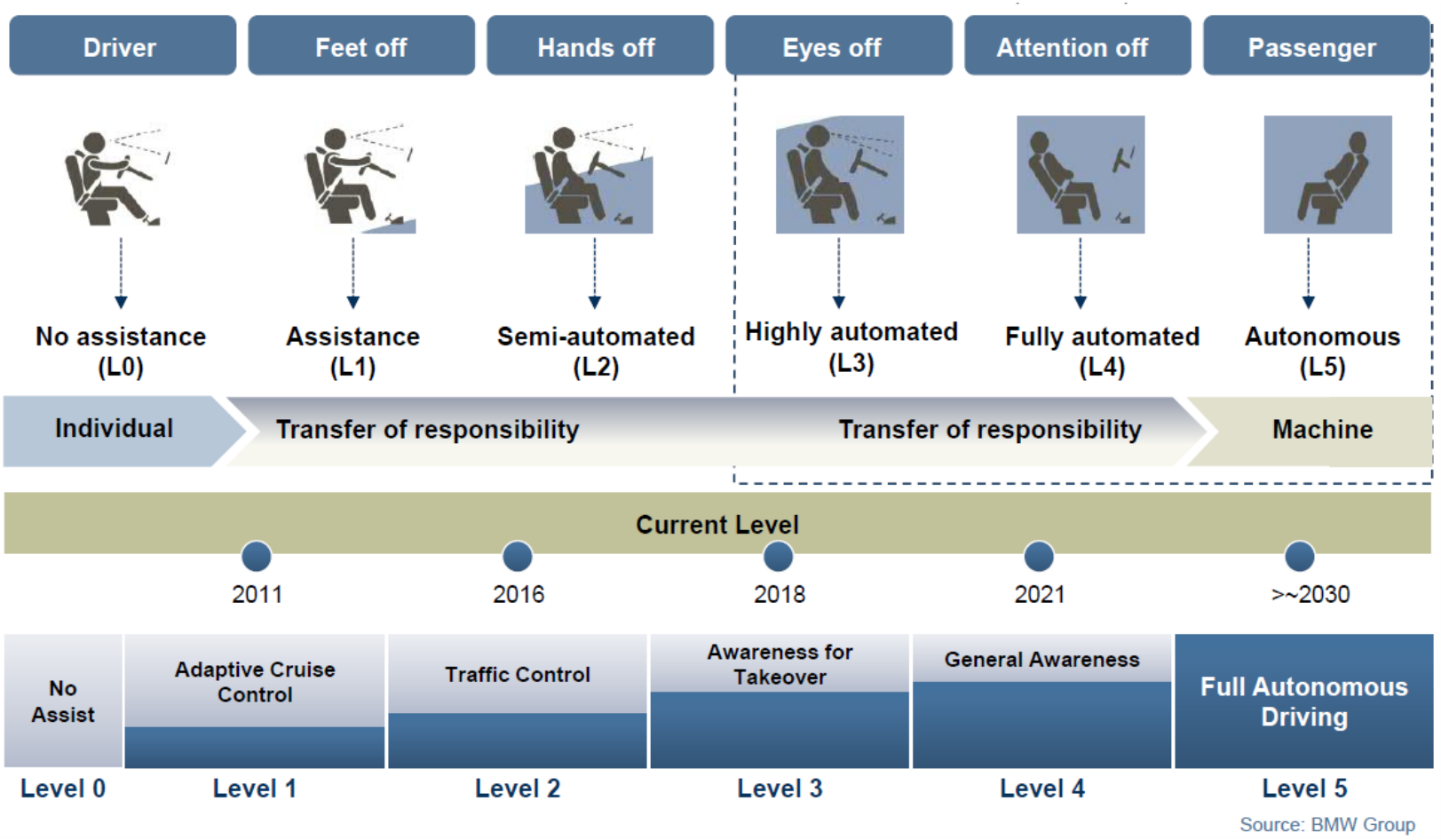
1. SAE INTERNATIONAL – J3016

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**
- **Does not provide specifications** for and **does not impose requirements** on driving automation systems

The 5 Levels of Autonomous Driving



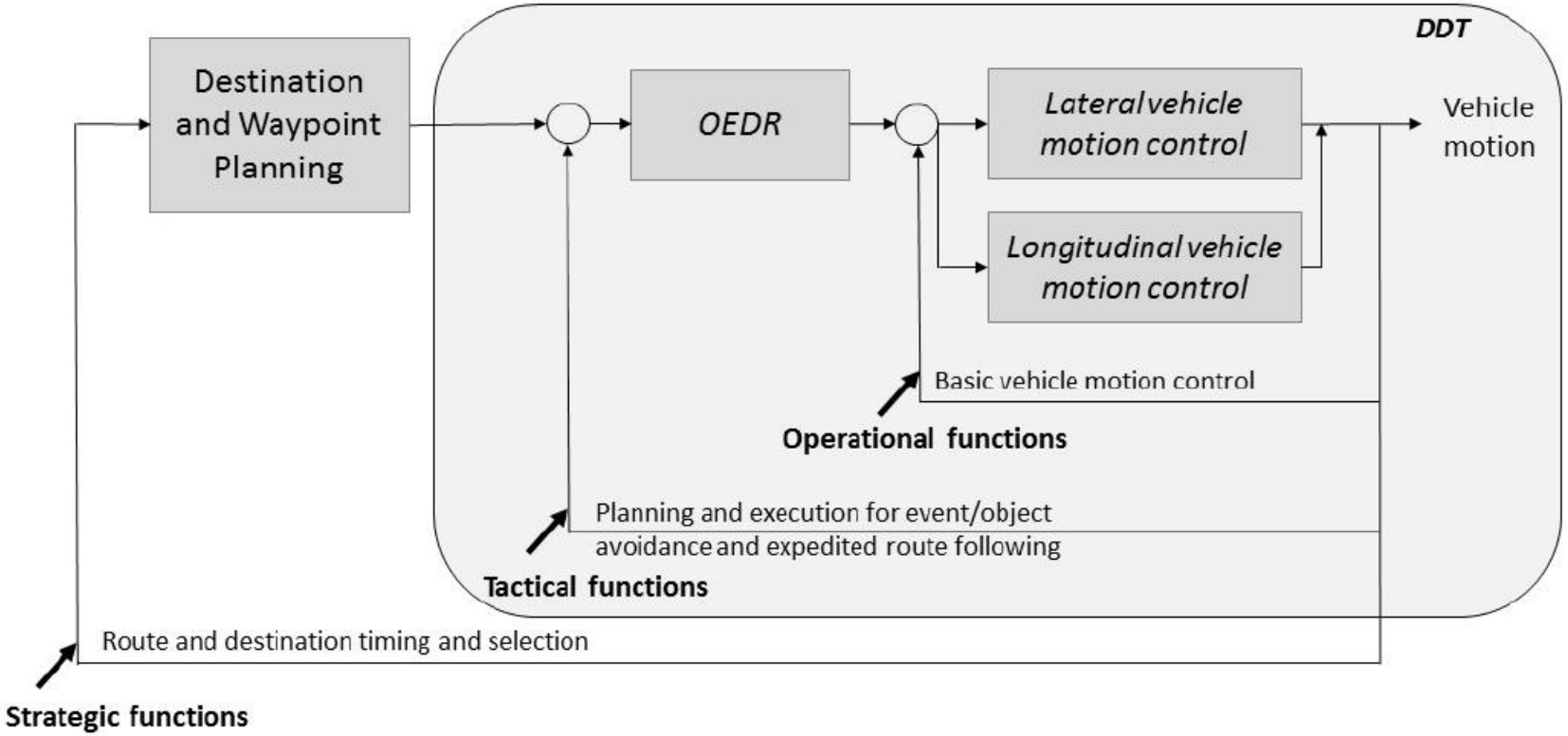
Dynamic Driving Task (DDT)

- 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

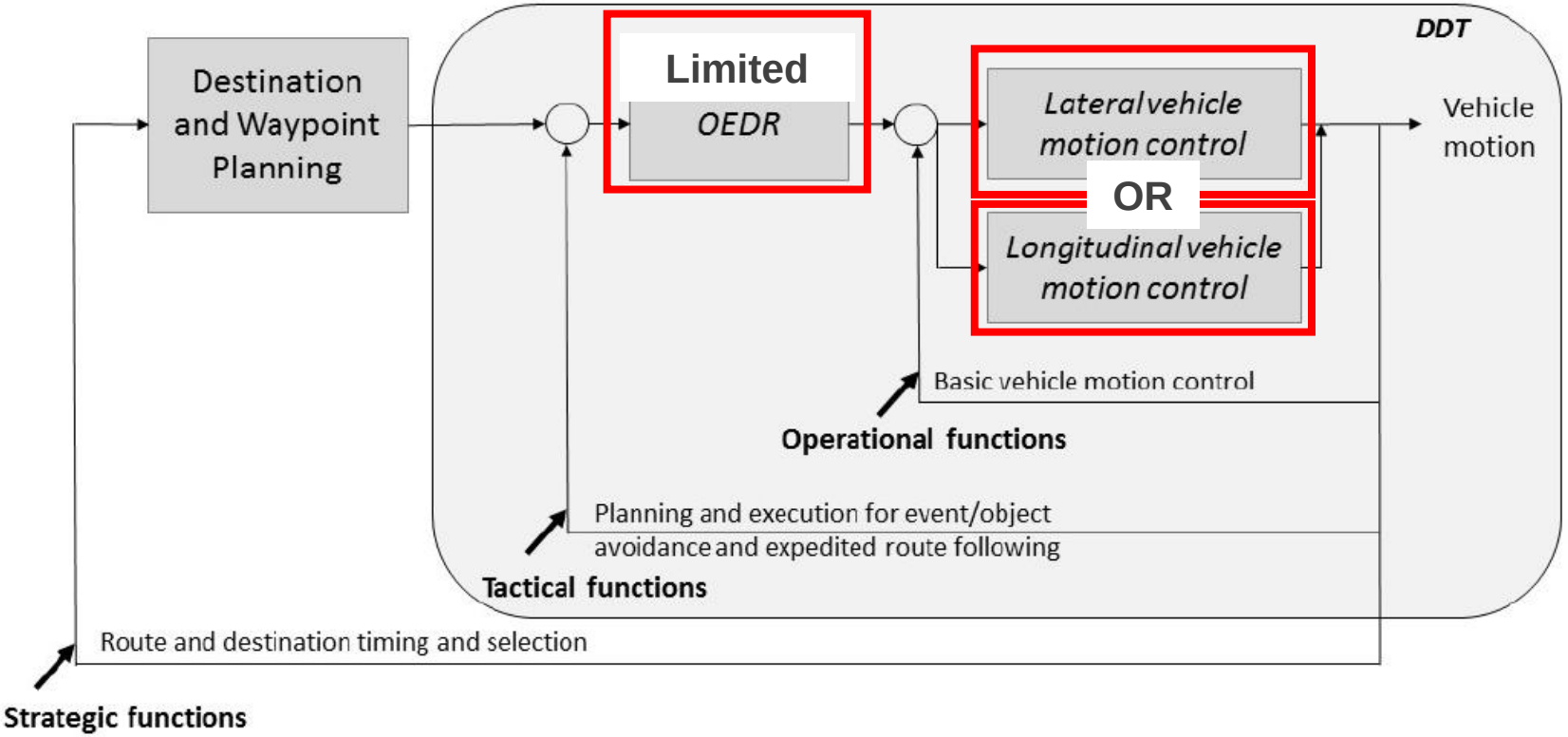
OEDR = object and event detection, recognition, classification, and response



