Integrating State Machine Analysis with STPA

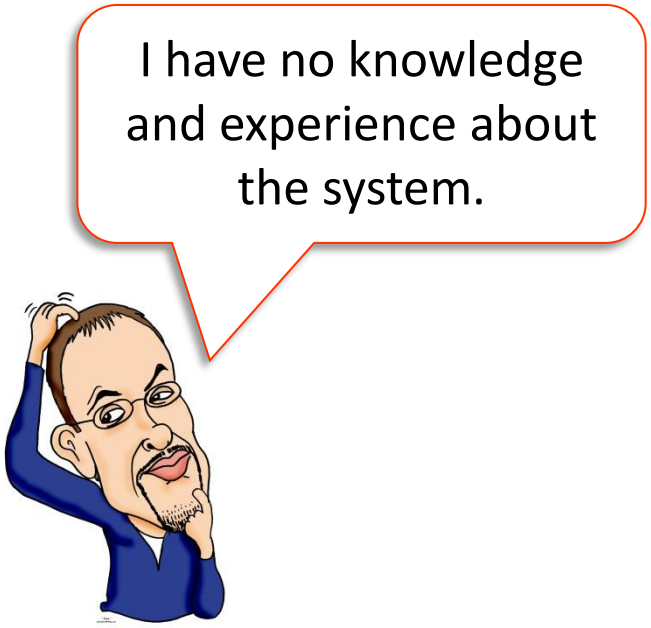
Asim Abdulkhaleq, Ph.D. Student
Institute of Software Technology
University of Stuttgart, Germany

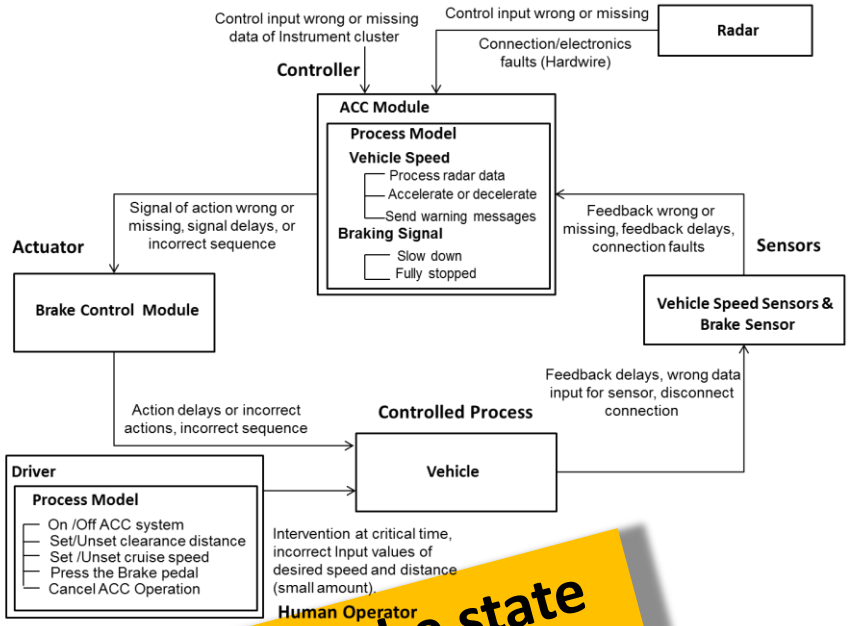
Joint work with:
Prof. Dr. Stefan Wagner

STAMP Workshop 2013
Cambridge, MIT, USA
28. March 2013

Integrating State Machine Analysis with STPA

- **Problem Statement:**
  - There is no systematic way to let the safety analyst know how to evaluate each control actions. Moreover, STPA does not represent system states, which have an effect on the safety of control action.

