CAMP
AUTOMATED VEHICLE RESEARCH (AVR)
PROJECT DELIVERABLES

Levasseur Tellis, Ford Motor Company

SAE INTERNATIONAL

Ford

AVR Project Objectives

- Develop functional descriptions of driving 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

CAMP AVR Project Structure

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

➢ Final report added to the public review docket (NHTSA-2014-0070) in December 2016

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 and automated function's role in proper usage

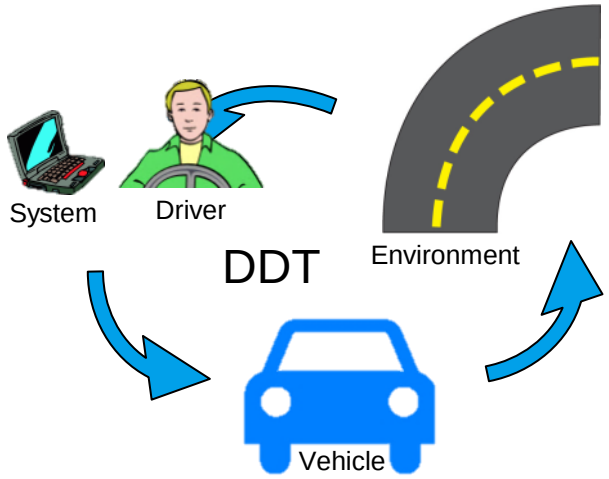
To What Do Levels Apply?

- Levels apply to the set of all the functions that a driver can engage simultaneously
  - Independent of which system provides the function
  - Independent of operational design domain restrictions
  - Also relevant for systems which can operate with different functions engaged to produce different levels of automation
  - Not necessary to define “feature,” “application,” or “system”
- Relevant for Level 2 capability determination

What Is Level 2 vs. Level 3 Automation?

At Level 3 the driving automation system is designed to perform the entire Dynamic Driving Task (DDT) when engaged by the driver

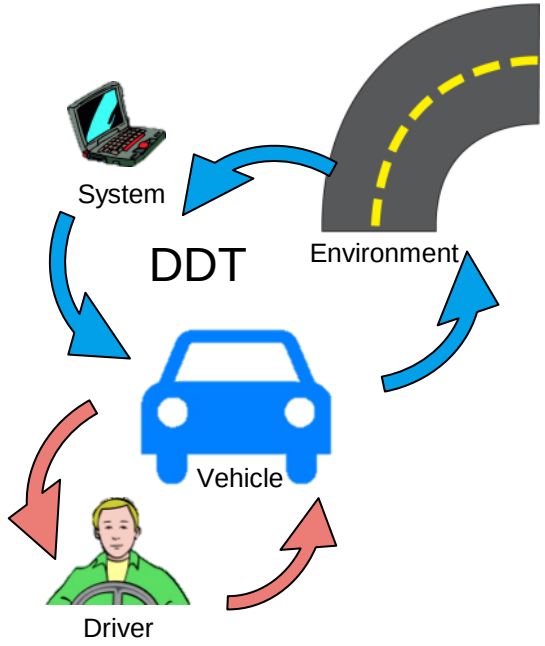
Establishes “bright line” distinction between “high” and “low” levels of driving automation



Driver performs all or part of the DDT. In Level 2, part of the DDT means OEDR* portion (supervising the driving automation and responding to unmanaged vehicle failures)

Level 1 & 2

* Driver’s role is **O**bject and **E**vent **D**etection and **R**esponse (OEDR).



In Level 3, “the driver loop” becomes the driver and the vehicle. Driver responds to driving automation requests and unmanaged vehicle failures.

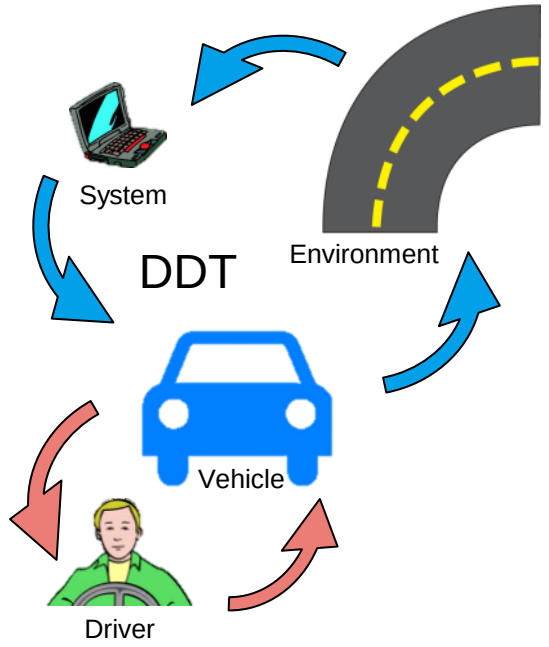
Level 3

* Driver’s role is **Automation Alert D**etection and **R**esponse

What Is Level 3 vs. Level 4 Driving Automation?