Graphics from SAE International J3016

Dynamic Driving Task (DDT)

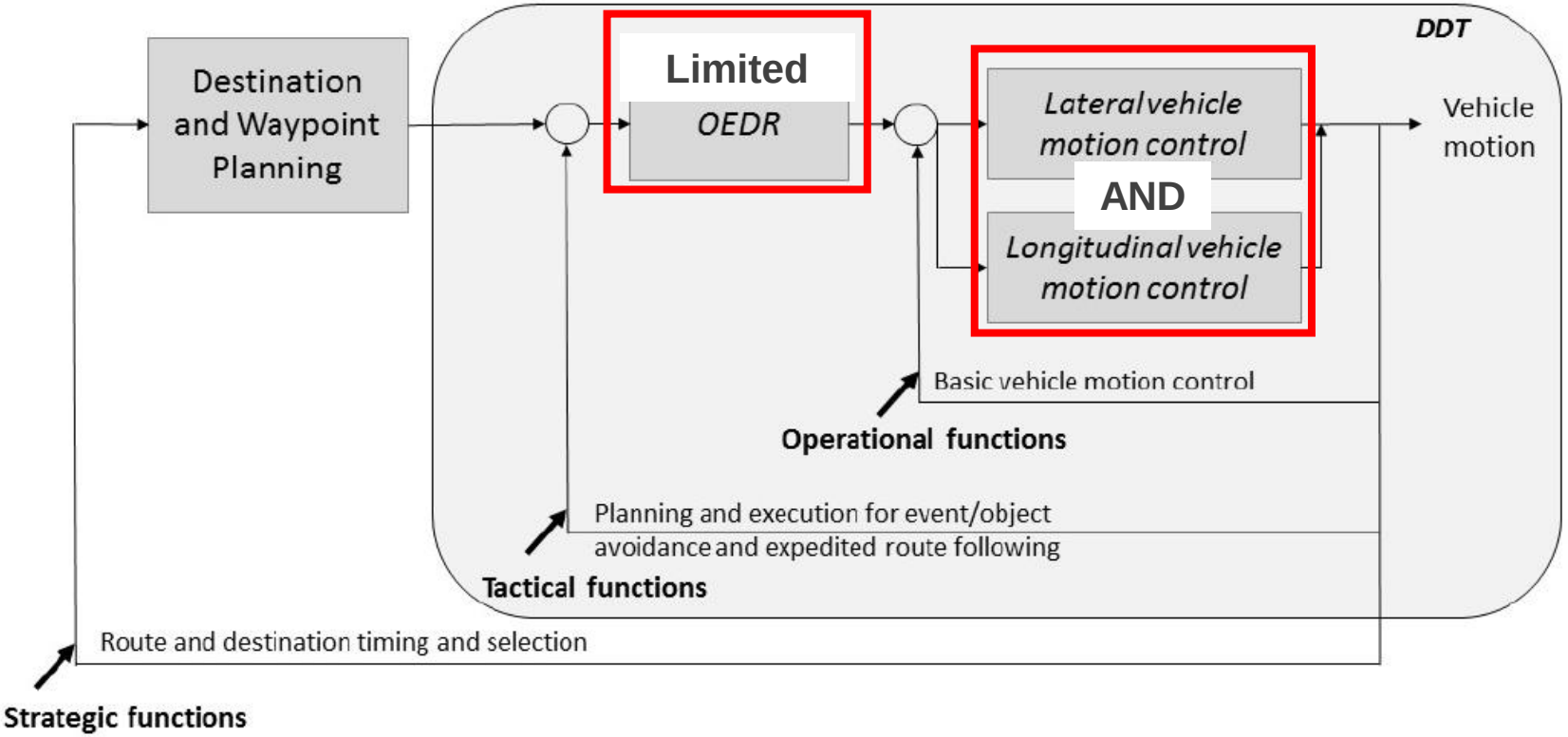
For Level 1



Graphics from SAE International J3016

Dynamic Driving Task (DDT)

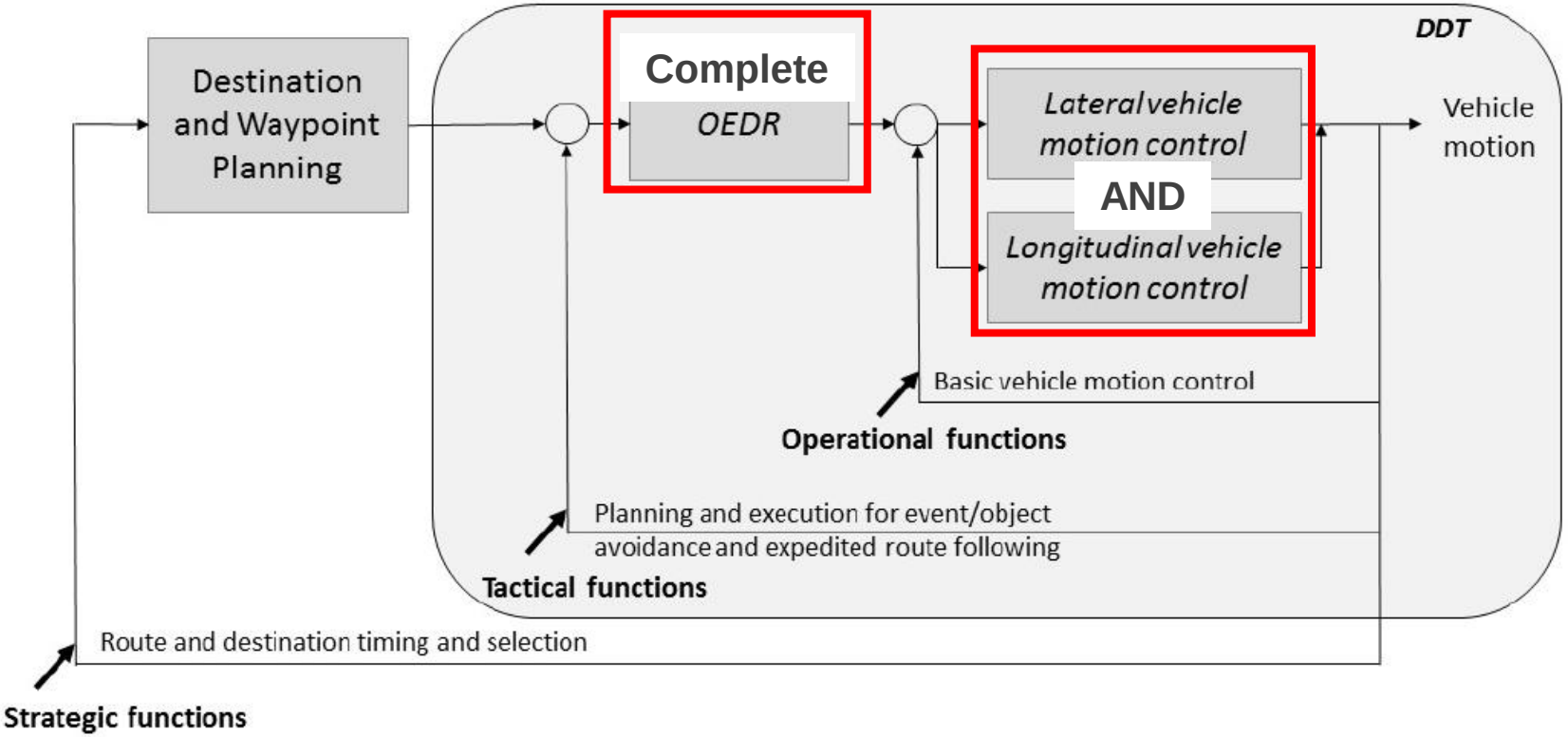
For Level 2



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**

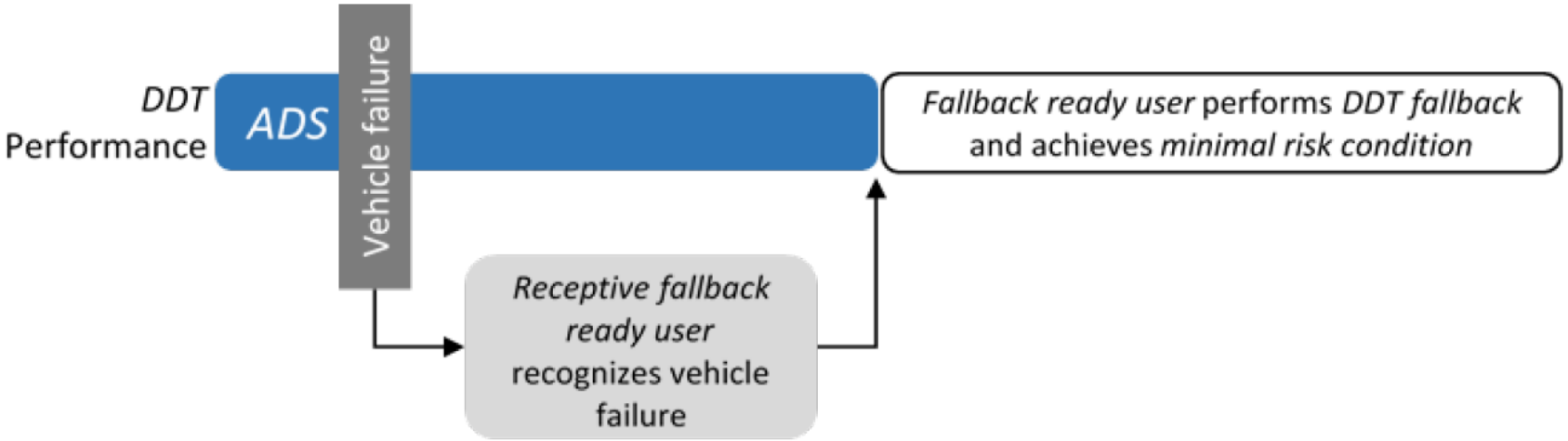
DDT Fallback

- 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)

