Technische Universität Braunschweig
Institut für Regelungstechnik
Institut für Verkehrssicherheit und Automatisierungstechnik

Evolution Issues of Automated Driving Functions by Application of Systemic Accident Analysis

On the Example of the Tesla Model S Fatality

René S. Hosse; **Gerrit Bagschik**; Markus Maurer; Klaus Bengler; Uwe Becker

April 23, 2017

Disclaimer

This contribution refers to public available information about accident #HWY16FH018 involving a Tesla Model S.

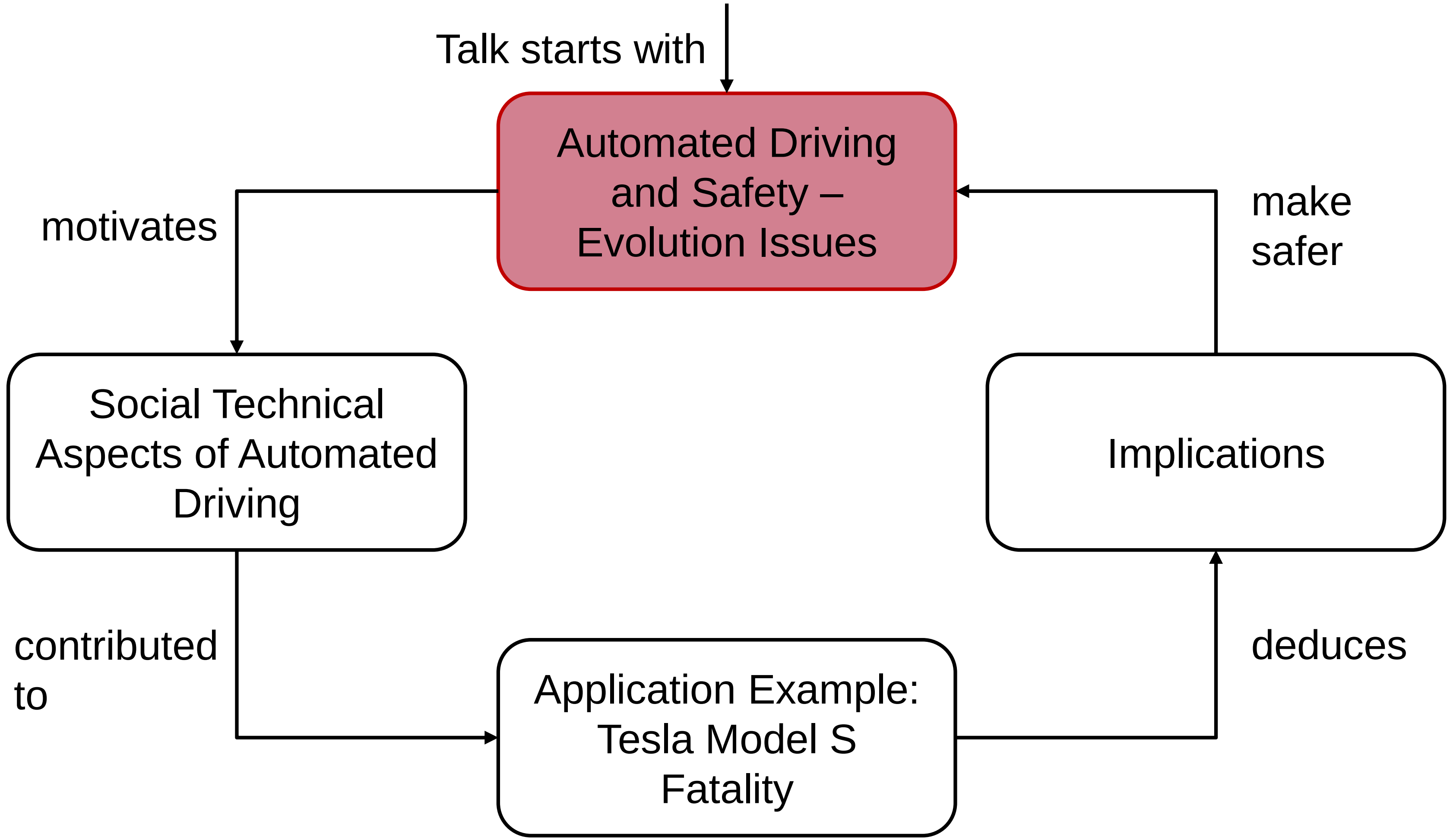
The investigation and models are developed according to Autopilot Version 7.X.

The final report of the National Transportation Safety Board is not taken into account.

The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect the official policy or position of TU Braunschweig or TU Munich.

Examples of analysis performed within this presentation are only examples. They should not be utilized in real-world analytic products as they are based only on very limited and dated public source information. Assumptions made within the analysis are not reflective of the position of TU Braunschweig or TU Munich.

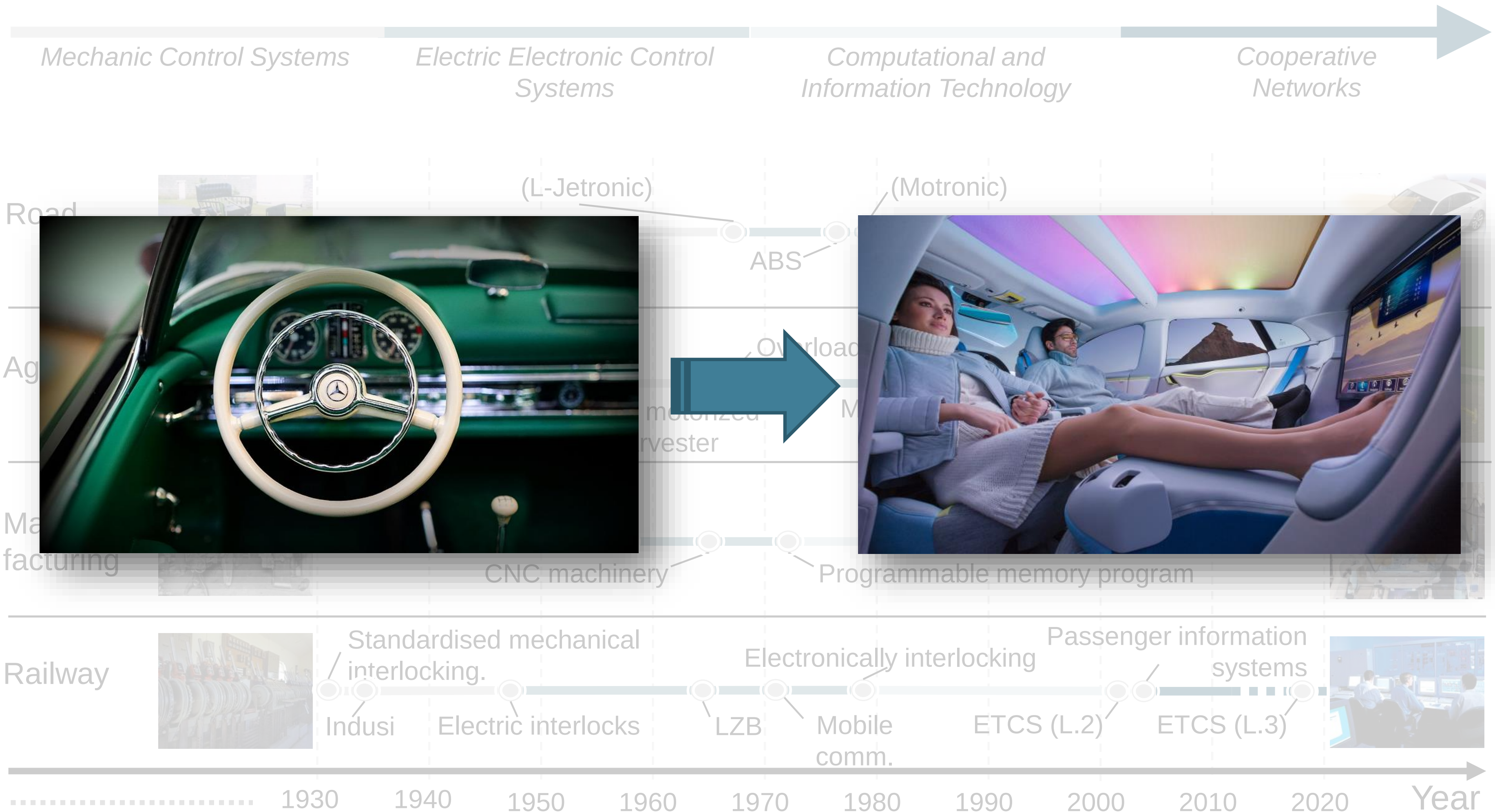
Agenda



Talk starts with
Automated Driving and Safety – Evolution Issues
motivates
Social Technical Aspects of Automated Driving
contributed to
Application Example: Tesla Model S Fatality
deduces
Implications
make safer

