STPA-based Method to Identify and Control Software Feature Interactions

John Thomas
Dajiang Suo

Quote

- “The hardest single part of building a software system is deciding precisely what to build.”

  -- Fred Brooks, *The Mythical Man-Month*

Quote

- "The hardest single part of building a software system is deciding precisely what to build. No other part of the conceptual work is as difficult as establishing the detailed technical requirements … No other part of the work so cripples the resulting system if done wrong. No other part is as difficult to rectify later."

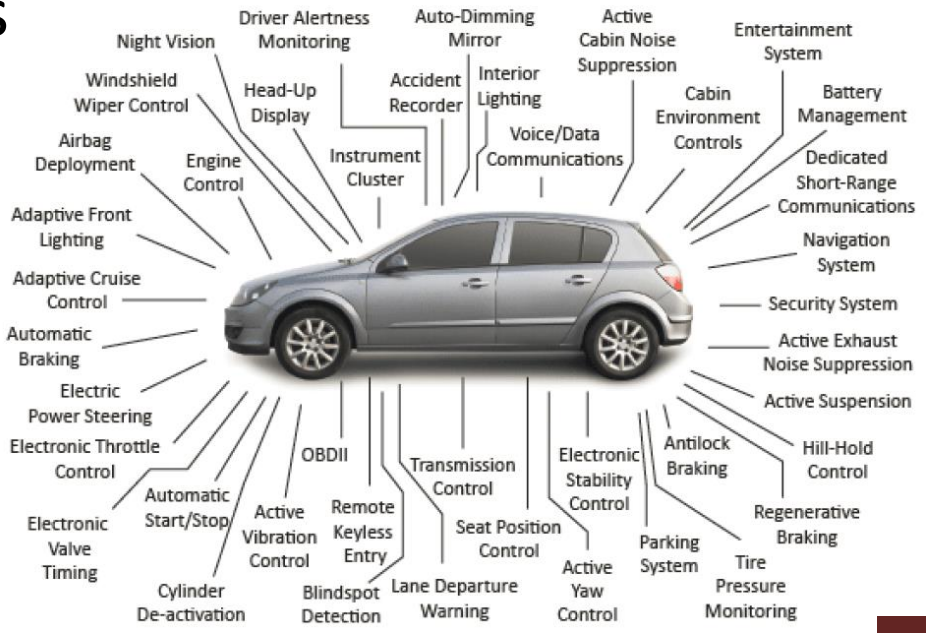
  -- Fred Brooks, *The Mythical Man-Month*

Project Overview

Goal: Integrate multiple advanced driver assistance features into one vehicle.

Problem: These control systems (features) may interact in dysfunctional or unexpected ways

- Large numbers of systems
- Emergent behavior:
  - Difficult to predict
  - Can lead to undesirable vehicle behavior



(Hommes, 2012)

Project Scope

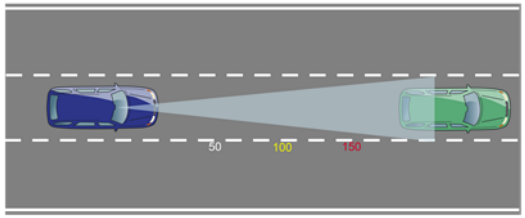
1) **Auto-Hold:** Automatic braking at stops

- Hold (or release) the brakes
- Increase the brake pressure

2) **Engine Stop-Start:** Reduce idling at traffic stops

- Shutoff the Engine
- Restart the Engine

3) **ACC w/Stop-Go:** Adaptive Cruise Control at all speeds



- Accelerate
- Brake

Project Scope

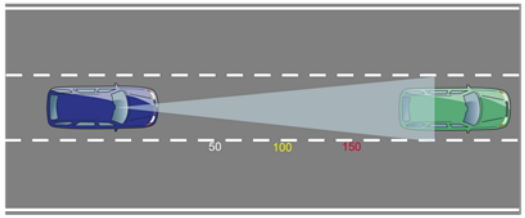
4) Shift by wire: Computer-controlled shifting