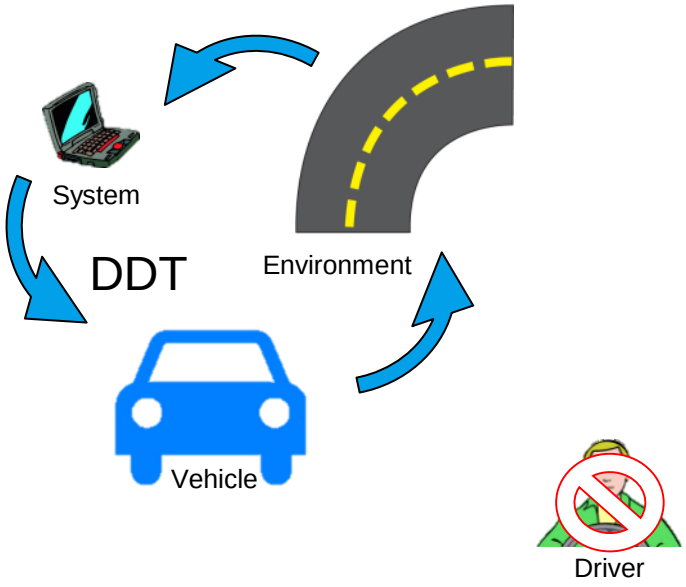
At Level 4 the driving automation system is designed to perform the entire Dynamic Driving Task (DDT) when engaged by the driver / operator

Establishes “bright line” distinction between Level 3 and Level 4 driving automation



In Level 3, “the driver loop” becomes the driver and the vehicle. Driver responds to driving automation requests.

Level 3



In Level 4, the driver has no role in the DDT

Level 4

* Driver / Operator has no role within the DDT

What Is The Role Of Driver In Operating Driving Automation?

Driving Automation is categorized by the driver's role in proper usage according to the feature's functional characteristics

Vehicle operational control

- Is the driver performing sustained **lateral and/or longitudinal control**?

Object and event sensing and response capability

- Is the driver required to **supervise** the automated feature?

