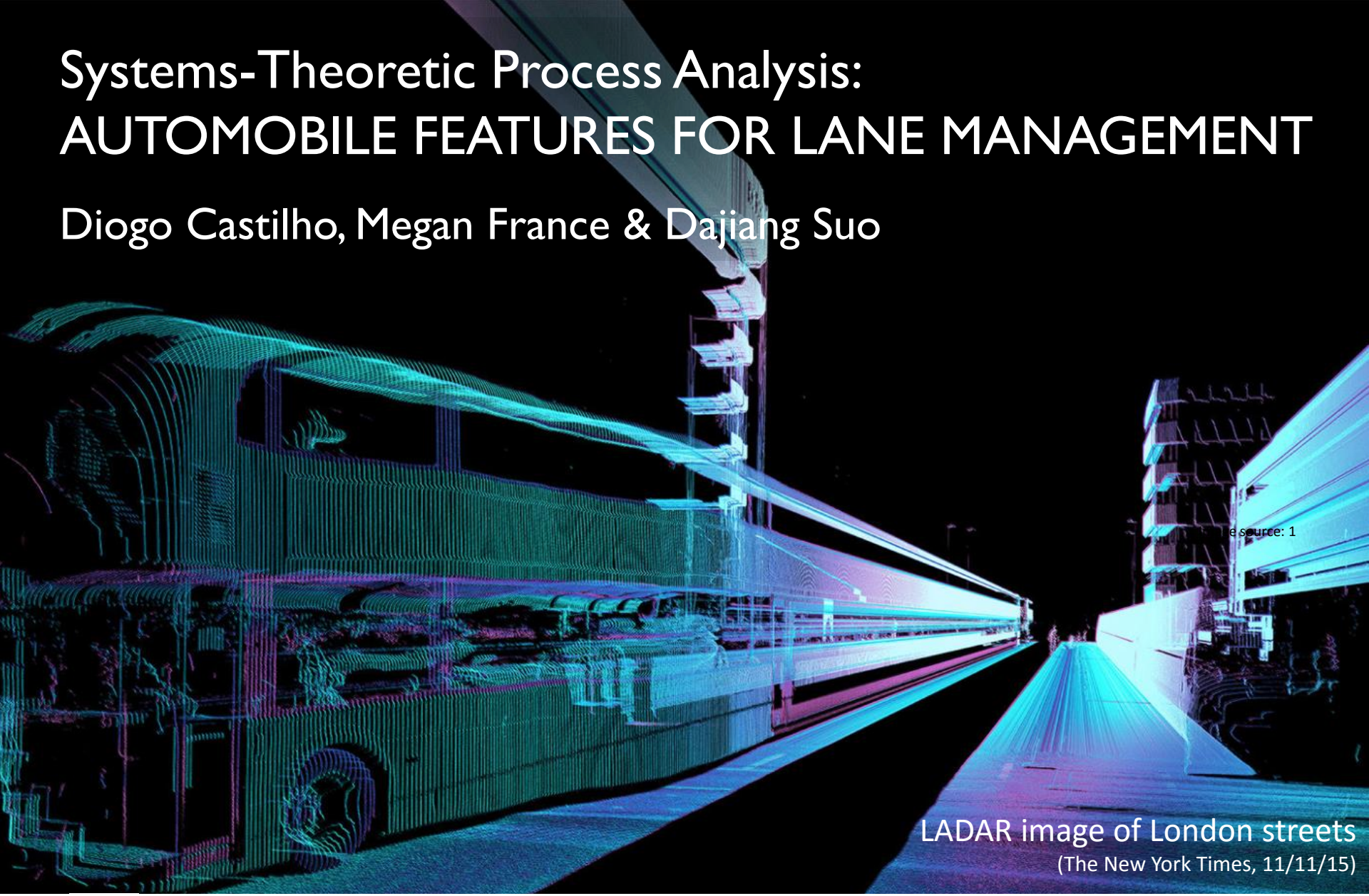
Systems-Theoretic Process Analysis: AUTOMOBILE FEATURES FOR LANE MANAGEMENT

Diogo Castilho, Megan France & Dajiang Suo



LADAR image of London streets
(The New York Times, 11/11/15)

MIT Systems Engineering Research Lab
STAMP Workshop 2016

AEROASTRO

MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

DISCUSSION

CONCLUSIONS

WHY STUDY AUTOMATED DRIVING?

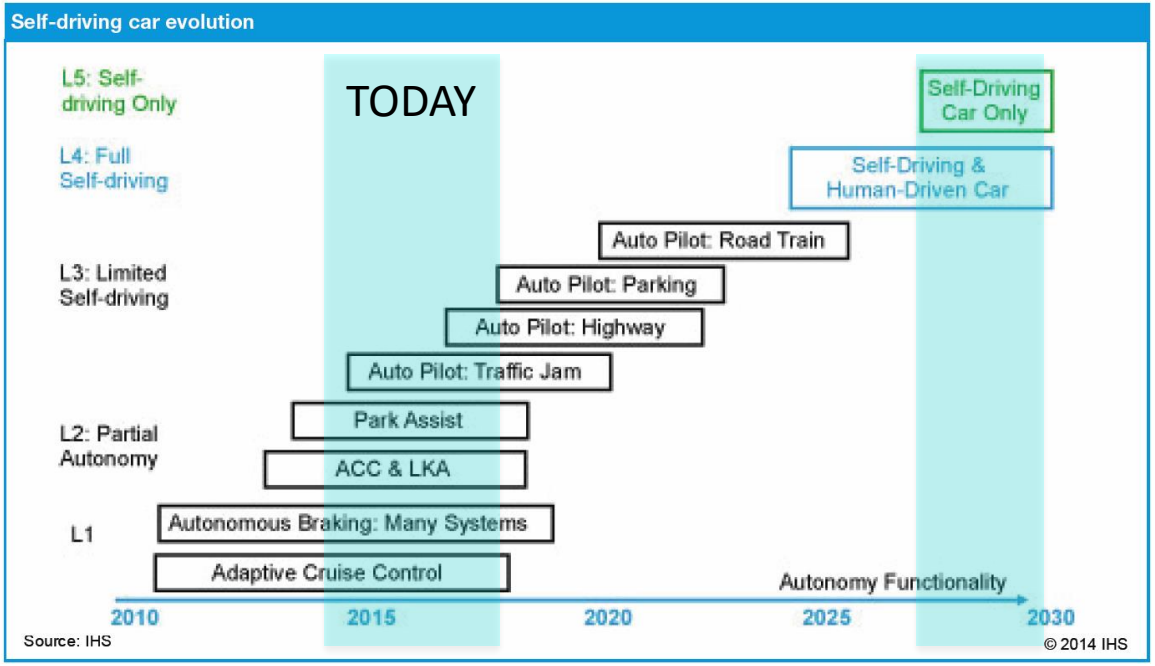


Image source: 2

- More features than ever on the market
- Predicted growth in the near future!