- Carry out driver shift requests
- Some automated behavior

5) Keyless ignition: Enable start when keyless remote is present

- Start vehicle
- Stop vehicle

6) Emergency Braking Assist: Automatic braking to avoid collision



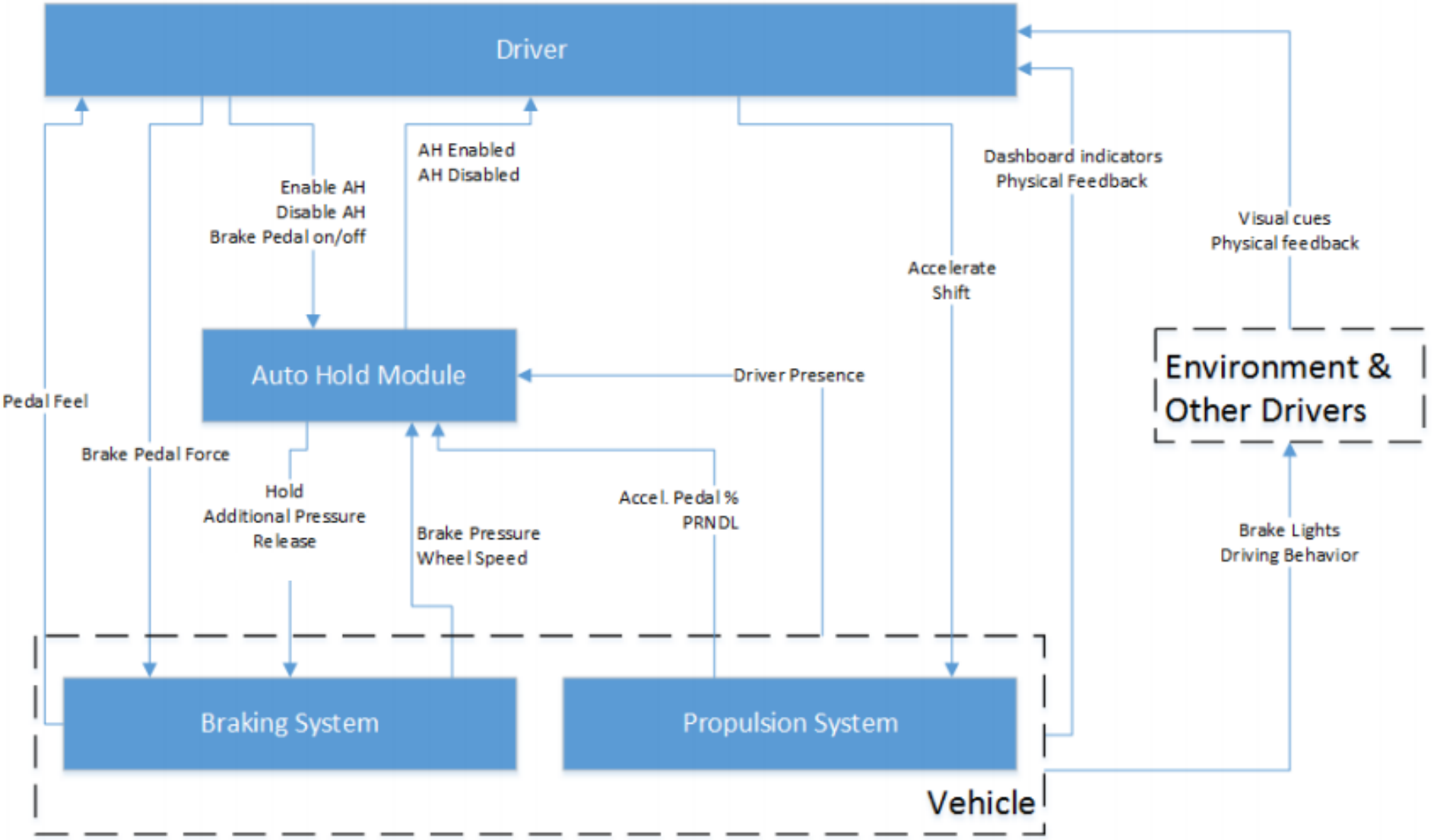
- Pre-charge
- Full Brake
- Release

Example: Automotive Auto-Hold

- If driver stops car and releases brake, car may roll
- Auto-Hold automatically applies brakes, prevents roll

Images: http://my.vw.com/2012-cc/performance/auto-hold
http://mlouisalocke.files.wordpress.com/2011/07/california_street_with_cable_car_san_francisco_california_1901.jpg

Control Structure



STPA Step 1: Unsafe Control Actions (UCA)

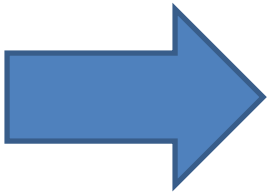
	Not provided causes hazard	Provided causes hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied too long
Hold Command	UCA-AH-1: Not providing HOLD when AH is on and driver stops vehicle with the brakes [G-1,2]	UCA-AH-2: Providing HOLD when driver is applying the accelerator [G-1] UCA-AH-3: Providing HOLD when AH is DISABLED [G-1] UCA-AH-4: Providing HOLD when vehicle is not at rest [G-1] UCA-AH-5: Providing HOLD when driver is not applying brake [G-1,2]	UCA-AH-6: Providing HOLD if the required time at rest has not been met [G-1]	N/A

Creating initial controller constraints

Unsafe Control Actions	Constraints
UCA-AH-1: Not providing HOLD when AH is on and driver stops vehicle with the brakes [G-1,2]	AH must provide HOLD when AH is on and driver stops vehicle with the brakes [G-1,2]
UCA-AH-2: Providing HOLD when driver is applying the accelerator [G-1]	AH must not provide HOLD when driver is applying the accelerator [G-1]
UCA-AH-3: Providing HOLD when AH is DISABLED [G-1]	AH must not provide HOLD when AH is disabled [G-1]
UCA-AH-4: Providing HOLD when vehicle is not at rest [G-1]	AH must not provide HOLD when vehicle is still moving [G-1]
UCA-AH-5: Providing HOLD when driver is not applying brake [G-1,2]	AH must not provide HOLD when brake pedal is not depressed [G-1,2]

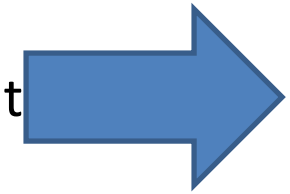
STPA Step 2: causal scenarios

- UCA-AH-8: Additional Pressure command is not provided when in hold mode and vehicle is slipping
  - What could cause this?
  - AH software believes vehicle is stationary (process model flaw) because rate of vehicle movement is too slow to detect (inadequate feedback)
  - Etc.



Requirements

- Additional pressure command is provided but vehicle continues moving (cmd not effective)
  - Why wouldn't the command be effective?
  - Powertrain is providing torque (forward or backward), counteracting braking force
  - Hydraulic pump fails, is delayed, has reached limit or has insufficient electric power
  - Etc.



