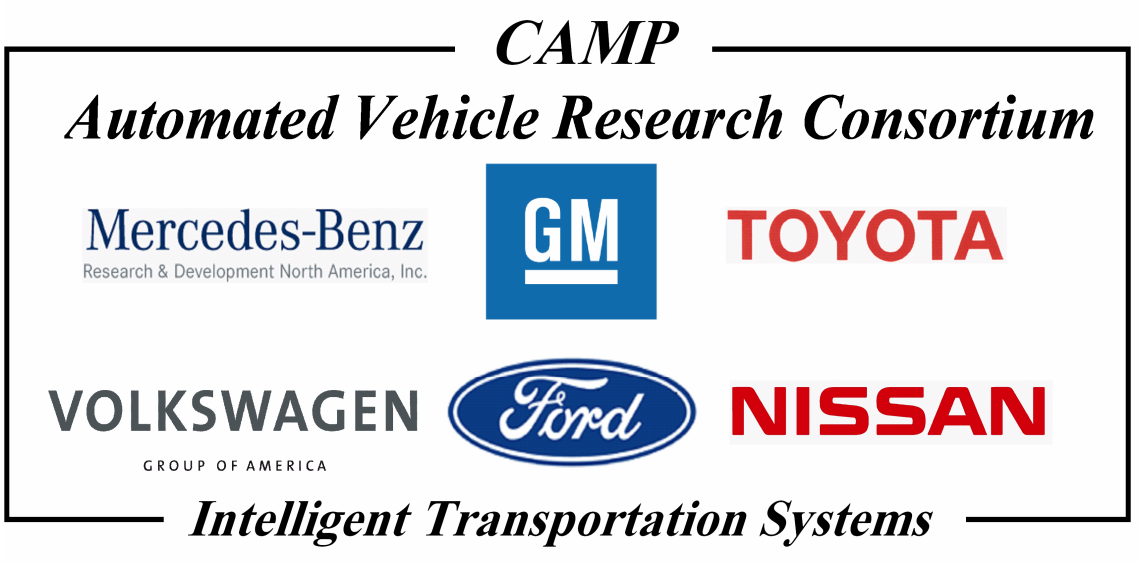


Development of Safety Principles by automation level

Levasseur Tellis
Ford Motor Company

CAMP AVR Project

- Project Started November 2013
- Project consisted six technical tasks
- Project Participants
  - Ford Motor Company
  - General Motors
  - Mercedes-Benz
  - Nissan
  - Toyota Motors
  - Volkswagen Group of America

AVR Project Objectives

- Develop functional descriptions of automation levels
- Develop list of potential driving automation features
- Develop a set of safety principles that apply by level
- Develop potential objective test methods as a framework for evaluating driving automation systems
- Coordinate with NHTSA
  - Human factors
  - Electronic control systems safety

Why Automation Levels Are Needed

- Critical safety discussions
  - Driver's role changes as automation levels change
  - Proper use of technology
- Common framework
  - Design
  - Customer education/training
  - Regulation
- Benefits to development, understanding and acceptance
  - Categorize technology based on functional attributes
  - Clarify driver's role in proper usage

Development of Top-Level Safety Principles

- A key deliverable of the AVR Consortium entailed
  - The creation of a hazard analysis in order to generate top-level safety principles intended to effectively and succinctly cover the identified hazards inherent in driving automation levels 2-5
  - The development of a set of solution-neutral, top-level, safety principles for each of the driving automation levels defined in a previous AVR task
  - Establish (where possible) safety guidance for driving automation systems, while leaving it to the OEM/system designer to generate plausible solutions

Process to Develop Safety Principles

1. Identify Potential **Losses**

2. Identify Potential **Hazards**

3. Draw **Control Structure**

4. Identify **Undesired Control Actions**

5. Identify **Safety Constraints**
(to eliminate undesired control actions)

6. Aggregate constraints into over-arching **principles for each level**

Utilize previous definitions of automation levels throughout

Functional Safety method based on System Theoretic Process Analysis (STPA) developed by Nancy Levesson

Automated Driving Losses and Hazards

Definition of a Loss: "***An undesired and unplanned event that causes human injury or property damage.***"

Definition of a Hazard: **"A system state that together with a worst-case set of external disturbances may lead to a loss."**