- Safety, efficiency, and opportunity for mobility

AUTOMATION LEVELS

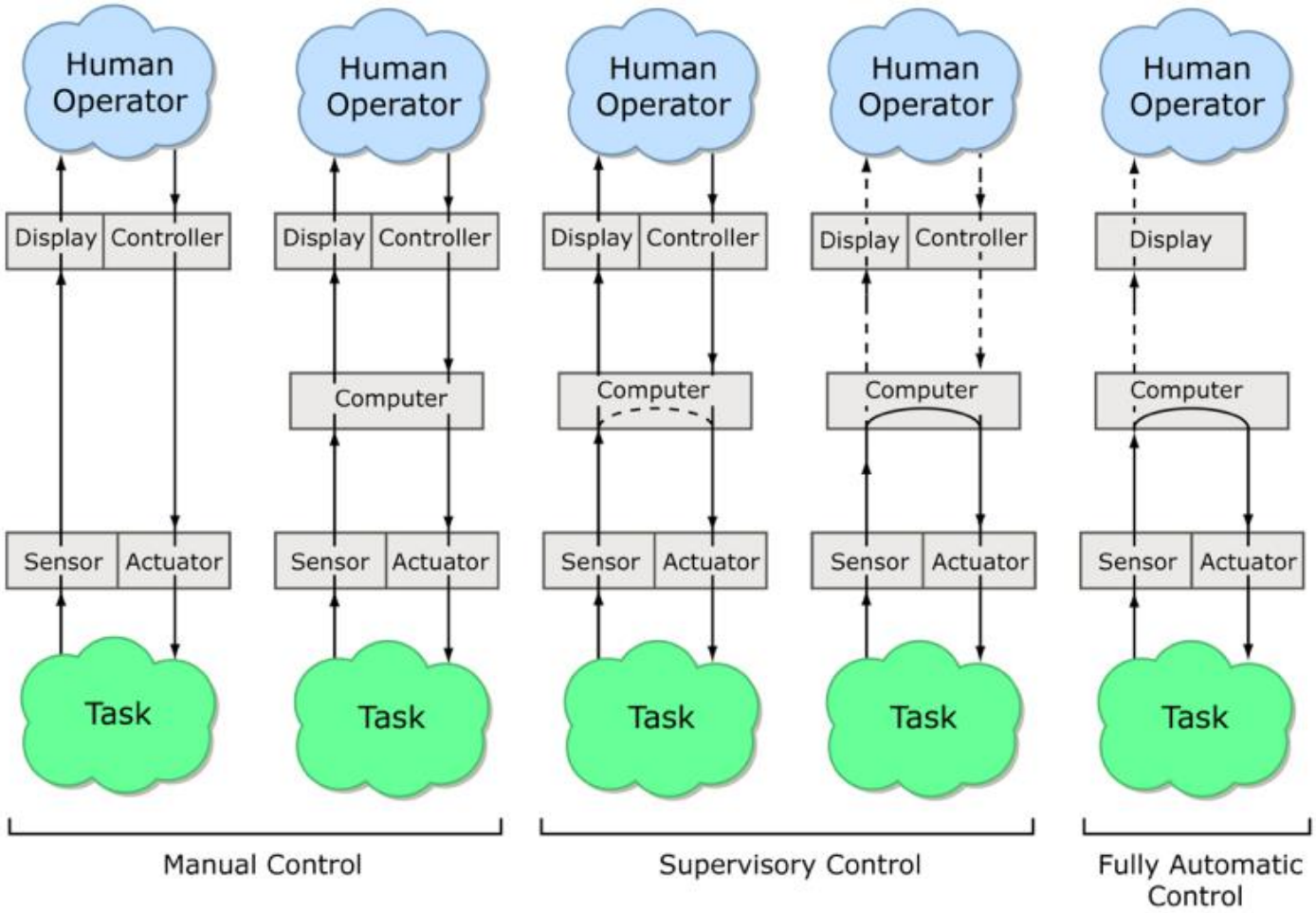


Image sources: 3. 4
AEROASTRO

AUTOMATION LEVELS

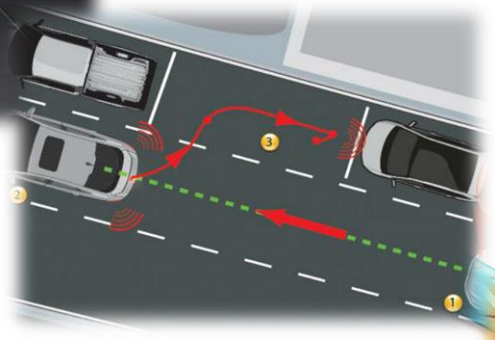
Level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)
Human driver **monitors the driving environment**						
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
Automated driving system **("system") monitors the driving environment**						
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	**High Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

AUTOMATION LEVELS

1. Driver Assistance

2. Partial Automation

3.Conditional Automation



... 5. Full Automation

Image sources: 5-8

MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

DISCUSSION

CONCLUSIONS

OUR PURPOSE

- **MIT 16.453 -** Human Systems Engineering
- Examine the **impact of automated lane management on safety** using STPA and human factors principles
- Use **Tesla Model S Autopilot Version 7.0** as a case study for human factors STPA

TEST CASE SELECTION

- Why use Tesla system for our analysis?
  - Media attention, information availability
  - Automation increase via software update
  - NOT sponsored by Tesla or any other manufacturer
- Generalizable method & results
  - Neither criticism nor advertisement for Tesla
  - ALL automated systems have some of these issues

