Applying STPA to Automotive Adaptive Cruise Control System

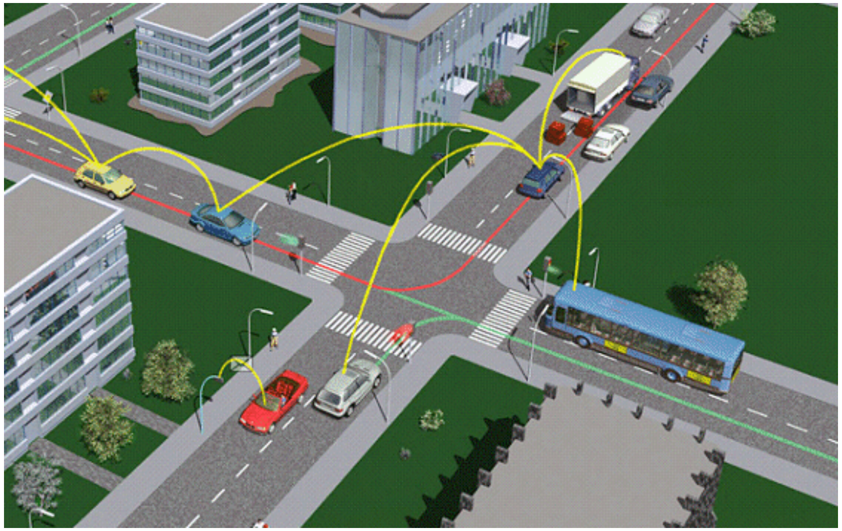
Dr. Qi Van Eikema Hommes
qhommes@mit.edu

April 18, 2012

Enhancing Automotive System Safety

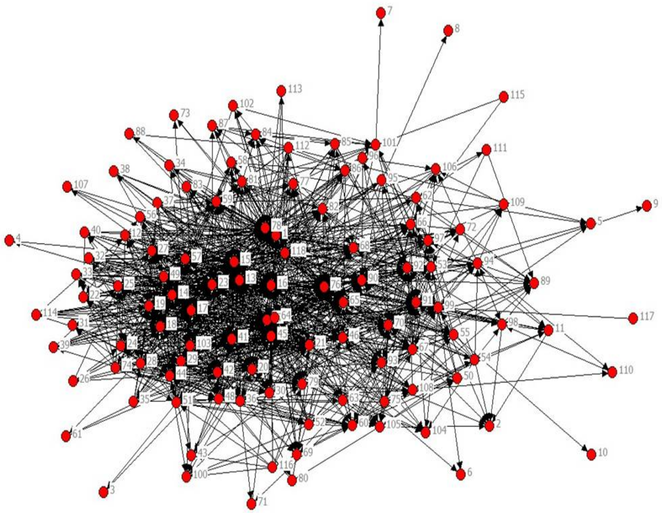
- Roadway and driver (1889 – 1960s)
  - Better roads, speed limit
  - Driver license 1913
  - Blaming the "nut behind the wheel"
- Vehicle design for crash survival and defective vehicle recalls (1960s – Today)
  - Blame the large automotive companies
  - NHTSA and Recall
  - Federal Motor Vehicle Safety Standards (FMVSS)
- Vehicle design for crash avoidance & driver override (Today and Tomorrow?)
  - http://www.cbc.ca/video/#/Shows/The_National/1242568525/ID=2210171357 (5'57" Mercedes, and 8'30" Lincoln parallel parking)