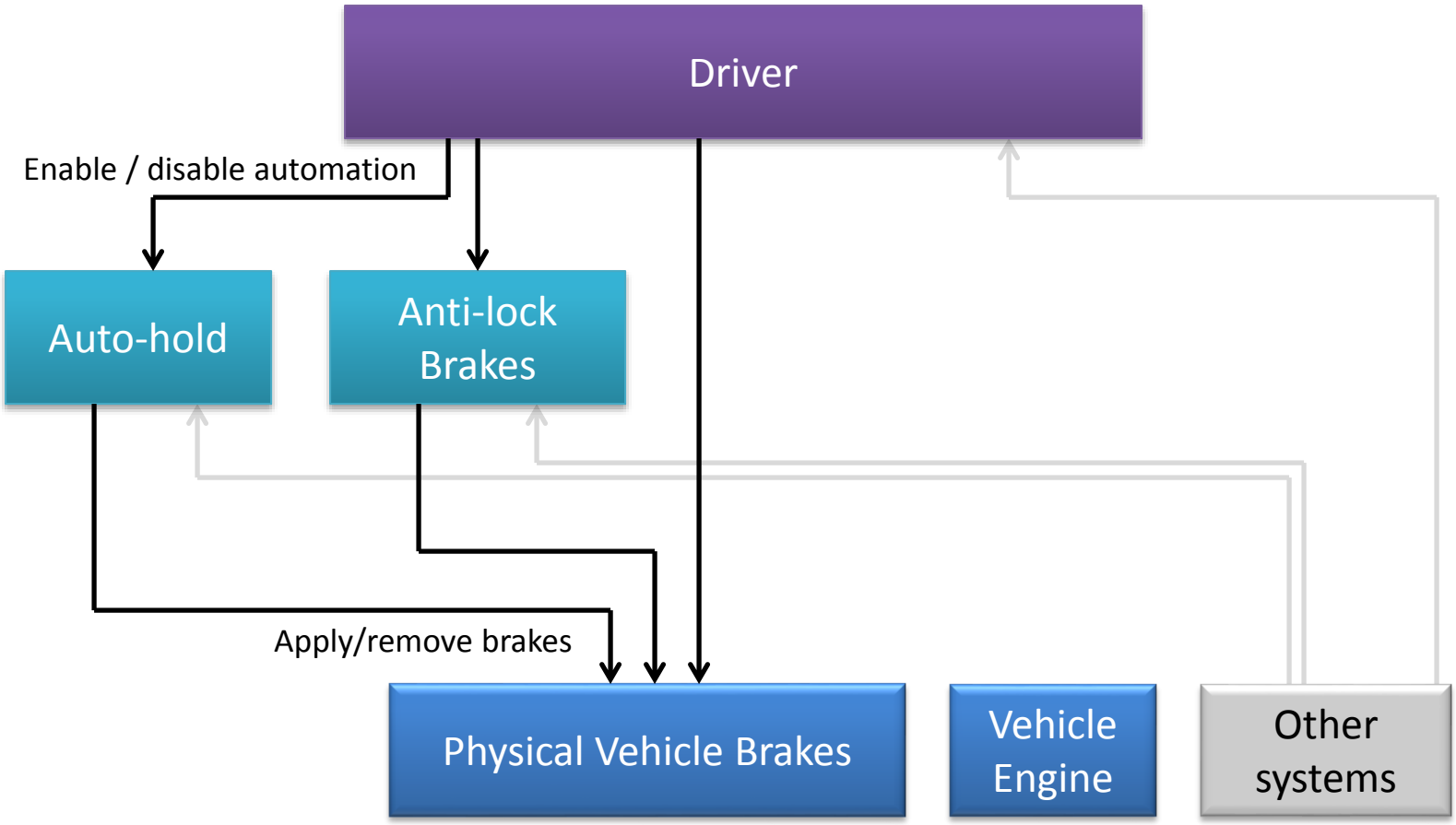
Requirements

Individual Analysis Summary

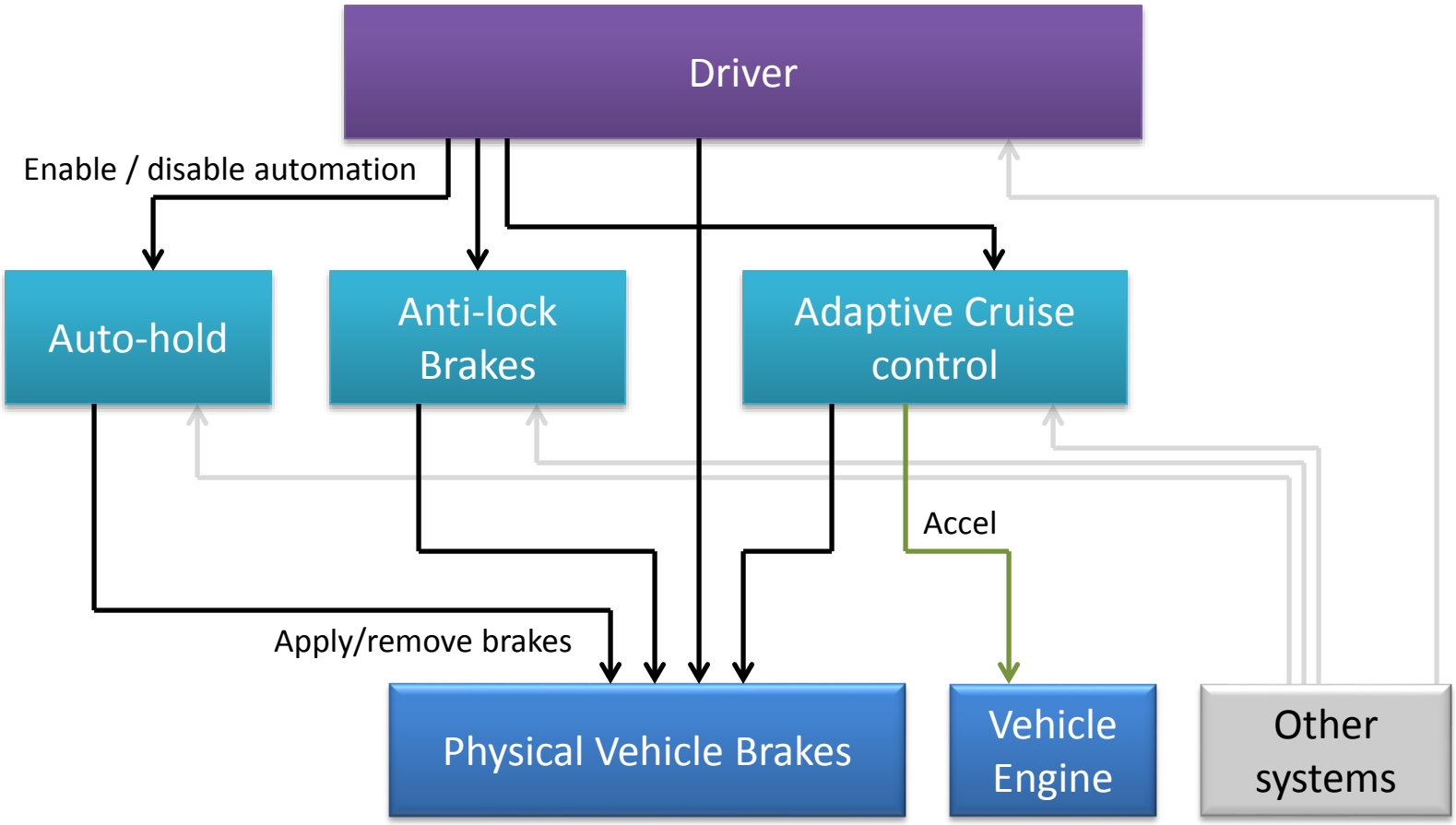
- Analyzed the design of each controller, implemented individually
  - Systems were designed independently
  - Each works relatively well on its own (although some problems were found)

- What if the controllers are *integrated* on the same vehicle?
  - Could Engine Stop-Start controller interfere with ACC?
    - Both control the engine
  - How do ACC and Auto-Hold manage the brakes simultaneously?
    - 2 controllers, 1 process
  - How do the controllers respond during off nominal situations?
  - Can the controllers issue conflicting commands?