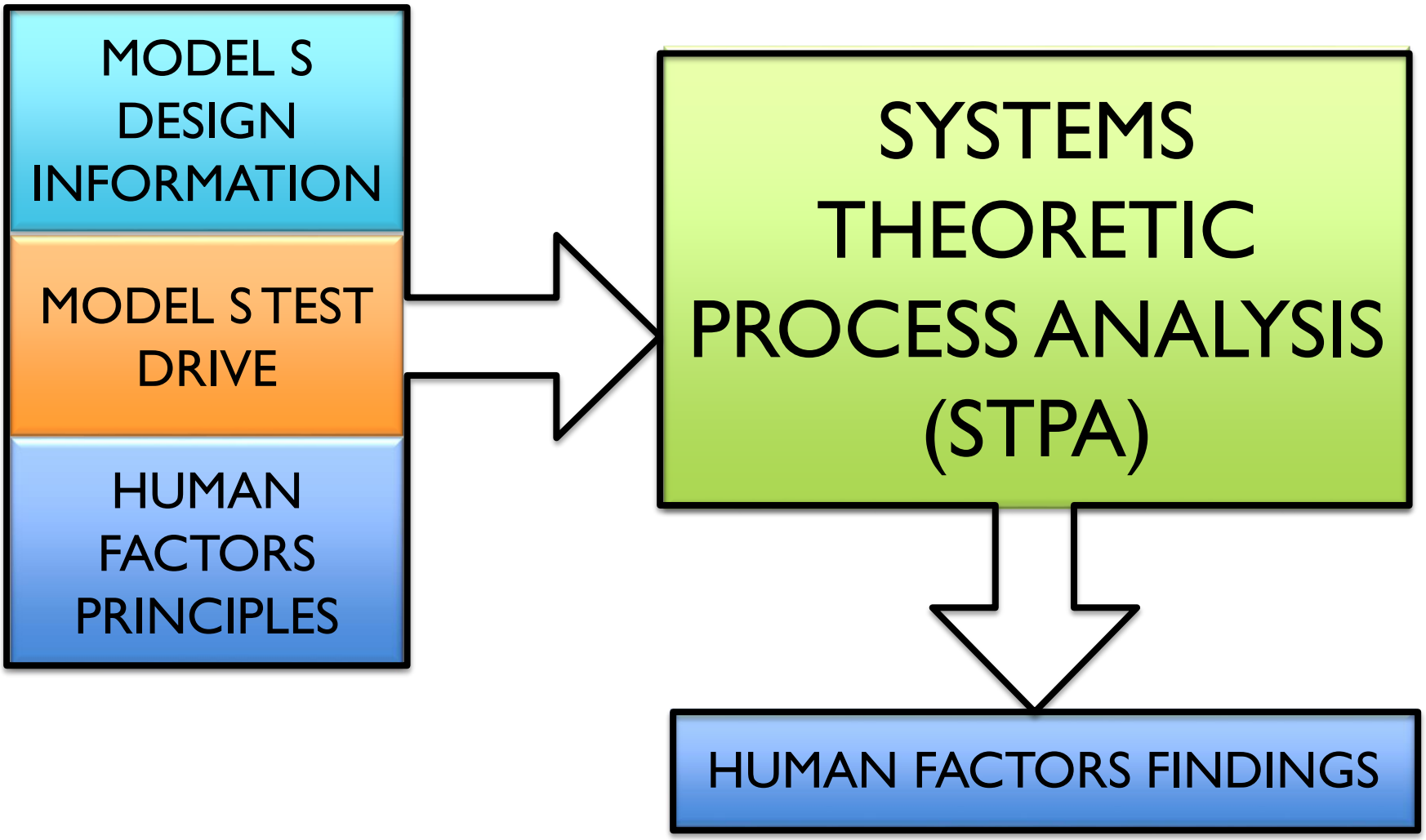
PARTIAL AUTOMATION

"the driving mode-specific **execution by one or more driver assistance systems**

of both **steering and acceleration/deceleration**

… with the **expectation that the human driver perform all remaining aspects** of the dynamic driving task" [4]

PROJECT STRUCTURE



MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

DISCUSSION

CONCLUSIONS

TESLA AUTOPILOT VERSION 7.0

Partial Automation Based on Driver Assistance Systems[9,10]

- Lane Assist
- Collision Avoidance
- Speed Assist
- Traffic-Aware Cruise Control
- Autosteer
- Auto Lane Change

} Autopilot Tech Package

BASIC AUTOPILOT FEATURES

- **Lane Departure and Side Collision Warning Systems**
  - Alerts even when autopilot features are not active
- **Forward Collision Warning**
  - Alerts the driver about vehicles close ahead
  - Engage the Automatic Emergency Braking system to reduce the severity of an impact (Mental Model)
- **Speed Assist**
  - Compares road signs and GPS data - speed limit

LANE MANAGEMENT FEATURES

- **Auto Lane Change**
  - Relies on Traffic-Aware Cruise Control and Autosteer
  - Driver uses the turn signal
  - Vehicle checks for other vehicles in adjacent lane