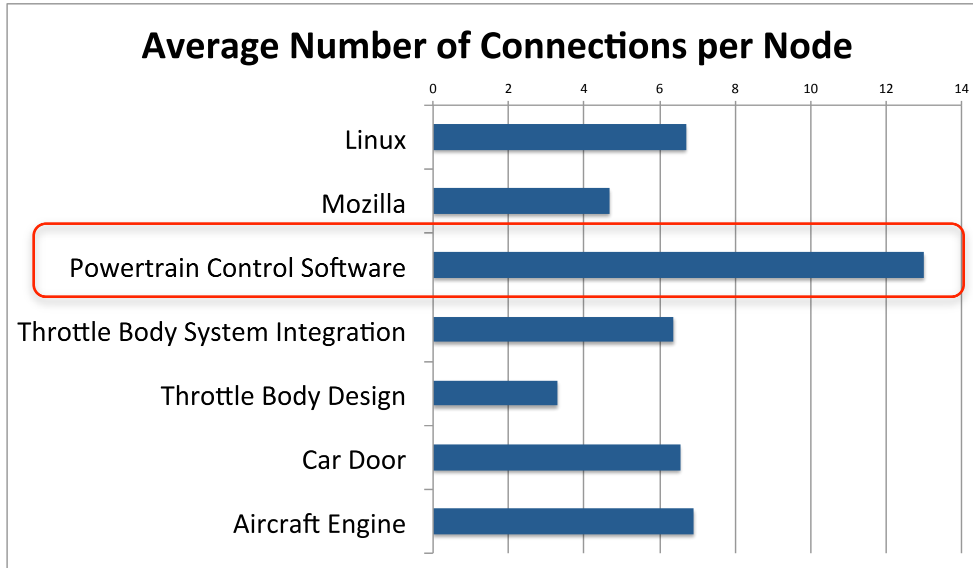
Automotive Systems Today and Tomorrow

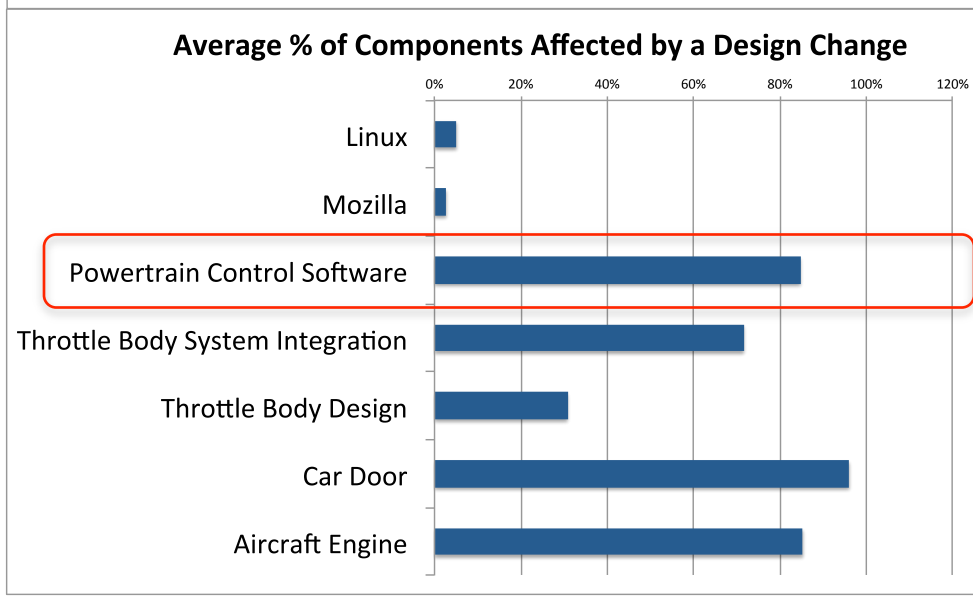


- **Cyber Physical Systems**- complex embedded devices networked to control physical hardware components.
- Software intensive.
- Automating many human tasks.
- The development teams are multidisciplinary and globally distributed.