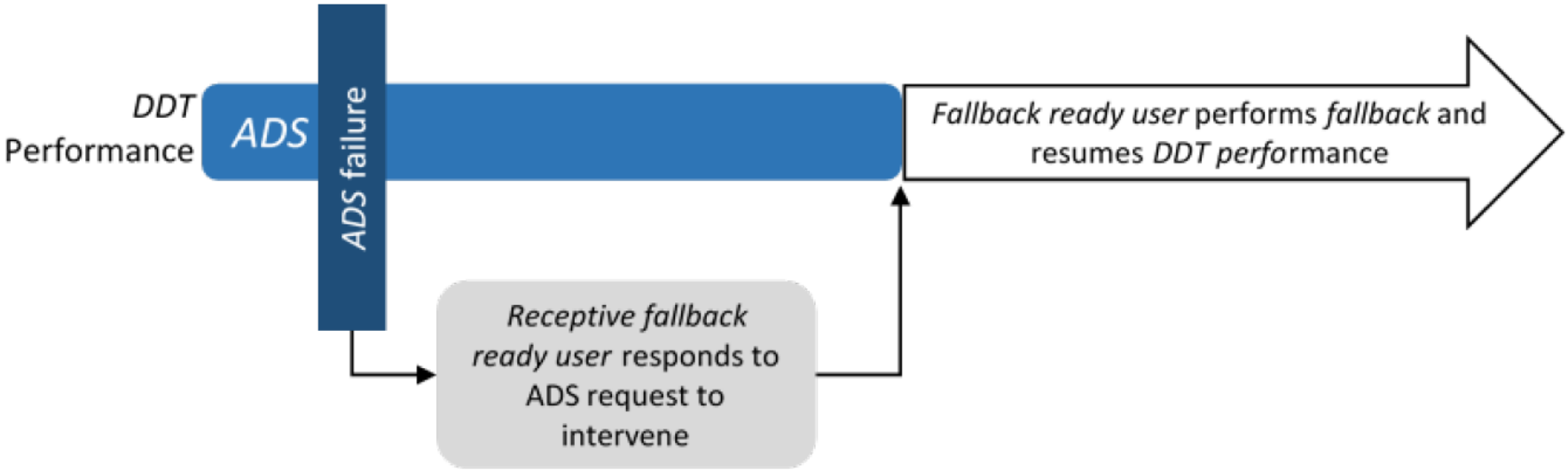
DDT Fallback Illustrative Examples:



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

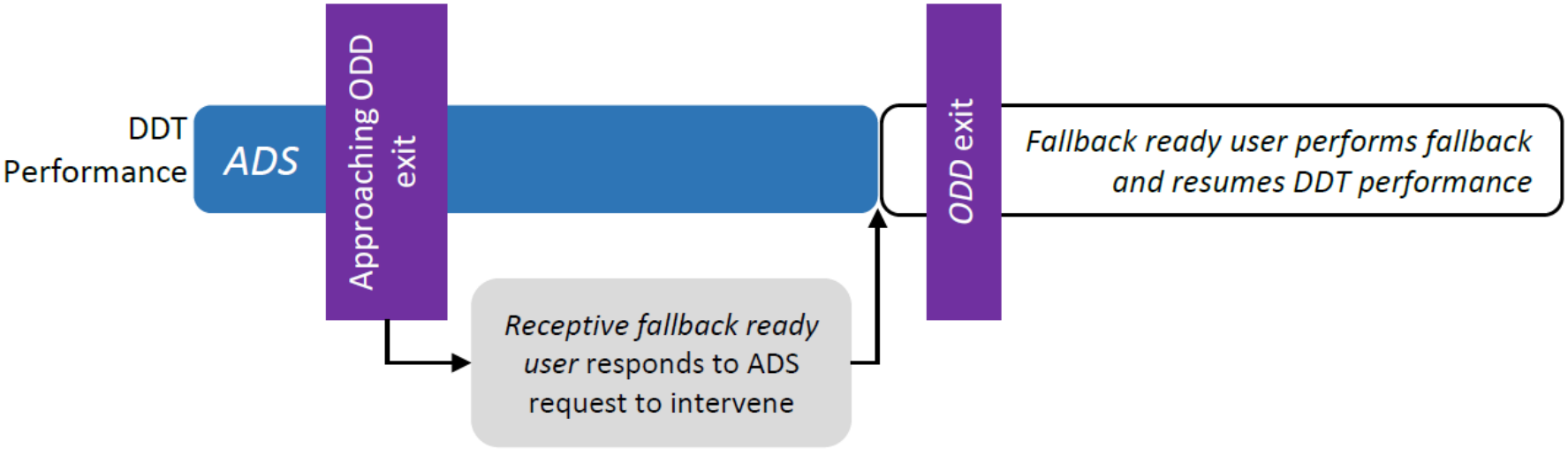
DDT Fallback Illustrative Examples:



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

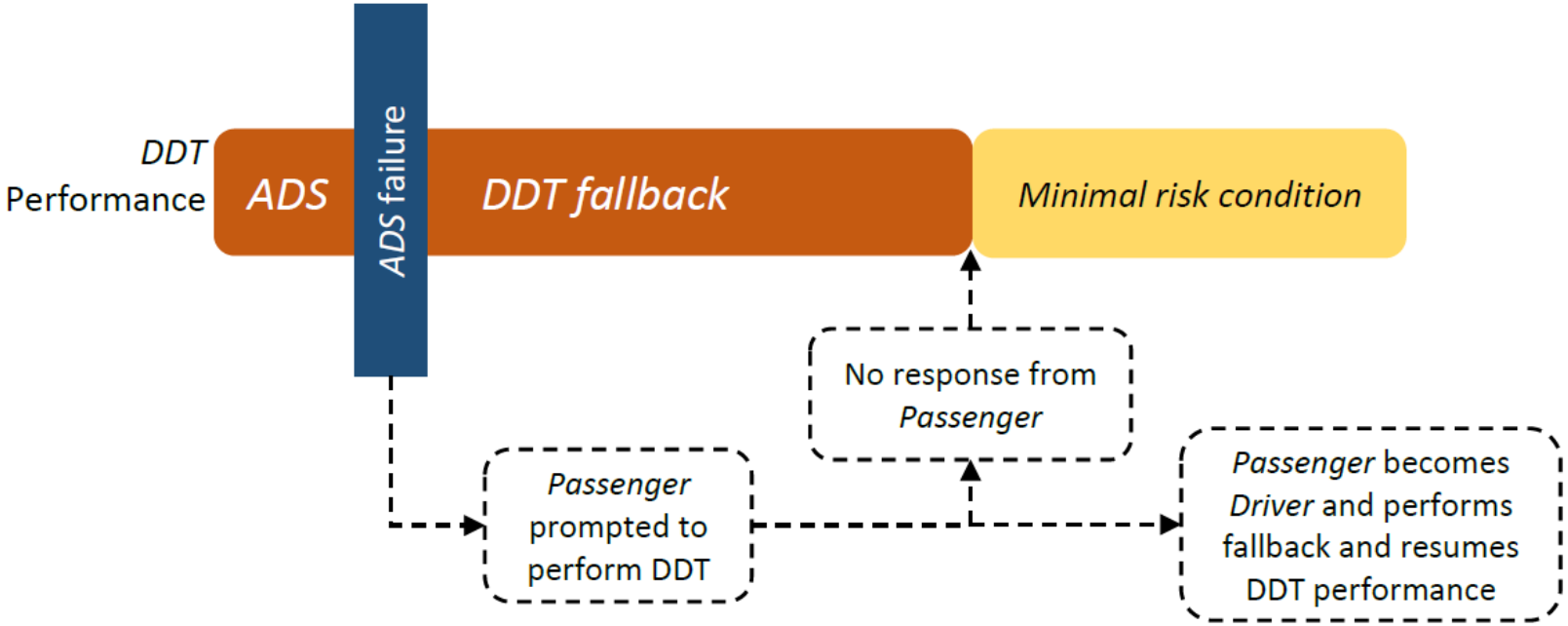
Graphics from SAE International J3016

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:

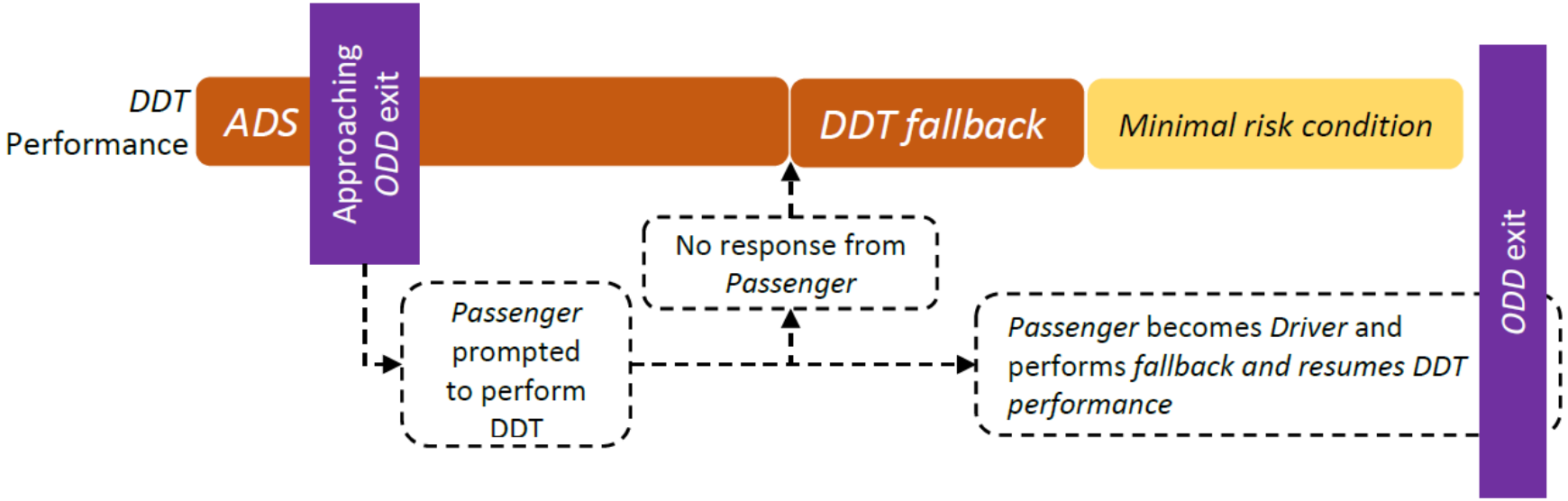


NOTE: Dotted lines represent optional conditions.

Sample use case sequence at **Level 4** showing *ADS* engaged and occurrence of **an *ADS* failure** that **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

DDT Fallback Illustrative Examples:

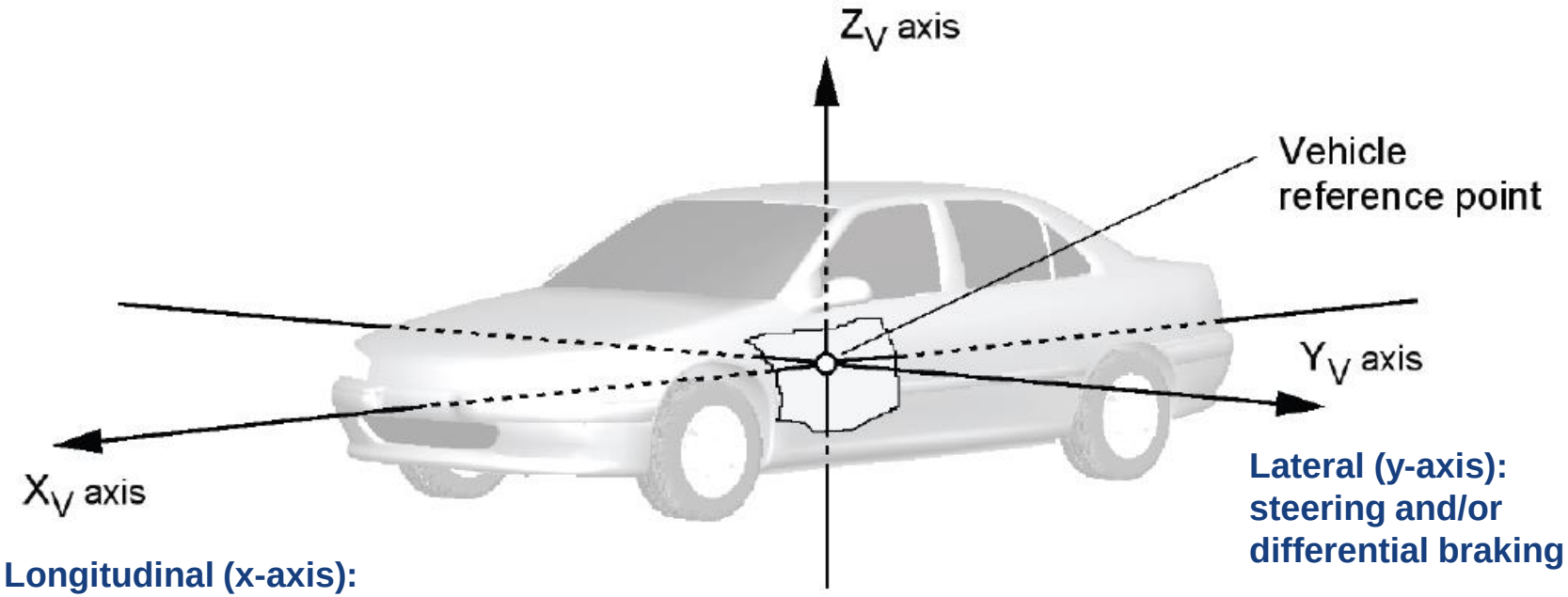


Use case sequence at **Level 4** showing *ADS* engaged with ***ODD* exit**, which **does not prevent continued *DDT* performance by an available human *user***. The *ADS feature* may prompt a *passenger* seated in the driver's seat (if available) to resume *DDT* performance; if no driver's seat with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



Graphics from SAE International J3016

Taxonomy of Driving Automation

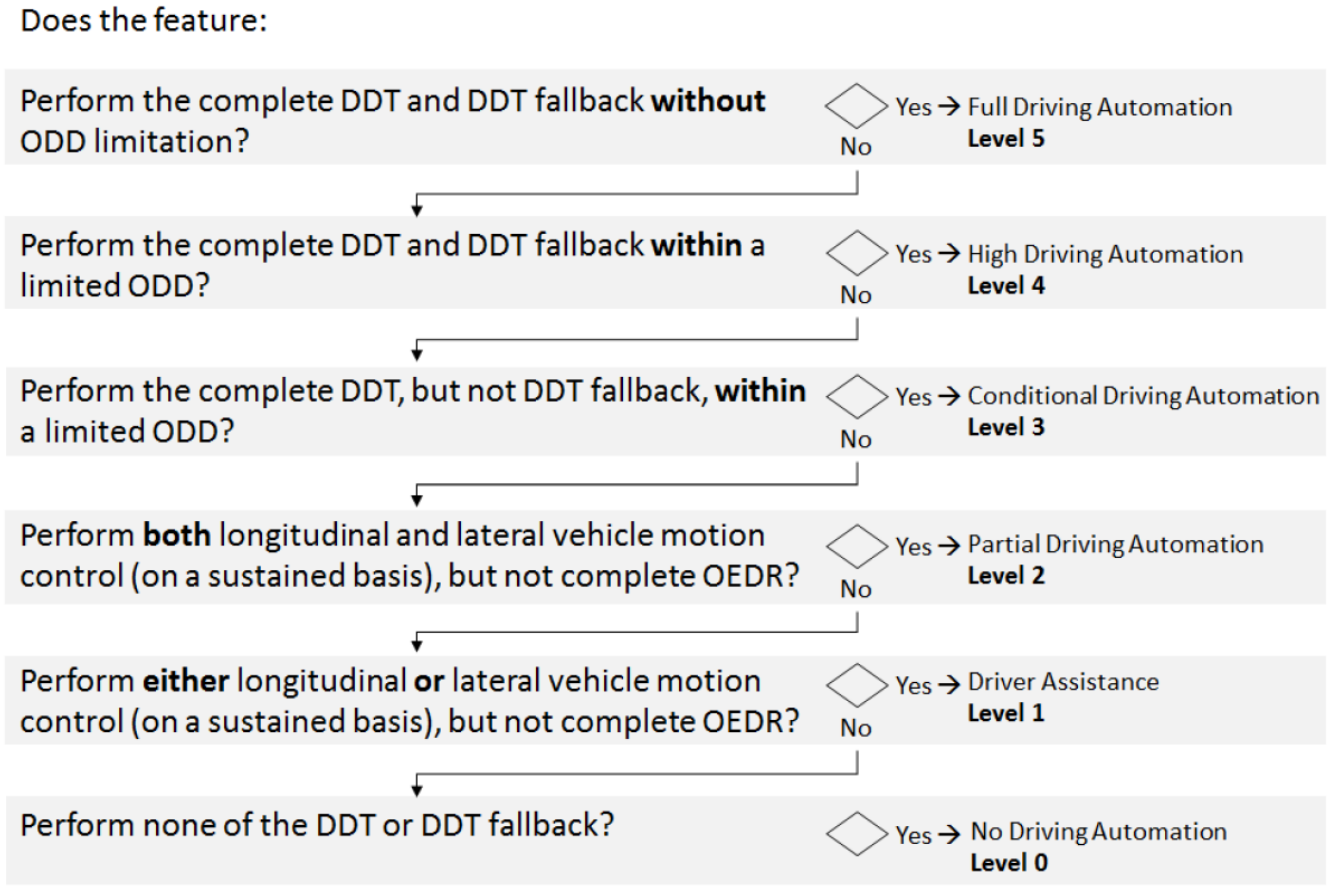
Level	Name	Narrative definition	DDT		DDT fallback	ODD
			Sustained lateral and longitudinal vehicle motion control	*OEDR*		
Driver* performs part or all of the *DDT						
0	**No Driving Automation**	The performance by the *driver* of the entire *DDT*, even when enhanced by *active safety systems*.	*Driver*	*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)**			*System*	***System***	*Fallback-ready user (becomes the driver during fallback)*	Limited
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.				
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



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*	

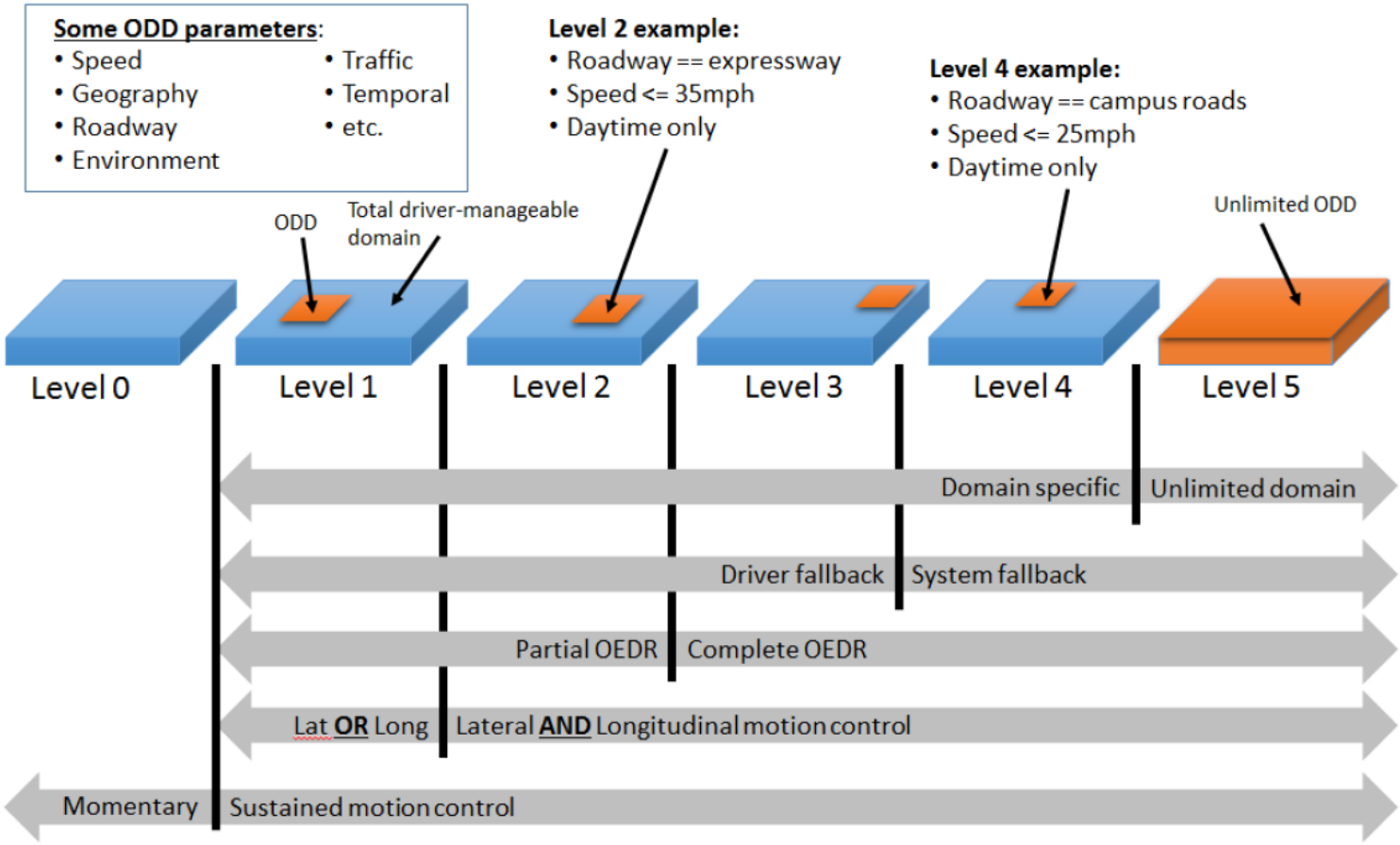
User roles while a driving automation system is engaged

