Short Exercise inspired by Tesla Autopilot

Spring 2016 Student project: Diogo Castilho, Megan France
Disclaimer

These exercises are not meant to represent a complete analysis, and they are not meant to exhaustively demonstrate STPA.

The exercises are only meant to introduce a few core concepts.
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

(Leveson and Thomas, 2018)
Automotive Example

• Losses
  – L-1. Loss of life or serious injury to people
  – L-2. Damage to the vehicle or objects outside the vehicle
  – L-3: Loss of mission (transportation)
  – L-4: Loss of customer satisfaction
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios

Identify Losses, Hazards
Define System boundary

System

Environment

Leveson and Thomas, 2018
High-level Control Structure

Driver

Enable
Disable
Etc.

Warning signals

Automation

Control Algorithms

Process Model

Change lane
Accelerate
Brake
Etc.

Environment

Vehicle

Sensors

Steer
Accelerate
Brake
Etc.

Manual override detected
Wheel speed
PRNDL
Etc.

Control
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios

Identify Losses, Hazards
Define System boundary
Environment
System

(Leveson and Thomas, 2018)
STPA: Unsafe Control Actions (UCA)

<table>
<thead>
<tr>
<th>Brake Command</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, too late, out of order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Automation

- Control Algorithms
- Process Model

Lane Change
- Accelerate
- Brake
- Etc.

Vehicle

Sensors

© Copyright John Thomas 2018
STPA: Unsafe Control Actions (UCA)

Example:
“_______  _______  _____cmd  when  _______”

Source Controller  Control Action  Context

<table>
<thead>
<tr>
<th>Brake Command</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, too late, out of order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
STPA: Unsafe Control Actions (UCA)

Example:
“Automation does not provide brake cmd when ______”

<table>
<thead>
<tr>
<th>Brake Command</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, too late, out of order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation does not provide brake cmd when _____</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Copyright John Thomas 2018
Example:

“Automation does not provide brake cmd when path is obstructed”

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Context</th>
<th>Type</th>
<th>Source Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brake Command</td>
<td>UCA-1: Automation does not provide Brake cmd when vehicle path is obstructed [L-1, L-2]</td>
<td>Not providing causes hazard</td>
<td>Providing causes hazard</td>
</tr>
</tbody>
</table>

© Copyright John Thomas 2018
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios

Identify Losses, Hazards

Define System boundary

Environment

System

(Leveson and Thomas, 2018)
Step 4: Potential causes of UCAs

UCA-1: Automation does not provide adequate braking commands when path is obstructed
Step 4: Potential causes of UCAs

UCA-1: Automation does not provide adequate braking commands when path is obstructed
Scenario #1

UCA-1: Autopilot does not provide adequate braking commands for obstacle ahead
High-level Control Structure

Driver
- Procedures
- Process Model

Environment
- Enable
- Disable
- Etc.

Warning signals

Automation
- Control Algorithms
- Process Model

Change lane
- Accelerate
- Brake
- Etc.

Manual override detected
- Wheel speed
- PRNDL
- Etc.

Vehicle

Sensors

Steer
- Accelerate
- Brake
- Etc.
**STPA: Unsafe Control Actions (UCA)**

<table>
<thead>
<tr>
<th>Steering Command</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Too early, too late, out of order</th>
<th>Stopped Too Soon / Applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UCA-2: Driver provides unsafe steering override cmds when autopilot is engaged [L-1,L-2]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Copyright John Thomas 2018
Step 4: Potential causes of UCAs

- Inadequate Procedures (Flaws in creation, process changes, incorrect modification or adaptation)
- Process Model (inconsistent, incomplete, or incorrect)
- Control input or external information wrong or missing
- Missing or wrong communication with another controller
- Inadequate or missing feedback
- Feedback Delays
- Inadequate or missing feedback
- Incorrect or no information provided
- Measurement inaccuracies
- Feedback delays
- Process output contributes to system hazard
- Unidentified or out-of-range disturbance
- Changes over time
- Component failures
- Conflicting control actions
- Delayed operation
- Inadequate operation
- Process input missing or wrong

**UCA-2: Driver provides unsafe steering override commands while autopilot is engaged**
Scenario #2

UCA-2: Driver provides unsafe steering override commands when autopilot is engaged