Systems-Theoretic Process Analysis: AUTOMOBILE FEATURES FOR LANE MANAGEMENT

Diogo Castilho, Megan France & Dajiang Suo

LADAR image of London streets
MOTIVATION AND BACKGROUND
PURPOSE AND PROJECT STRUCTURE
SYSTEM OVERVIEW
TEST DRIVE
STPA RESULTS
DISCUSSION
CONCLUSIONS
WHY STUDY AUTOMATED DRIVING?

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

- Safety, efficiency, and opportunity for mobility
# Automation Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Narrative definition</th>
<th>Execution of steering and acceleration/deceleration</th>
<th>Monitoring of driving environment</th>
<th>Fallback performance of dynamic driving task</th>
<th>System capability (driving modes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Automation</td>
<td>the full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Human driver</td>
<td>n/a</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>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</td>
<td>Human driver and system</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>2</td>
<td>Partial Automation</td>
<td>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</td>
<td>System</td>
<td>Human driver</td>
<td>Human driver</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Automation</td>
<td>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</td>
<td>System</td>
<td>System</td>
<td>Human driver</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>4</td>
<td>High Automation</td>
<td>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</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>Some driving modes</td>
</tr>
<tr>
<td>5</td>
<td>Full Automation</td>
<td>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</td>
<td>System</td>
<td>System</td>
<td>System</td>
<td>All driving modes</td>
</tr>
</tbody>
</table>
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”
PROJECT STRUCTURE

- **MODEL S DESIGN INFORMATION**
- **MODEL S TEST DRIVE**
- **HUMAN FACTORS PRINCIPLES**

**SYSTEMS THEORETIC PROCESS ANALYSIS (STPA)**

**HUMAN FACTORS FINDINGS**
MOTIVATION AND BACKGROUND
PURPOSE AND PROJECT STRUCTURE
SYSTEM OVERVIEW
TEST DRIVE
STPA RESULTS
DISCUSSION
CONCLUSIONS
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.
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)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Test Drive Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed Assist</td>
<td>Maintain selected speed</td>
</tr>
<tr>
<td>Traffic-Aware Cruise Control</td>
<td>Maintain distance to a car ahead</td>
</tr>
<tr>
<td>Autosteer</td>
<td>Lane Keeping</td>
</tr>
<tr>
<td>Auto Lane Change</td>
<td>Lane Changing</td>
</tr>
</tbody>
</table>

Image source: Diogo Castilho
MOTIVATION AND BACKGROUND
PURPOSE AND PROJECT STRUCTURE
SYSTEM OVERVIEW
TEST DRIVE
STPA RESULTS
DISCUSSION
CONCLUSIONS
SYSTEM ACCIDENTS AND HAZARDS

System Level Accidents

<table>
<thead>
<tr>
<th>A-1</th>
<th>Loss of life and injury</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-2</td>
<td>Economic loss</td>
</tr>
</tbody>
</table>

System Level Hazards

<table>
<thead>
<tr>
<th>H-1</th>
<th>Vehicle does not maintain safe distance from nearby vehicles</th>
</tr>
</thead>
<tbody>
<tr>
<td>H-2</td>
<td>Vehicle does not maintain safe distance from terrain and other obstacles</td>
</tr>
<tr>
<td>H-3</td>
<td>Vehicle occupants exposed to harmful effects and/or health hazards</td>
</tr>
</tbody>
</table>
SAFETY CONTROL STRUCTURE

Driver

Enable autopilot
Disable autopilot
Change lane

Warning signals
Dashboard indicators
Audio chime
Visual Clues
Physical feedback

Display

Lane Management System

Disengage
Change lane
Keep lane
Accelerate
Reduce Speed

Physical Vehicle

Steering
Gas Pedal
Brake
# UNSAFE CONTROL ACTIONS

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

REFERENCES