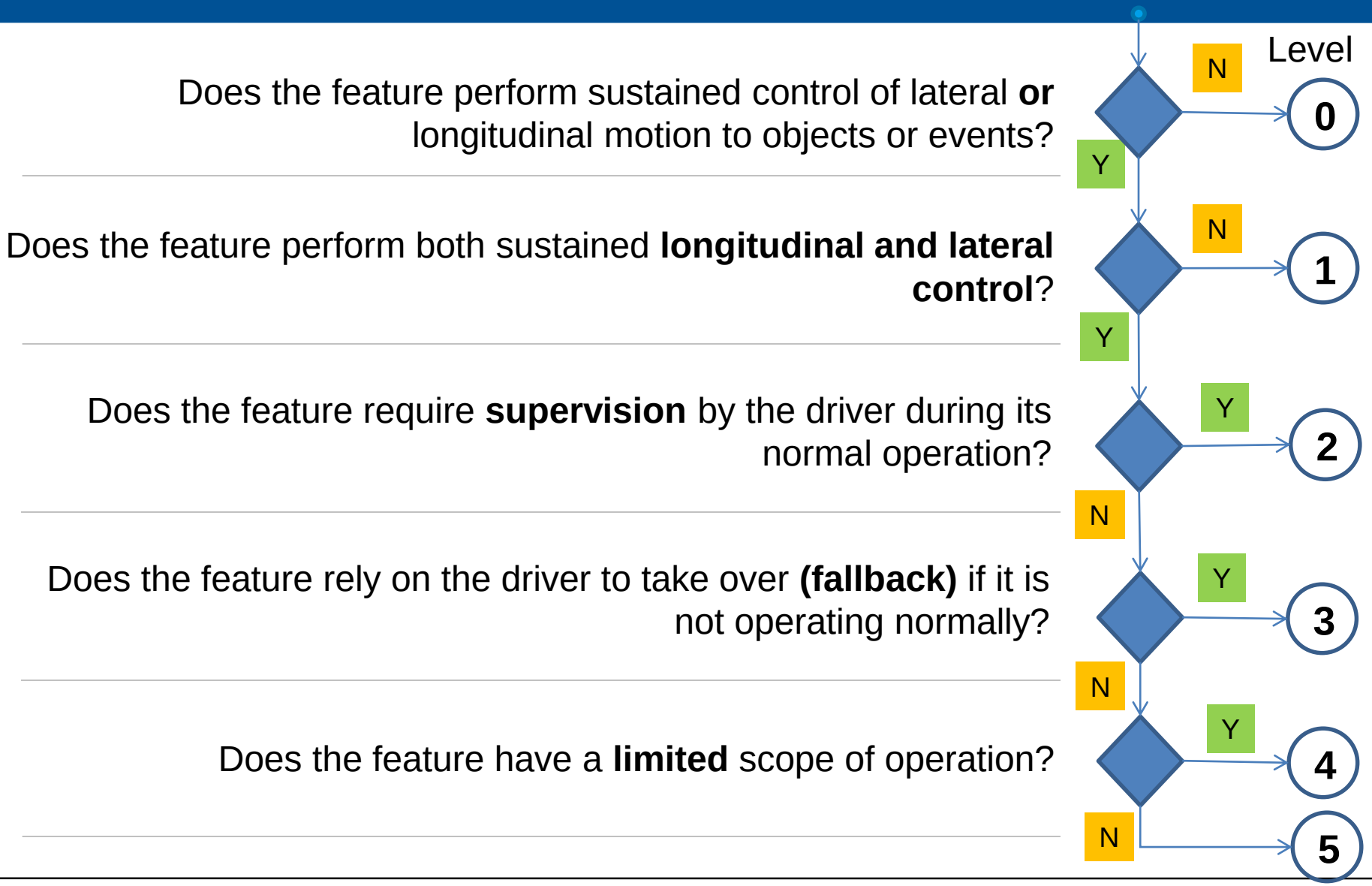
Automation backup strategy

- Will the driver act as **fallback** in case the vehicle or automated feature is not operating normally?

Operational conditions

- Can the driver use the automated feature at all times or is it conditionally or modally **limited**?

Automated Level Categorization Flow Chart for Automation Designers



Mapping Features to Levels using Methodology

Driving Automation Methodology Question	Sustained Lateral **OR** Longitudinal control?	Sustained Lateral **AND** Longitudinal Control?	Driver supervision required?	Driver required outside normal operation?	Limited scope of operation?	
Driving Automation characteristic	Control to the external environment		Sensing and response	Fallback	Operational conditions	
Response to methodology question confirms level or proceeds to next question	Yes, move to next question		No, move to next question			
	No, stop at this level		Yes, stop at this level			
Driving Automation Level	**0**	**1**	**2**	**3**	**4**	**5**
Electronic Stability Control (ESC)	No ↑					
Conventional Cruise control	No ↑					
Adaptive cruise control (ACC)	Yes →	No ↑				
ACC with Lane Keeping (steering support)	Yes →	No ↑				
ACC with Lane Centering	Yes →	Yes →	Yes ↑			
Highway pilot	Yes →	Yes →	No →	Yes ↑		
Automated Parking System	Yes →	Yes →	No →	No →	Yes ↑	
Robotic Taxi	Yes →	Yes →	No →	No →	No →	↑

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
- 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 by Automation Level

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

Employed Functional Safety practices 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