Loss	**Vehicle Collision with a Threatening Object**
H1	**Vehicle leaves the roadway**
H2	**Vehicle loses traction or stability**
H3	**Vehicle comes too close to threatening objects in the roadway**
H4	**Vehicle violates traffic laws, rules, and norms**

Note: By definition, hazards are Identical for all levels of automation

Task 6 – Safety Principles

Three Actors Engaged in Driving Automation

Vehicle Operator*

Driving Automation

Vehicle Systems

All three are necessary to describe how automation impacts the performance of the dynamic driving task (DDT)

* - e.g., driver

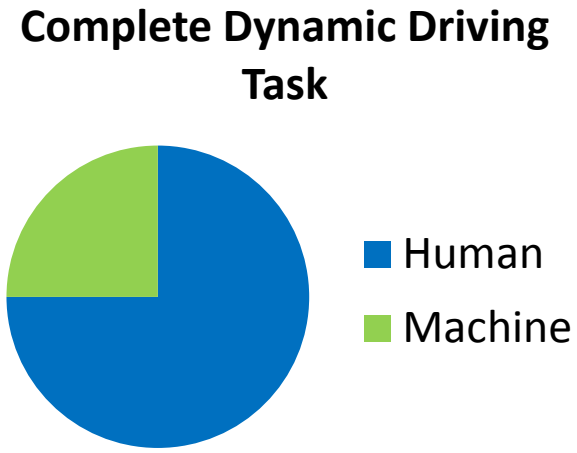
Clear roles of the driver and automation critical in development of Safety Principles

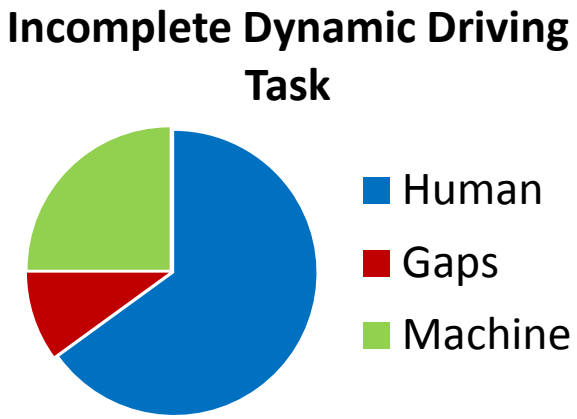
Dynamic Driving Task (DDT) Allocation:

- DDT must be entirely completed on a sustained basis
- Driver performs all aspects of DDT not performed by the driving automation system

Safety outcome of automated driving:

- The potential of automated driving can only be realized if the driver understands their role in DDT completion
- Driver needs to complete remaining portions of DDT unless complete replacement by the driving automation system is available
- Driver's use of the driving automation system plays a significant role in net safety benefit





Safety Constraints Aggregated to Safety Principles

Undesired Control Action	Safety Constraint	Potential Principles
Human driver provides incorrect control when control not needed, when **human OEDR is not engaged due to lack of attention or understanding.**	Human OEDR shall be engaged	**For Level 2 automation, avoidance of hazards is dependent on the human driver performing the OEDR subtask and completing the DDT.**
Human driver provides incorrect control when control not needed, when **human OEDR is not engaged due to inability to perceive environment.**	**Human OEDR shall be engaged;** **human driver shall able to perceive environment.**	**For Level 2 automation, avoidance of hazards is dependent on the human driver performing the OEDR subtask and completing the DDT.** **Human driver must be able to perceive environment.**
Human driver does not provide correct control, or provides control incorrectly, late or early, when control is needed to avoid a hazard, when automation is inactive.	Human driver shall correctly control the vehicle when control is needed to avoid a hazard and automation is inactive	**For Level 2 automation, avoidance of hazards is dependent on the human driver performing the OEDR subtask and completing the DDT.**