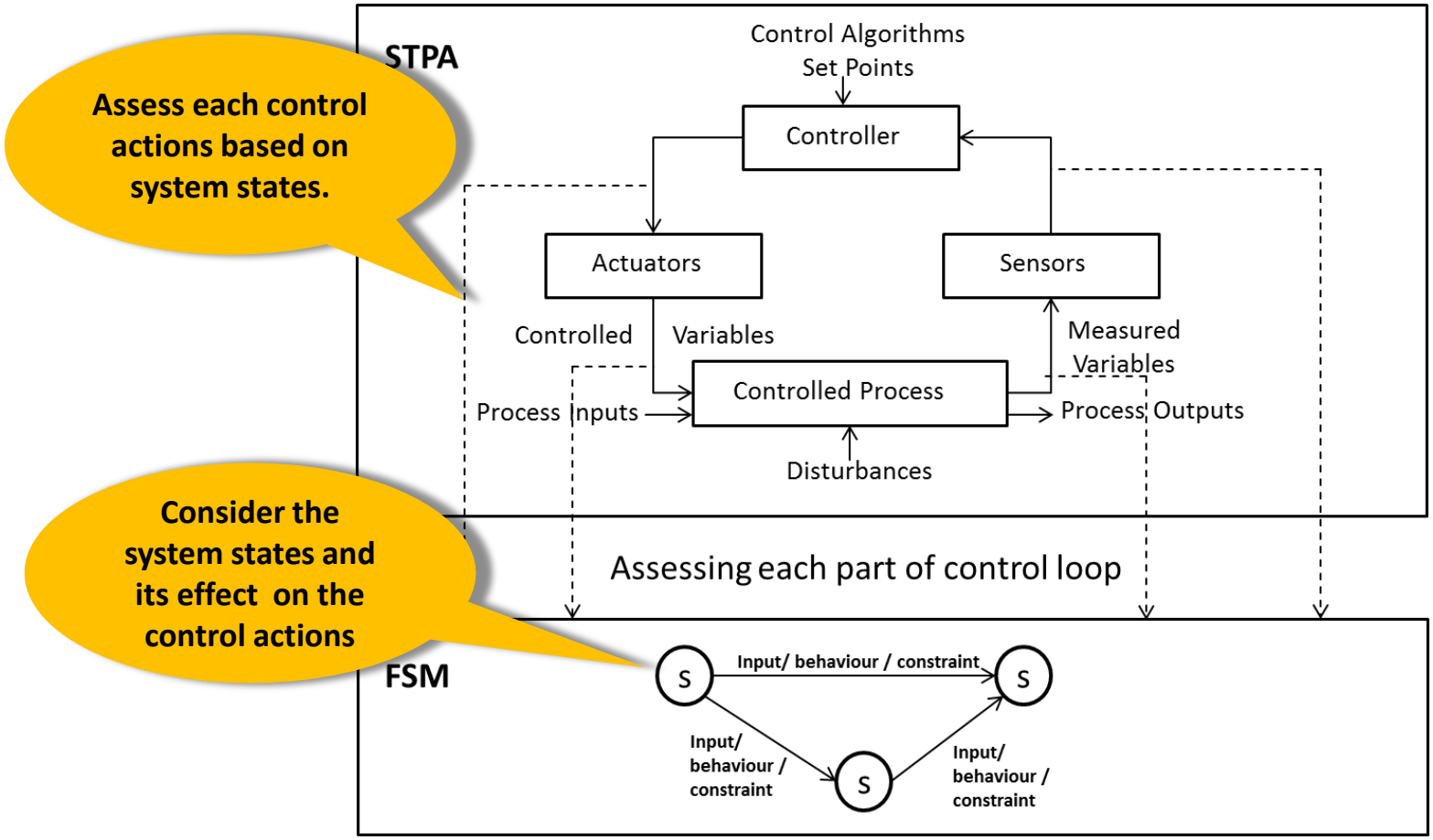




- **Research Objectives:**
  - Fill this gap and find w… …rysing the dynamic behaviour of systems during ST…
  - We plan to investig… …s modeling and analysis techniques.

For that, we integrated the state machine analysis with STPA.