Safety Principles Actors

Three Actors Engaged in Driving Automation

Vehicle Operator*

Driving Automation

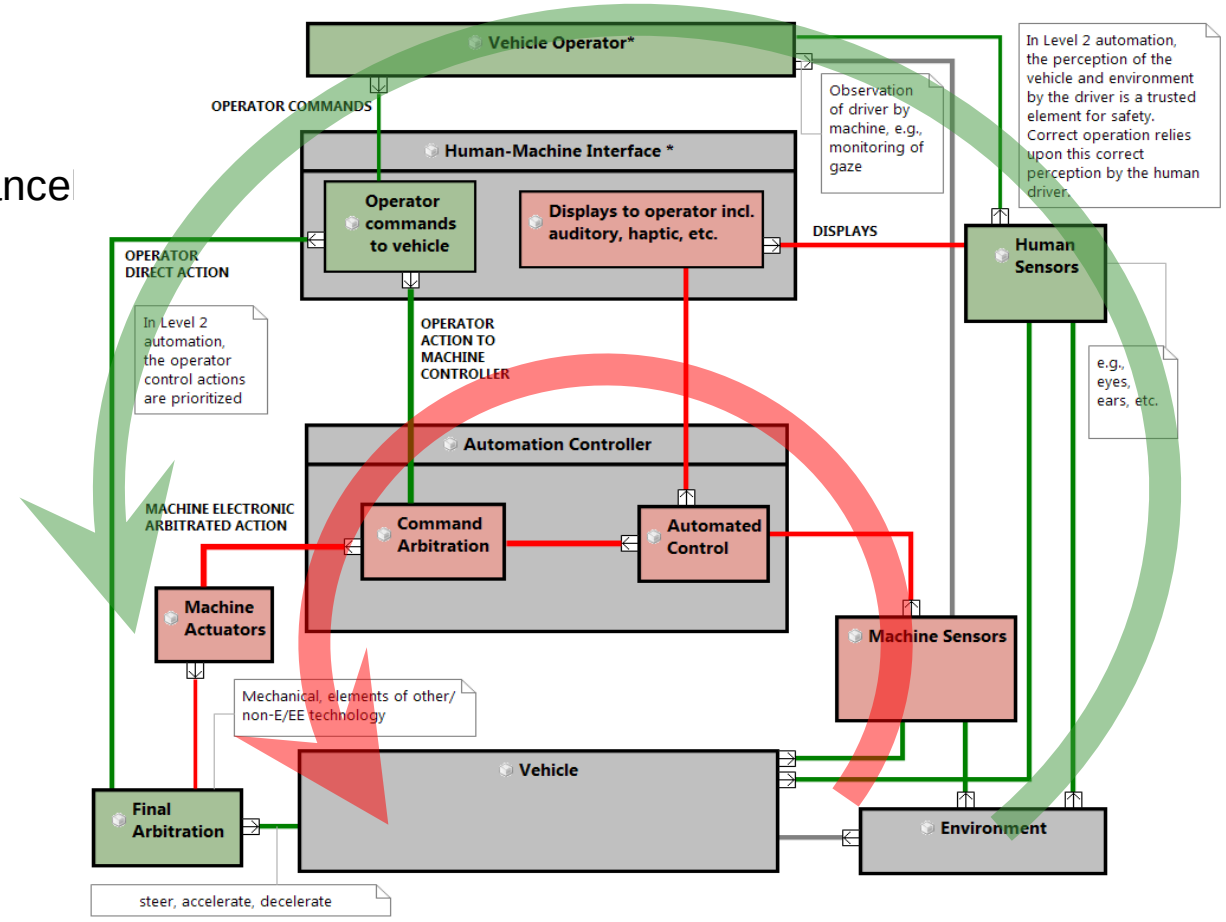
Vehicle Systems

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

** - e.g., driver*

Level 2 Principles

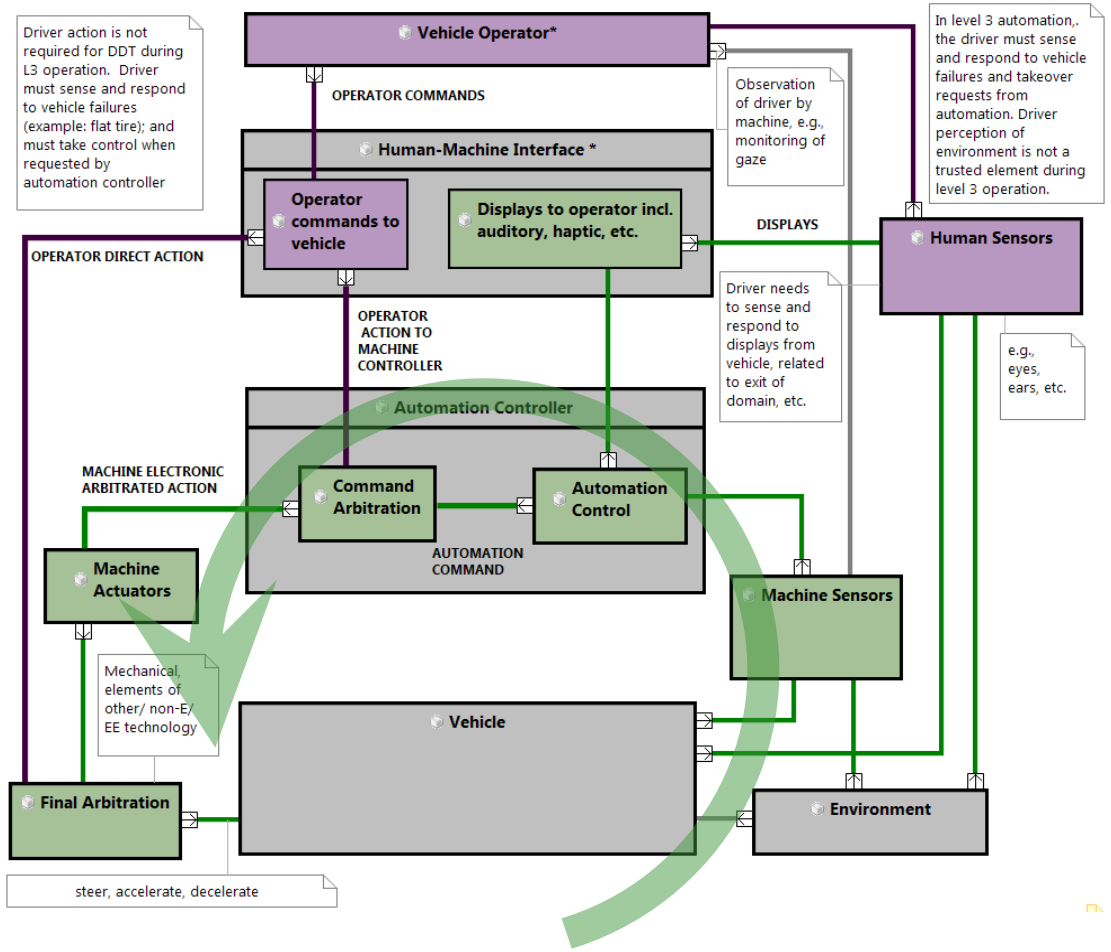
- Driver
  - Operational Readiness
  - OEDR
  - Decision to initiate/ override/ cancel automation
  - Fallback control in the event of vehicle or automation failure
- Vehicle
  - Vehicle Controls
  - Visibility
  - Driver control
- Automation - controllability