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

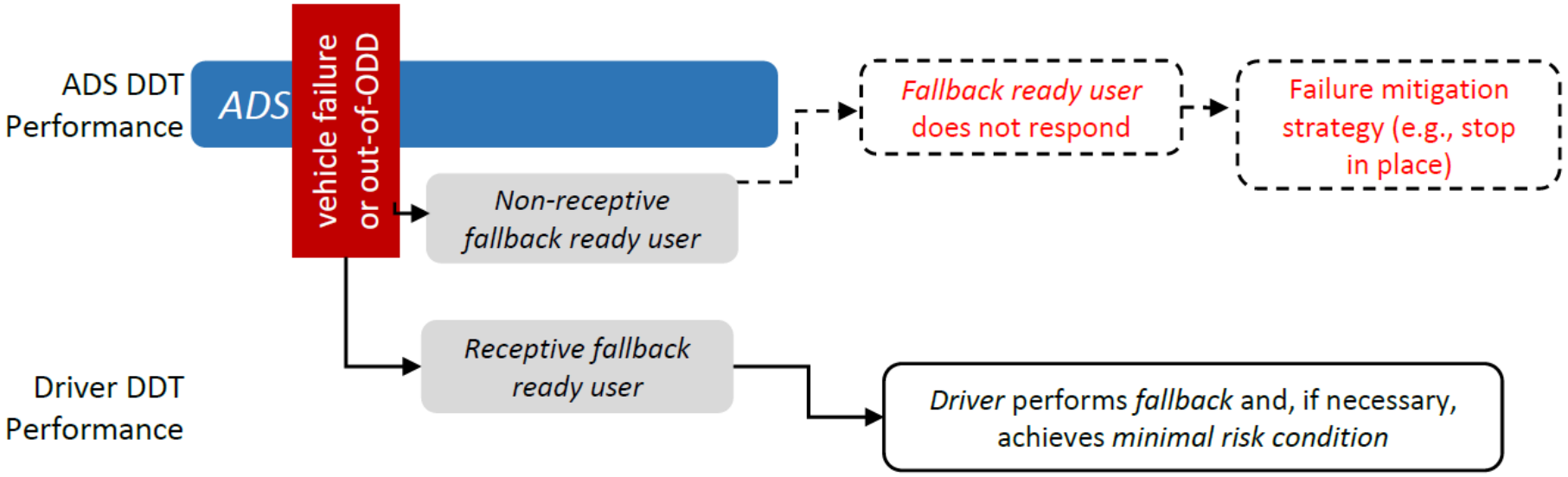
Request to Intervene

- 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*

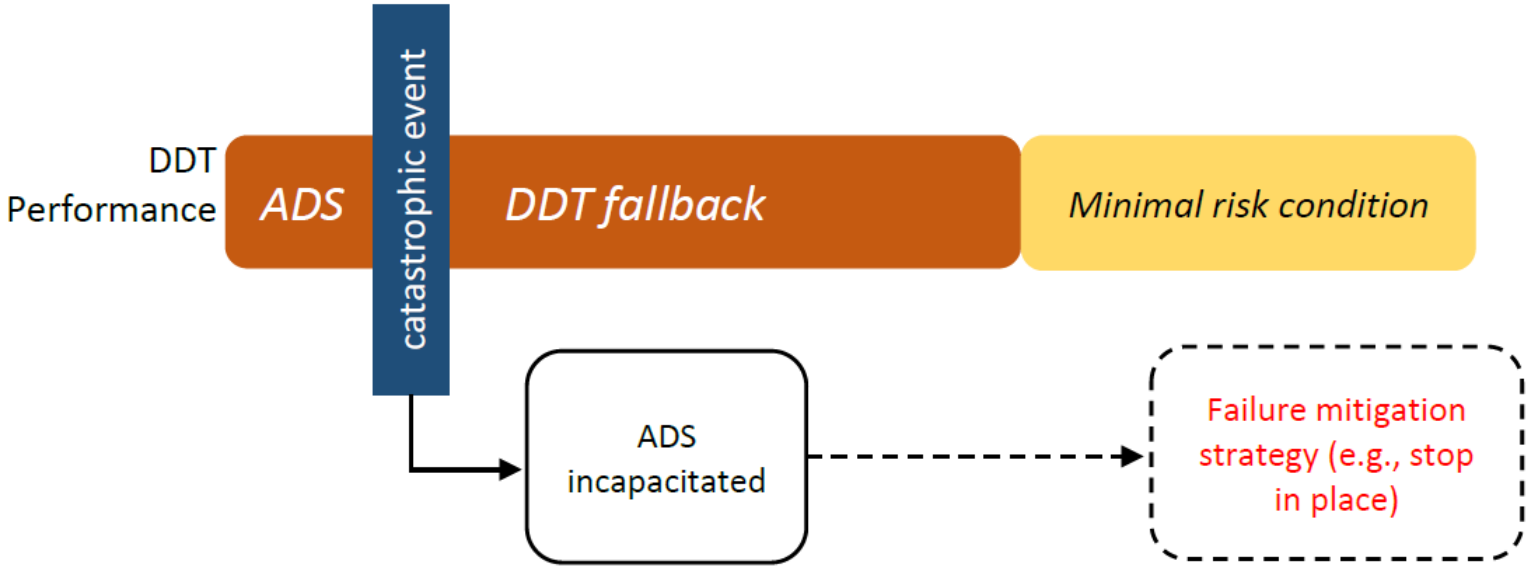
DDT Fallback vs Failure Mitigation Strategy (FMS)



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

SSC's 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)

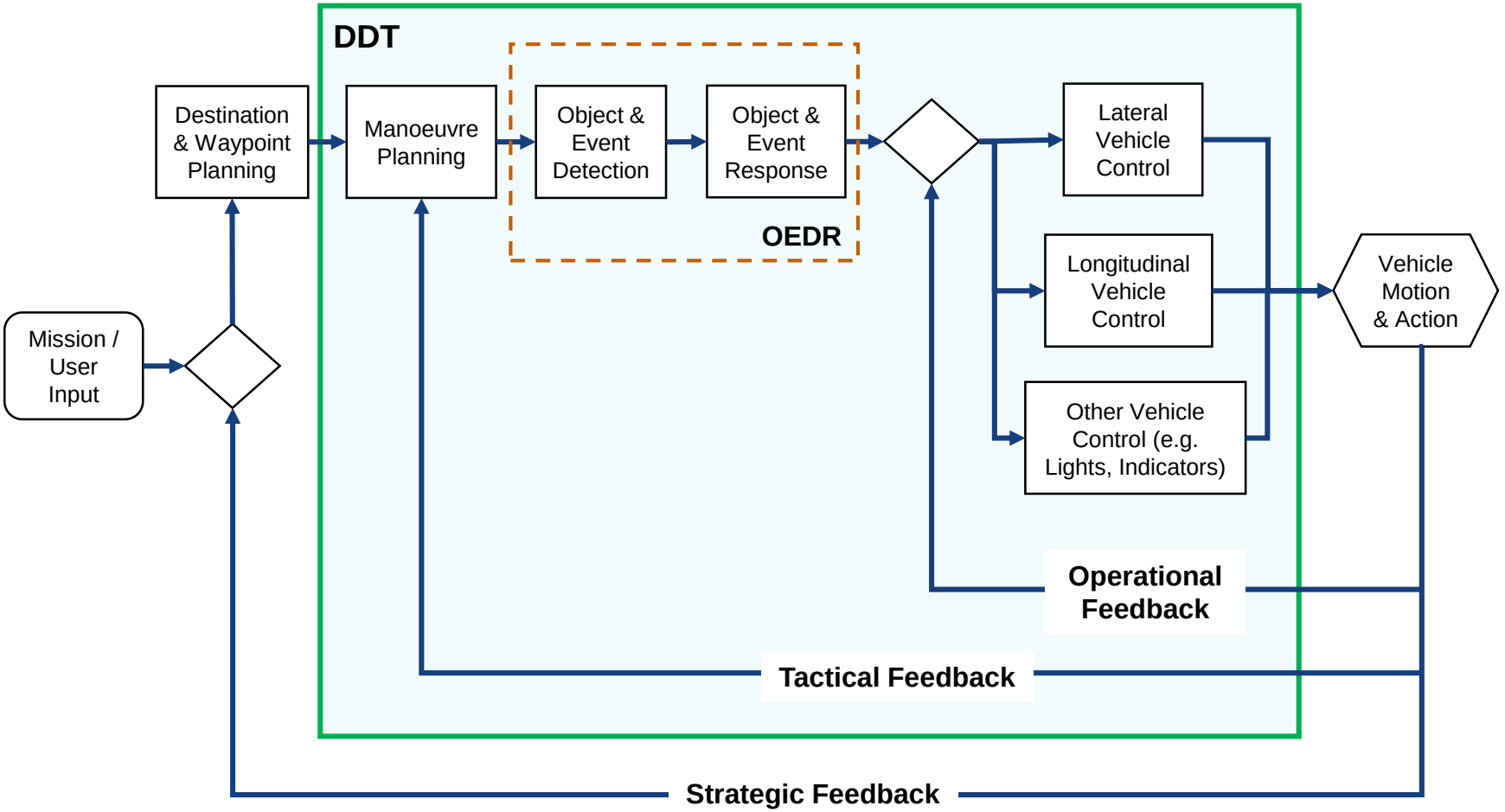
d) Motor insurance companies

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

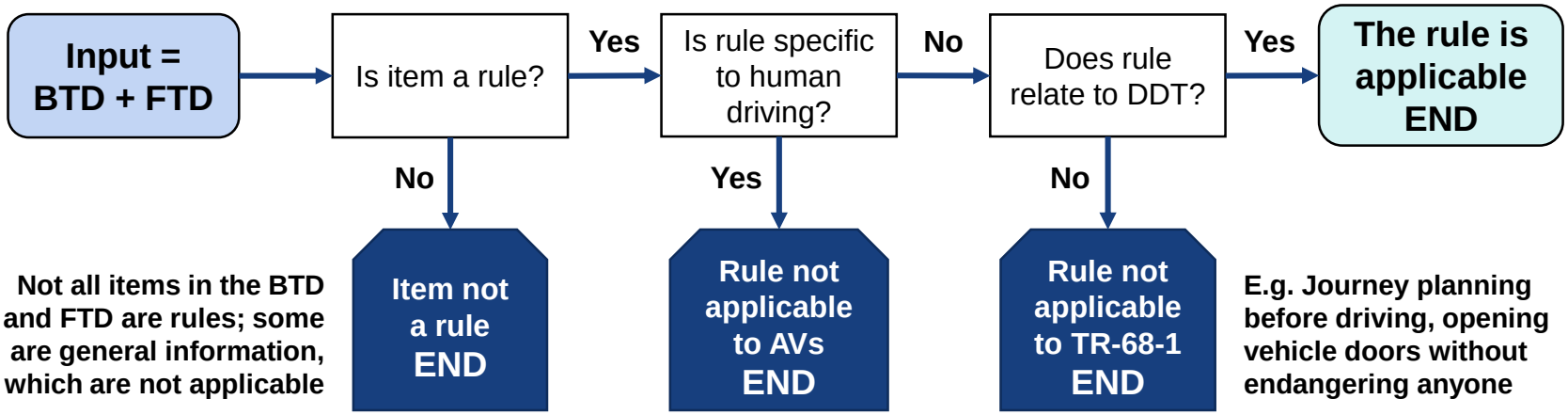
d) **AVs are expected to only depend on on-vehicle systems to provide safe operation**. In other words, if any critical events occur (e.g. malfunctions, power loss, cyberattacks), the AVs cannot rely on any off-vehicle systems (e.g. wireless communications) to execute safety measures

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:



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

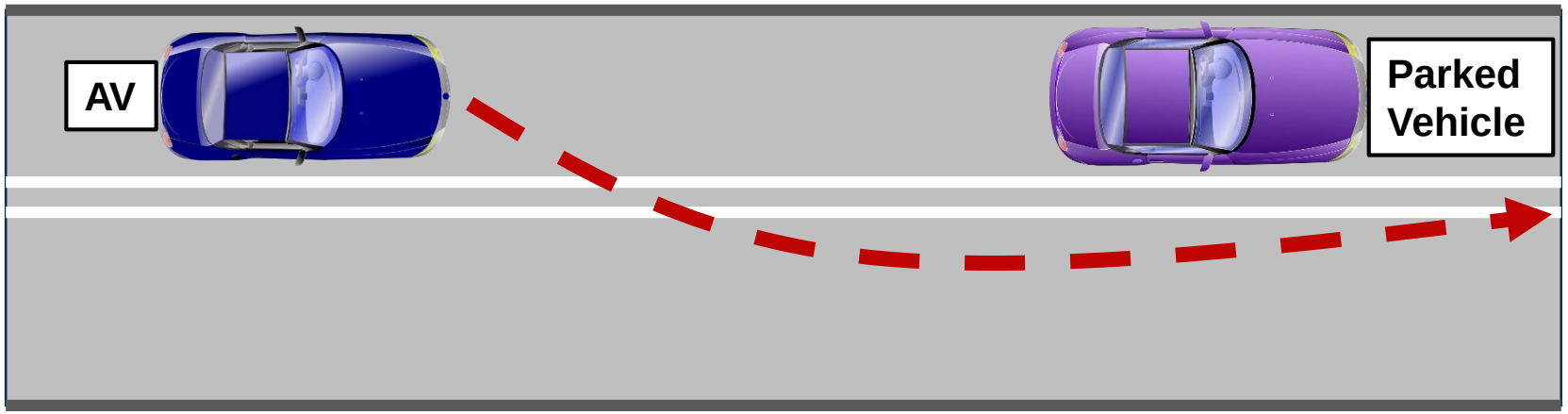
- Able to violate driving rules if not doing so will lead to unnecessary traffic obstruction, provided if Rule A still applies (i.e. no unreasonable safety risks taken)

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

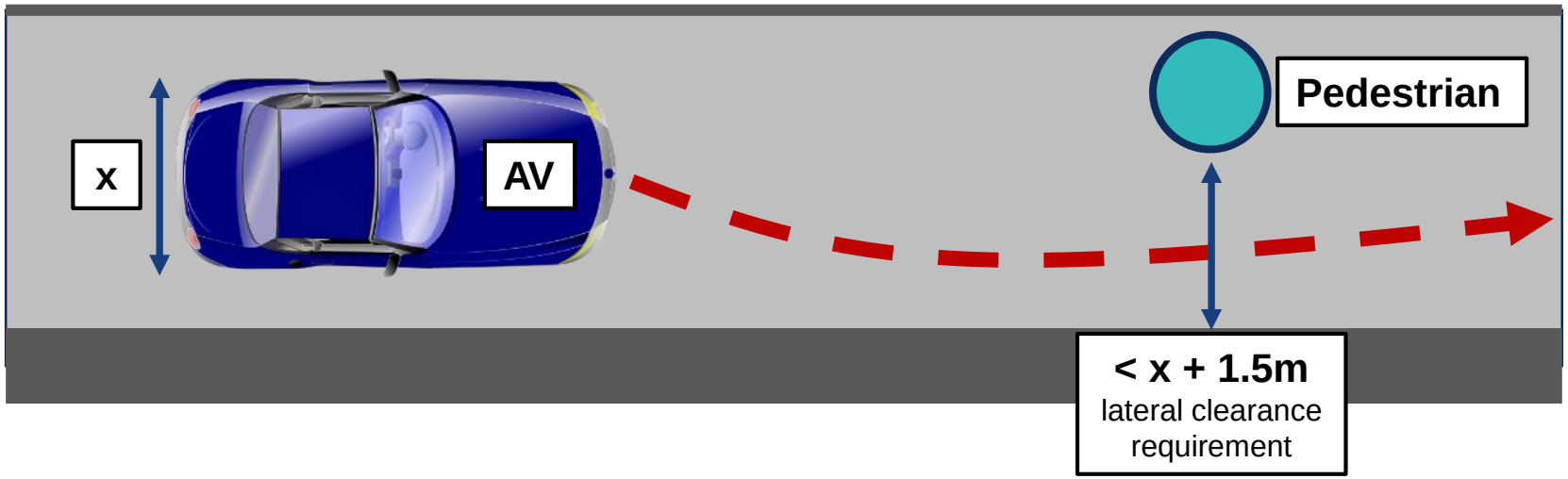


Content and Graphics adapted from TR-68-1

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

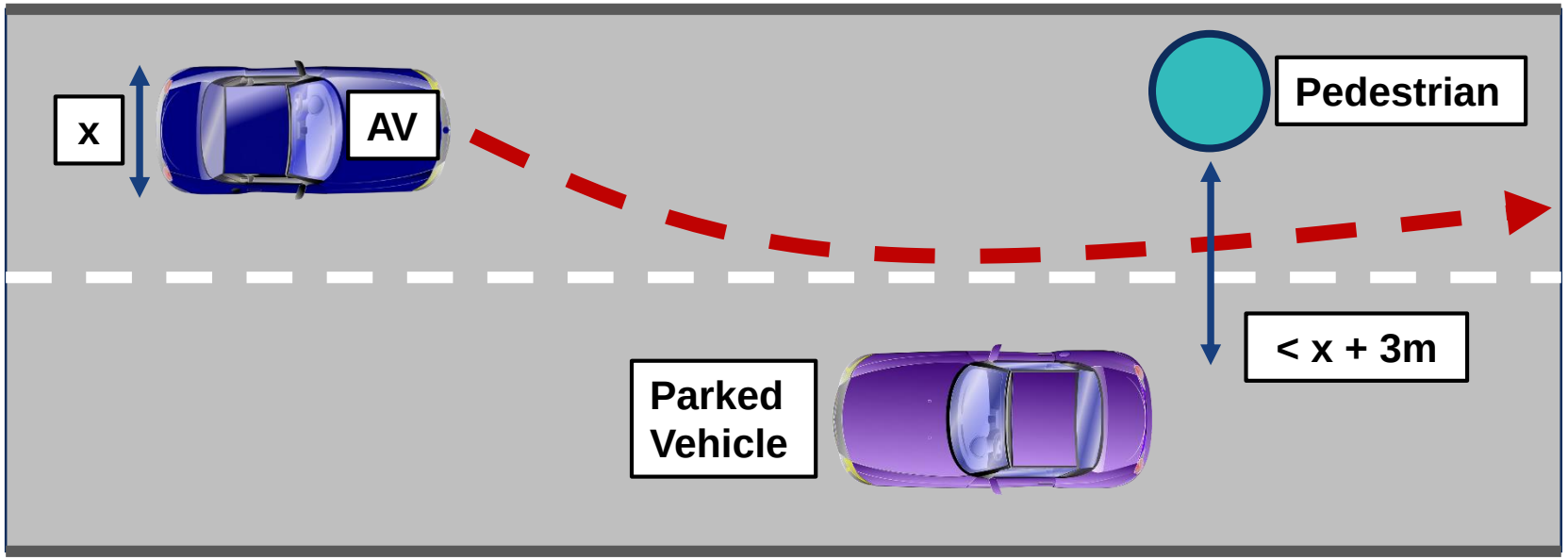


Content and Graphics adapted from TR-68-1

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

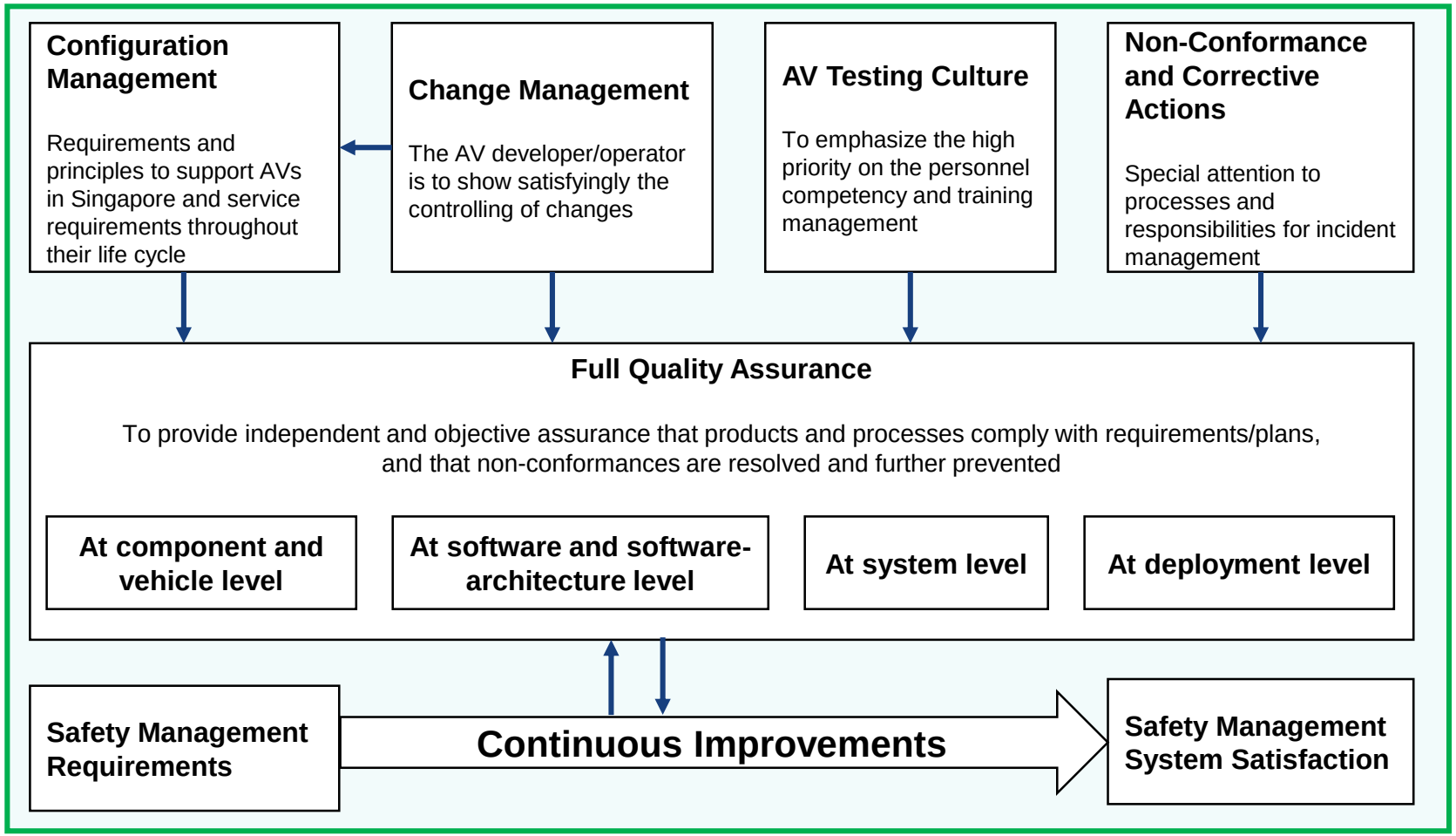
Purpose of TR-68-2 (Safety):