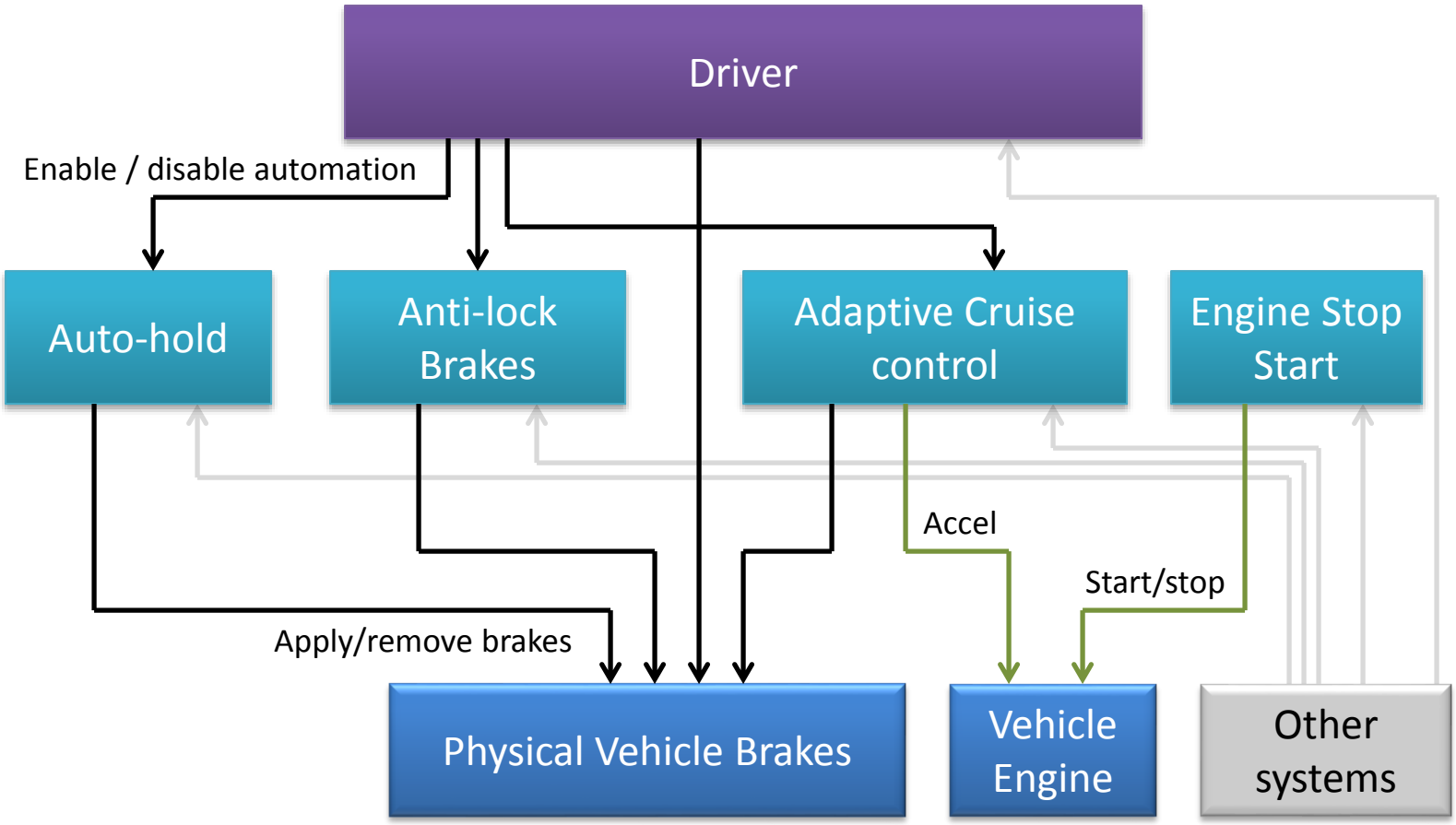
How to handle many controllers?