The Powertrain Control Software System



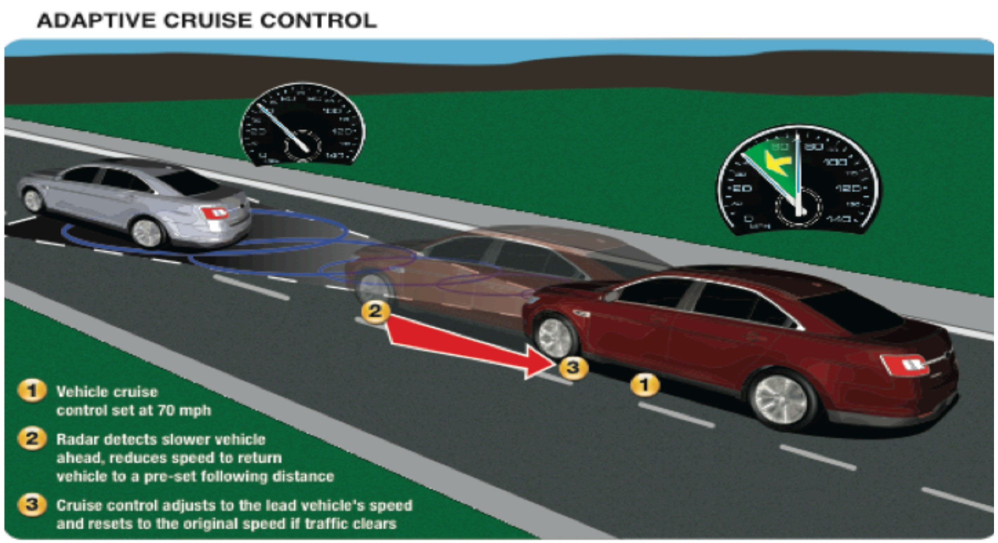


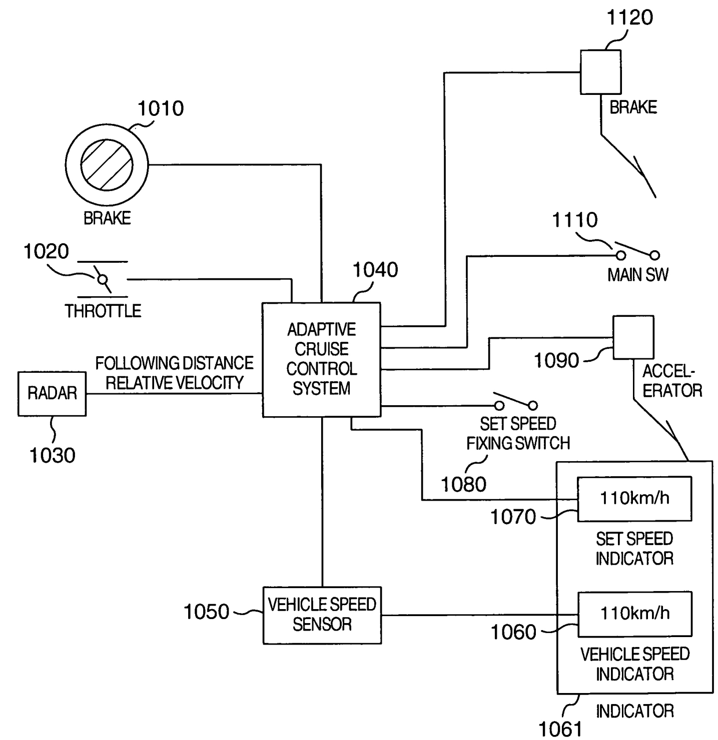


- 1 production-level software
- 117 software modules (red dots)
- 1423 interactions (black lines)
- 39 such production software releases per year
- <2 weeks per release