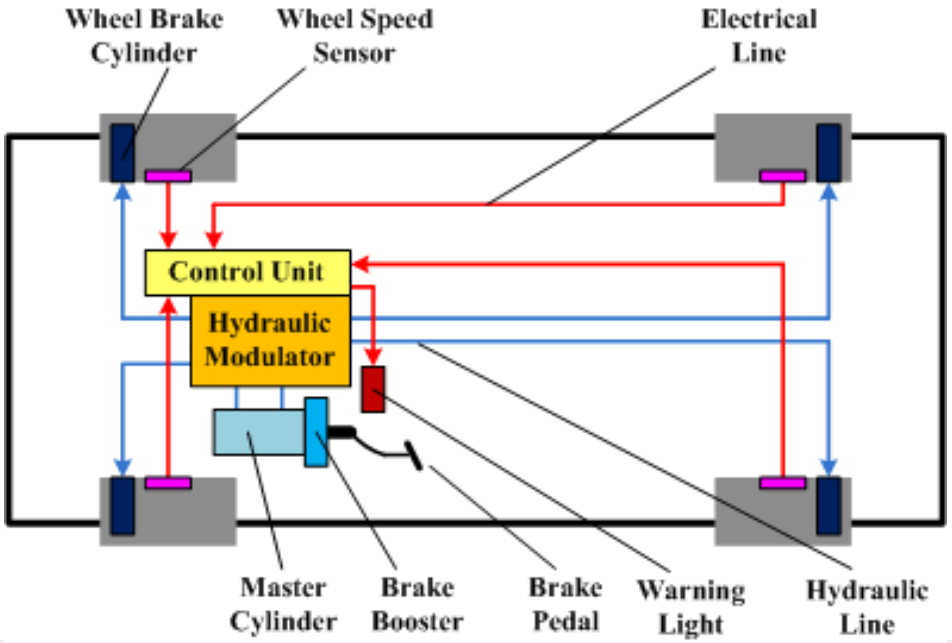
Proposed Methodology

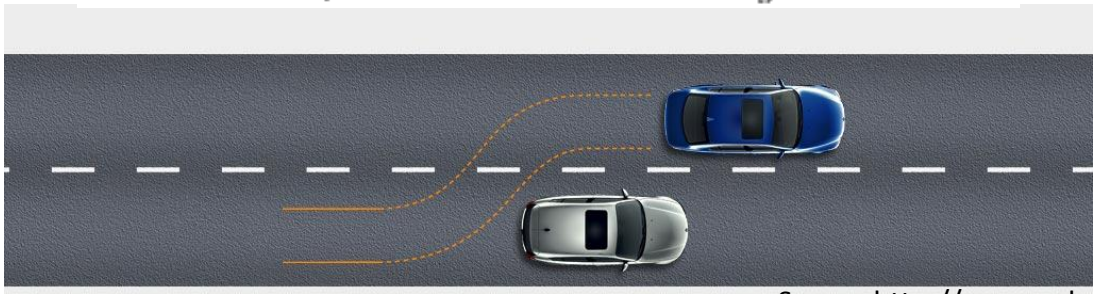


- **Proposed methodology aims to:**
  - Use STPA to identify the potential for inadequate scenarios.
  - Use Finite State Machine (FSM) to model the dynamic behaviour of the system.
  - Assess each control action with FSM based on all the possible system states .

Study Object: Anti-Lock Braking System (ABS)

- **Anti-Lock Braking System** is a safety system on motor vehicles which prevents the wheels from locking while braking.
- **The ABS Architecture:**