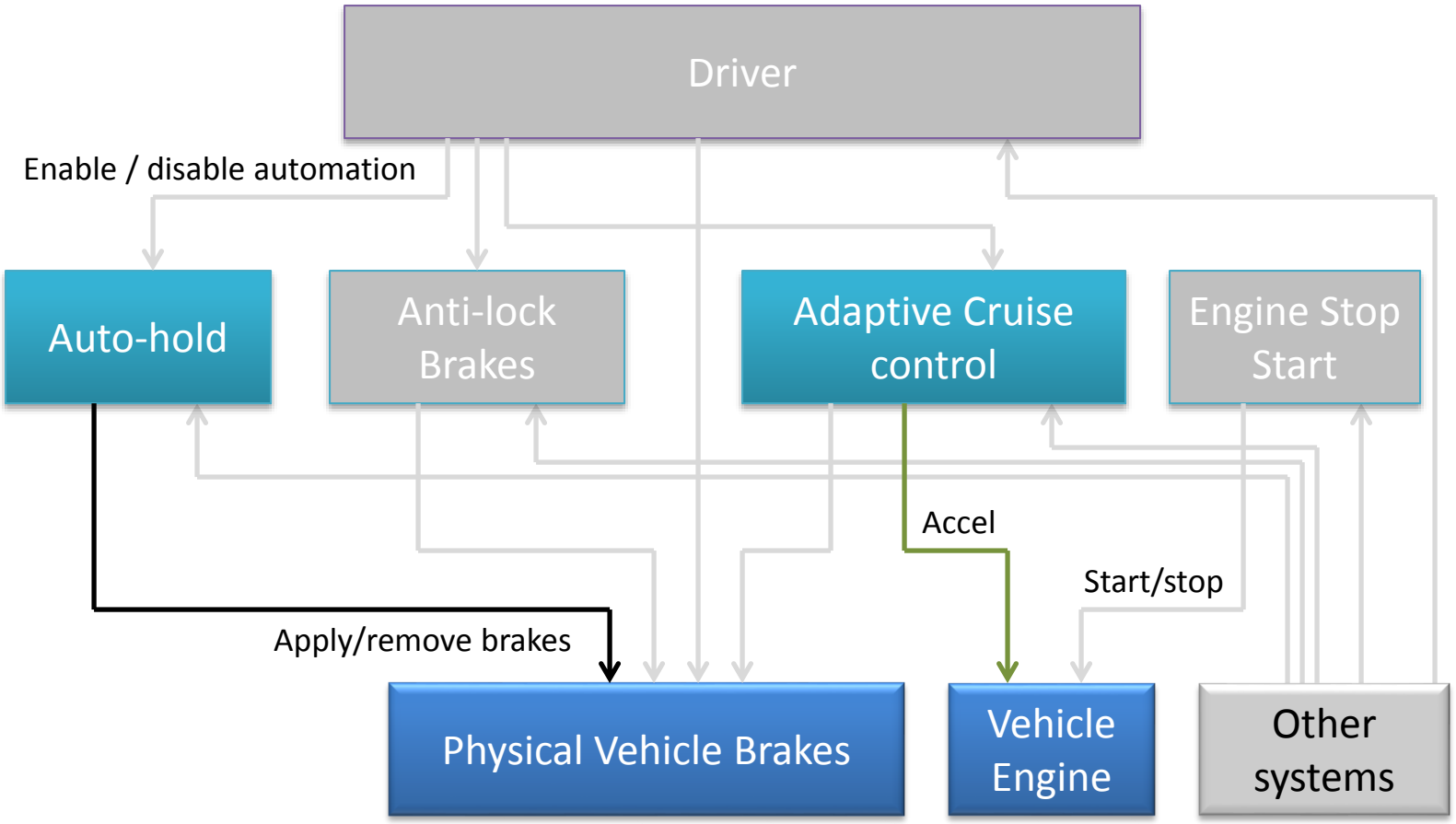
How to handle many controllers?



How to handle many controllers?



How to handle many controllers?

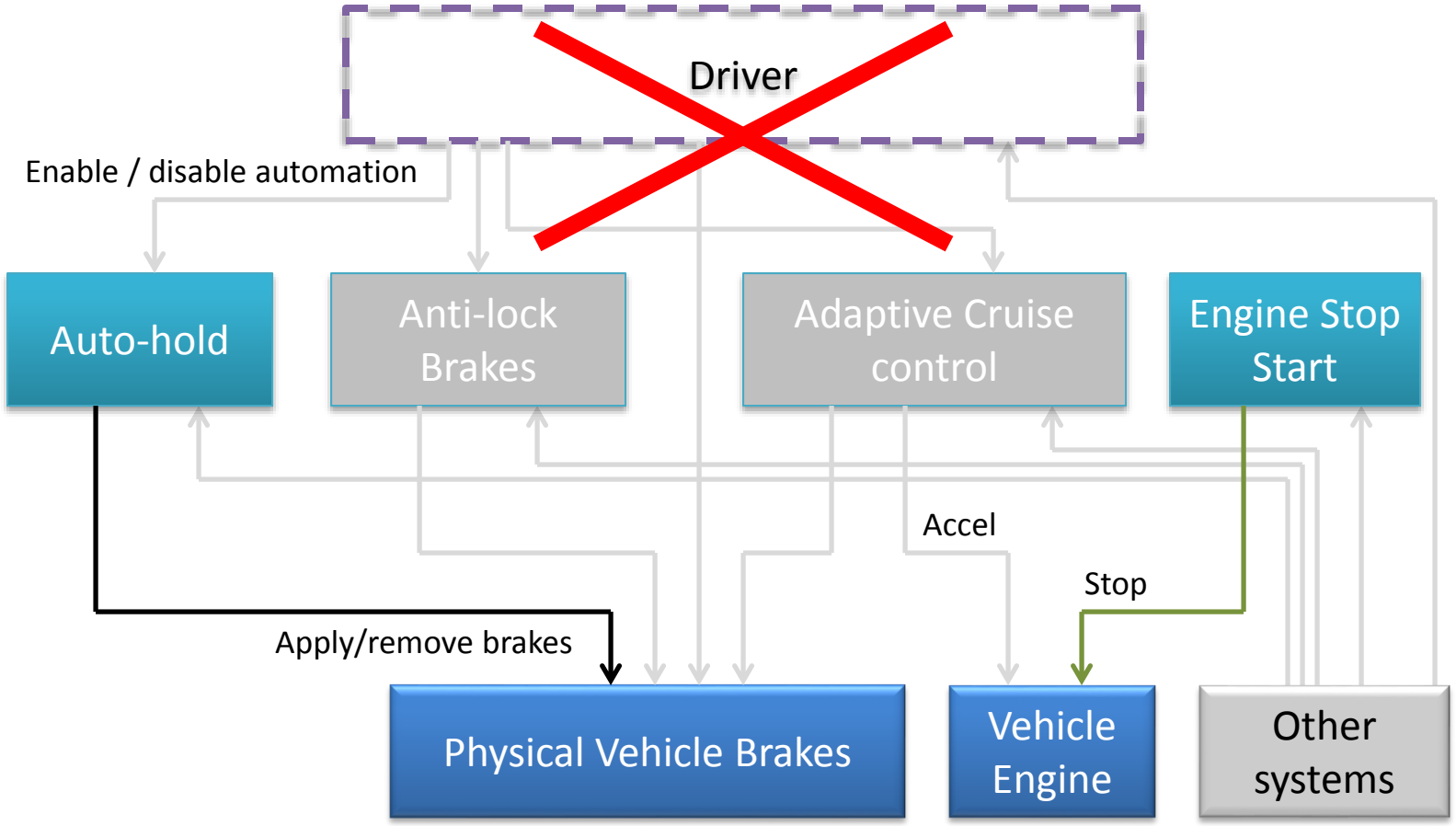


Example interaction:

Auto-hold applies brakes

ACC tries to accelerate

How to handle many controllers?