Hommes, DETC2008-DTM-49140

Adaptive Cruise Control Design





Hommes, IDETC 2012 - 70527

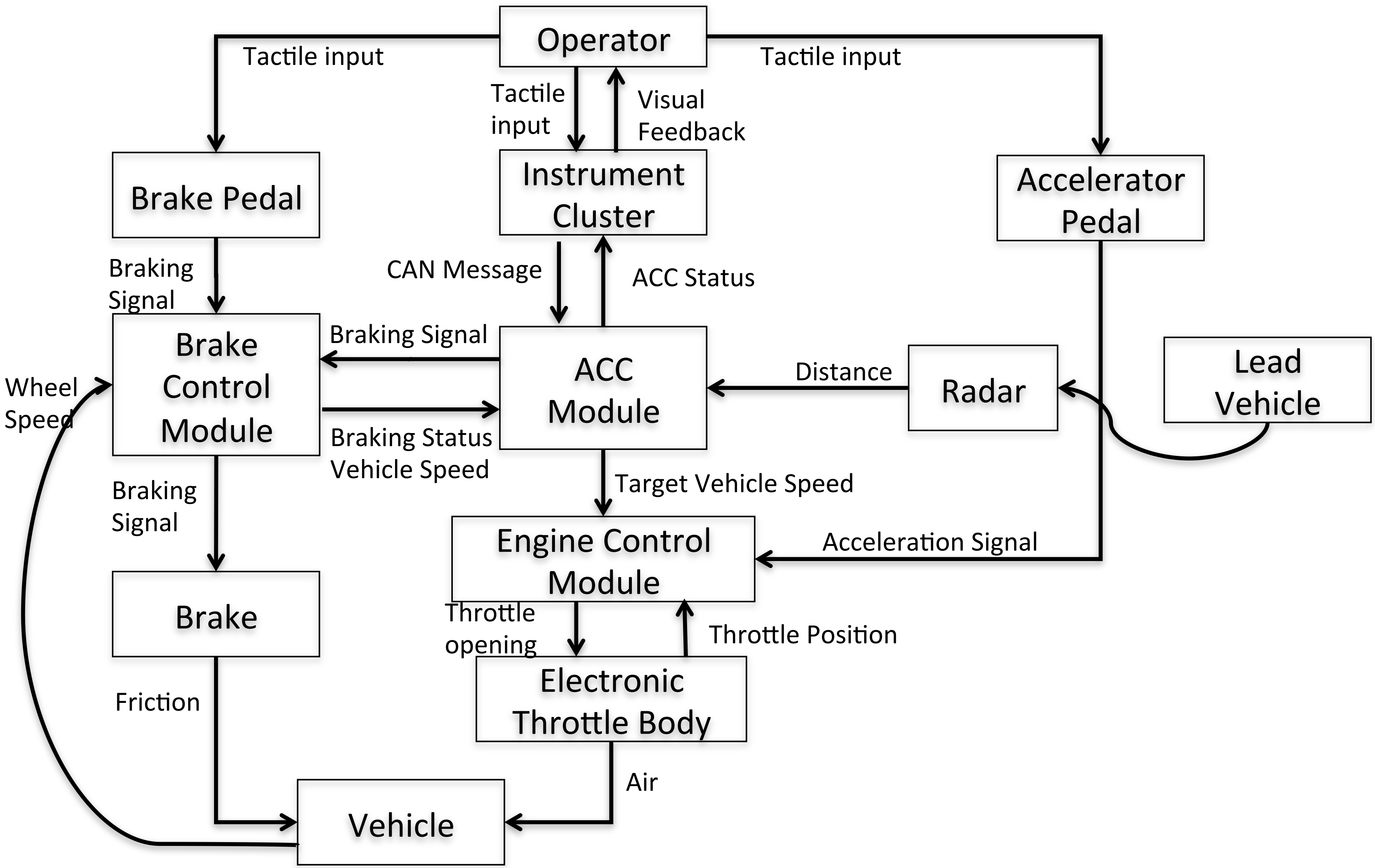
Accident, Hazard

- Accident: vehicle occupants are injured while ACC is engaged.
- Hazards:
  - H1: ACC did not maintain a safe distance from the object in the front, resulting in collision.
  - H2: ACC slows down the vehicle too abruptly, and vehicle is rear-ended.

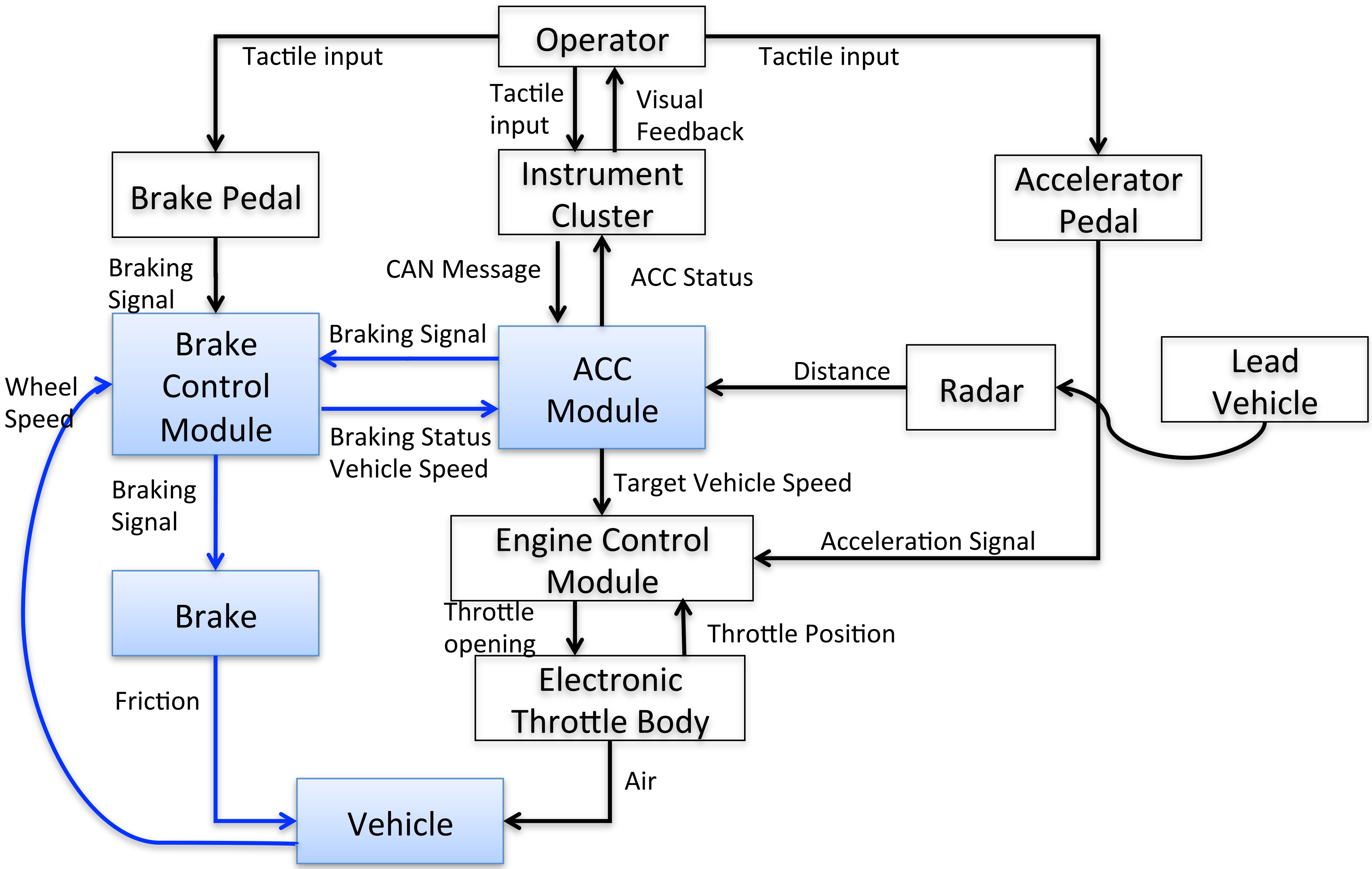
System Safety Constraints and Requirements