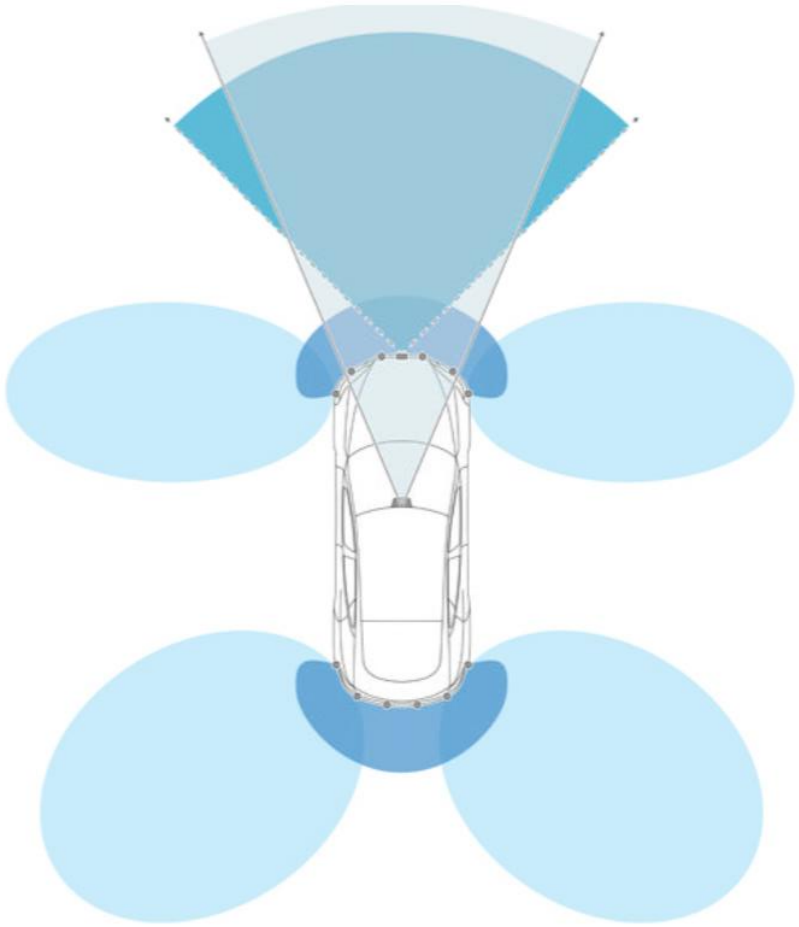
- **Overtake Acceleration:**
  - Activates when the driver triggers auto lane change
  - Without driver pressing accelerator, the vehicle accelerates to match the speed of traffic

LANE MANAGEMENT FEATURES

- **Traffic-Aware Cruise Control**
  - Selected time to impact
  - Selected speed if no car ahead

- **Autosteer**
  - Middle of the lane
  - Follows the car ahead if lane markings are not detected

AUTOPILOT SENSOR LIMITATIONS



Limitations

Many factors can impact the performance of Driver Assistance components, causing them to be unable to function as intended. These include (but are not limited to):

- Poor visibility (due to heavy rain, snow, fog, etc.).
- Bright light (oncoming headlights or direct sunlight).
- Damage or obstructions caused by mud, ice, snow, etc.
- Interference or obstruction by object(s) mounted onto Model S (such as a bike rack or a sticker).
- Narrow or winding roads.
- A damaged or misaligned bumper.
- Interference from other equipment that generates ultrasonic waves.
- Extremely hot or cold temperatures.

⚠ Warning: The list above does not represent an exhaustive list of situations

MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

DISCUSSION

CONCLUSIONS

TEST DRIVE WITH TESLA MODEL S

Video source: Diogo Castilho

TEST DRIVE WITH TESLA MODEL S

- Interface evaluation
- Sources of Mode Confusion
- Handling qualities

  (Gain and Time Delay)

Image source: Diogo Castilho

Feature	Test Drive Task
Speed Assist	Maintain selected speed
Traffic-Aware Cruise Control	Maintain distance to a car ahead
Autosteer	Lane Keeping
Auto Lane Change	Lane Changing

MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

DISCUSSION

CONCLUSIONS

SYSTEM ACCIDENTS AND HAZARDS

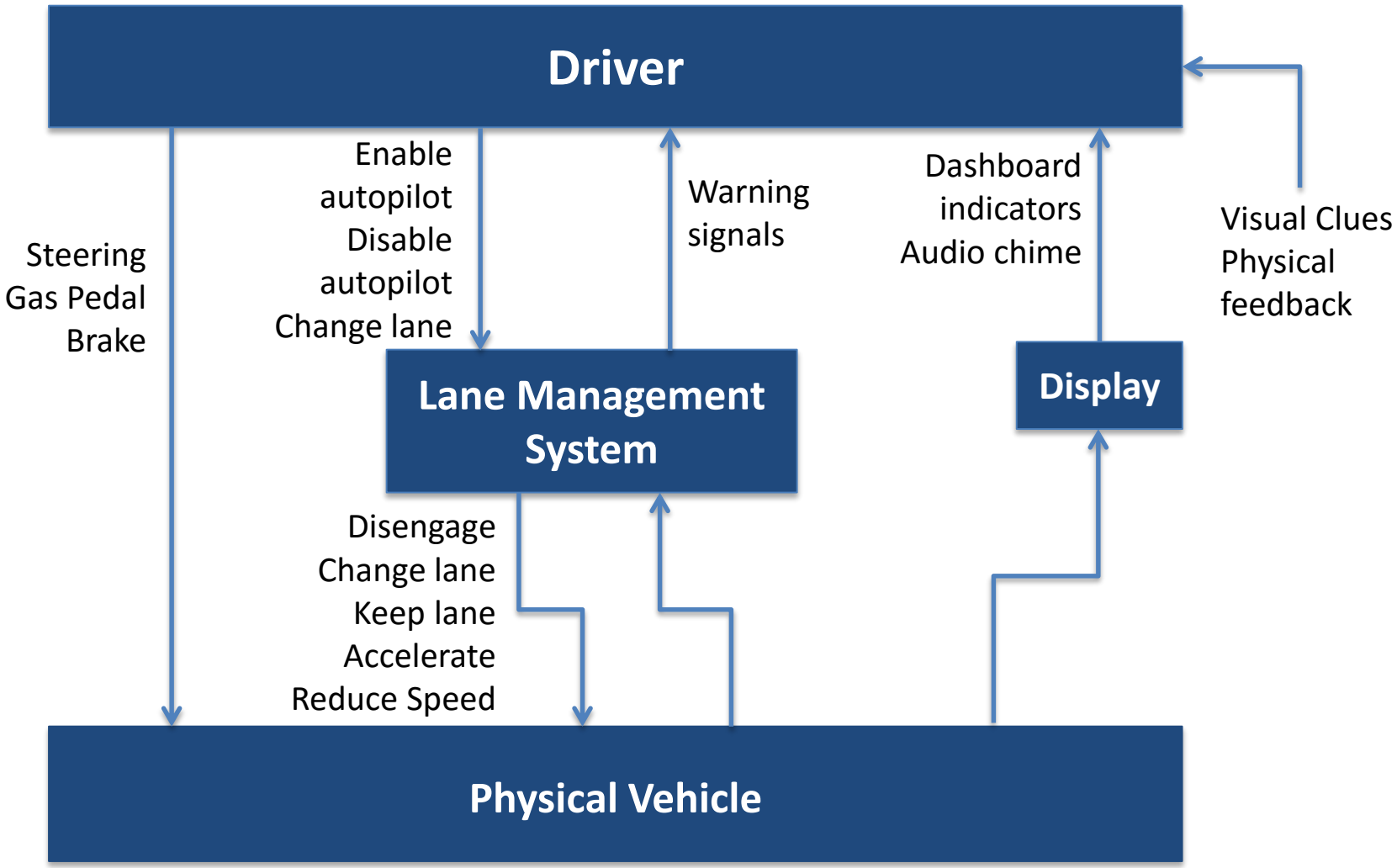
System Level Accidents

A-1	Loss of life and injury
A-2	Economic loss

System Level Hazards

H-1	Vehicle does not maintain safe distance from nearby vehicles
H-2	Vehicle does not maintain safe distance from terrain and other obstacles
H-3	Vehicle occupants exposed to harmful effects and/or health hazards

SAFETY CONTROL STRUCTURE



UNSAFE CONTROL ACTIONS

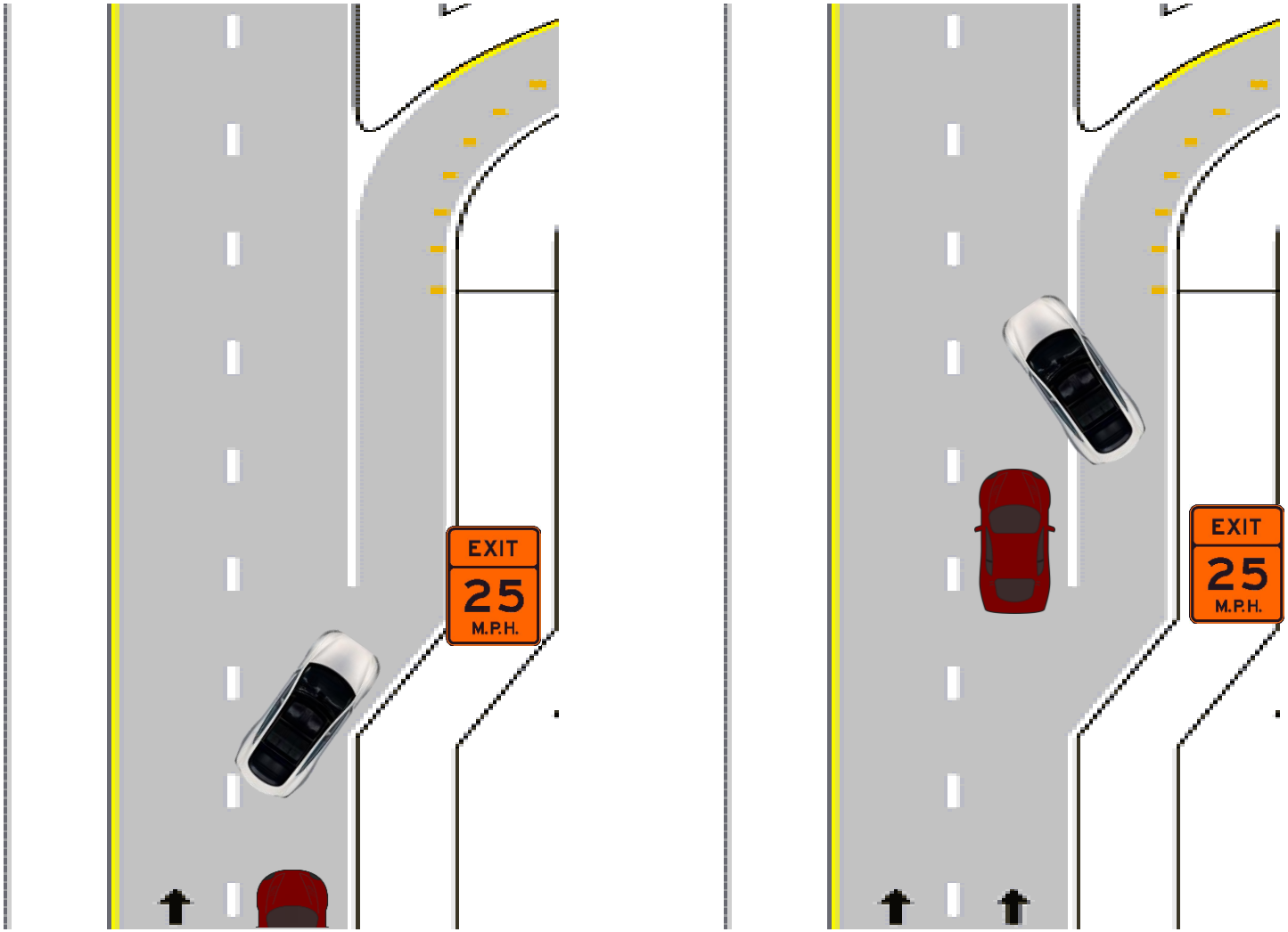
Controller	Control Action	Not providing causes hazards	Providing causes hazards	Incorrect Timing / Order	Stopped too soon / Applied too long
Driver	**Steering**	-	UCA-7: Driver provides steering can cause hazards if autopilot is changing the lane to the opposite direction	-	-
Driver	**Steering**	UCA-8: Driver does not provide steering to avoid obstacles when autopilot does not react	-	-	-
Auto-Pilot	**Lane changing**	UCA-13: Auto-pilot Not providing lane changing automatically causes hazards	-	-	-
Auto-Pilot	**Reduce Speed**	UCA-17: Auto-pilot does not provide reducing speed can cause hazards if range and range rate of current vehicle is above the limit	-	-	-

SCENARIO A

- **UCA: Driver provides steering commands when autopilot is keeping the lane.**

- **Scenario:** Driver provides steering commands when autopilot is keeping the lane because the driver realizes that the autopilot has followed the right lane marking onto an exit ramp. This causes a hazard because autopilot speed assist has reduced the speed to match exit ramp speed limit, and is now travelling too slowly for highway travel, and a vehicle is approaching from the rear.