- **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

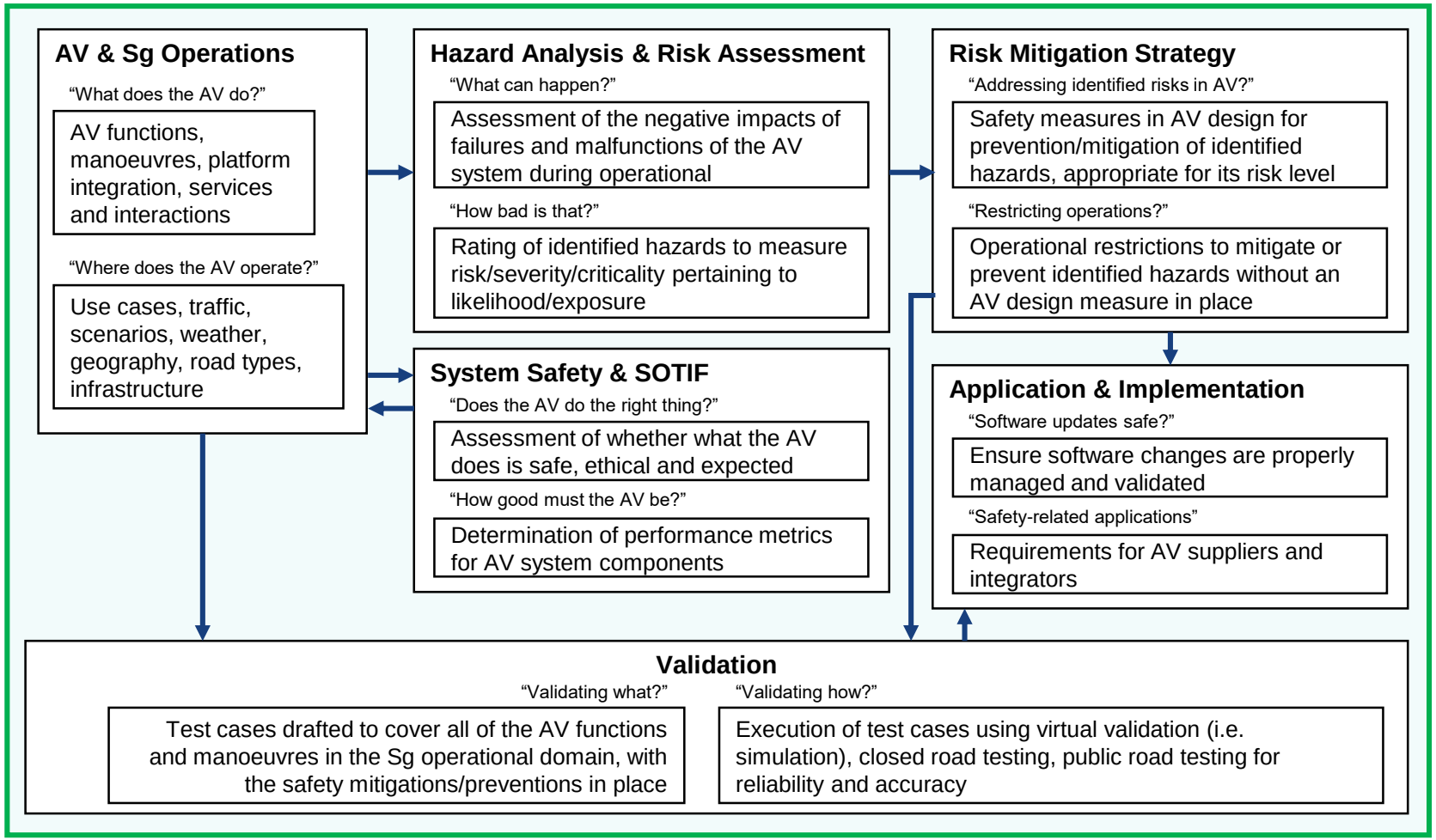
Quality Management System Overview



Content and Graphics adapted from TR-68-2

TR-68 Part 2: Safety

Safety Management System Overview



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):

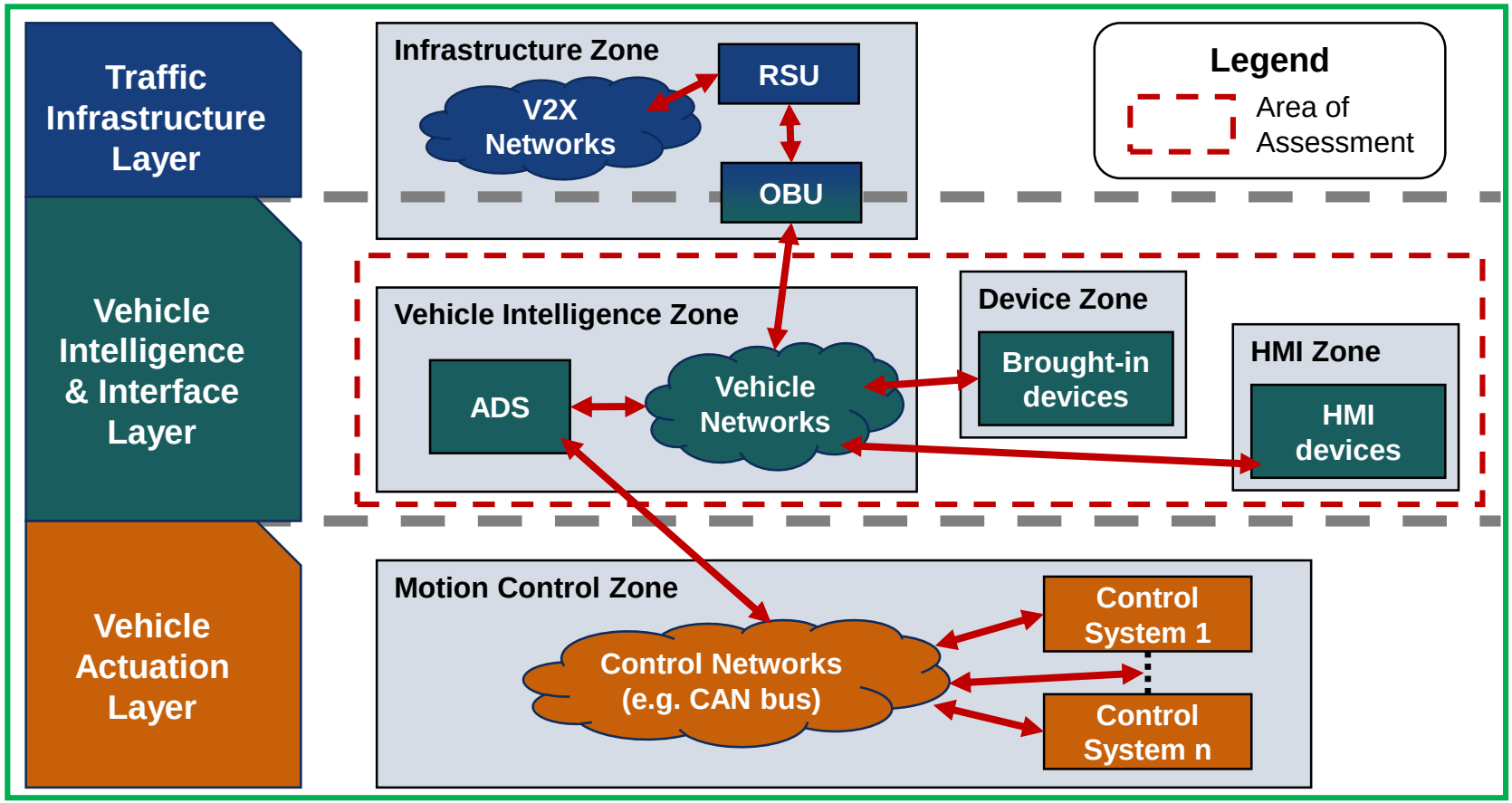
- **TR for enhanced cybersecurity framework for AVs**
  - Sg does not manufacture vehicles; dependent on AV developer/operator for security-by-design processes
  - Independent approach required to ensure foolproof cybersecurity (i.e. conducting cybersecurity assessment of AVs before deploying them on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



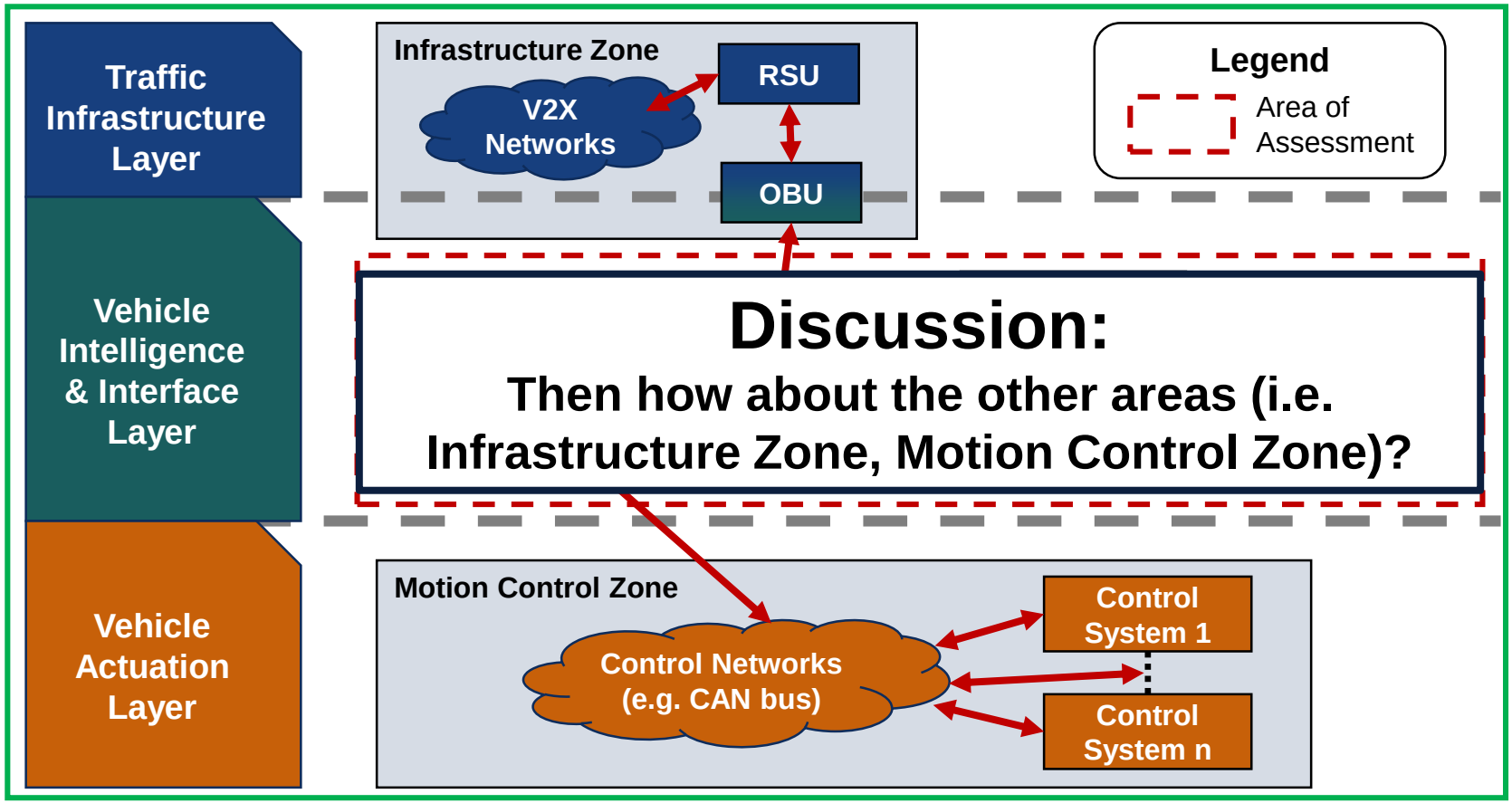
RSU = roadside units, OBU = On-Board Unit,
V2X = Vehicle to everything, ADS = Automated Driving System,
CAN = Controller Area Network