- Design constraints:
  - ACC should not let the vehicle gets in contact with the object ahead.
  - ACC should not brake too abruptly.
- Design requirements:
  - ACC shall maintain a TBD amount of distance between the vehicle and the object in front when engaged.
  - ACC shall limit vehicle deceleration to no more than TBD m/s^2.

Control Structure

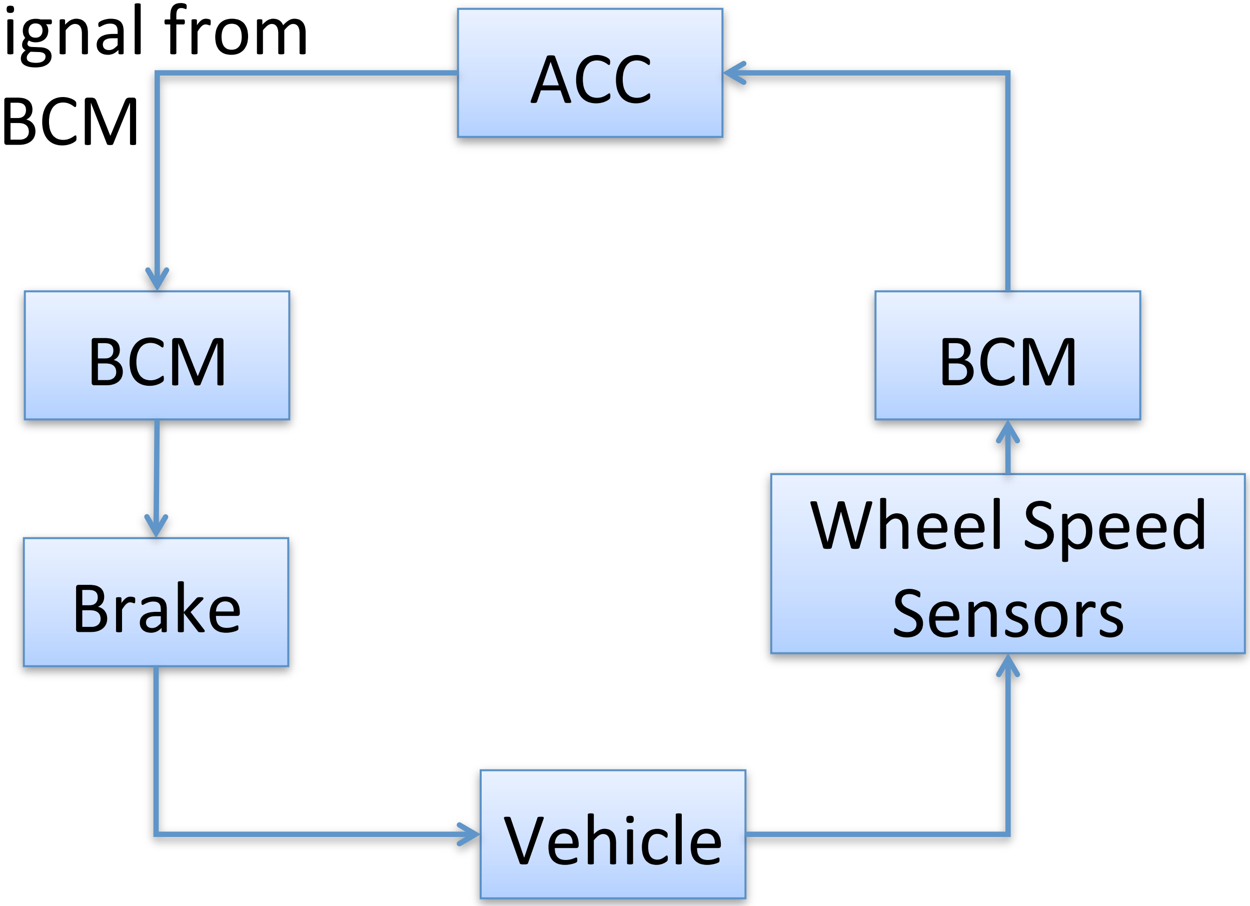


Example: ACC – BCM Control Loop



Reformatted Control Loop

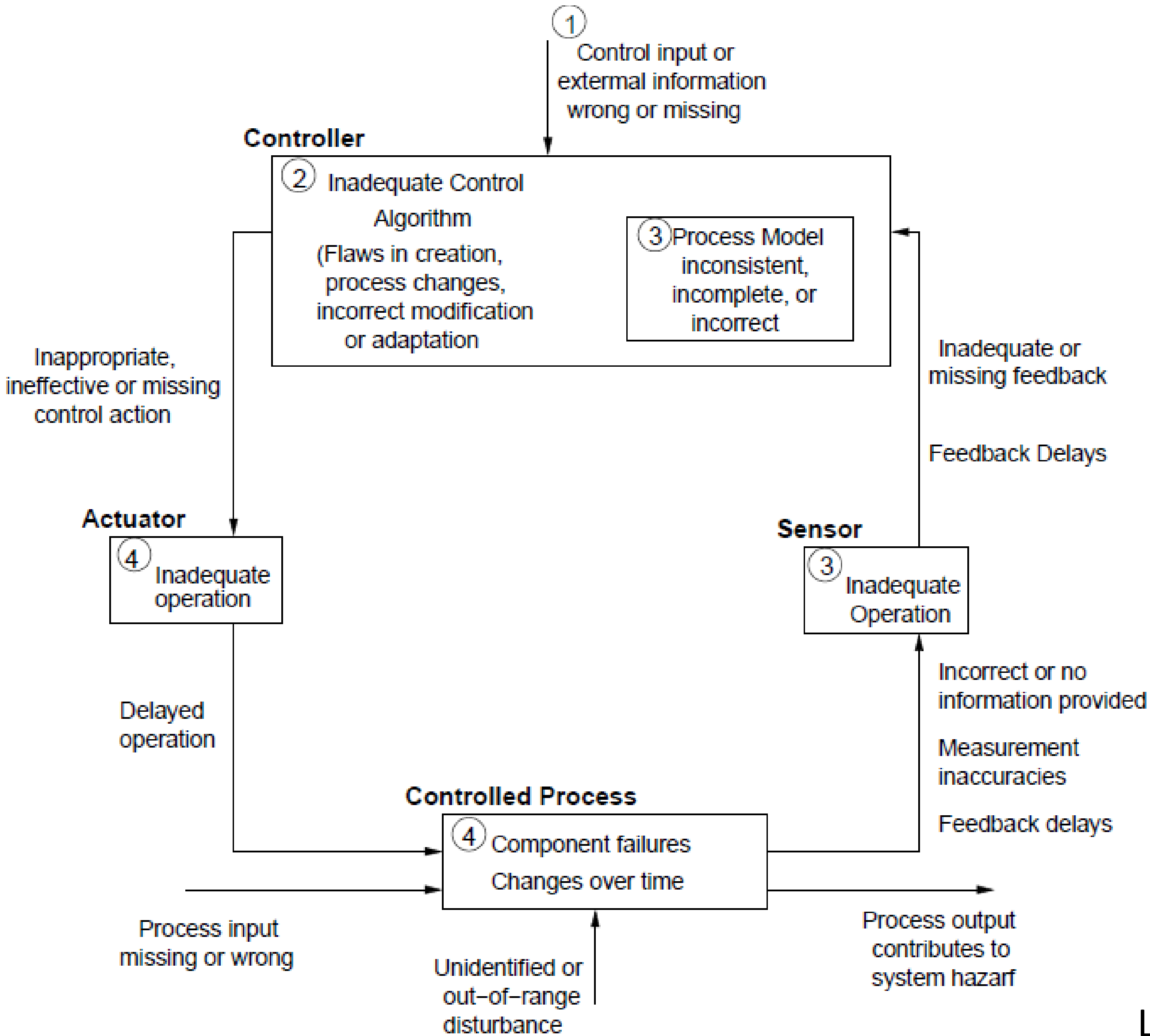
Control Action:
Brake Signal from
ACC to BCM