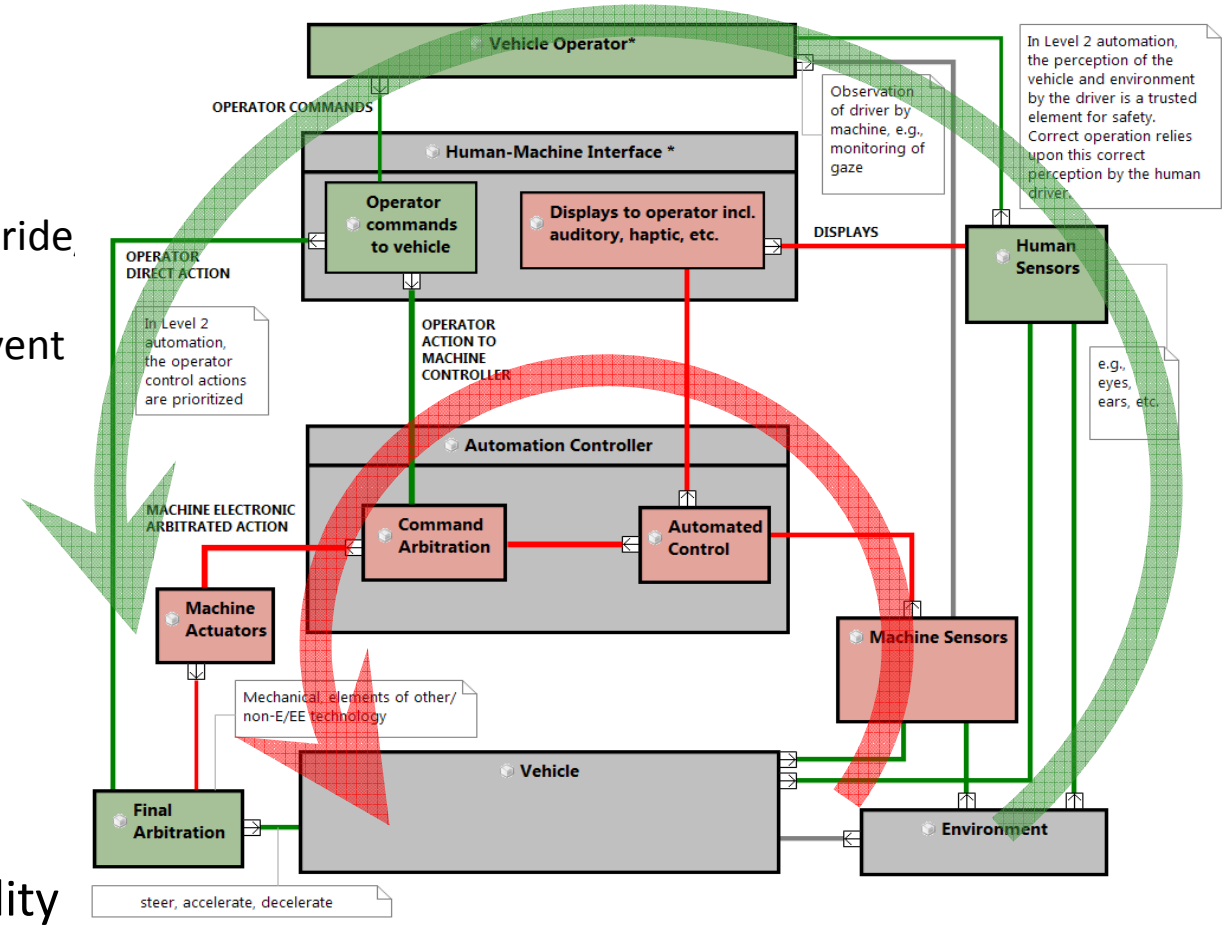
Principle on human driver OEDR

Principle on vehicle design

Principle on human driver OEDR

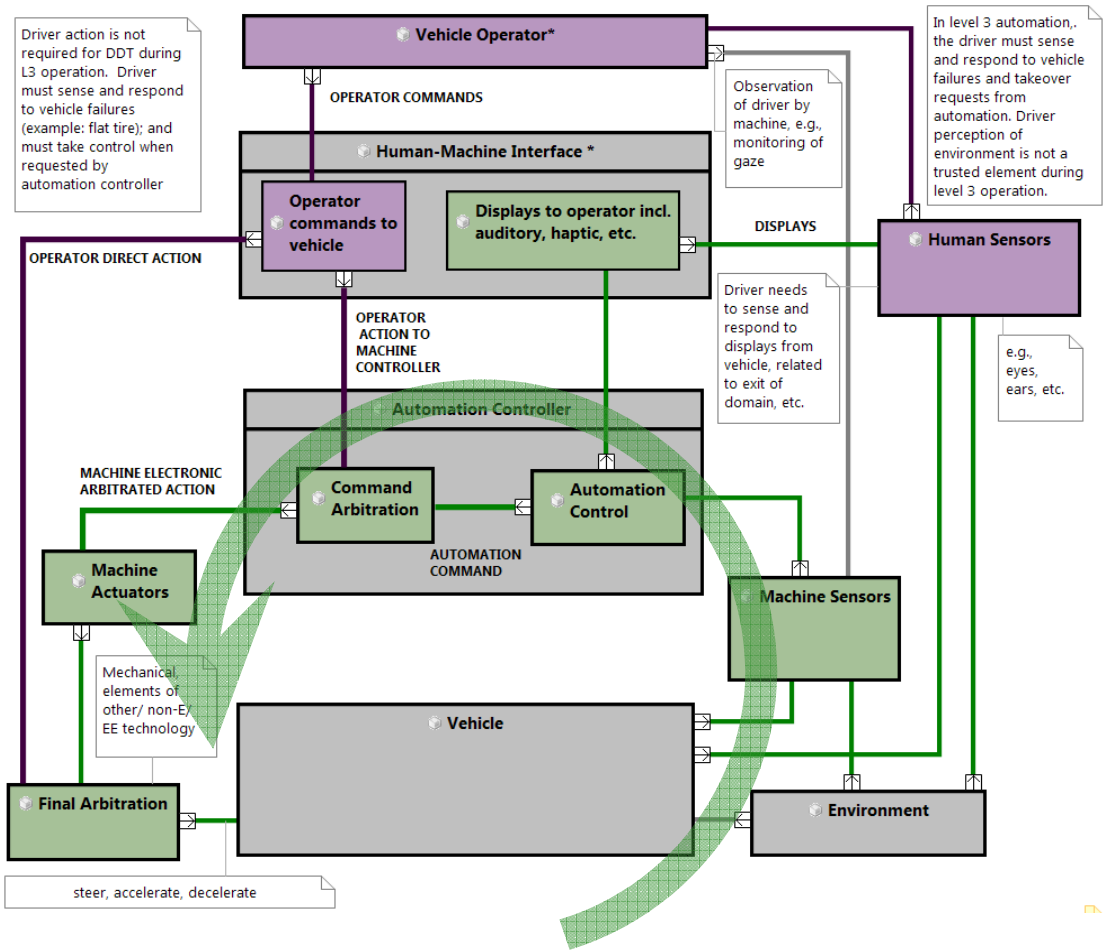
Level 2 Principles

- Driver
  - Operational Readiness
  - OEDR
  - Decision to initiate/ override, cancel automation
  - Fallback control in the event of vehicle or automation failure
- Vehicle
  - Vehicle Controls
  - Visibility
  - Driver control
- Automation - controllability