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

TR-68 Part 3: Security

Cybersecurity Key Principles:

Security-by-design

- 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

Defence-in-depth

- **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)

Continuous Operational Management & Oversight

- 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**

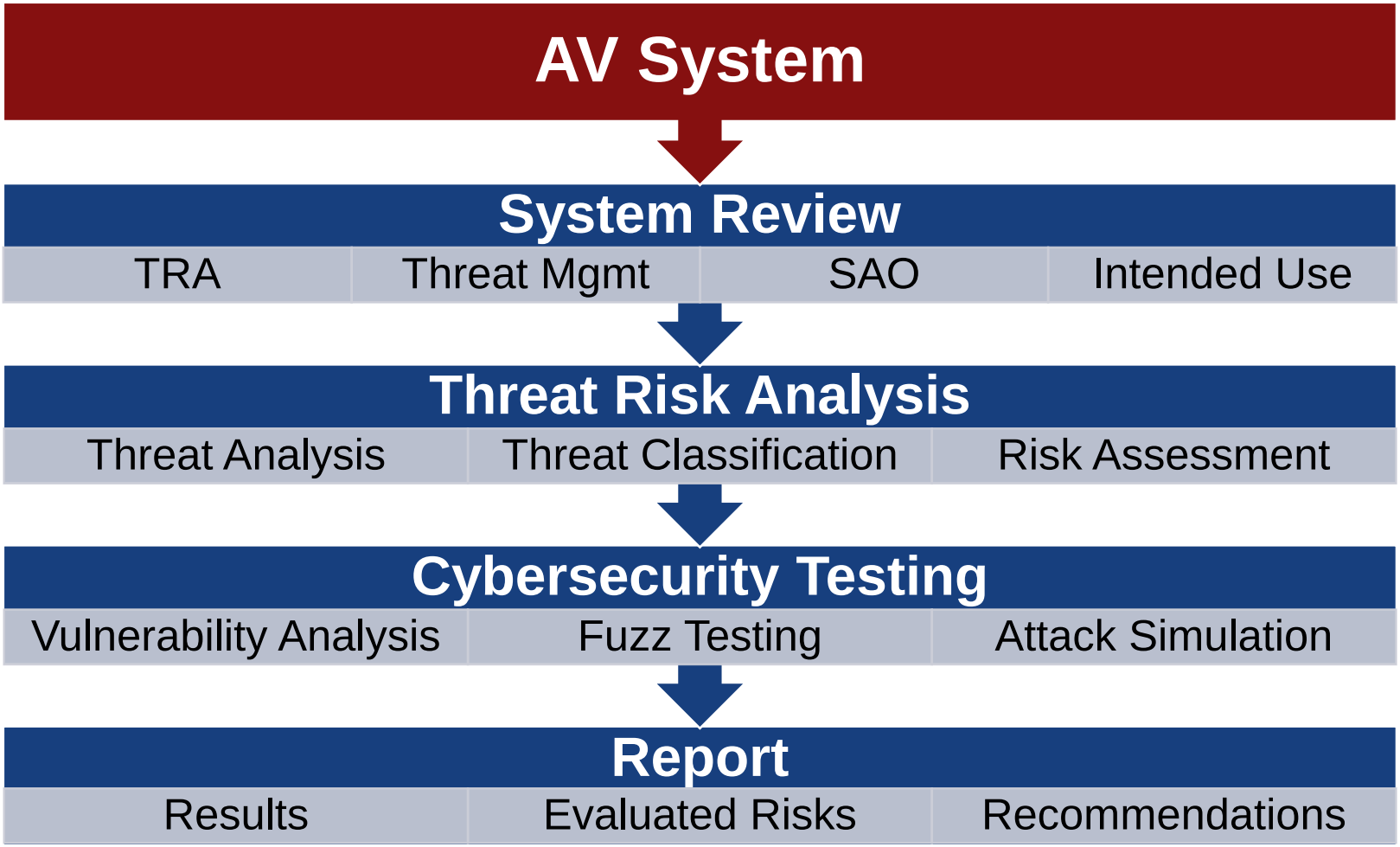
Resiliency

- 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:

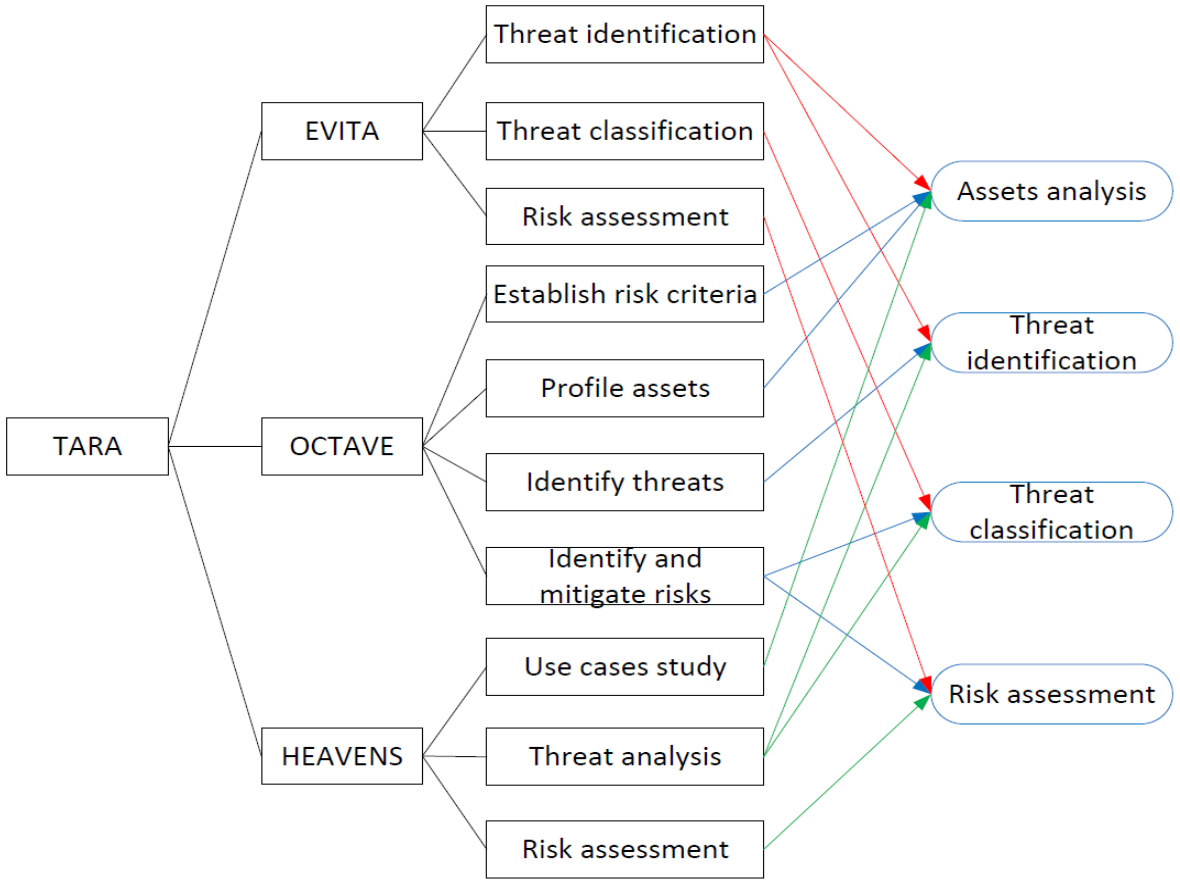


TRA = Threat Risk Assessment
SAO = System Architecture Overview

Content adapted from TR-68-3

TR-68 Part 3: Security

Various Methods for TARA:

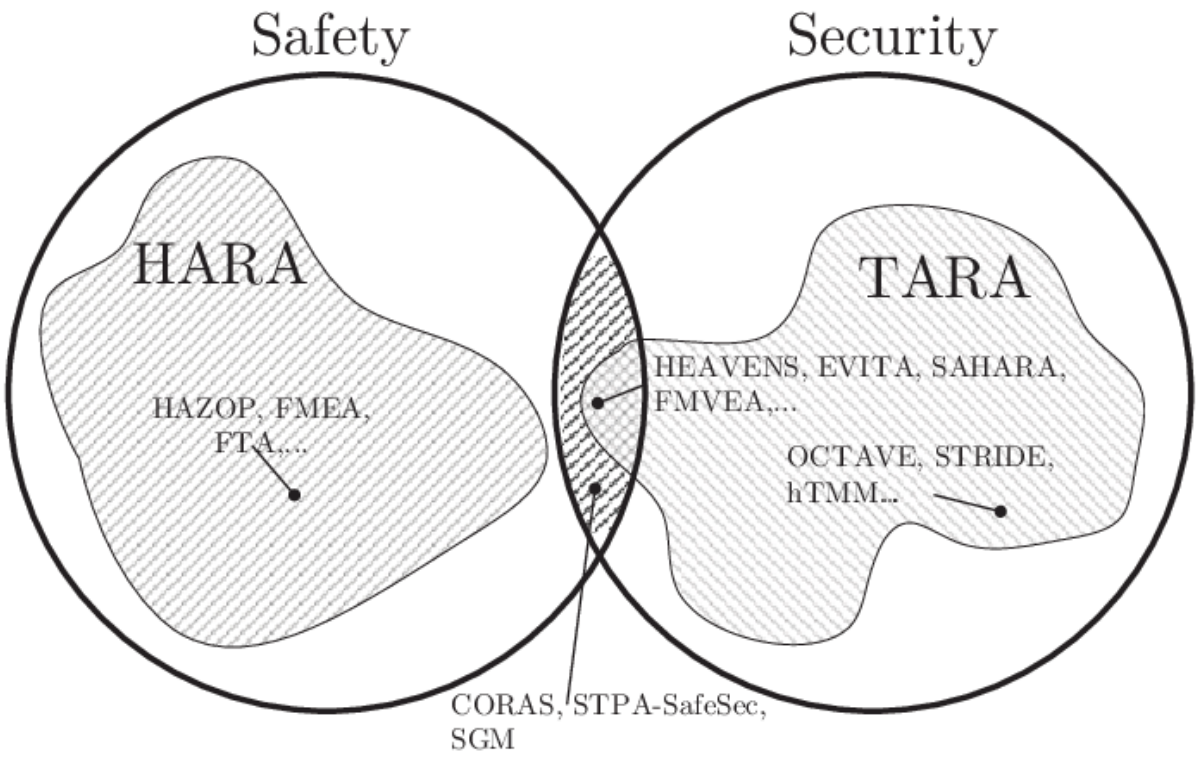


Graphics from *On the Alignment of Safety and Security for Autonomous Vehicles* by Cui, et al.

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.

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!

Main References

- SAE International - J3016
- Singapore Standards Council – TR-68-1/2/3
- Cui, Jin & Sabaliauskaite, Giedre. (2017). On the Alignment of Safety and Security for Autonomous Vehicles
- Dürrwang, Jürgen & Braun, Johannes & Rumez, Marcel & Kriesten, Reiner & Pretschner, Alexander. (2018). Enhancement of Automotive Penetration Testing with Threat Analyses Results. 1. 21. 10.4271/11-01-02-0005