Automated Driving and Safety – Evolution Issues

Increasing Automation throughout Domains



Automated Driving and Safety – Evolution Issues

„Operators act always as prescribed“

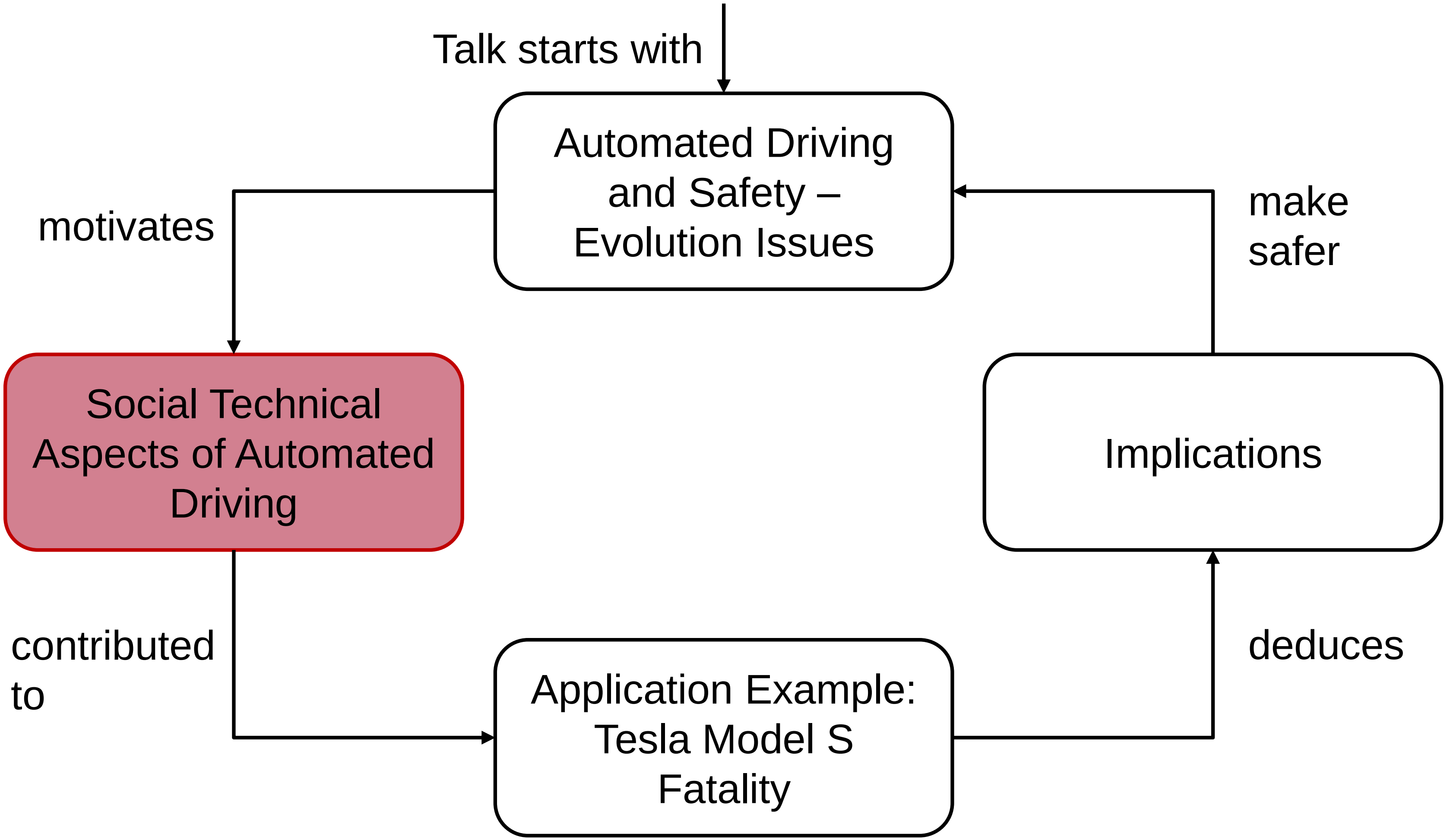
Common advices by automotive user guides:

„Drivers are required to remain engaged and aware when piloting functions are engaged“

„Drivers must keep their hands on the wheel“

Source: youtube

Agenda


Talk starts with
Automated Driving and Safety – Evolution Issues
motivates
Social Technical Aspects of Automated Driving
contributed to
Application Example: Tesla Model S Fatality
deduces
Implications
make safer

Socio-technical Aspects of Automated Driving
Role of human in automated vehicles

Name	Lateral & long. control	Surveillance of environment	Fallback layer	Domain of operation
Assisted	Driver & System	Driver	Driver	Limited
Partial automation	System	Driver	Driver	Limited
Conditional automation	System	System	Fallback ready user	Limited
High automation	System	System	System	Limited
Full automation	System	System	System	Unlimited

SAE, “J3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles”, 2016

Socio-technical Aspects of Automated Driving
Role of human in automated vehicles

Name	Lateral & long. control	Surveillance of environment	Fallback layer	Domain of operation
Assisted	Driver & System	Driver	Driver	Limited
Partial automation	System	Driver	Driver	Limited
Conditional automation	System	System	Fallback ready user	Limited
High automation	System	System	System	Limited
Full automation	System	System	System	Unlimited

Socio-technical Aspects of Automated Driving
Role of human in the vehicle

Name	Lateral & long. control	Surveillance of environment	Fallback layer	Domain of operation
Partial automation	System	Driver	Driver	Limited

Todays market systems provide level 2 automation

- Humans are designed as a permanent supervisor for the system
- Overruling is necessary

But: Studies from the early 80s show

- “that it is impossible for even a highly motivated human being to maintain effective visual attention towards a source of information on which very little happens, for more than about half an hour.”

L. Bainbridge, “Ironies of automation,” Automatica, vol. 19, no. 6, pp. 775–779, 1983

Socio-technical Aspects of Automated Driving
Role of human in the vehicle

Name	Lateral & long. control	Surveillance of environment	Fallback layer	Domain of operation
Partial automation	System	Driver	Driver	Limited

Warning: Traffic-Aware Cruise Control is designed for your driving comfort and convenience and is not a collision warning or avoidance system.

It is your responsibility to stay alert, drive safely, and be in control of the vehicle at all times.

Never depend on Traffic-Aware Cruise Control to adequately slow down Model S. Always watch the road in front of you and be prepared to take corrective action at all times.

Failure to do so can result in serious injury or death.

Tesla Model S Manual, p.68, 2016

Socio-technical Aspects of Automated Driving
Role of humans in the development process