SCENARIO A

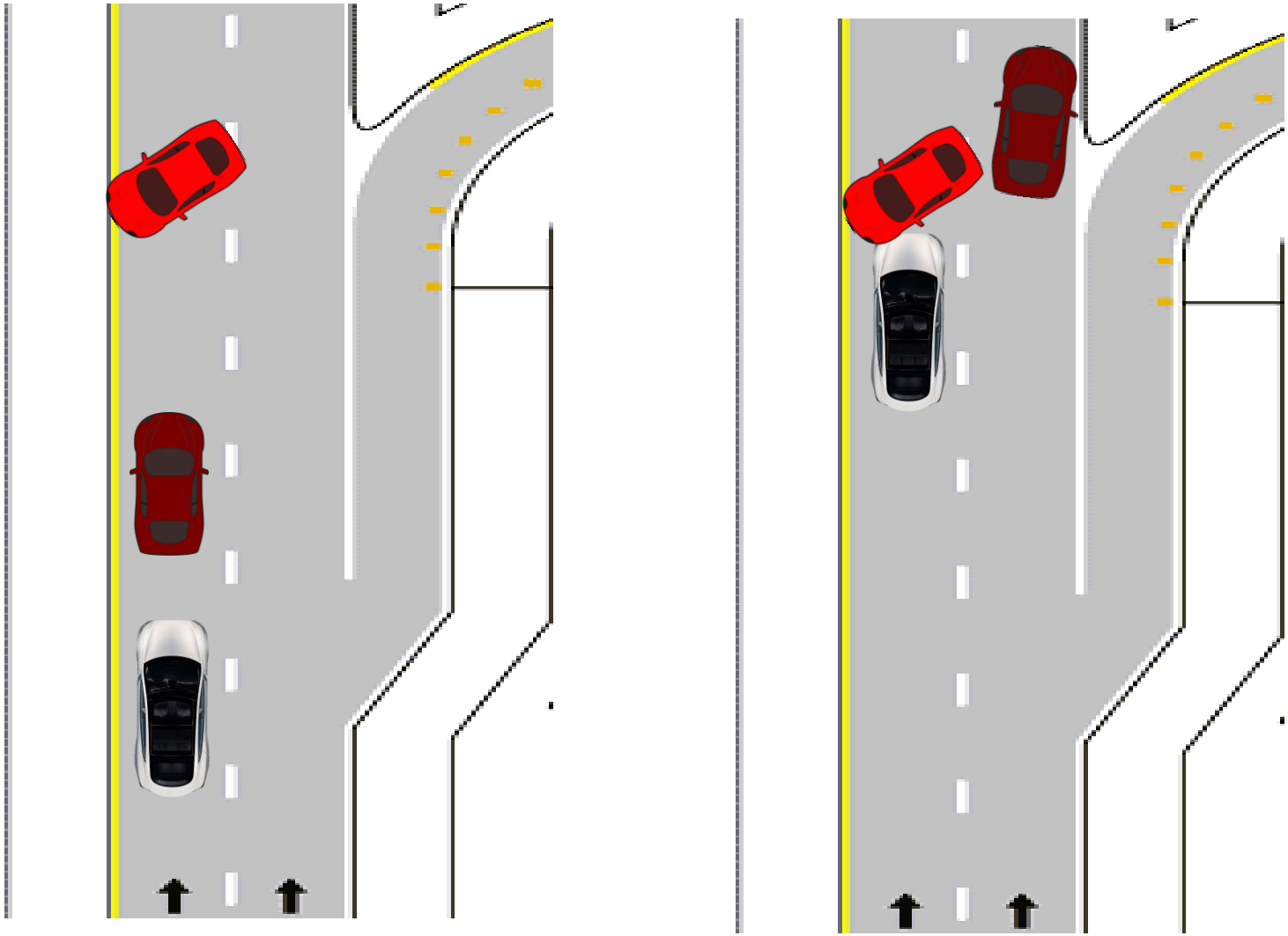


SCENARIO B

- **UCA: Driver does not steer around debris when autopilot is not programmed to handle such situations.**

- **Scenario:** Driver does not brake when the autopilot doesn't react to a collision risk ahead. The driver incorrectly believed that autopilot would break or swerve around the debris. Autosteer had been keeping the lane when the car in front swerved, leaving inadequate time for collision avoidance to take effect.