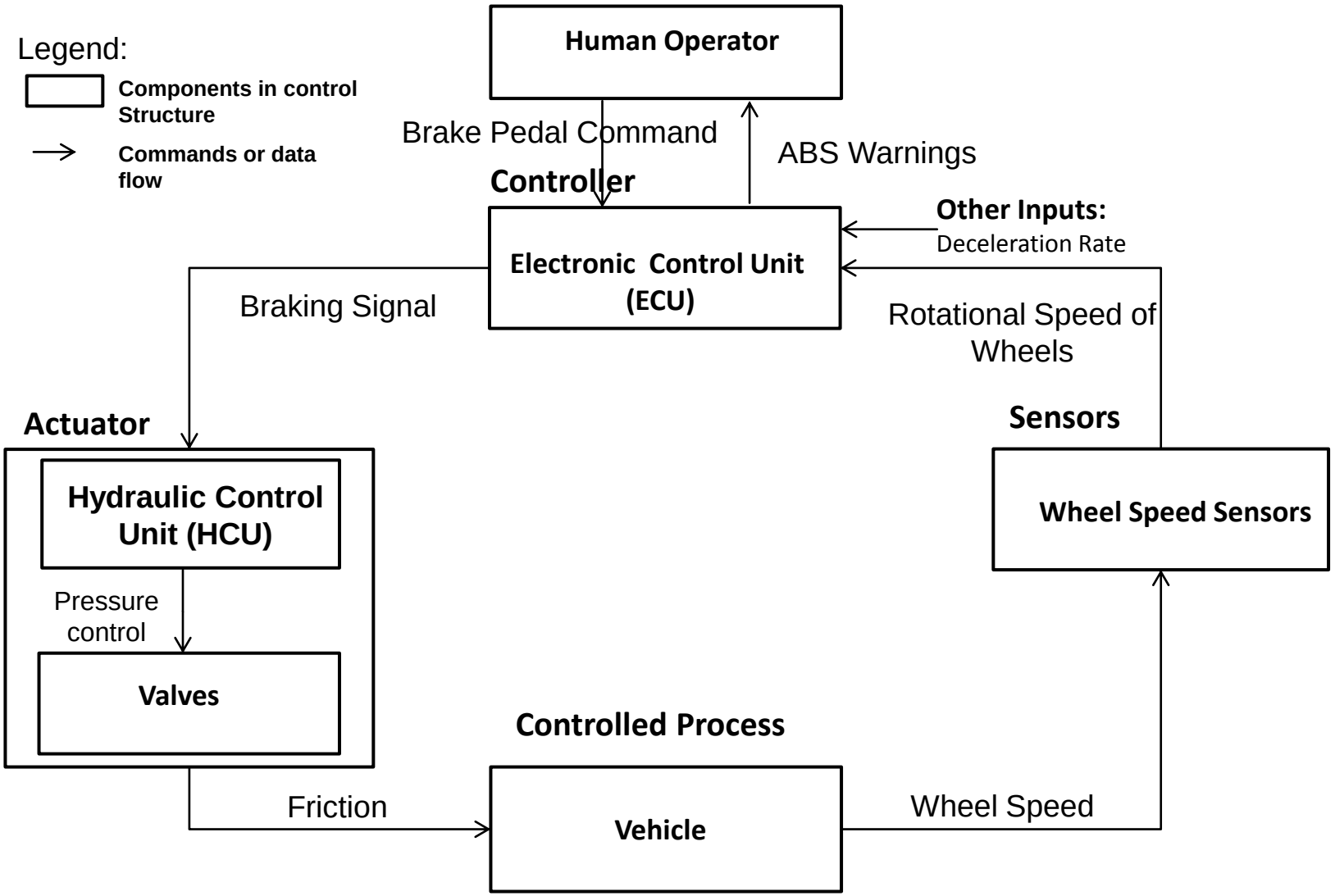




Source http://www.pakwheels.com

Unsafe Control Actions (UCAs)

Unsafe Control Action: Brake event applied but not received by ABS



Unsafe Control Actions (UCAs)

- **Examples of potentially inadequate control actions of ABS system:**

Control Actions	Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped too soon
Brake Pedal Command	Brake event applied but not received by ABS [H.1]	Brake event is too short	Brake event provided too late	Brake event stopped too soon

I must evaluate each row to determine whether it is a hazardous state, but how?

You can assess them based on timing information, but what about other factors such as the states of the system?

