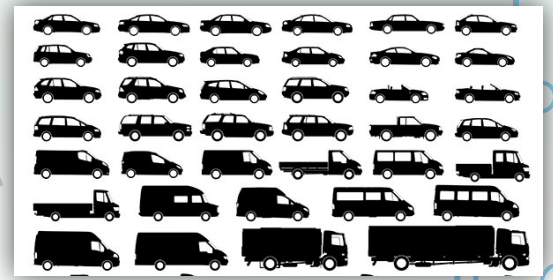
Building Behavioral Competency into STPA Process Models for Automated Driving Systems

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.



1. Nowakowski C., Schladover S, and Chan C-Y, "Regulatory Issues and Potential Regulatory Strategies for Highly Automated Vehicles (AVs)", AVS 2015.

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

Two Potential Approaches

Safety Constraints

Step 1: Potential AV Accidents

Assumption:

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

Accident	Description
A-1	Two or more vehicles collide
A-2	Vehicle collides with non-fixed obstacle[2]
A-3	Vehicle crashes into terrain[3]
A-4	Vehicle occupants injured without vehicle collision

2. Other obstacle includes pedestrians, bikers, animals, etc.
3. Terrain includes fixed, permanent objects such as guard rails, trees, bridges, signage, pavement, etc.

Step 1: Potential AV Hazards

Hazards

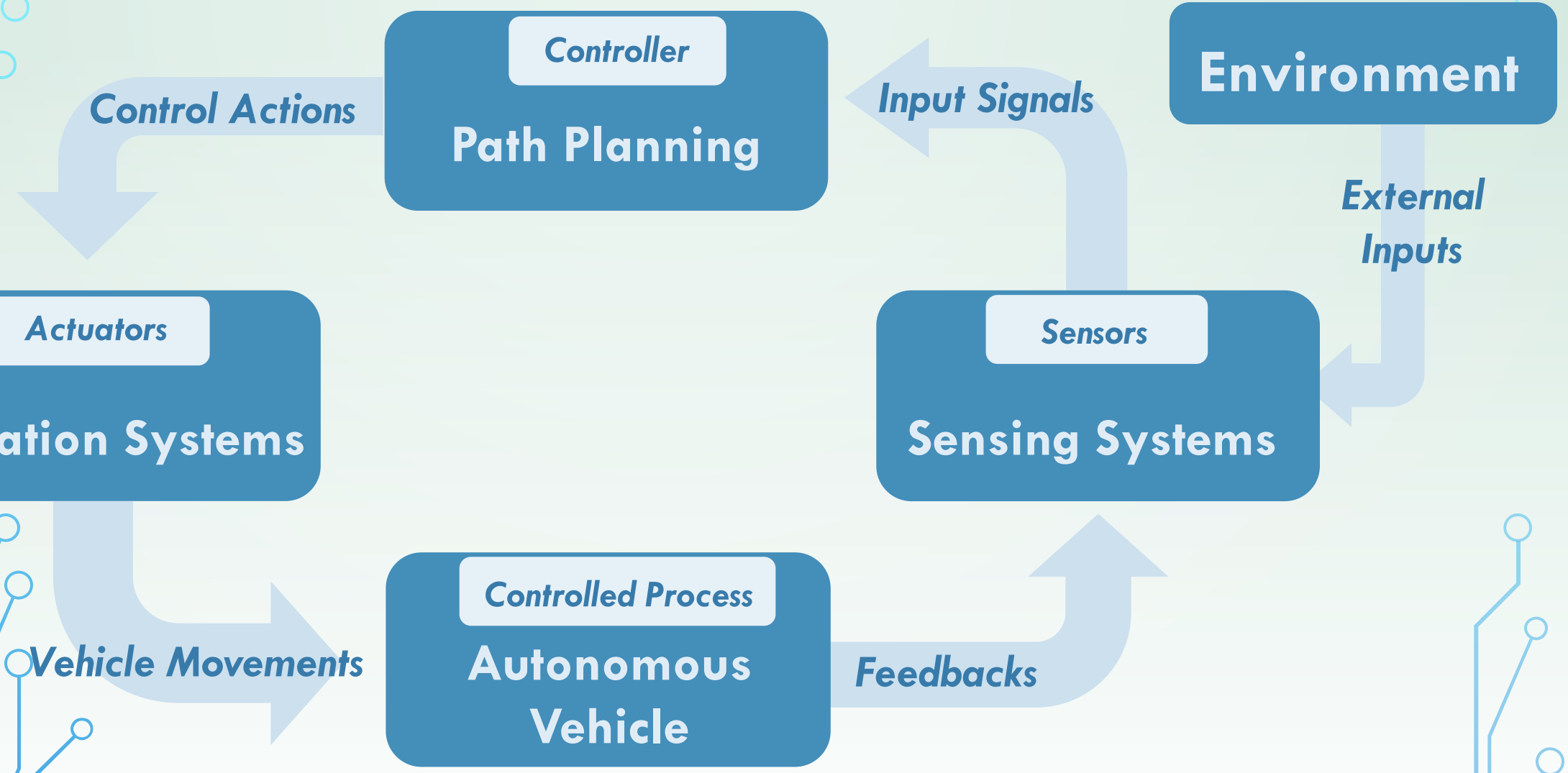
Vehicle Level

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

System Level

Motion Control Hazard	Description	Accidents
MCH-1	Unwanted or Excessive Positive Longitudinal Motion	A-1, A-2, A-3
MCH-2	Unwanted or Excessive Negative Longitudinal Motion	A-1, A-2, A-3
MCH-3	Unwanted or Excessive Lateral Motion	A-1, A-2, A-3

Step 2: Control Structure



Step 3: Unsafe Control Action (Approach 1)

Syntax Construction