SCENARIO B



MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

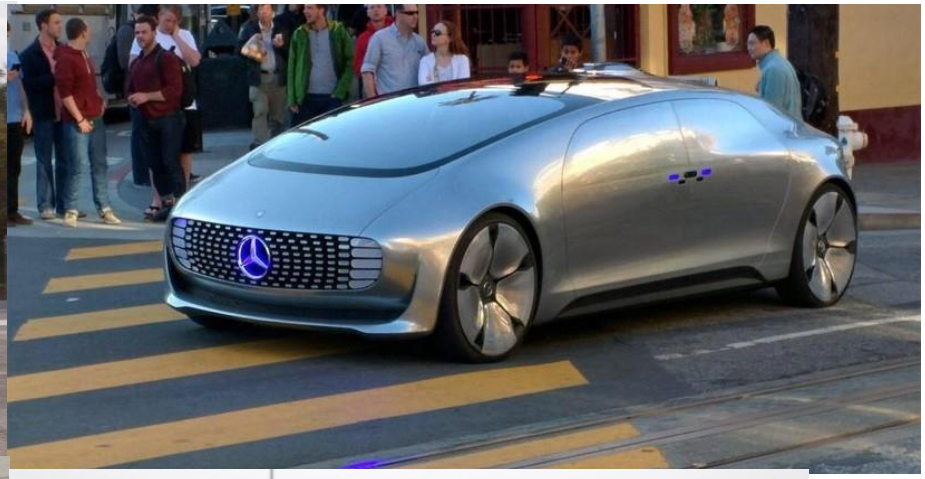
DISCUSSION

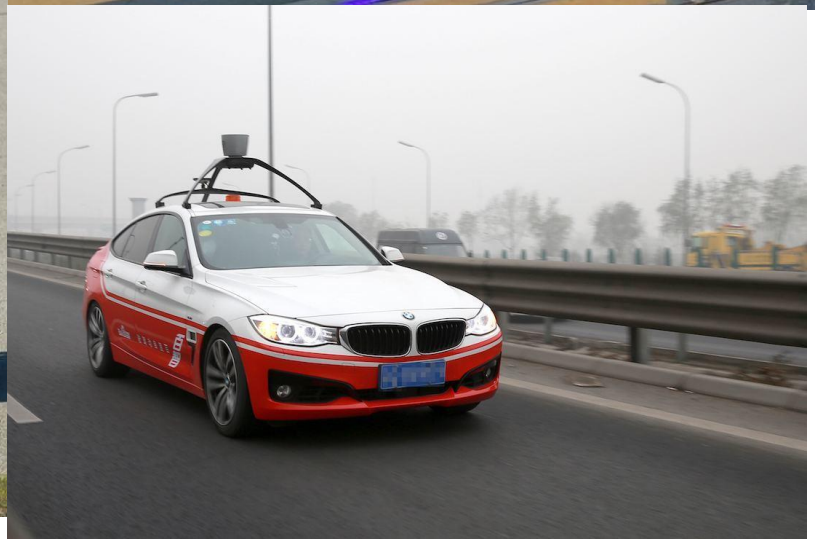
CONCLUSIONS

CHANGES IN AUTOPILOT 7.1

- Reality
  - House connection
  - Summon
  - Private Uber
  - Restriction in residential roads
- Why stepping back?
- Are we afraid?

They are coming!





WHEN DO WE HAVE ENOUGH SCENARIOS?

DISCUSSION: HUMAN FACTORS

Physical Interface Level

- **Multi-function lever → ambiguity[10]**
  - Can enable autosteer with double pull on lever
  - Single pull on lever engages speed assist
  - Push lever to pause and resume speed assist, keeping target speed

- **Difficult to differentiate levers**
  - Autopilot, Turn signal, and wheel position are all controlled by adjacent levers[10]
  - Need to color, shape, size, or location code

DISCUSSION: HUMAN FACTORS

System design / architecture level

- **Partial automation limitations** [12, 13]
  - Inability to steer around obstacles and navigate
  - Conditional limitations
- **Overtrust issues**
  - Driver may misunderstand the automation purpose or process

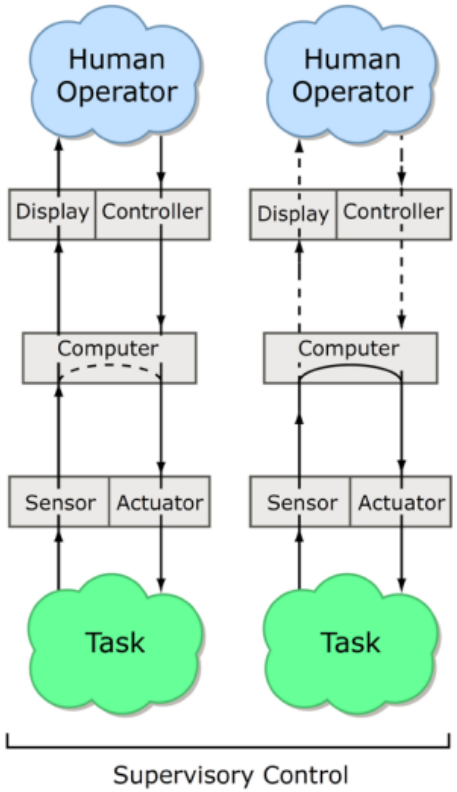
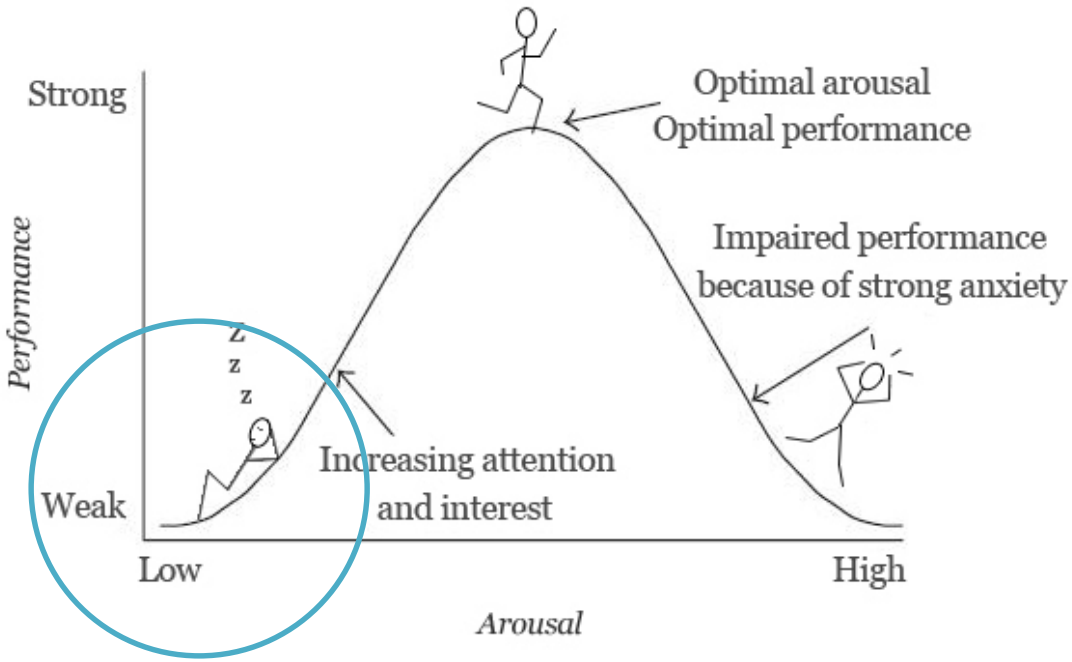


Image source: 3

DISCUSSION: HUMAN FACTORS

- **Workload, Yerkes-Dodson Law**[12,16]
  - Poor performance in low workload conditions
  - Partial automation still requires driver action