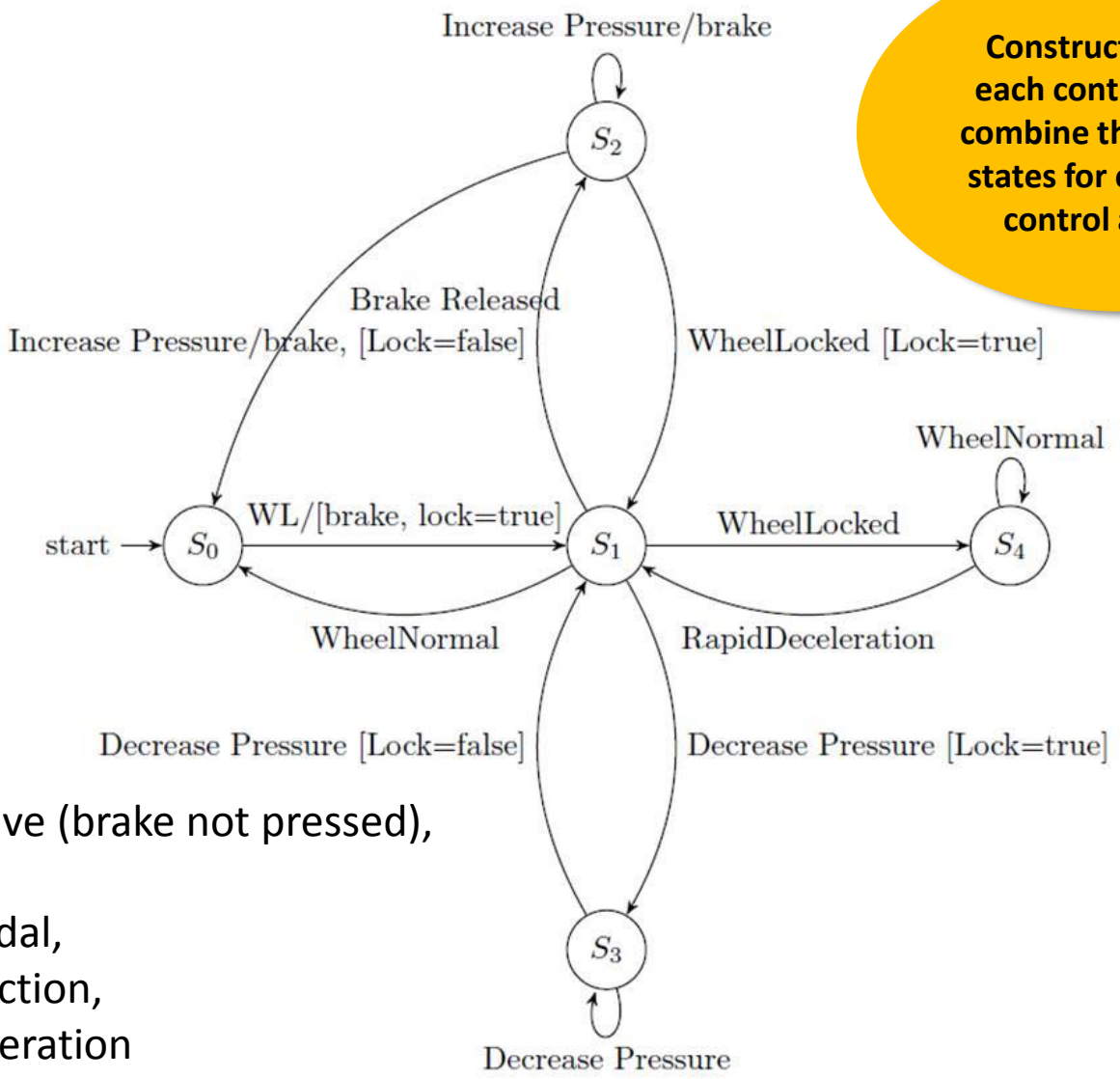
FSM Construction

- **In ABS example:**
  - ECU controller has four operating modes: **Inactive, handleLock, applyBrakePedal** and **reducePressure.**
  - Valve component has three modes**: open, block** and **release.**
  - HCU actutor has three modes: **Inactive, stopPump** and **openPump**.

How to evaluate the control action whether it leads to hazard or not by considering all potential combinations of relevant states?

FSM can be used to determine the system states that affect the safety of the control action

FSM Construction of Controller (ECU)



Construct FSM for each controller and combine the relevant states for evaluating control actions.

Where: S0 = inactive (brake not pressed),
S1=handlelock,
S2= applyBreakPedal,
S3= pressureReduction,
S4= MonitorDeceleration
and WL= WheelLocked.

The Extend Control Actions Table of UCA 1.

The control action table for the brake pedal command **based on the potential combination of system states.**

Control Actions	Wheel Status	Wheel Speed	Valve Status	Hazardous?
Brake Pedal Command	Locked	slow	open	Yes
Brake Pedal Command	Locked	fast	open	Yes
Brake Pedal Command	Locked	slow	close	No

E.g. Unsafe Control Action:

If we consider *the brake pedal command* that can be a hazardous control action, it consists of the values of the following process model state variables:

- ✓ The brake pedal is pressed.
- ✓ Valve is open.
- ✓ Wheel is locked.
- ✓ The wheel speed exceeded a preset maximum level.

E.g. Refine Safety Constraints: When brake pedal is pressed, the status of wheel lock should be false, the status of valve should be closed and the wheel speed should not exceed a preset maximum level.

The End…

Thank You!