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

Social Technical Aspects of Automated Driving

motivates

Application Example: Tesla Model S Fatality

contributed to

Implications

make safer
deduces

Talk starts with

Automated Driving and Safety – Evolution Issues

Social Technical Aspects of Automated Driving

motivates

Application Example: Tesla Model S Fatality

contributed to

Implications

make safer
deduces
Automated Driving and Safety – Evolution Issues
Increasing Automation throughout Domains

**Mechanic Control Systems**
- Road
- Ag
- Manufactoring

**Electric Electronic Control Systems**
- Electric interlocks
- L-ZB
- Mobile comm.
- ETCS (L.2)
- ETCS (L.3)

**Computational and Information Technology**
- Standardised mechanical interlocking
- Electronically interlocking
- Passenger information systems

**Cooperative Networks**
- Totally Integrated Automation (TIA)
- Programmable memory program

**Year**
- 1930
- 1940
- 1950
- 1960
- 1970
- 1980
- 1990
- 2000
- 2010
- 2020

- Jetronic
- Motronic
- CAN
- C2C
- ABS
- ESP
- e-Call

R.S. Hosse, G. Bagschik, M. Maurer, K. Bengler, U. Becker | STAMP Workshop 2017 | MIT
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“
Agenda

Talk starts with

Automated Driving and Safety – Evolution Issues

Social Technical Aspects of Automated Driving

motivates

centered to

Application Example: Tesla Model S Fatality

make safer

deduces

Implications
### Socio-technical Aspects of Automated Driving

#### Role of human in automated vehicles

<table>
<thead>
<tr>
<th>Name</th>
<th>Lateral &amp; long. control</th>
<th>Surveillance of environment</th>
<th>Fallback layer</th>
<th>Domain of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisted</td>
<td>Driver &amp; System</td>
<td>Driver</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>Partial automation</td>
<td>System</td>
<td>Driver</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>Conditional automation</td>
<td>System</td>
<td>System</td>
<td>Fallback ready user</td>
<td>Limited</td>
</tr>
<tr>
<td>High automation</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Limited</td>
</tr>
<tr>
<td>Full automation</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

### Socio-technical Aspects of Automated Driving

#### Role of human in automated vehicles

<table>
<thead>
<tr>
<th>Name</th>
<th>Lateral &amp; long. control</th>
<th>Surveillance of environment</th>
<th>Fallback layer</th>
<th>Domain of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisted</td>
<td>Driver &amp; System</td>
<td>Driver</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>Partial automation</td>
<td>System</td>
<td>Driver</td>
<td>Driver</td>
<td>Limited</td>
</tr>
<tr>
<td>Conditional automation</td>
<td>System</td>
<td>System</td>
<td>Fallback ready user</td>
<td>Limited</td>
</tr>
<tr>
<td>High automation</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Limited</td>
</tr>
<tr>
<td>Full automation</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>
Socio-technical Aspects of Automated Driving
Role of human in the vehicle

<table>
<thead>
<tr>
<th>Name</th>
<th>Lateral &amp; long. control</th>
<th>Surveillance of environment</th>
<th>Fallback layer</th>
<th>Domain of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial automation</td>
<td>System</td>
<td>Driver</td>
<td>Driver</td>
<td>Limited</td>
</tr>
</tbody>
</table>

Today's 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.”

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Lateral &amp; long. control</th>
<th>Surveillance of environment</th>
<th>Fallback layer</th>
<th>Domain of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial automation</td>
<td>System</td>
<td>Driver</td>
<td>Driver</td>
<td>Limited</td>
</tr>
</tbody>
</table>

⚠️ 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.