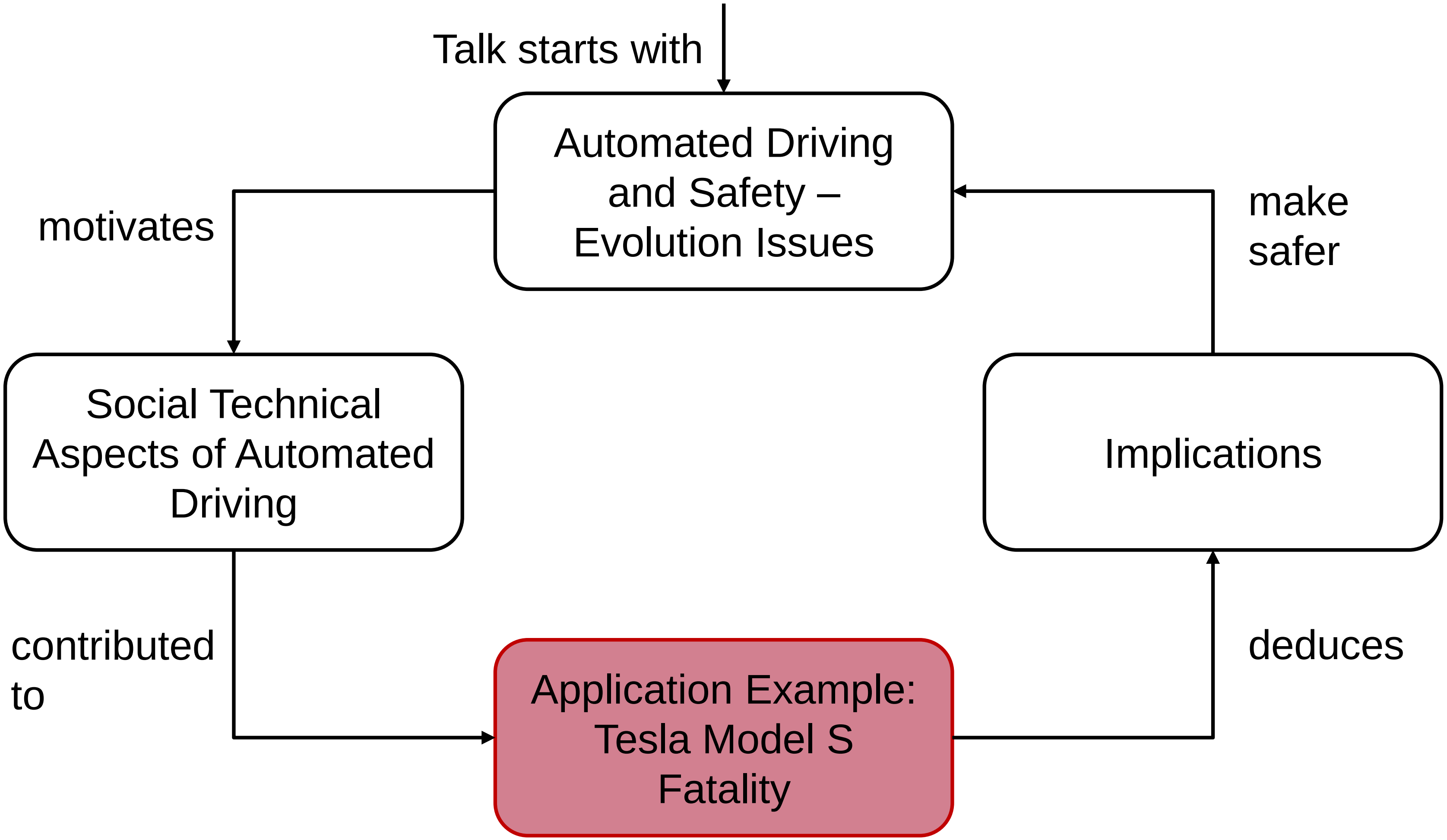
- Automation of driving task is not a completely new topic
- First driver assistance systems came in 1995 (first ACC on Mitsubishi)
- Introduction of new systems must be planned and analyzed

- Project RESPONSE 3 gives a code of practice (2006)
- Guidelines on safe function definitions
  - For example do not use „safe" in the name of an assisting system
  - Functional system boundaries like standing objects in early radar sensors
  - Explicit communication of inadequacies

- Clear definition of responsibilities
- Supervision of responsibilities
- Create correct expectations of system performance

A. Knapp, M. Neumann, M. Brockmann, R. Walz, and T. Winkle, Code of Practice for the Design and Evaluation of ADAS. RESPONE 3

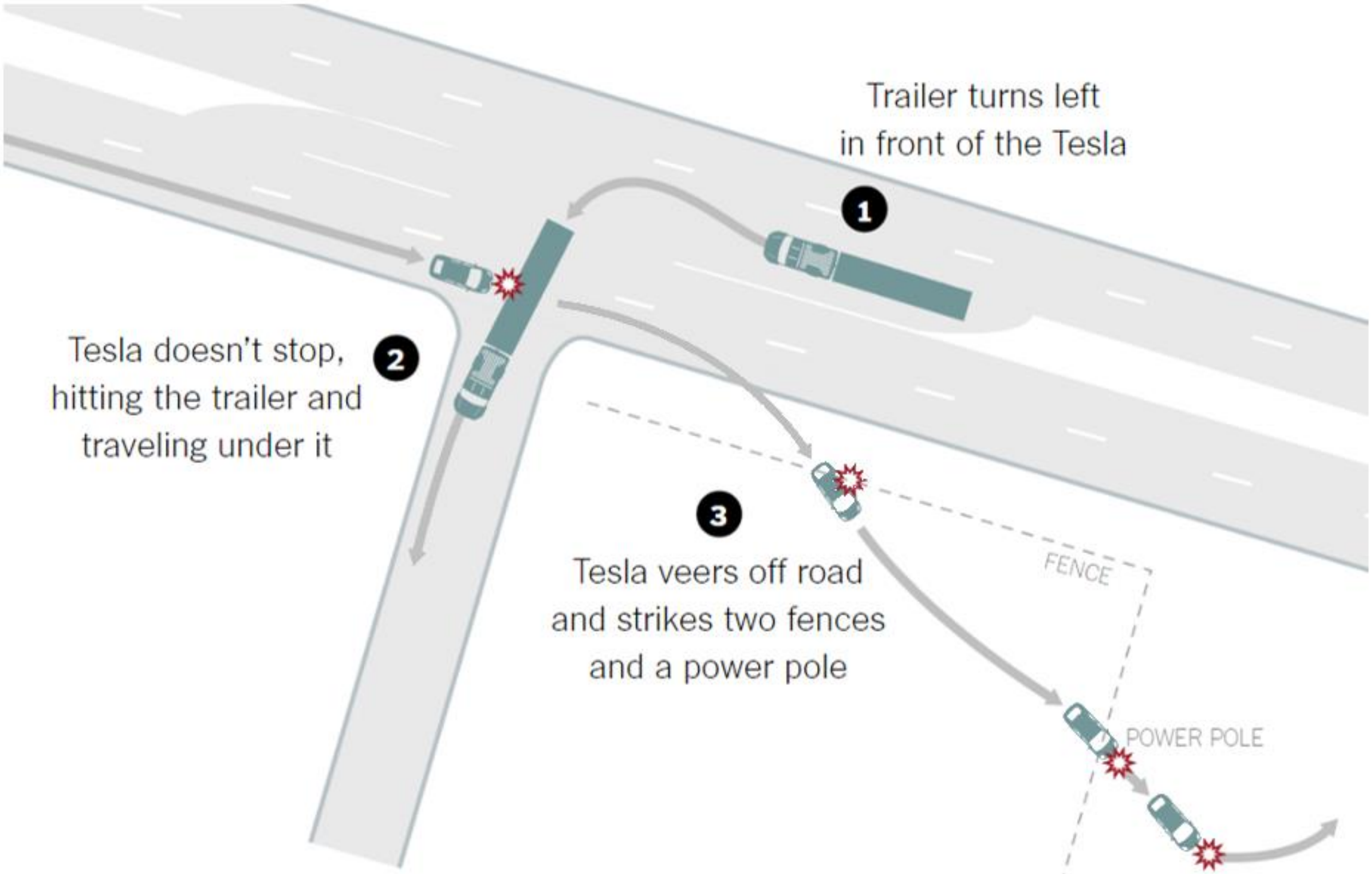
Agenda



Talk starts with
Automated Driving and Safety – Evolution Issues
motivates
Social Technical Aspects of Automated Driving
contributed to
Application Example: Tesla Model S Fatality
deduces
Implications
make safer

Application Example: Tesla Model S Fatality

Accident Introduction



A. Singhvi and K. Russell, "Inside the Self-Driving Tesla Fatal Accident," The New York Times, 01-Jul-2016

Application Example: Tesla Model S Fatality

Step 0: Accidents and Hazards

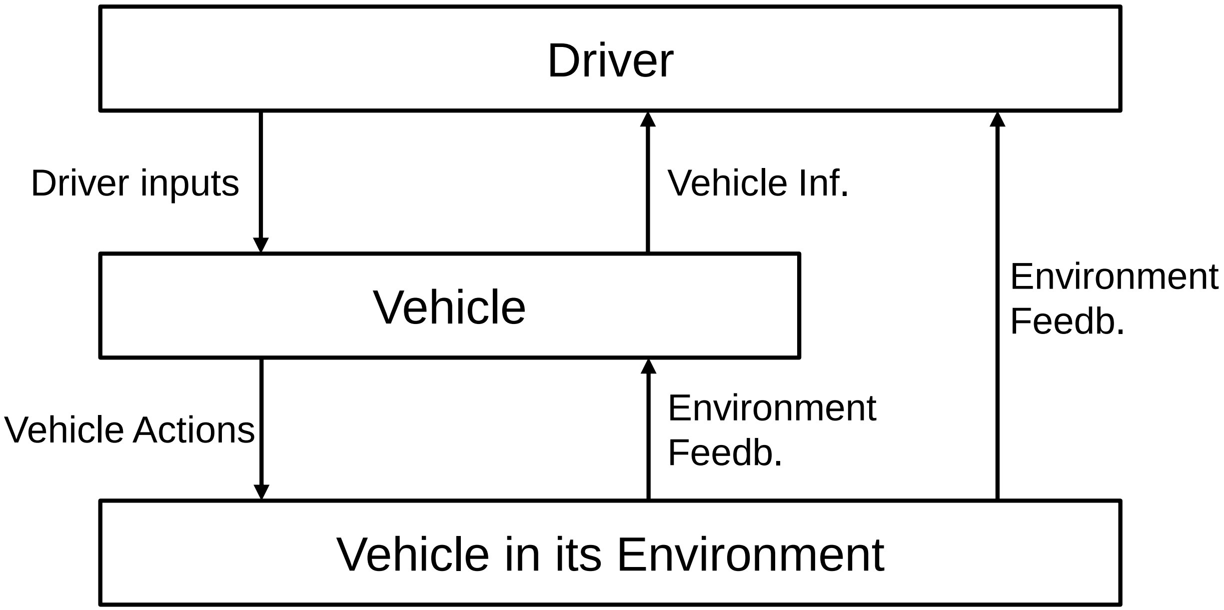
No.	Accident
1	Vehicle crashes when Autopilot is active