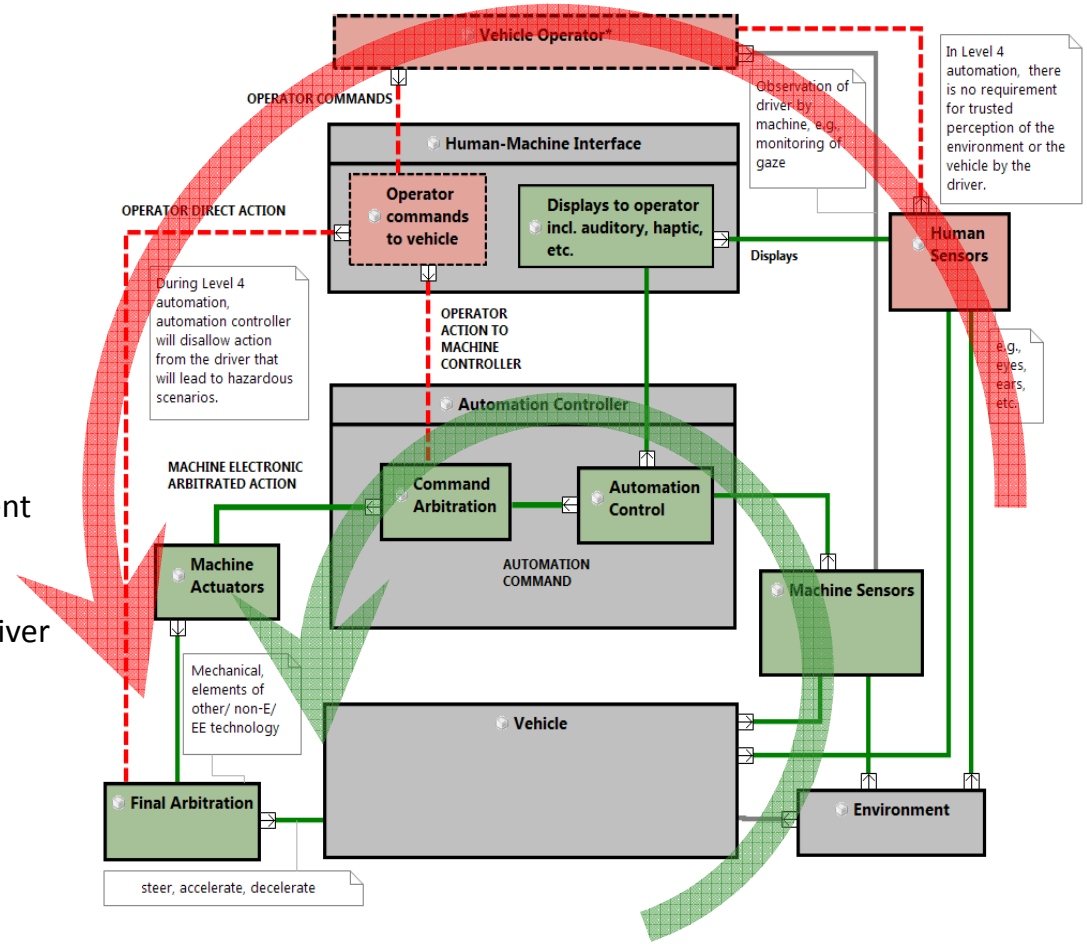
Level 3 Principles

- Driver
  - Operational Readiness
  - Decision to initiate/ override/ cancel automation
  - Fallback control in event of vehicle failure
- Vehicle
  - Vehicle Controls
  - Visibility
  - Driver Control
- Automation
  - Driver initiated
  - Persistent indication of high automation
  - Complete OEDR
  - Validate operational domain
  - Controllability during override or cancel



Level 4 & 5 Principles

- **Driver/Operator**
  - Operational Readiness
  - Decision to initiate operation
- **Vehicle**
  - Driver controls if low automation available
  - Visibility if human driver is present
- **Automation**
  - Complete OEDR
  - Persistent indication of high automation if human driver is present
  - Fail safe operation
  - Validate operational domain
  - May not immediately respond to driver request



Summary of Principles – I

Safety principle related to:	When automation is engaged at: Level 2	Level 3	Level 4	Level 5
Driver/ Operator	assures operational readiness (SP 2.1 i)	← (SP 3.1)	← (SP 4.1)	← (SP 5.1)
	relied upon to avoid hazards, by completing the OEDR subtask and DDT (SP 2.1 ii)			
		activates automation for first time in drive cycle (SP 3.4)	← (SP 4.5)	← (SP 5.5)
		determines if vehicle failure occurs and takes control (SP 3.10 i)		
		understands that direct driver input will cause a transition to lower lever automation and driver will then control those inputs (SP 3.10 ii)		
		takes control when requested by automation (SP 3.10 iii)		
		understands that after automation request to take control, automation will only remain in control for a limited time (SP 3.10 iv)		
Vehicle systems	designed such that the driver is capable of fully performing DDT (lateral / longitudinal control and OEDR) (SP 2.2)	← (SP 3.2)	← Note - include if vehicle is capable of lower level automation	← Note - include if vehicle is capable of lower level automation

Summary of Principles – II

Safety principle related to:	*When automation is engaged at:*			
	Level 2	**Level 3**	**Level 4**	**Level 5**
Automation Controller (part 1)	arbitrate between defined driver inputs and driving automation commands by prioritizing the driver input (SP 2.3 i)	← (SP 3.3 i)		
	allow driver to take full control at any time (SP 2.3 ii)	← (SP 3.3 ii)		
	may verify defined driver input before deactivating driving automation (SP 2.3 iii)	← (SP 3.3 iii)		
		provides persistent indication to driver of operation in high automation state (SP 3.5)	← Note - include if vehicle is capable of lower level automation	← Note - include if vehicle is capable of lower level automation
		provides indication to driver of request to transition to lower level automation (SP 3.6)	← Note - include if vehicle is capable of lower level automation	← Note - include if vehicle is capable of lower level automation
		competently performs the DDT within its operational design domain (SP 3.7 i)	← (SP 4.2 i)	competently performs the DDT in all domains (SP 5.2)