---

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
Agenda

Talk starts with

Automated Driving and Safety – Evolution Issues

Social Technical Aspects of Automated Driving

motivates

implications

Application Example: Tesla Model S Fatality

make safer

deduces

Impact of Fatality

Application Example: Tesla Model S Fatality

Implications
Application Example: Tesla Model S Fatality

Accident Introduction

**Application Example: Tesla Model S Fatality**

**Step 0: Accidents and Hazards**

<table>
<thead>
<tr>
<th>No.</th>
<th>Accident</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vehicle crashes when Autopilot is active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Driver does not provide required attention to driving tasks and environment</td>
</tr>
<tr>
<td>2</td>
<td>Autopilot does not react to other road crossing vehicles/obstacles</td>
</tr>
</tbody>
</table>
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

- Driver
  - Driver inputs
    - Vehicle Actions
  - Vehicle Info.
- Vehicle
  - Environment Feedb.
- Vehicle in its Environment
Application Example: Tesla Model S Fatality
Step 0: Autopilot Control Structure

Driver

Steering Wheel
- steering angle
- engages
- target speed
- provides delta/target action

Brake Pedal
- engagement
- target speed
- provides delta/target action

Accelerator Pedal
- target speed
- provides delta/target action

Driver Control Inputs
- target speed
- engages/disengages
- controls

Autopilot HMI
- engages/disengages
- provides trajectory
- assessed environment model

Autopilot

Trajectory Follow-Up Controller
- provides delta/target action

Data Fusion and Assessment

INS
- provides delta/target action

Camera
- provides delta/target action

Radar
- provides delta/target action

Vehicle Dynamics Controllers
- provides delta/target action

Vehicle in its Environment

Vehicle Dynamics

Steering System
- controls

Brake System
- controls

Drivetrain
- controls

Other tasks
- performs

R.S. Hosse, G. Bagschik, M. Maurer, K. Bengler, U. Becker | STAMP Workshop 2017 | MIT
## Application Example: Tesla Model S Fatality

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

<table>
<thead>
<tr>
<th>Control action</th>
<th>Required but not provided</th>
<th>Unsafe action provided</th>
<th>Incorrect timing</th>
<th>Stopped too soon/applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overrule/Deactivate</td>
<td>Driver inputs do not overrule Autopilot</td>
<td></td>
<td>Driver inputs deactivate Autopilot too late</td>
<td></td>
</tr>
<tr>
<td>Enable</td>
<td></td>
<td>Autopilot is enabled unintended</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send mode status</td>
<td>Autopilot does not send mode status</td>
<td>Autopilot sends mode status when not enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide assessed environment model</td>
<td>Environment model not provided (not updated)</td>
<td>Environment model provided when not required</td>
<td>Environment model provided too late (Same) model provided too long</td>
<td></td>
</tr>
</tbody>
</table>
Application Example: Tesla Model S Fatality
Step 0: Control Structures

Basic Model Concept: Driver Control Structure

- Driver inputs to Vehicle
- Vehicle outputs to Environment
- Vehicle actions to Vehicle
- Environment feedback to Vehicle

Driver

Vehicle

Vehicle in its Environment

Driver Control Structure

23.04.2017
R.S. Hosse, G. Bagschik, M. Maurer, K. Bengler, U. Becker | STAMP Workshop 2017 | MIT
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**

<table>
<thead>
<tr>
<th>Control action</th>
<th>Required but not provided</th>
<th>Unsafe action provided</th>
<th>Incorrect timing</th>
<th>Stopped too soon/applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steer</td>
<td>Driver does not steer Model S when required</td>
<td></td>
<td>Driver steers Model S too late</td>
<td></td>
</tr>
<tr>
<td>Enable Autopilot</td>
<td>Driver enables Autopilot when not allowed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send changelogs</td>
<td>Tesla does not send changelogs when required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authoring</td>
<td>Tesla does not author the manual when required</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Application Example: Tesla Model S Fatality