No.	Hazards
1	Driver does not provide required attention to driving tasks and environment
2	Autopilot does not react to other road crossing vehicles/obstacles

Application Example: Tesla Model S Fatality

Step 0: Control Structures

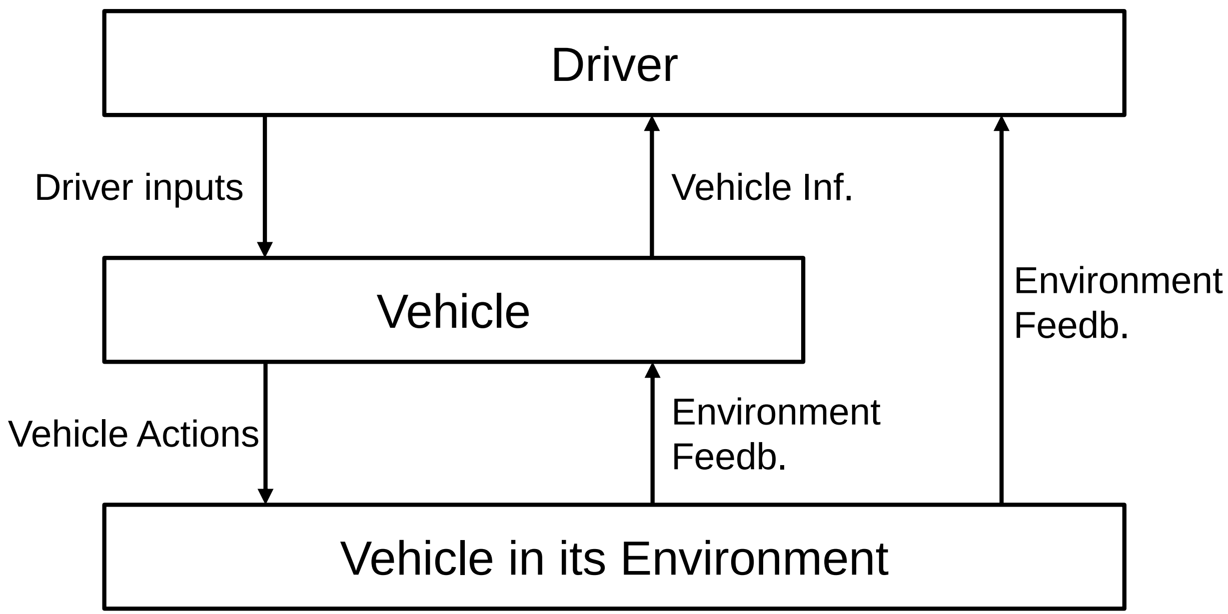
Basic Model Concept:



Application Example: Tesla Model S Fatality

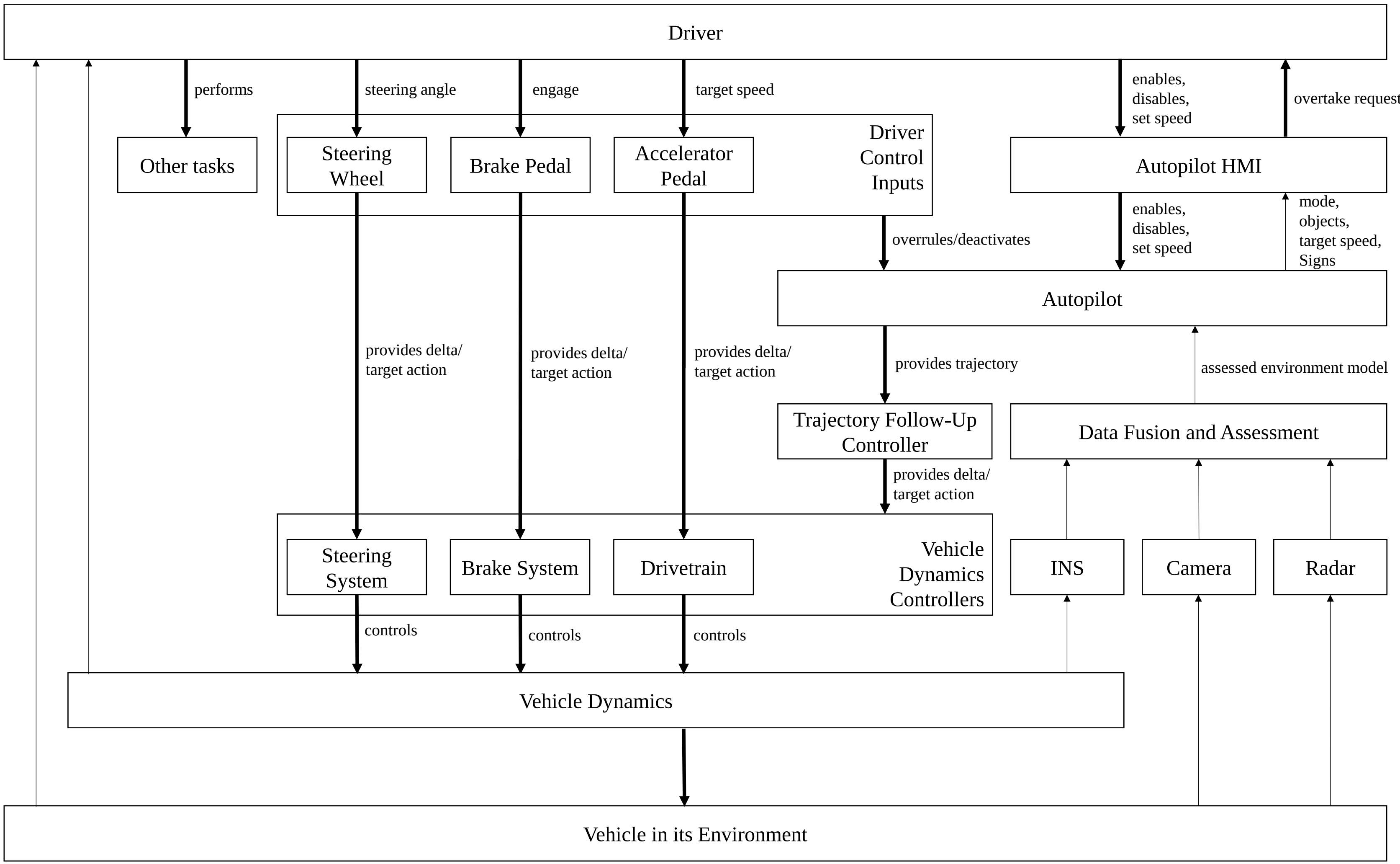
Step 0: Control Structures

Basic Model Concept: Autopilot Control Structure



Application Example: Tesla Model S Fatality

Step 0: Autopilot Control Structure



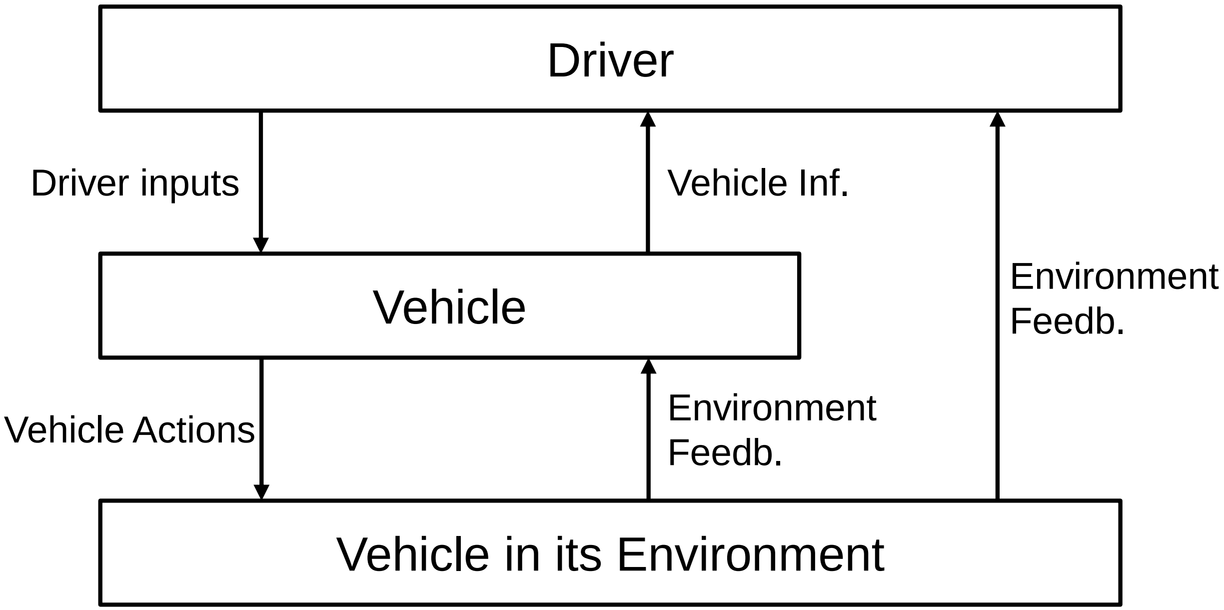
Application Example: Tesla Model S Fatality

Step 1: (Selected) Unsafe Control Actions by Autopilot Controls

Control action	Required but not provided	Unsafe action provided	Incorrect timing	Stopped too soon/applied too long
Overrule/ Deactivate	Driver inputs do not overrule Autopilot		Driver inputs deactivate Autopilot too late	
Enable		Autopilot is enabled unintended		
Send mode status	Autopilot does not send mode status	Autopilot sends mode status when not enabled		
Provide assessed environment model	Environment model not provided (not updated)	Environment model provided when not required	Environment model provided too late	(Same) model provided too long

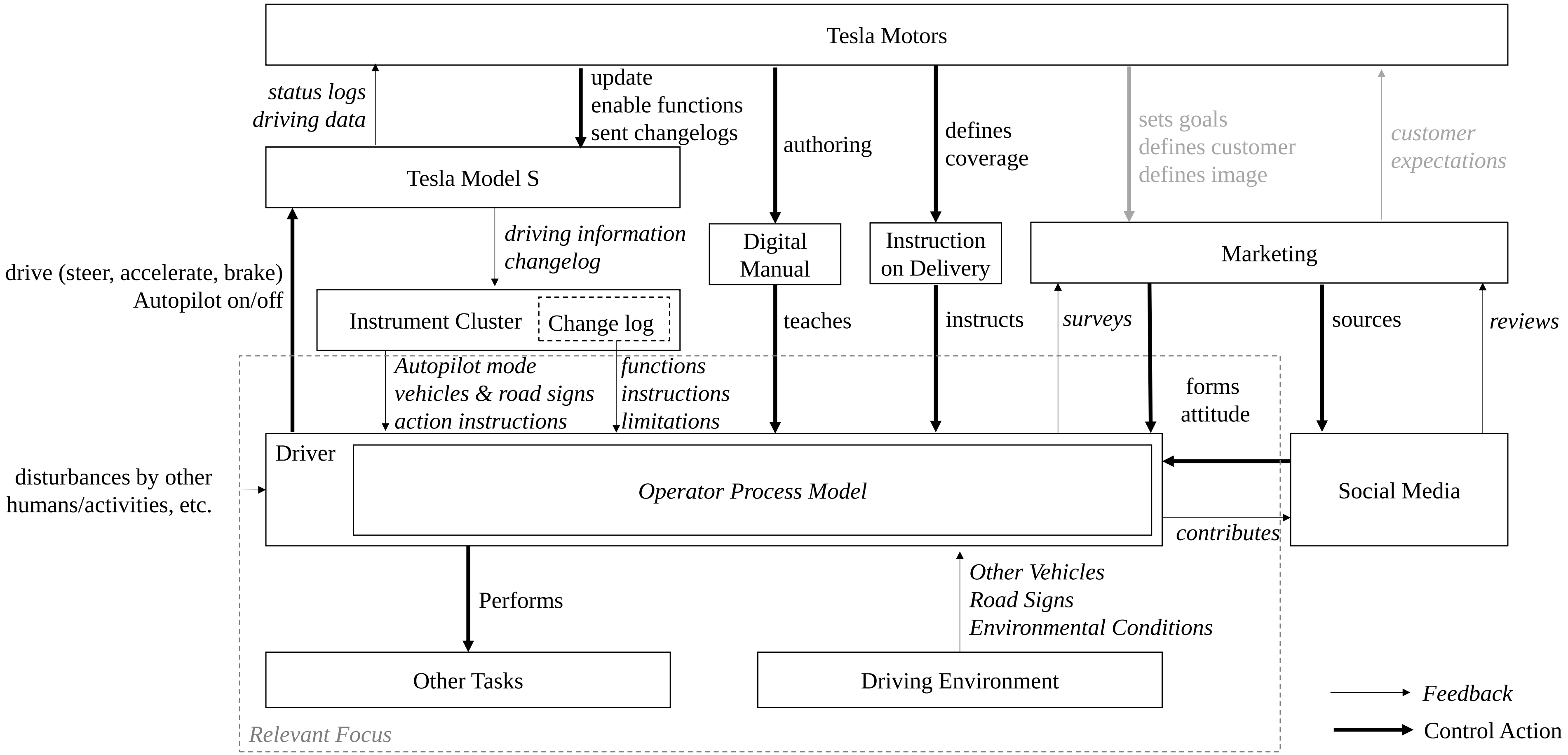
Application Example: Tesla Model S Fatality
Step 0: Control Structures

Basic Model Concept: Driver Control Structure



Application Example: Tesla Model S Fatality

Step 0: Driver Control Structure



Application Example: Tesla Model S Fatality

Step 1: (Selected) Unsafe Control Actions by Driver Controls

Control action	Required but not provided	Unsafe action provided	Incorrect timing	Stopped too soon/applied too long
Steer	Driver does not steer Model S when required		Driver steers Model S too late	
Enable Autopilot		Driver enables Autopilot when not allowed		
Send changelogs	Tesla does not send changelogs when required			
Authoring	Tesla does not author the manual when required			