Summary of Principles – III

Safety principle related to:	*When automation is engaged at:*			
	Level 2	**Level 3**	**Level 4**	**Level 5**
Automation Controller (part 2)		prohibit entry into automated driving when domain is not achieved (SP 3.7 ii)	← (SP 4.2 ii)	
		vehicle/automation system single point failure shall not cause immediate loss of total control (SP 3.8)	designed such that any single failure does not lead to a hazardous situation (SP 4.3)	← (SP 5.3)
		before exiting domain or in advance of automation failure that impacts DDT performance, system shall transfer control to the driver (SP 3.9)	ability to engage minimal risk condition when necessary (SP 4.2-iii)	← (SP 5.2)
		verified driver inputs shall cause transition to lower level automation (SP 3.9 i)	may delay requests by operator to take over/stop automation when necessary to avoid identified hazards (SP 4.4)	← (SP 5.4)
		system shall maintain operational condition that affords reasonable transition time to driver (SP 3.9 ii)		

Key Take-aways

- Hazards and losses to be considered in the development of safety principles per driving automation level were developed
- Generic control structure was put together to describe each driving automation level and facilitate the creation of safety principles by level
- Level 2 driving automation systems are intended to complement but not substitute for the human driver in performing the Dynamic Driving Task (DDT) and the safety principles developed for Level 2 highlight this intention.
- The most significant safety principle placed on a Level 3 driving automation systems is that when it is engaged, the DDT is performed solely by the driving automation system within a limited ODD (e.g., geographical location, environmental condition, speed, etc.
- The most significant safety principle placed on Level 4 and 5 driving automation systems is that operator requests to take over part or all of the DDT may not be immediately granted as the system may be operating in domains where human control is not allowed or could cause an undesired hazard/control action.

BACKUP

Lower Levels (1-2) of Automation

Automation Level Name	Automation Level Narrative Description	Dynamic Driving Sub-Tasks		Functional Capability	
		Sustained Execution of Lateral and/or Longitudinal Control	Object & Event Detection and Response (OEDR)	Fallback Performance of Dynamic Driving Task	Driving Mode Circumstance, Location Capabilities
Driver performs all or part of the dynamic driving task and general system functional capabilities					
0 No Automation	The full-time performance by the driver of all aspects of the dynamic driving task, even when enhanced by warning or event-based intervention systems	Driver	Driver	Driver	None of the DDT is automated
1 Driver Assistance	The driving mode-specific execution by a system of either sustained lateral **OR** sustained longitudinal control using sensing data and with the expectation that the driver performs the remainder of the dynamic driving task	Driver and system	Driver	Driver	Some driving modes
2 Partial Automation	The driving mode-specific execution by one or more systems of both sustained lateral **AND** sustained longitudinal control using sensing data with the expectation that the driver performs the remainder of the dynamic driving task	**System**	Driver	Driver	Some driving modes

Higher Levels (3-5) of Automation

Automation Level Name	Automation Level Narrative Description	Dynamic Driving Sub-Tasks		Functional Capability	
		Sustained Execution of Lat. and/or Long. Control	Object & Event Detection and Response (OEDR)	Fallback Performance of Dynamic Driving Task	Driving Mode Circumstance, Location Capabilities
Automated driving system performs all the dynamic driving task and general system functional capabilities					
3 Conditional Automation	Automated driving system features in this level automate the complete dynamic driving task, providing appropriate responses to relevant objects and events. However, the automation is situationally-limited in functional capabilities both in terms of driving modes, circumstances, and/or locations and, particularly in terms of fallback performance capability. There is the expectation that the driver will respond appropriately to a request to resume performance of the dynamic driving task	System	**System**	Driver	Some driving modes
4 High Automation	The driving mode-specific performance by a system of all aspects of the dynamic driving task, providing appropriate responses to relevant objects and events, even if a driver does not respond appropriately to a request to resume performance of the dynamic driving task	System	System	**System**	Some driving modes
5 Full Automation	The full-time performance by a system of all aspects of the dynamic driving task, providing appropriate responses to relevant objects and events, under all on-road driving conditions legally available to a driver	System	System	System	
Automated driving system performs complete dynamic driving task, providing appropriate responses to relevant objects and events, and greater functional capability					