Example interaction:

Auto-hold applies brakes

Engine-Stop-Start turns engine off

Driver exits vehicle

Driver may be going to look under hood (so be careful starting engine)

Brute force approach (incomplete)

Brute Force Limitations

- Doesn't scale well
  - Growth rates:
  - $O(n^2)$ for 2 control actions (2-D matrix)
  - $O(n^3)$ for 3 control actions (3-D matrix)
  - $O(n^x)$ for X control actions
- Matrix includes all possible combinations
  - Bottom-up
  - Have to analyze everything, including many safe and acceptable scenarios
  - No way to do abstraction

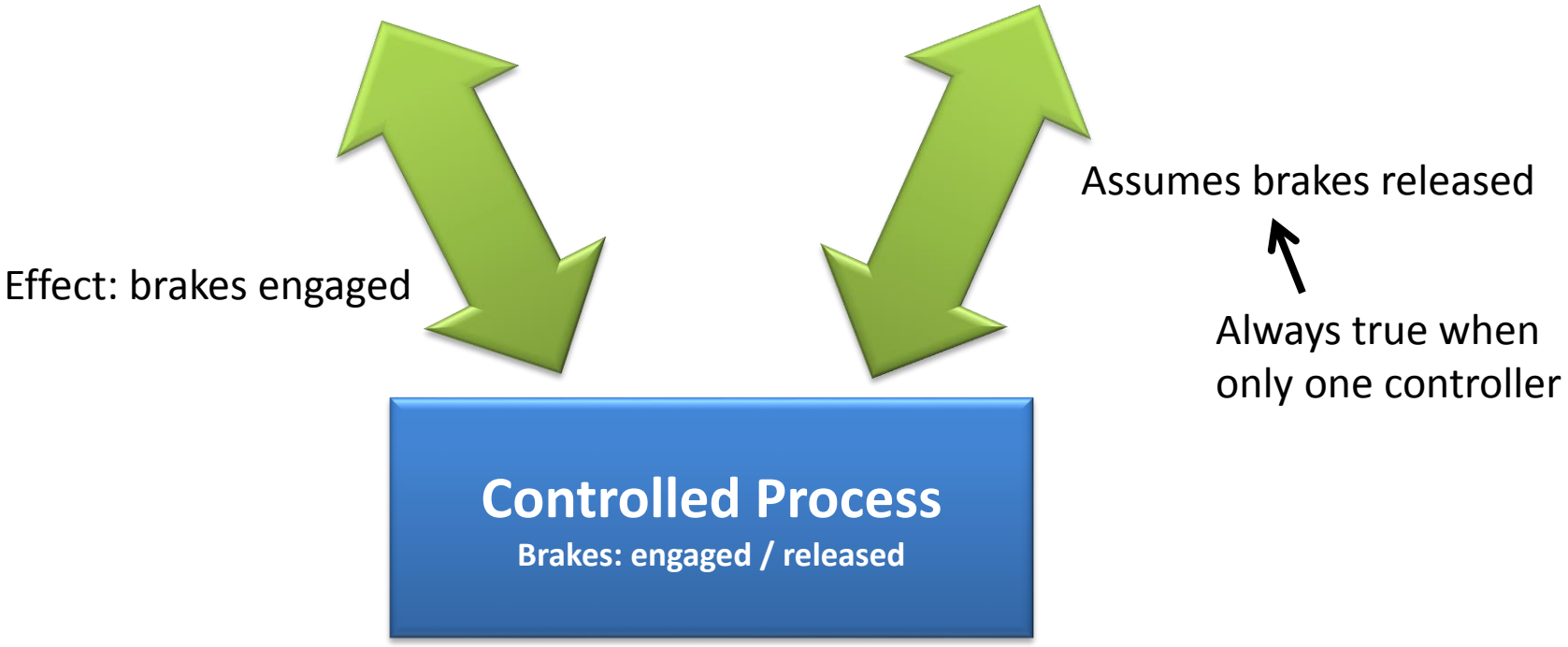
Understanding the Problem

Auto-hold:

- Applies brakes

Adaptive Cruise Control:

- Applies engine throttle



Control Actions and Conditions

	Auto-hold	Adaptive Cruise Control
Conditions assumed/required		
Control Action	Apply Brakes	Apply Engine Throttle
Conditions affected		

Control Actions and Conditions

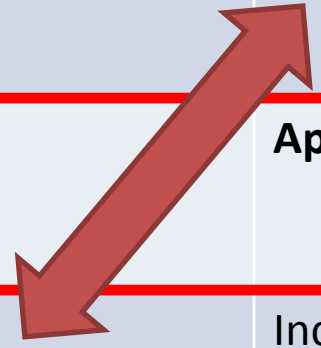
	Auto-hold	Adaptive Cruise Control
Conditions assumed/required	Wheels not rotating	
Control Action	**Apply Brakes**	**Apply Engine Throttle**
Conditions affected	Brakes engaged	

Control Actions and Conditions

	Auto-hold	Adaptive Cruise Control
Conditions assumed/required	Wheels not rotating	Brakes released
Control Action	**Apply Brakes**	**Apply Engine Throttle**
Conditions affected	Brakes engaged	Increased engine speed

Control Actions and Conditions

	Auto-hold	Adaptive Cruise Control
Conditions assumed/required	Wheels not rotating	Brakes released
Control Action	**Apply Brakes**	**Apply Engine Throttle**
Conditions affected	Brakes engaged	Increased engine speed



How could this combination happen?

- ACC stops on a hill following leading car, AH activates and engages brakes, leading car accelerates and ACC applies throttle to follow. AH detects wheel movement, assumes current brake force is insufficient, and automatically increases brake force.