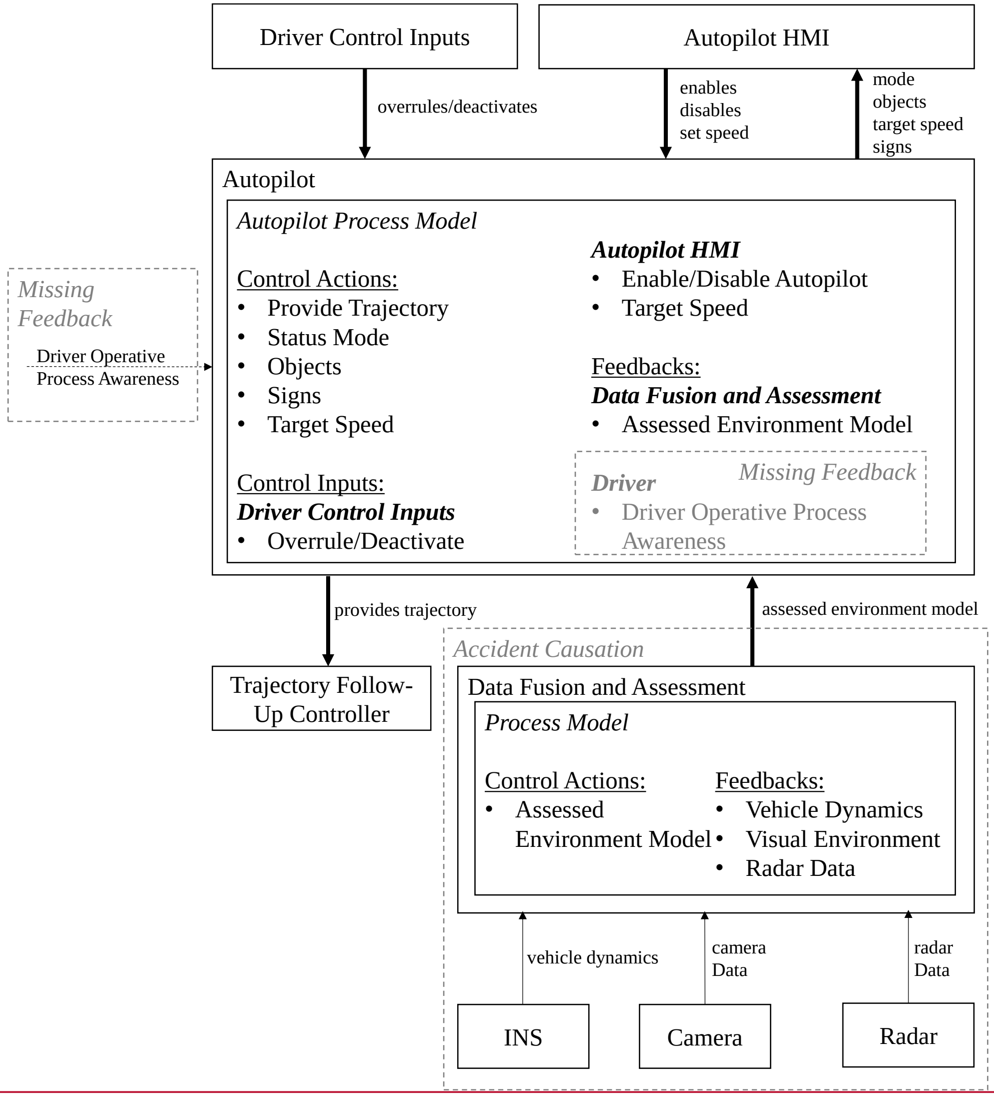
Application Example: Tesla Model S Fatality

Step 1: Violated Safey Constraints

No.	UCA	Safety constraint
UCA 3	Autopilot does not send objects to Autopilot HMI when required	Autopilot must send objects to Autopilot HMI when required
UCA 4	Autopilot does not send road signs to Autopilot HMI when required	Autopilot must send road signs to Autopilot HMI when required
UCA 20	Data Fusion and Assessment does not provide assessed environment model to Autopilot when required	Data Fusion and Assessment must provide assessed environment model to Autopilot when required
UCA 34	Driver does not brake Model S when required	Driver must brake Model S when required
UCA 68	Driver performs other tasks when not allowed	Driver must not perform other tasks when not allowed

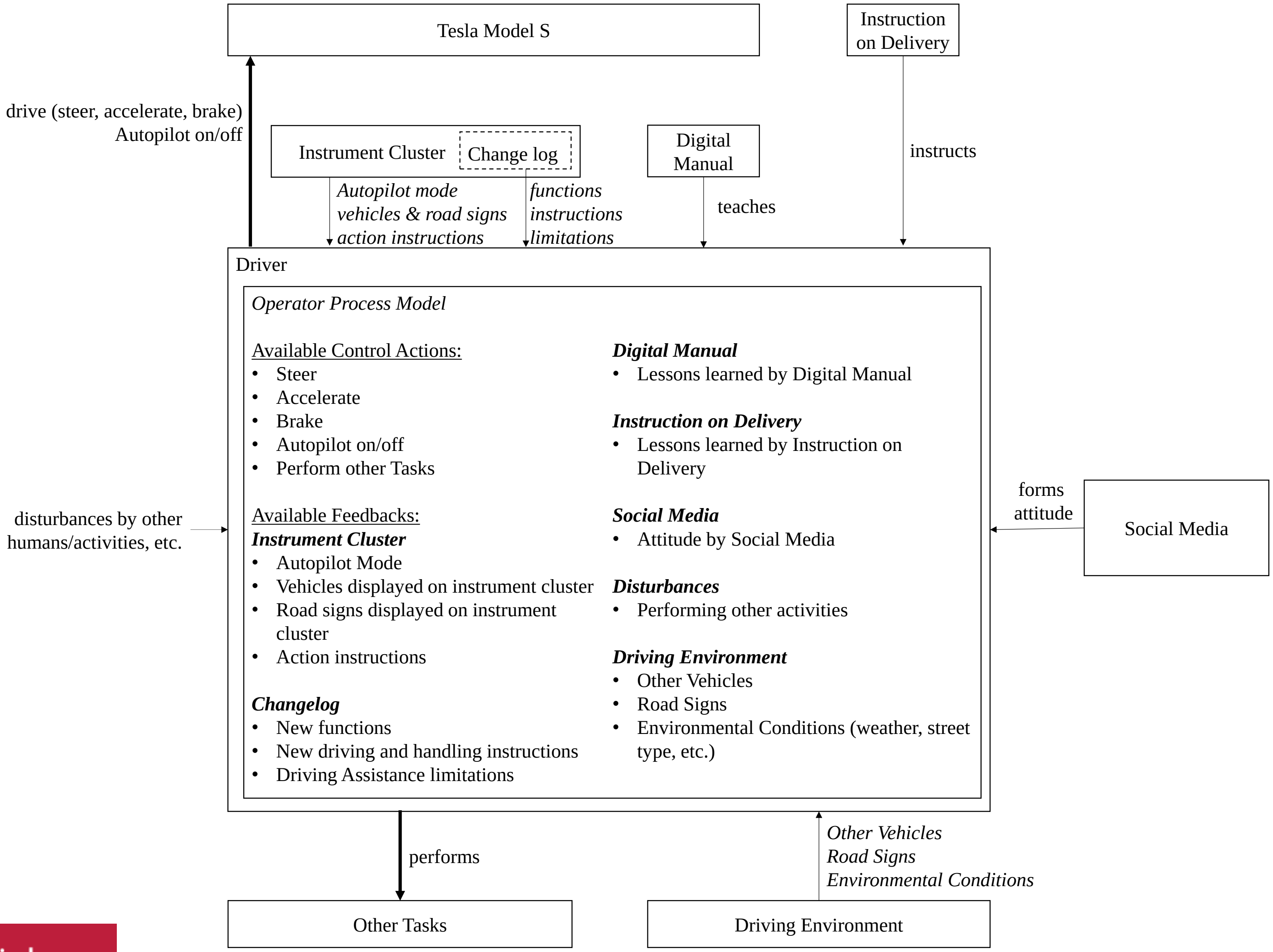
Application Example: Tesla Model S Fatality