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

OEM

- Mission
- Advanced Research
- Geography
- Partnerships

Brainstorm

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

Step 3: Unsafe Control Action (Approach 2)

Syntax Construction

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

OEM

- Mission
- Advanced Research
- Geography
- Partnerships

Regulatory

- Federal
  - ODD[4] (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

4. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/.../13069a-ads2.0_090617_v9a_tag.pdf AUTOMATED DRIVING SYSTEMS **2.0**: A VISION FOR SAFETY

Step 3: Unsafe Control Action (Operational Context)

Approaching, Stopping, Merging, etc.

Interacting with Intersection, Lane change, etc.

Hills, Curve Road, Day, Night, etc.

Pedestrian, Cyclist, etc.

Motion Characteristics + ODD

Operational Context

Example

Motion Characteristics

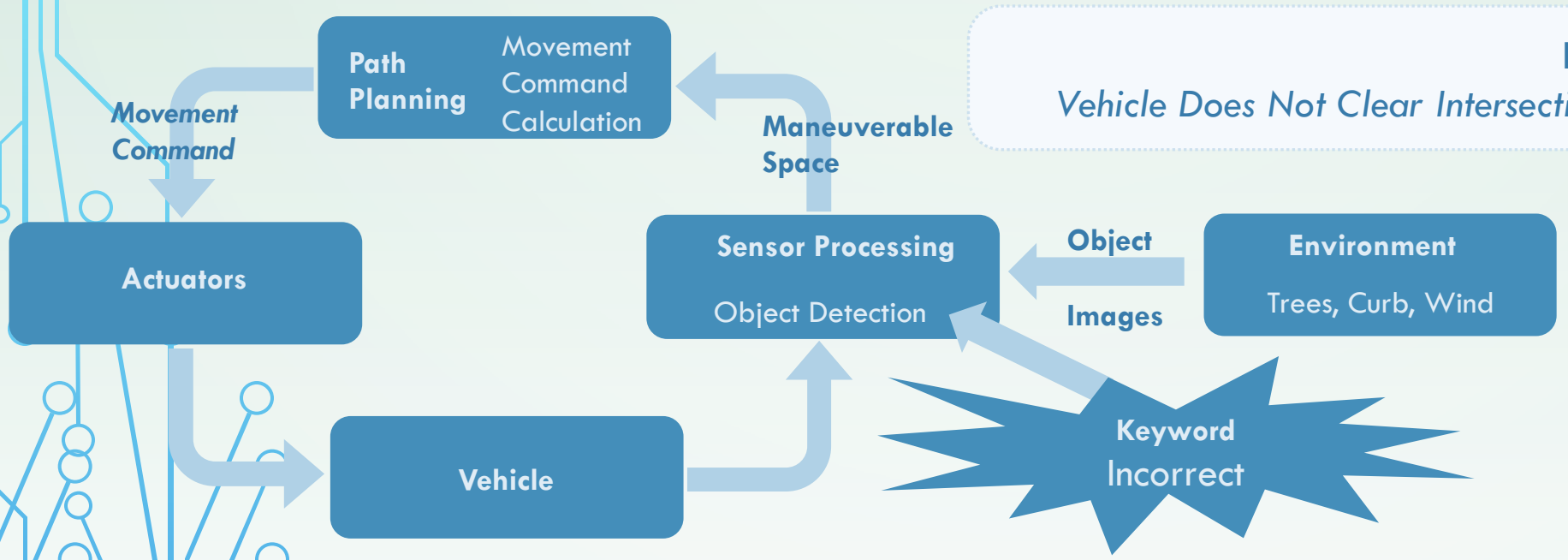
Approaching an intersection with Circular Green Signal

Turning Right at an intersection with Circular Green Signal

ODD

Step 4: Potential Hazardous Scenario (Example)

Path Planning + **Providing Incorrect** + **Trajectory** + **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

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.

System 1
Path Planning

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

System 2
Sensor Processing

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!