Finding Safety-Critical Causes of Mode Confusion Using Model Checking

Alyssa Byrnes and Dr. Cynthia Sturton, UNC Chapel HIll
www.vehical.org

Motivation

- Ambiguities in cyber-physical system specifications can cause mode confusion for their operators.
- System ambiguity: causes different behavior in systems built with the same specification.
- Interface Ambiguity: the system is not effectively communicating its internal state to the driver.
- It is good to have some ambiguities in a system so that we are not over communicating to the driver.
- Question: Which ambiguities do we care about?

Case Study: Adaptive Cruise Control

- Cruise Control: Car maintains a set speed
- Adaptive Cruise Control: Car also determines speed by observing the car in front
- System Specification: ISO 15622:2018

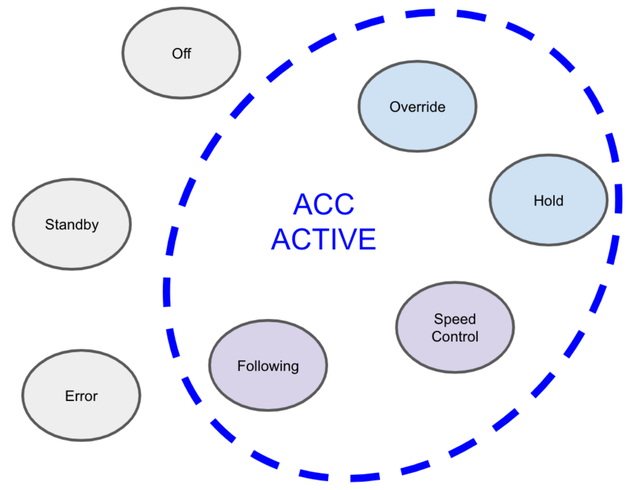
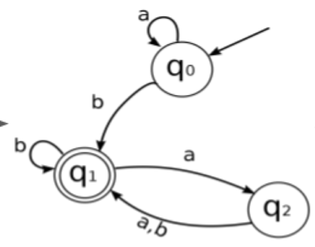


Figure 1: Model Representation of an Adaptive Cruise Control System

Methodology

Old System Specification



System Model Checking
Done in Uclid

System Ambiguities: checked for nondeterminism

Interface ambiguities: checked for observational nondeterminism, indirect mode changes, lack of operator authority

User Model
Done in Python
A mapping of scenarios to expected human reactions

Cyber-physical Model Checking
Done in dReach
Given a system state and a user action, determined if car would crash.

New System Specification

Results

- Found 23 transitions that violated determinism caused by 3 major system ambiguities.
- Found 52 transitions that violated at least one of the properties of the interface ambiguities.

Broader Impact

- Provides a general framework for other scientists to check for mode confusion in their cyber-physical systems
- Helps to create better specifications that produce safer systems

2019 NSF Cyber-Physical Systems Principal Investigators' Meeting
November 21-22, 2019 | Crystal City, Virginia

Award ID#: 1545126