Step 2: Autopilot Process Models and Contextual Factors

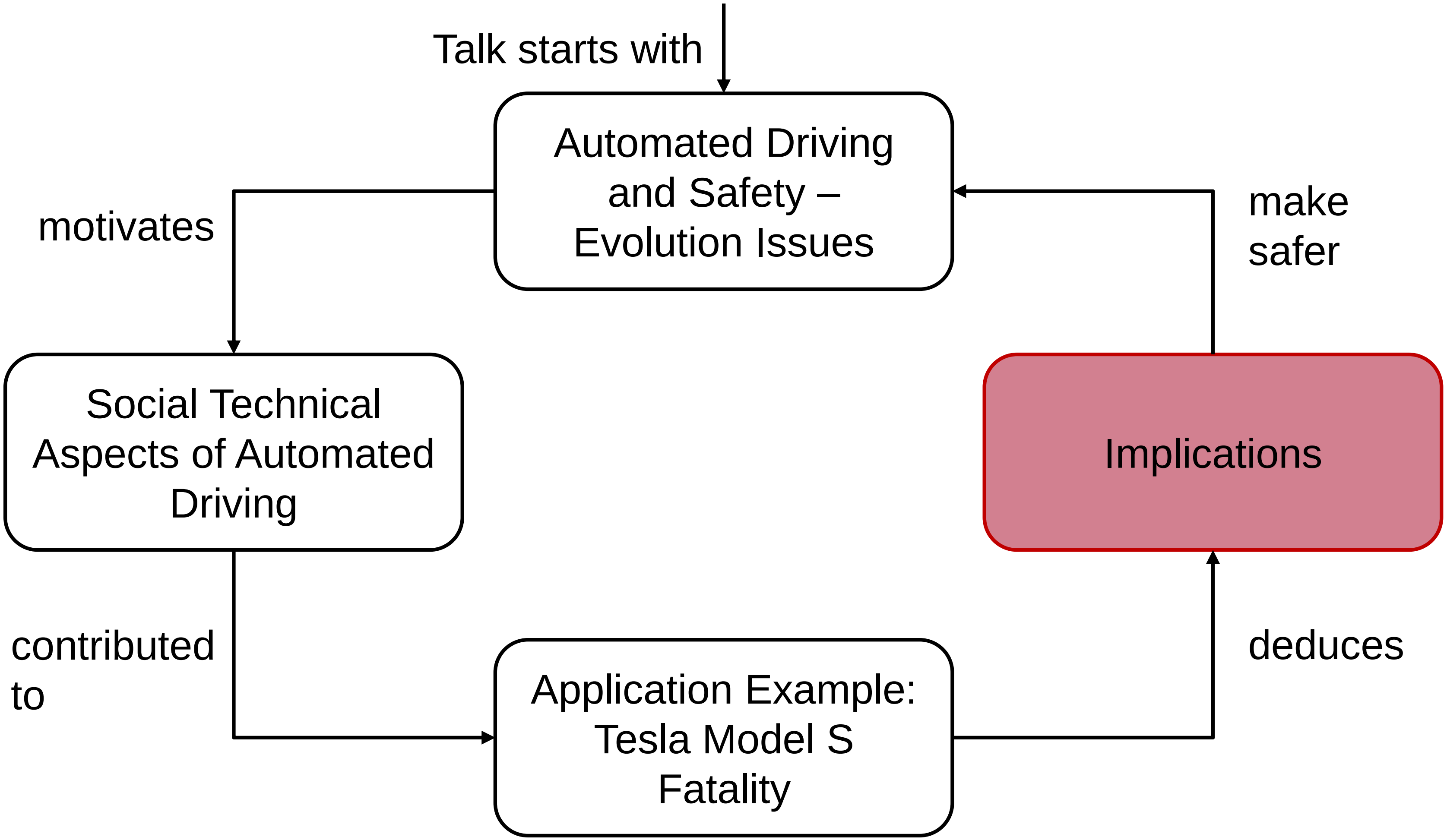


Application Example: Tesla Model S Fatality

Step 2: Driver Process Models and Contextual Factors

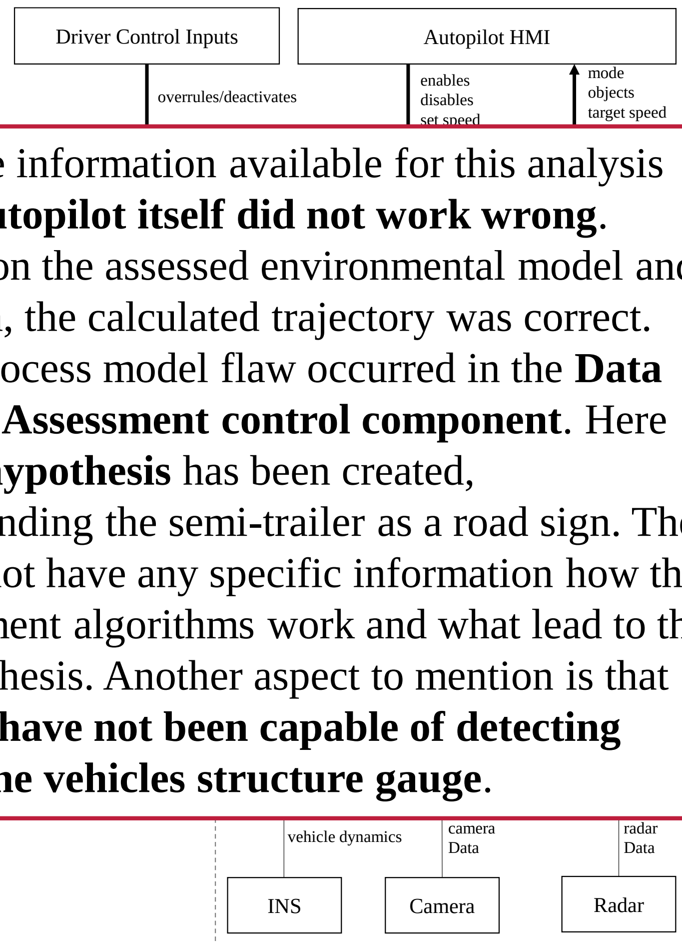


Agenda


Talk starts with
Automated Driving and Safety – Evolution Issues
motivates
Social Technical Aspects of Automated Driving
contributed to
Application Example: Tesla Model S Fatality
deduces
Implications
make safer

Application Example: Tesla Model S Fatality

Step 2: Autopilot Process Models and Contextual Factors



As far as the information available for this analysis goes, the **Autopilot itself did not work wrong**. Depending on the assessed environmental model and sensory data, the calculated trajectory was correct. The main process model flaw occurred in the **Data Fusion and Assessment control component**. Here the **wrong hypothesis** has been created, misunderstanding the semi-trailer as a road sign. The authors do not have any specific information how the data assessment algorithms work and what lead to the faulty hypothesis. Another aspect to mention is that the **sensors have not been capable of detecting objects in the vehicles structure gauge**.

Application Example: Tesla Model S Fatality

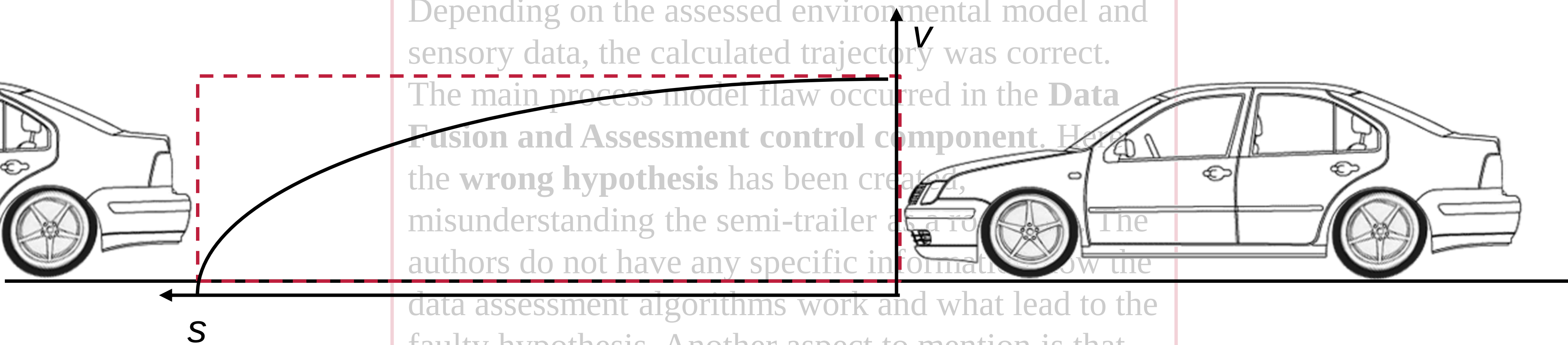
Step 2: Autopilot Process Models and Contextual Factors

Example: Vehicle Structure Gauge Principle

Driver Control Inputs | Autopilot HMI

overrules/deactivates | enables disables set speed | mode objects target speed

As far as the information available for this analysis goes, the **Autopilot itself did not work wrong**. Depending on the assessed environmental model and sensory data, the calculated trajectory was correct. The main process model flaw occurred in the **Data Fusion and Assessment control component**. Here, the **wrong hypothesis** has been created, misunderstanding the semi-trailer as a ro[illegible]. The authors do not have any specific information how the data assessment algorithms work and what lead to the faulty hypothesis. Another aspect to mention is that the **sensors have not been capable of detecting objects in the vehicles structure gauge**.