Generic Level 2 STPA Control Diagram

Level 3 Principles

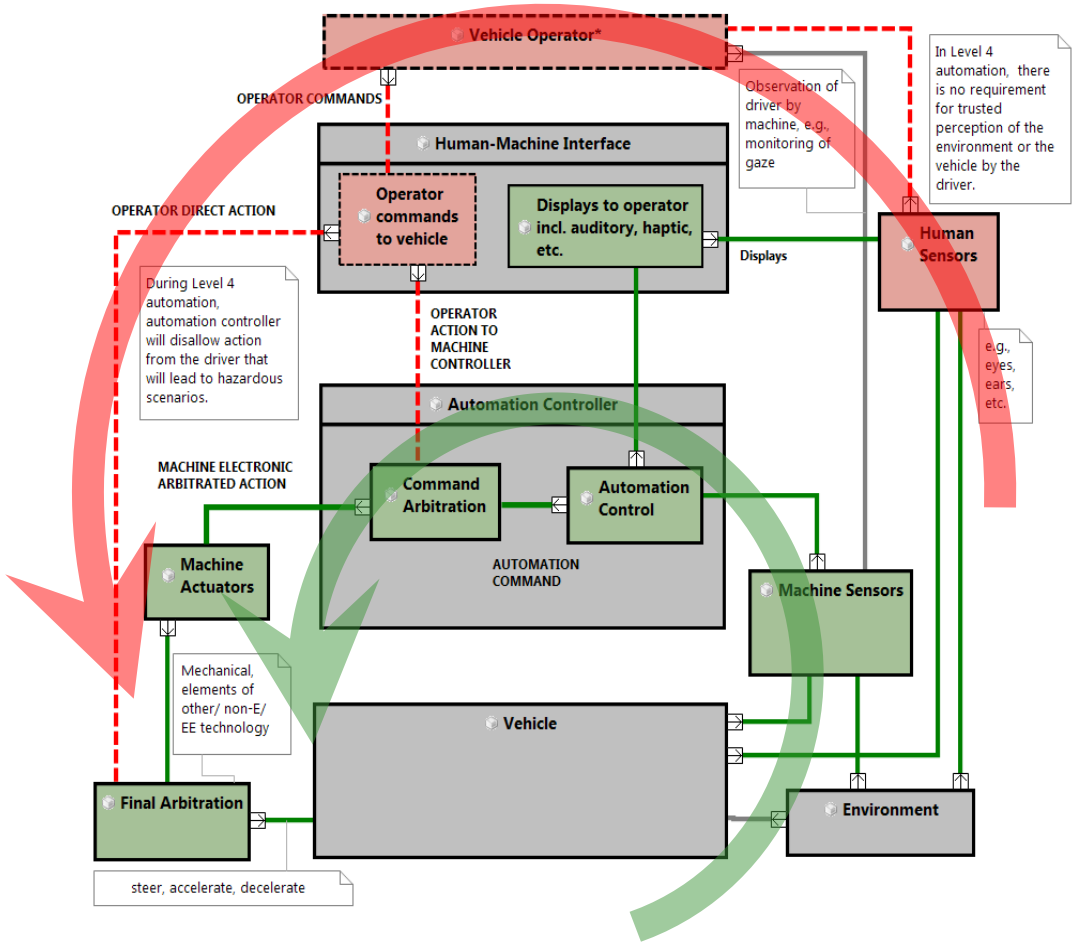
- Driver
  - Operational Readiness
  - Decision to initiate/ override/ cancel automation
  - Fallback control in event of vehicle failure
- Vehicle
  - Vehicle Controls
  - Visibility
  - Driver Control
- Automation
  - Driver initiated
  - Persistent indication of high automation
  - Complete OEDR
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