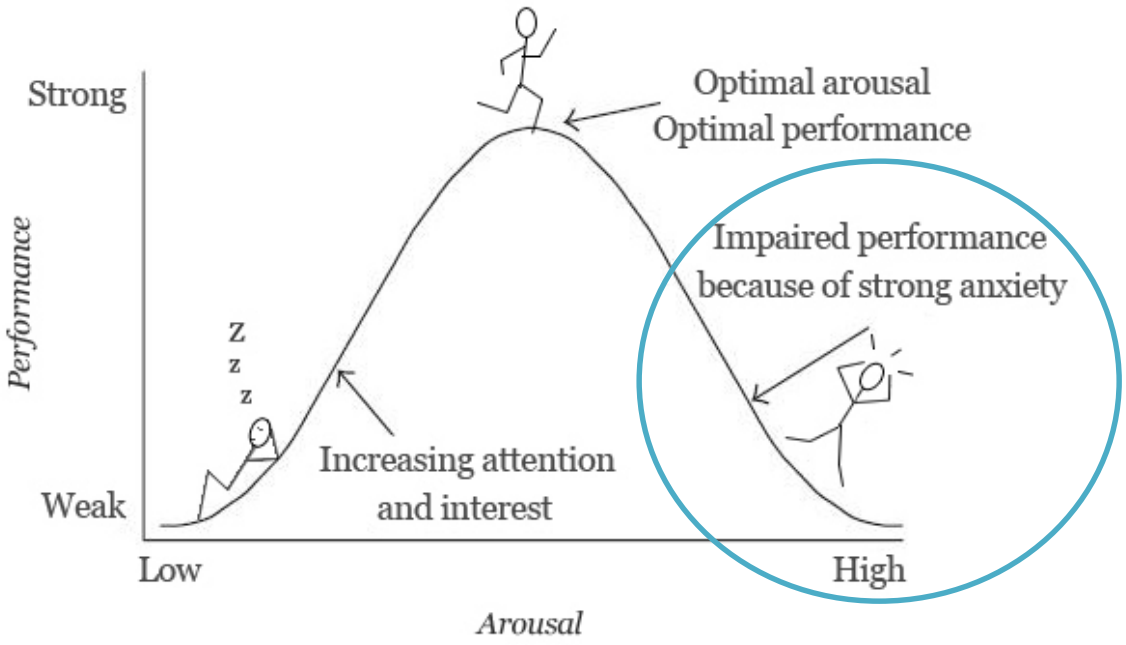
- **Changing Level of Automation**
  - Triggered by event/ task complexity



DISCUSSION: HUMAN FACTORS

- **Workload, Yerkes-Dodson Law**[12,16]
  - Poor performance in low workload conditions
  - Partial automation still requires driver action

- **Changing Level of Automation**
  - Triggered by event/ task complexity



DISCUSSION: HUMAN FACTORS

What do we do? Some considerations…

- **Examine appropriateness of the design**
  - Consider reducing the need for human response, OR
  - Consider increasing human responsibility to maintain awareness

- **Improve driver mental models**
  - How is the feature marketed?
  - Is there brief, clear documentation available?
  - Or is the design intuitive in the first place?

Image source: 14

MOTIVATION AND BACKGROUND

PURPOSE AND PROJECT STRUCTURE

SYSTEM OVERVIEW

TEST DRIVE

STPA RESULTS

DISCUSSION

CONCLUSIONS

CONCLUSIONS

- Using STPA helped us identify hazards, unsafe actions, and possible causal scenarios
- STPA scenarios clearly reveal human factors issues with automated lane management features – with broad applicability
- We recommend using STPA with a focus on human factors for similar systems

ACKNOWLEDGEMENTS

- Dr. Nancy Leveson & Dr. John Thomas
- Dr. Leia Stirling
- Scholarship from CNPQ
- And Dajiang Suo!

REFERENCES

1. Manaugh, G. (2015, November 11). The Dream Life of Driverless Cars. Retrieved December 7, 2015.
2. Fully self-driving cars expected by 2030, says forecast - UPDATE. (2014, January 3). Retrieved December 7, 2015.
3. Stirling, L. (2015, November 3). *Automation* [PowerPoint slides]. Retrieved from https://learning-modules.mit.edu
4. SAE J 3016: Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. (2014). SAE International.
5. Audi adaptive cruise control. (2015). Retrieved December 8, 2015, from http://www.audi.com.pk/sea/brand/pk/models/a6/a6_saloon/Equipment/safety/audi_adaptive_cruise.html
6. De Looper, C. (2015, October 15). Tesla Pushes 'Autopilot' Update: Model S Can Now Drive Itself. Retrieved December 7, 2015, from http://www.techtimes.com/articles/95502/20151015/tesla-pushes-autopilot-update-model-s-now-drive-itself.htm
7. Enhanced Active Park Assist. (2014, August 26). Retrieved December 7, 2015, from http://www.grandledgeford.com/blog/enhanced-active-park-assist/
8. Kelly, S. (2014, May 28). 8 Big Questions About Google's Self-Driving Car. Retrieved December 7, 2015, from http://mashable.com/2014/05/28/google-self-driving-car-prototype/#N08BVn2h75qB
9. Model S. (n.d.). Retrieved December 7, 2015, from https://www.teslamotors.com/models
10. Model S Owner's Manual. (2015). Tesla Motors.
11. Leveson, N. (2012). *Engineering a safer world systems thinking applied to safety*. Cambridge, Mass.: The MIT Press.

REFERENCES

12. Proctor, R., & Van Zandt, T. (2008). *Human factors in simple and complex systems* (Second ed.). Boca Raton, Florida: CRC Press, Taylor & Francis Group.
13. Sheridan, T. (2012). Chapter 38: Supervisory Control. In G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (4th ed.). Hoboken: John Wiley & Sons.
14. PLC Automation. (n.d.). Retrieved December 7, 2015, from http://www.plcedge.com/plc-automation.html
15. Yerkes Dodson Law. (n.d.). Retrieved December 7, 2015, from https://www.adelaide.edu.au/uni-thrive/revive/stress/
16. Yerkes, R. M. & Dodson, J. D. (1908). "The relation of strength of stimulus to rapidity of habit formation" *Journal of Comparative Neurology and Psychology, 18,* 459-482.
17. Endsley, M. R. (1995). "Toward a theory of situation awareness in dynamic systems." *Human Factors 37*(1), 32-64.