Building Behavioral Competency into STPA Process Models for Automated Driving Systems

Shawn A. Cook, Hsing-Hua Fan, Krzysztof Pennar, Padma Sundaram
General Motors
Introduction

• Behavioral Competency is an AV’s minimal ability to respond to external hazards, operate in typical traffic conditions, and obey traffic laws with reasonable etiquette.¹

• Behavioral Competency is realized at the vehicle level.

• Main focus will be an approach for Unsafe Control Action (UCA) generation for the brain of an AV.

---

STPA Process

Step 1: Identify Potential Accidents and Hazards
Step 2: Construct the Control Structure
Step 3: Identify Unsafe Control Actions
Step 4: Identify Potential Hazardous Scenarios

Safety Constraints
Step 1: Potential AV Accidents

Assumption:
Both AV and Non-AV vehicles share the same motor vehicle accident scenarios.

<table>
<thead>
<tr>
<th>Accident</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-1</td>
<td>Two or more vehicles collide</td>
</tr>
<tr>
<td>A-2</td>
<td>Vehicle collides with non-fixed obstacle&lt;sup&gt;2&lt;/sup&gt;</td>
</tr>
<tr>
<td>A-3</td>
<td>Vehicle crashes into terrain&lt;sup&gt;3&lt;/sup&gt;</td>
</tr>
<tr>
<td>A-4</td>
<td>Vehicle occupants injured without vehicle collision</td>
</tr>
</tbody>
</table>

<sup>2</sup> Other obstacle includes pedestrians, bikers, animals, etc.  
<sup>3</sup> Terrain includes fixed, permanent objects such as guard rails, trees, bridges, signage, pavement, etc.
## Step 1: Potential AV Hazards

<table>
<thead>
<tr>
<th>Vehicle Level Hazard</th>
<th>Description</th>
<th>Accidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>H-1</td>
<td>Vehicle does not maintain safe distance from nearby vehicles</td>
<td>A-1</td>
</tr>
<tr>
<td>H-2</td>
<td>Vehicle does not maintain safe distance from terrain and other obstacles</td>
<td>A-2, A-3</td>
</tr>
<tr>
<td>H-3</td>
<td>Vehicle occupants exposed to harmful effects, and/or health hazards</td>
<td>A-4</td>
</tr>
<tr>
<td>H-4</td>
<td>Vehicle enters uncontrollable or unrecoverable state</td>
<td>A-1, A-2, A-3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Motion Control Hazard</th>
<th>Description</th>
<th>Accidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCH-1</td>
<td>Unwanted or Excessive Positive Longitudinal Motion</td>
<td>A-1, A-2, A-3</td>
</tr>
<tr>
<td>MCH-2</td>
<td>Unwanted or Excessive Negative Longitudinal Motion</td>
<td>A-1, A-2, A-3</td>
</tr>
<tr>
<td>MCH-3</td>
<td>Unwanted or Excessive Lateral Motion</td>
<td>A-1, A-2, A-3</td>
</tr>
</tbody>
</table>
Step 2: Control Structure

- **Environment**
  - External Inputs
  - Input Signals

- **Path Planning**
  - Controller

- **Sensing Systems**
  - Sensors

- **Actuation Systems**
  - Actuators

- **Autonomous Vehicle**
  - Controlled Process
  - Vehicle Movements

- **Feedbacks**
  - Control Actions
Step 3: Unsafe Control Action (Approach 1)

Syntax Construction

Source Controller + Type of CA + Control Action + When + Context

OEM
- Mission
- Advanced Research
- Geography
- Partnerships

Path Planning + Providing Too Late + Longitudinal Movement + When + Making a Turn at an Intersection

Brainstorm

Context

When

Making a Turn at an Intersection

Path Planning

Providing Too Late

Longitudinal Movement

When

Making a Turn at an Intersection

Brainstorm
Step 3: Unsafe Control Action (Approach 2)

Syntax Construction

Source Controller + Type of CA + Control Action + When + Context

OEM
- Mission
- Geography

Regulatory
- Federal
- ODD (Operational Design Domain)
- State (Motor Vehicle Code)

Operational Context

Path Planning + Providing Incorrect + Trajectory + When +

- Approaching an intersection with Circular Green Signal
- Turning Right at an intersection with Circular Green Signal

Step 3: Unsafe Control Action (Operational Context)

**Motion Characteristics** + **ODD**

- Approaching, Stopping, Merging, etc.
- Interacting with Intersection, Lane change, etc.
- Hills, Curve Road, Day, Night, etc.
- Pedestrian, Cyclist, etc.

**Operational Context**

Example:

- Approaching an intersection with Circular Green Signal
- Turning Right at an intersection with Circular Green Signal
- Pedestrian, Cyclist, etc.
Step 4: Potential Hazardous Scenario (Example)

Potential Hazardous Scenario
Vehicle Does Not Clear Intersection when Turning at Intersection

Causal Factor
Foliage classified incorrectly as a moving object because it swayed around in the windy condition.
Safety Constraints (Example)

Source (Regulatory):
(a) A driver facing a circular green signal shall proceed straight through or turn right or left or make a U-turn unless a sign prohibits a U-turn. Any driver, including one turning, shall yield the right-of-way to other traffic and to pedestrians lawfully within the intersection or an adjacent crosswalk.

UCA
Path Planning provides a movement that is incorrect and hazardous when approaching circular green signal and making a right turn at an intersection.

Potential Hazardous Scenario
Vehicle does not clear intersection when turning at intersection.

Safety Constraint:
**PATH PLANNING MUST INCLUDE THE ABILITY TO PASS THROUGH AN INTERSECTION IN MOVEMENT CALCULATION BEFORE MOVING FORWARD INTO AN INTERSECTION.**

Safety Constraint:
**SENSOR PROCESSING MUST HAVE CONFIDENCE AND REDUCE FALSE POSITIVE IN DISTINGUISHING TRUE MOVING TARGET.**

Safety Constraint:
**SENSOR PROCESSING MUST HAVE FOLIAGE AS A CLASS IN MACHINE LEARNING LIST.**
Summary

Pros:
• Numerous potentially hazardous scenarios for AV competency can be generated through STPA.
• UCA generation will be easier to document or automate in the future for AV analyses using operational keywords.
• Safety Constraints can be generated for each system/subsystem in the chain of causal factors.

Cons:
• Iterative process and refinement can be time consuming.
• Analysis can still grow very large.
Conclusions

• STPA is an iterative process with continuous refinement.
• STPA can provide hazardous scenarios.
• Operational context, derived from behavior competencies and regulations, can be an approach for defining context for UCA generation.
• Incorporating regulatory recommendations as part of the context for control action generation can support alignment with regulatory body expectations.
Questions?

• Thank you!