STPA Step 1: Unsafe Control Actions

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped too Soon or Applied Too Long
Brake Signal from ACC to BCM	Vehicle does not brake when the distance to the lead vehicle is less than the value set by the operator. (H1)	Commanded decceleration amount is too small when the vehicle is too close to the object in the front. (H1)	Braking is commanded too late when the distance to the lead vehicle is too close. (H1)	Braking stops before the safety distance between the vehicles are reached. (H1)
		Braking is commented when the distance to the lead vehicle is larger than the set value. (H2)		
		Braking is too fast/harsh when the didstance to the lead vehicle is less than the set value. (H2)		

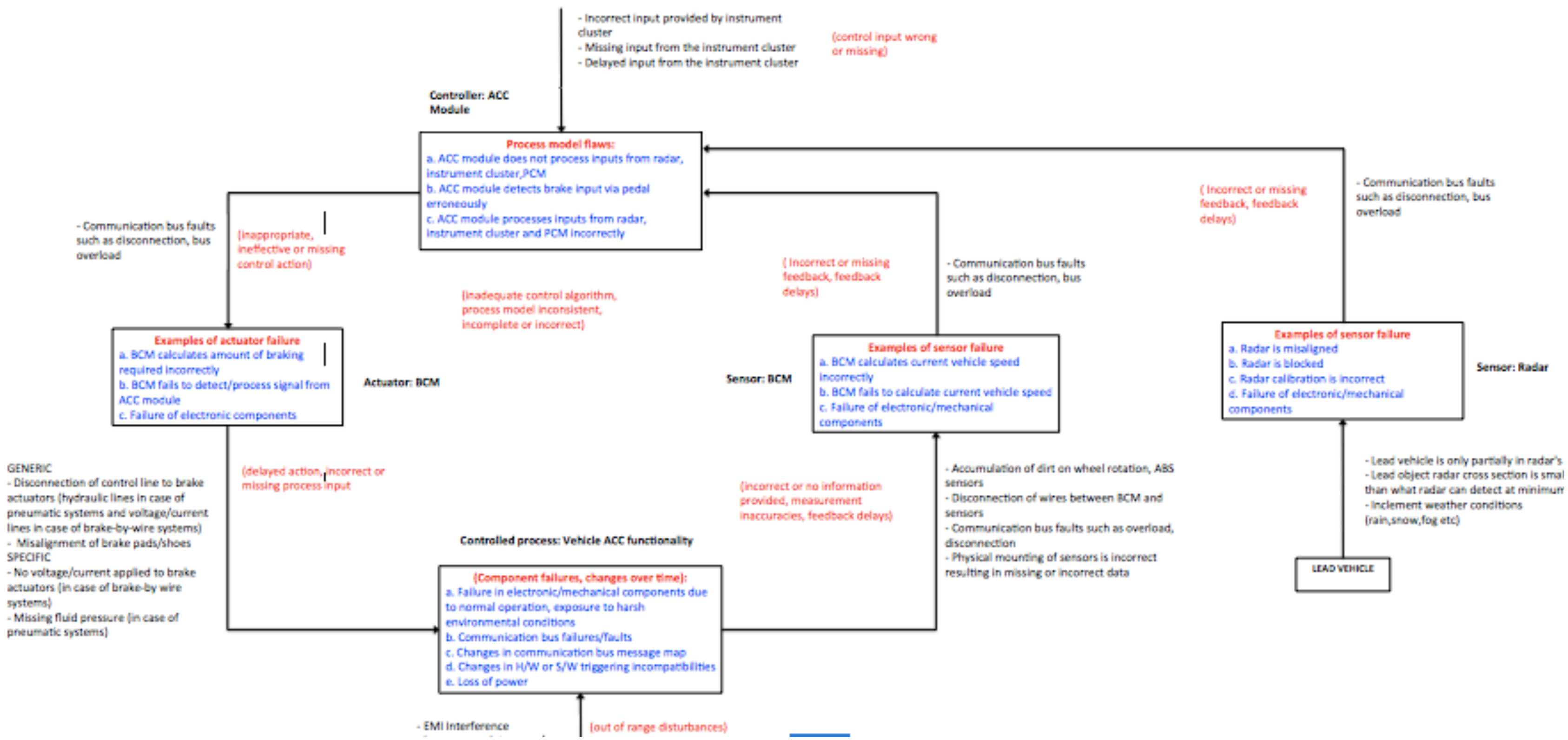
STPA Step 2: Causal Analysis with Guidewords