New Approach

	AH			ESS		ACC w/SG		Driver	
	Hold	Release	AP	Engine start	Engine stop	Accel	Decel	Accel	Brake
Design assumptions / Conditions required to be effective	Car stopped; Battery power available; Little or no propulsion torque; Ability assume brake control	Driver present (to prevent rollback)	Battery power available; Little or no propulsion torque; AH controls brakes (AH in hold mode)	Battery power available; Engine off	Vehicle stopped	Propulsion ready (engine running, in gear); Brakes not applied	Battery power available; Ability to assume brake control; Little or no propulsion torque	Propulsion ready (engine running, in gear) Brakes not applied	Power available (power brakes); Little or no propulsion torque; Brake pedal connected
System states / conditions changed	AH controls brakes; Brakes applied; Brake pedal disconnected	AH releases brake control (brake pedal connected)	AH braking force increased	Electric power significantly reduced for 2s, power available after 2s (battery charging, power brakes, etc), Propulsion ready after 2s (engine running, idle propulsion torque),	ropulsion not eady (engine off, no propulsion torque); Limited attery power available	Increased propulsion torque	ACC controls brakes; Brakes applied; Brake pedal disconnected	Increased propulsion torque	Driver controls brakes; Brakes applied

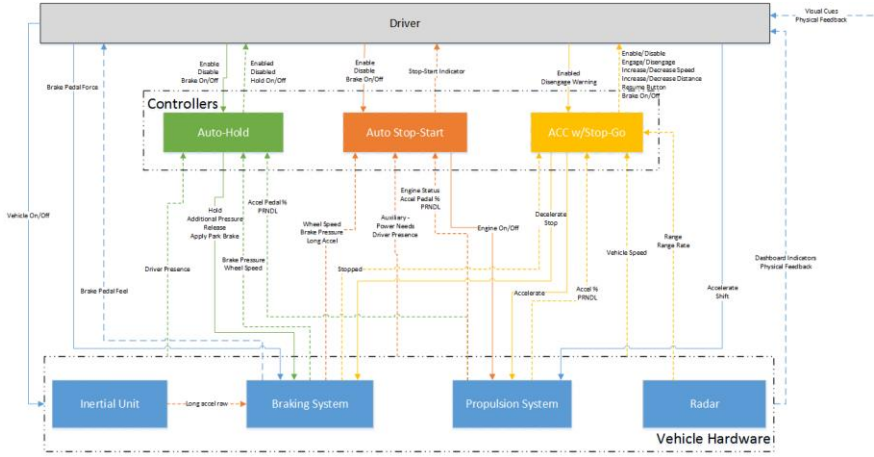
O(2n) – This is scalable!

New Approach

Stop-Start	Engine start	Engine stop	Etc.
Conditions Assumed / Required	**SS Enabled:** Yes ***AUTO-STOPPED*:** Yes **Vehicle Held:** Yes **Restart Possible:** Yes **Driver Present:** Yes **Range:** !=P **&** !=N	**Vehicle Held:** Yes **Wheels Rotating:** No **Restart Possible:** Yes **Auxiliary Power Needs:** Low **Driver Present:** Yes **Gas Pedal:** No **Range**: !=P,R,N	
Conditions Affected	**Engine:** On – power reduced temporarily **Idle Torque:** Yes ***AUTO-STOPPED*:** No	**Power:** Off **Idle Torque:** No ***AUTO-STOPPED*:** No	

Could be formalized to automatically identify conflicting interactions

Results 1



Control actions:

- Auto-Hold applies the parking brake
- ACC attempts to accelerate

Problems/Conflicts:

- ACC does not have the authority to dis-engage the EPB
- Auto-Hold attempting to secure the vehicle while it's held by ACC

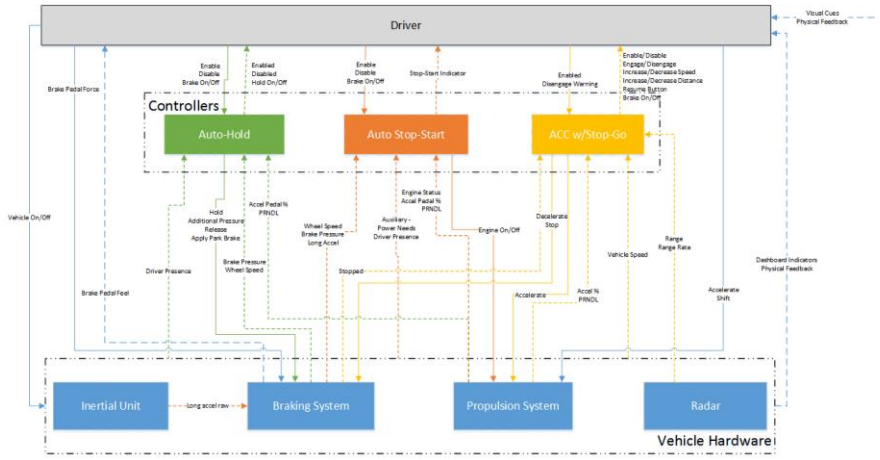
Potential Solutions :

- R-1: ACC may disengage EPB
- R-2: ACC may monitor the state of the EPB
- R-3: EPB may monitor the state of ACC
- R-4: Issuing the EPB turns the features 'off'
- R-5: Auto-Hold could be disabled when ACC is active (ACC can hold car at stop)

Results 2

Context:

- AH is holding brakes on hill
- Battery charge is low (but sufficient for restart)
- ESS turns engine off to save fuel
- Reduced torque causes vehicle to move



Controller Response:

- AH attempts to increase brake pressure
- Stop-Start attempts to start vehicle

Problem:

- Battery voltage drops, vehicle starts but cannot increase brake pressure for 2s

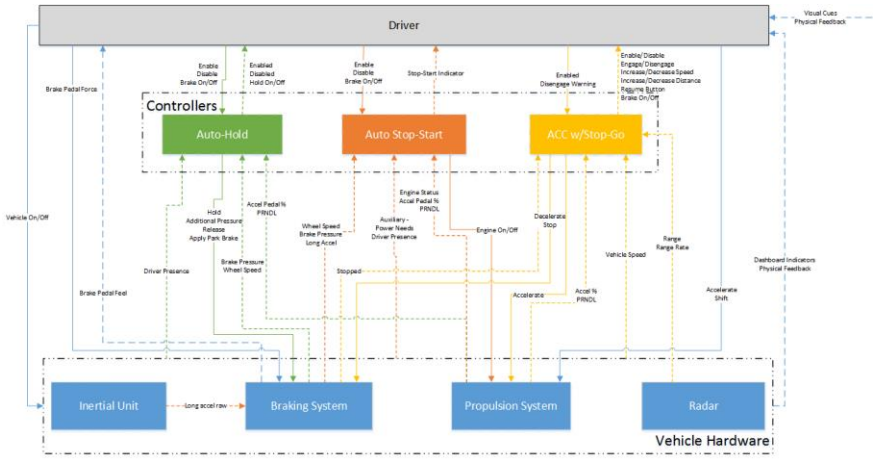
Potential Solutions / Requirements:

- R-1: AH pump must operate at a low battery voltage
- R-2: ESS must warn AH so pressure can be increased before engine turns off
- R-3: Battery threshold must be sufficient to guarantee simultaneous restart and brake pump

Results 3

Context:

- Auto-Hold is holding vehicle
- ESS stops engine to save fuel
- Driver shifts to reverse
- Driver steps on gas to back up



Problem:

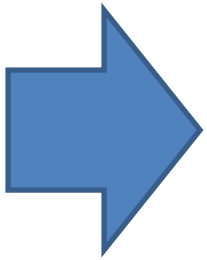
- ESS cannot *Start* the engine (prevented by FMVSS 102)
- AH cannot *Release* (insufficient engine torque)

Potential Solutions / Requirements?