Generic Level 3 STPA Control Diagram

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



Generic Level 4 & 5 STPA Control Diagram

System Design Impacts - Level 3 Automation

Safety Principle 3.9: Before exiting the operational design domain, upon occurrence of a driving automation system failure that prevents performance of the DDT, the driving automation system shall request the driver to take control:

i. Verified driver control inputs shall cause transition from Level 3 into a lower level of automation

ii. The driving automation system shall maintain an operating condition that affords a controlled transition to driver control, regardless of whether the transition is prompted by fault within the driving automation system, or prompted by violation of the intended operational design domain

System Design Principles:

- **Longitudinal and Lateral Control**

Ability to recognize defined driver inputs for lateral and longitudinal control vs. that of the automation's, and always prioritize the driver's input request.

- **Sensing**

Ability to completely perform all Object Event Detection and Respond appropriately within its Operational Design Domain. The sensing has to be able to access when the vehicle is leaving its Operational Design Domain, and provide this assessment in enough time for the driver/operator who was not actively monitoring the automation or driving environment to take over vehicle control.

- **Human Machine Interface (HMI)**

Inform driver/operator that the vehicle is approaching the limits of its Operational Design Domain. The HMI must be able to get the driver back in the Object Event Detection loop before the vehicle exits the Operational Design Domain.

System Design Impacts:
Level 3 Driving Automation

Safety Principle 3.10: The driver must understand the following:

i. The driver's role is to determine if there has been a vehicle failure that may impact the safe operation of the vehicle, and to take over control of the vehicle when such a failure occurs

ii. In response to a driver request to take over performance of the DDT, the primary response from the driving automation system is to transition out of Level 3 automation and into a lower driving automation level

iii. When the driving automation system is requesting the driver to take control of the vehicle, the driver's role is to respond by taking over control

iv. After requesting the driver to take control, the driving automation system will remain in control for a limited time period

System Design Principles:

- **Longitudinal and Lateral Control**

Ability to recognize defined driver inputs for lateral and longitudinal control vs. that of the automation's, and always prioritize the driver's input request.

- **Sensing**

Ability to completely perform all Object Event detection and respond appropriately within its Operational Design Domain until the driver takes over.

- **HMI**

Inform driver/operator that the vehicle is approaching the limits of its Operational Design Domain. The HMI must be able to get the driver back in the Object Event Detection loop before the vehicle exits the Operational Design Domain.

Example:
Level 2 vs Level 3 Traffic Jam Assist Feature

Traffic Jam Assist Use Case: Driving on a straight road with the feature engaged, the driver encounters an issue in the roadway that is out of the Operational Design Domain (disabled vehicle, debris from a truck falls in the roadway, object in the roadway)

Level 2 Design Principles:

- **Longitudinal and Lateral Control**

Ability to perform sustained lateral and longitudinal within the Operational Design Domain (not a requirement to completely perform the long &lat control) and perform in a manner that is predictable & repeatable. The control must also prioritize operator requests at any time.

- **Sensing**

Perform in a manner that is predictable & repeatable (not a requirement to completely perform the complete OEDR)

- **HMI**

As the automation does not have to recognize this issue , it is the driver's role to monitor the environment. The automation shall be designed in such a manner that it does not encourage the driver to leave the Object Event Detection and Response loop.

Level 3 Design Principles:

- **Longitudinal and Lateral Control**

Ability to perform sustained lateral and longitudinal control for everything within the Operational Design Domain without any input from the driver/operator and perform in a manner that is predictable & repeatable. The control must also prioritize operator requests at any time.

- **Sensing**

Ability to completely perform all Object Event detection and respond appropriately within its ODD. The sensing has to be able to access when the vehicle is approaching the limits of its Operational Design Domain.

- **HMI**

Must inform the driver who is not monitoring the environment in enough time for the driver to resume control of the vehicle (re-enter the Object Event Detection and Response loop) before exiting the ODD. The driver must remain in the Automation Alert Detection and Response loop.

System Design Impacts
Level 4 Driving Automation

Safety Principle 4.2: When activated, the driving automation system shall perform the DDT and fallback as needed within its application-specific ODD, providing the appropriate responses to relevant objects and events. This includes but is not limited to**:**

i. Continuous assessment of operation within actual versus operational design domain

ii. Prohibiting entry into automated driving when the operational domain is not achieved

iii. Ability to achieve minimal risk condition if necessary due to any one of the following:

   a) Operator failure to respond appropriately to pending exit of the ODD
   b) A failure that prevents performance of the complete DDT

System Design Principles:

- **Longitudinal and Lateral Control**

Ability to perform sustained lateral and longitudinal control for everything within the Operational Design Domain without any input from the driver/operator, and perform well enough to get the vehicle to a safe harbor. The control must also deny operator requests to stop automation if stopping automation puts the vehicle in a hazardous state.