### Step 1: Violated Safety Constraints

<table>
<thead>
<tr>
<th>No.</th>
<th>UCA</th>
<th>Safety constraint</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCA 3</td>
<td>Autopilot does not send objects to Autopilot HMI when required</td>
<td>Autopilot must send objects to Autopilot HMI when required</td>
</tr>
<tr>
<td>UCA 4</td>
<td>Autopilot does not send road signs to Autopilot HMI when required</td>
<td>Autopilot must send road signs to Autopilot HMI when required</td>
</tr>
<tr>
<td>UCA 20</td>
<td>Data Fusion and Assessment does not provide assessed environment model to Autopilot HMI when required</td>
<td>Data Fusion and Assessment must provide assessed environment model to Autopilot HMI when required</td>
</tr>
<tr>
<td>UCA 34</td>
<td>Driver does not brake Model S when required</td>
<td>Driver must brake Model S when required</td>
</tr>
<tr>
<td>UCA 68</td>
<td>Driver performs other tasks when not allowed</td>
<td>Driver must not perform other tasks when not allowed</td>
</tr>
</tbody>
</table>
Application Example: Tesla Model S Fatality
Step 2: Autopilot Process Models and Contextual Factors

Autopilot

**Autopilot Process Model**

*Control Actions:*
- Provide Trajectory
- Status Mode
- Objects
- Signs
- Target Speed

*Control Inputs:*

**Driver Control Inputs**
- Overrule/Deactivate

**Autopilot HMI**

*Enables*
- Set speed

*Disables*
- Objects
- Target speed
- Signs

*Feedbacks:*

**Data Fusion and Assessment**
- Assessed Environment Model

**Autopilot HMI**

*Driver*
- Driver Operative Process Awareness

**Missing Feedback**
- Driver Operative Process Awareness

**Trajectory Follow-Up Controller**

*Provides trajectory*

**Data Fusion and Assessment**

*Process Model*

*Control Actions:*
- Assessed Environment Model

*Feedbacks:*
- Vehicle Dynamics
- Visual Environment
- Radar Data

**INS**
- Camera Data

**Radar**
- Radar Data

23.04.2017

R.S. Hosse, G. Bagschik, M. Maurer, K. Bengler, U. Becker | STAMP Workshop 2017 | MIT
Application Example: Tesla Model S Fatality
Step 2: Driver Process Models and Contextual Factors

Operator Process Model
Available Control Actions:
- Steer
- Accelerate
- Brake
- Autopilot on/off
- Perform other Tasks

Available Feedbacks:
Instrument Cluster
- Autopilot Mode
- Vehicles displayed on instrument cluster
- Road signs displayed on instrument cluster
- Action instructions

Changelog
- New functions
- New driving and handling instructions
- Driving Assistance limitations

Digital Manual
- Lessons learned by Digital Manual

Instruction on Delivery
- Lessons learned by Instruction on Delivery

Social Media
- Attitude by Social Media

Disturbances
- Performing other activities

Driving Environment
- Other Vehicles
- Road Signs
- Environmental Conditions (weather, street type, etc.)

forms attitude

Social Media

forms

Driver

Tesla Model S

Instruction on Delivery

Instruction on Delivery

Digital Manual

Instruction on Delivery

Digital Manual

Instruction on Delivery

Digital Manual

Instruction on Delivery

Digital Manual

Instruction on Delivery

Digital Manual

Instruction on Delivery

Social Media

forms

Other Vehicles
Road Signs
Environmental Conditions

Driving Environment

perform

Other Tasks

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

Instrument Cluster

Autopilot mode
vehicles & road signs
action instructions

functions
limitations

Changelog

Other Tasks

Disturbances

perform

disturbances by other humans/activities, etc.

23.04.2017

R.S. Hosse, G. Bagschik, M. Maurer, K. Bengler,
U. Becker | STAMP Workshop 2017 | MIT
Agenda

Talk starts with

Automated Driving and Safety – Evolution Issues

Social Technical Aspects of Automated Driving

motivates

contributed to

Application Example: Tesla Model S Fatality

make safer

deduces

Implications
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.
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: 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

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.

23.04.2017
R.S. Hosse, G. Bagschik, M. Maurer, K. Bengler, U. Becker | STAMP Workshop 2017 | MIT
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