Scalability

How well does this scale to larger systems?

- Adaptive Cruise Control
- Engine Stop-Start
- Auto-hold



- Adaptive Cruise Control
- Engine Stop-Start
- Auto-hold
- Keyless ignition
- Shift by wire
- Emergency Braking

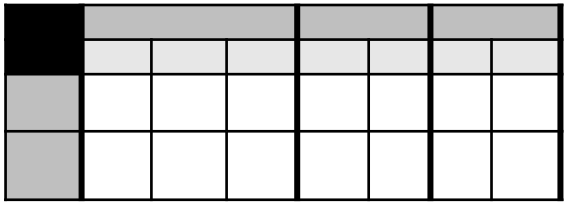
New Approach

	SBW			EBA		Keyless Ignition	
	Park	Neutral	Drive	Full Brake	Release	Engine start	Engine Stop
Design assumptions / Conditions required to be effective	Car stopped; Battery power available; Little or no propulsion torque	Battery power available; Driver present (to prevent rollback); Little or no propulsion torque	Battery power available; Little or no propulsion torque; Driver present (to control acceleration)	Battery power available; Ability to assume brake control; little or no propulsion torque	Vehicle held; driver present (to control brake)	Engine off; Battery power available; Driver present (fob); propulsion disconnected	Vehicle stopped; engine on
System states / conditions changed	Propulsion disconnected; vehicle held	Propulsion disconnected; vehicle not held	Propulsion connected; vehicle not held	Brakes applied; EBA controls brakes	Brakes not applied; EBA releases brake control	Electric power significantly reduced for 2s, power available after 2s (battery charging, power brakes, etc), Propulsion ready after 2s (engine running, idle propulsion torque),	Propulsion not ready (engine off, no propulsion torque); Limited battery power available

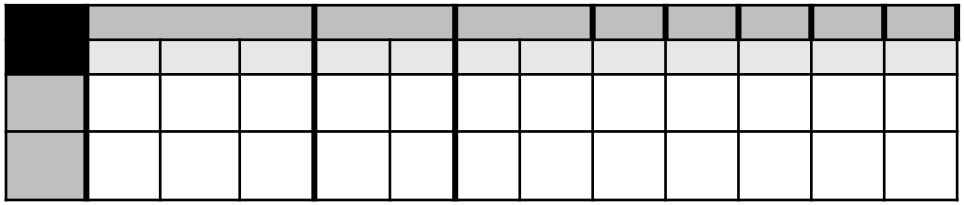
O(2n) – This is scalable!

Scalability of STPA-based approach

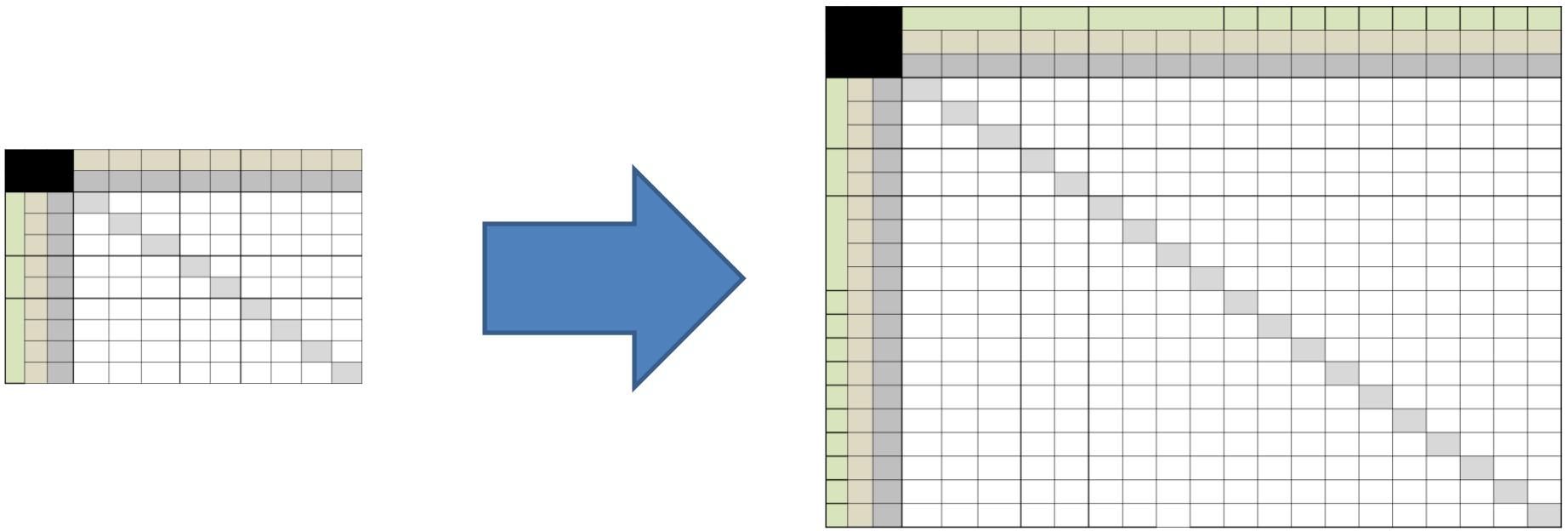
- 3 controllers



- 6 controllers



Scalability of traditional approach



3 controllers

6 controllers

Summary

- Provides a way to analyze interactive effects
  - Can be automated
- Scalable to very complex systems, more than 2 control actions
- Can help identify unexpected system behaviors
- Can help generate requirements, check existing requirements
- Identify conflicts between goals or between requirements, make sure tradeoffs are conscious choice
- Leverages existing STPA analysis, requirements for independent systems