- **Sensing**

Ability to completely perform all Object Event detection and respond appropriately within its Operational Design Domain. The sensing has to access when the vehicle is approaching the limits of its ODD, and the automation must acquire an area to bring the vehicle to a safe harbor before it leaves the ODD (minimal risk condition).

- **HMI**

Inform driver/operator that the vehicle is leaving the ODD for Level 4.

Example:
Level 4 Traffic Jam Assist Feature

Traffic Jam Assist Use Case: Driving on a straight road with the feature engaged, the driver encounters an issue in the roadway that is out of the Operational Design Domain (disabled vehicle, debris from a truck falls in the roadway, object in the roadway)

Level 4 Design Principles:

- **Longitudinal and Lateral Control**

Ability to perform sustained lateral and longitudinal control for everything within the Operational Design Domain without any input from the driver/operator. The control must also prioritize automation control over driver /operator control when it is not safe to transfer control to the driver/operator.

- **Sensing**

Ability to completely perform all Object Event detection and respond appropriately within its domain. The sensing has to be able to access when the vehicle is approaching the limits of its Operational Design Domain, and acquire an area to bring the vehicle to a safe harbor (minimal risk condition). Has to determine when it is unsafe for the driver to take control of the DDT within a Operational Design Domain for Level 4 automation

- **HMI**

Inform driver/operator that the vehicle is leaving the Operational Design Domain.

Development of potential objective test methods

- Objectives
  - Focused on Levels 2 & 3
  - Identified real-world use cases
  - Defined preliminary objective test methods
  - Identified testing challenges

- Level 2 Testing – Driver Control
  - Applied the Level 2 safety principles from Task 6
  - Assessed driver's ability to resume/complete Dynamic Driving Task when system cannot manage a hazard
  - Considered testing methods for publicly available systems/concepts

- Level 3 Testing Challenges – System Performance
  - Applied the Level 3 safety principles from Task 6 (more extensive than Level 2)
  - Considered test scenarios

Development of potential objective test methods

- Classification and Operational Description (COD)
  - Document completed by manufacturer
  - Supports OEM test procedure proposal
  - Includes system description, automation level, safety principles and use cases

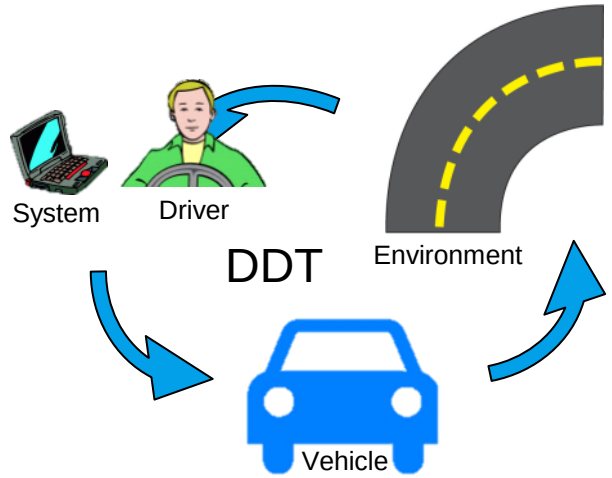
- Preliminary Test Concepts
  - Parking Assist, Traffic Jam Assist, High Speed Automated Cruise
  - Test methods are specific to system
  - Driver needs to have the ability to override or terminate system operation

- Addressed only Level 2
  - Imminent availability
  - System concepts are publicly available (not so for Level 3+)
  - Concluded that Level 3+ are virtually unlimited, design specific and beyond project scope

Conclusion(s)
Driving Automation Level 2

- **Level 2 Motion Control**
  - Should be predictable, repeatable, and allow the driver to take over
- **Level 2 Sensing**
  - Should be predictable & repeatable
- **Level 2 HMI**
  - Should not encourage driver complacency (must not suggest that it is ok for a driver to completely leave the Object and Event Detection loop)

.