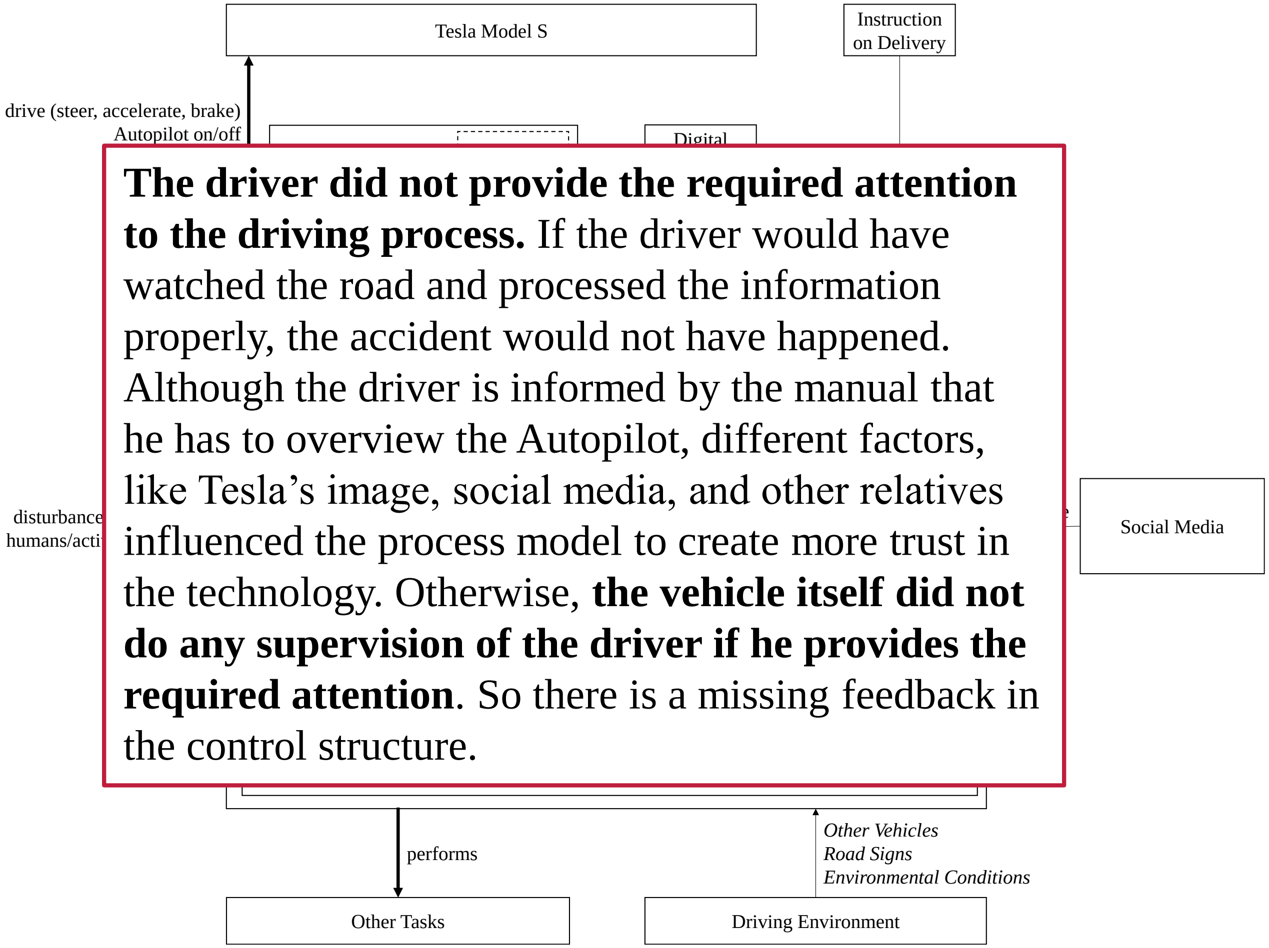


vehicle dynamics | camera Data | radar Data

INS | Camera | Radar

Application Example: Tesla Model S Fatality

Step 2: Driver Process Models and Contextual Factors



The driver did not provide the required attention to the driving process. If the driver would have watched the road and processed the information properly, the accident would not have happened. Although the driver is informed by the manual that he has to overview the Autopilot, different factors, like Tesla's image, social media, and other relatives influenced the process model to create more trust in the technology. Otherwise, **the vehicle itself did not do any supervision of the driver if he provides the required attention**. So there is a missing feedback in the control structure.

Application Example: Tesla Model S Fatality

Step 2: Driver Process Models and Contextual Factors

Example: Eye Detection and/or Hands on Wheel Detection

Tesla Model S

Instruction on Delivery

drive (steer, accelerate, brake)
Autopilot on/off

Digital

The driver did not provide the required attention
...cess. If the dri...
...nd processed t...
...ent would not l...
...r is informed b...
... the Autopilot, ...
... social media, ...
...cess model to c...
...herwise, **the ve...**
do any supervision of the driver if he provides the required attention. So there is a missing feedback in the control structure.

performs

Other Vehicles
Road Signs
Environmental Conditions

Other Tasks

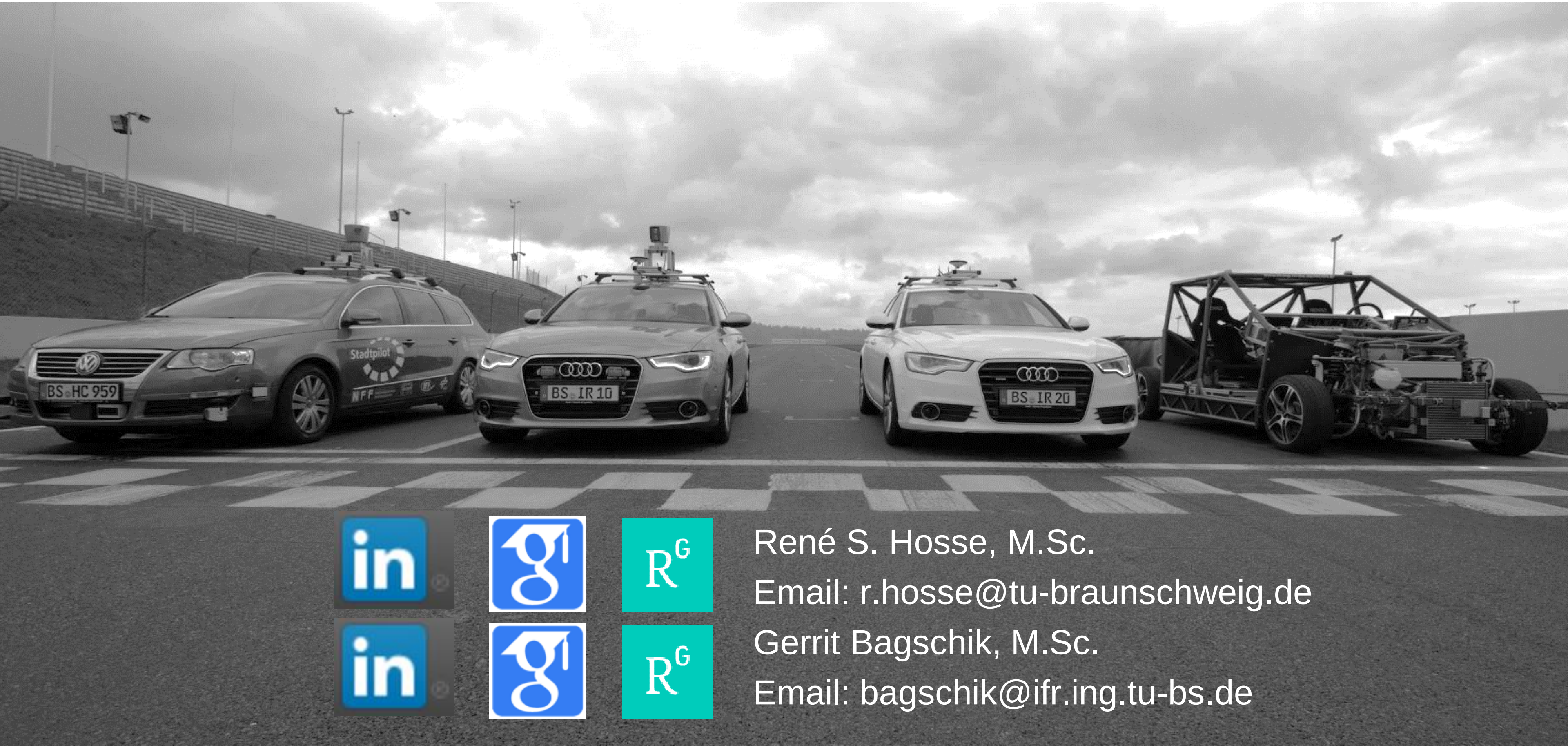
Driving Environment

Conclusions

The fatal crash of the Tesla Model S shows that development of safe automated vehicles must take socio-technical aspects into account. STAMP and CAST, respective STPA for forward analysis, can integrate the human in the roles of operator, traffic participant and manufacturer of a system.

The proposed categorization of control actions to determine unsafe behavior do not explain the main causes of the aforementioned fatal accident. For example, the assessed environmental model is sent to the driving controller in right order and right time but contained wrong information about the environment. To explain why the accident still happened further explanation is needed.

Contact information



René S. Hosse, M.Sc.
Email: r.hosse@tu-braunschweig.de
Gerrit Bagschik, M.Sc.
Email: bagschik@ifr.ing.tu-bs.de