Driver performs all or part of the DDT. In Level 2, part of the DDT means OEDR* portion (supervising the driving automation and responding to unmanaged vehicle failures)

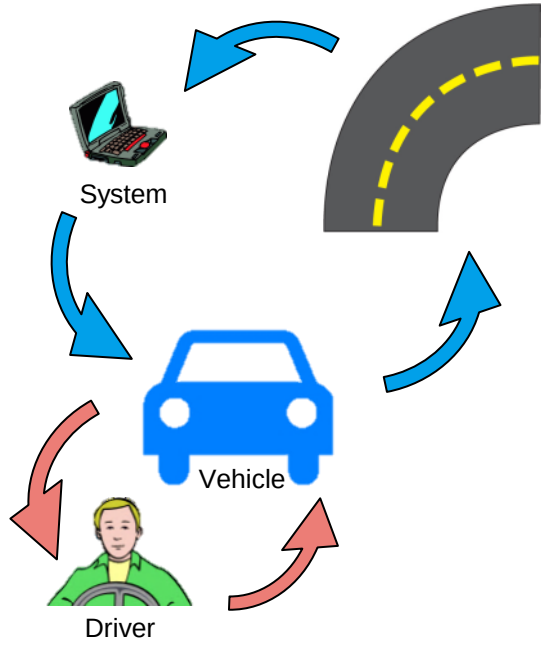
Level 1 & 2

* Driver's role is **O**bject and **E**vent **D**etection and **R**esponse (OEDR).

Conclusion(s)
Driving Automation Level 3

- **Level 3 Motion Control**
  - Should be predictable, repeatable, and allow the driver to take over
  - Should perform all motion control within the ODD without input from the driver/operator
- **Level 3 Sensing**
  - Should be predictable & repeatable
  - Should perform all Object Detection within the ODD, and respond appropriately
  - Should know when it is encountering a situation outside its ODD in enough time to inform the driver/operator
  - Level 3 sensing is the same as Level 4 & 5 with the exception that Level 3 sensing does not have to find a safe harbor in the event of an upcoming exit from the ODD
- **Level 3 HMI**
  - HMI Strategy for Level 3 functionality requires invention (to bring a driver who has left the Object Event detection and response loop back)

.



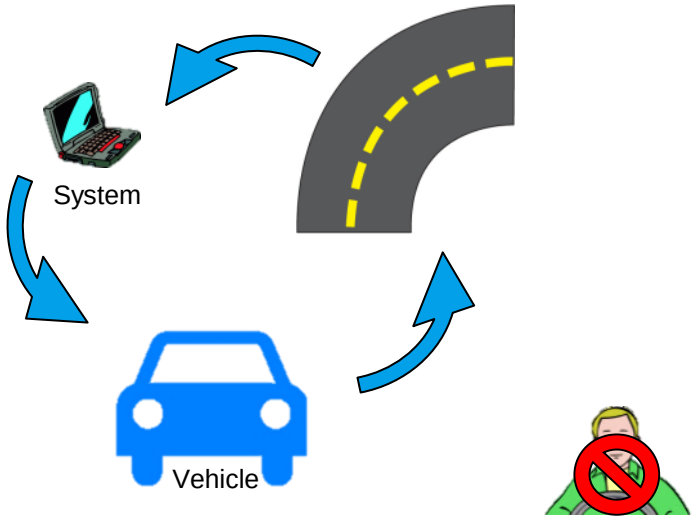
In Level 3, “the driver loop” becomes the driver and the vehicle. Driver responds to driving automation requests and unmanaged vehicle failures.

Level 3

* Driver’s role is **Automation Alert D**etection and **R**esponse

Conclusion(s)
Driving Automation Level(s) 4 & 5

- **Level 4 & 5 Motion Control**
  - Should be predictable, repeatable, and allow the driver to take over (if possible)
  - Should perform all motion control within the ODD without input from the driver/operator
  - Should be capable of bring the vehicle to the minimum risk condition in the event of an automation or vehicle failure
- **Level 4 & 5 Sensing**
  - Should be predictable & repeatable
  - Must perform all Object Detection within the ODD, and respond appropriately
  - Should be able to acquire safe harbors
  - Should know when it is encountering a situation outside its ODD in enough time to bring the vehicle to a safe harbor
  - Should determine when it is hazardous to transfer control back to the driver
- **Level 4 & 5 HMI**
  - If the vehicle is capable of transitioning to a Level 0-3 automation, the HMI must inform the driver that it is no longer operating at Level 4 automation.



In Level 4, the driver has no role in the DDT

Level 4&5

* Driver / Operator has no role within the DDT

Potential Areas for Future Collaboration

- Industry, government and other stakeholder cooperation is needed to
  - Develop fundamental Level 4 automation functions needed for a particular ODD
  - Alignment on principles for minimum risk condition implementation

- Ongoing Research geared towards
  - Identifying the likelihood and the manner in which drivers may not comply with the Safety Principles in Level 2 and Level 3 Driving Automation
  - System usages (i.e., analysis of ‘things gone wrong’)
  - Identifying the likelihood and manner in which drivers will likely comply with the Safety Principles in Level 2 and Level 3 Driving Automation
  - System usages (analysis of ‘things gone right’)
  - Developing Human Machine Interface (HMI) design guidelines intended to support drivers in complying with the relevant Safety Principles for the system they are utilizing
  - Evaluate HMI design guideline real world performance