Leveson 2012

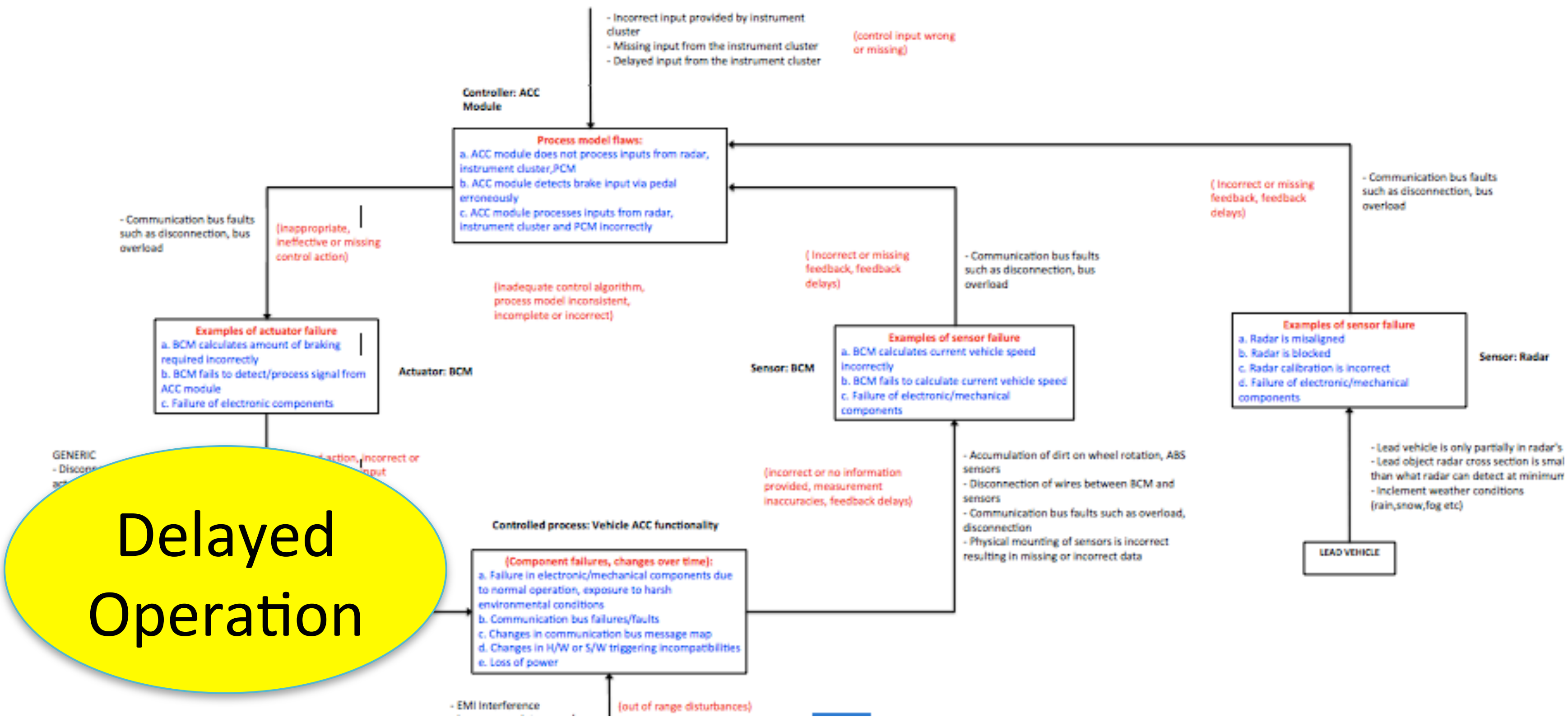
Causal Analysis Results

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.



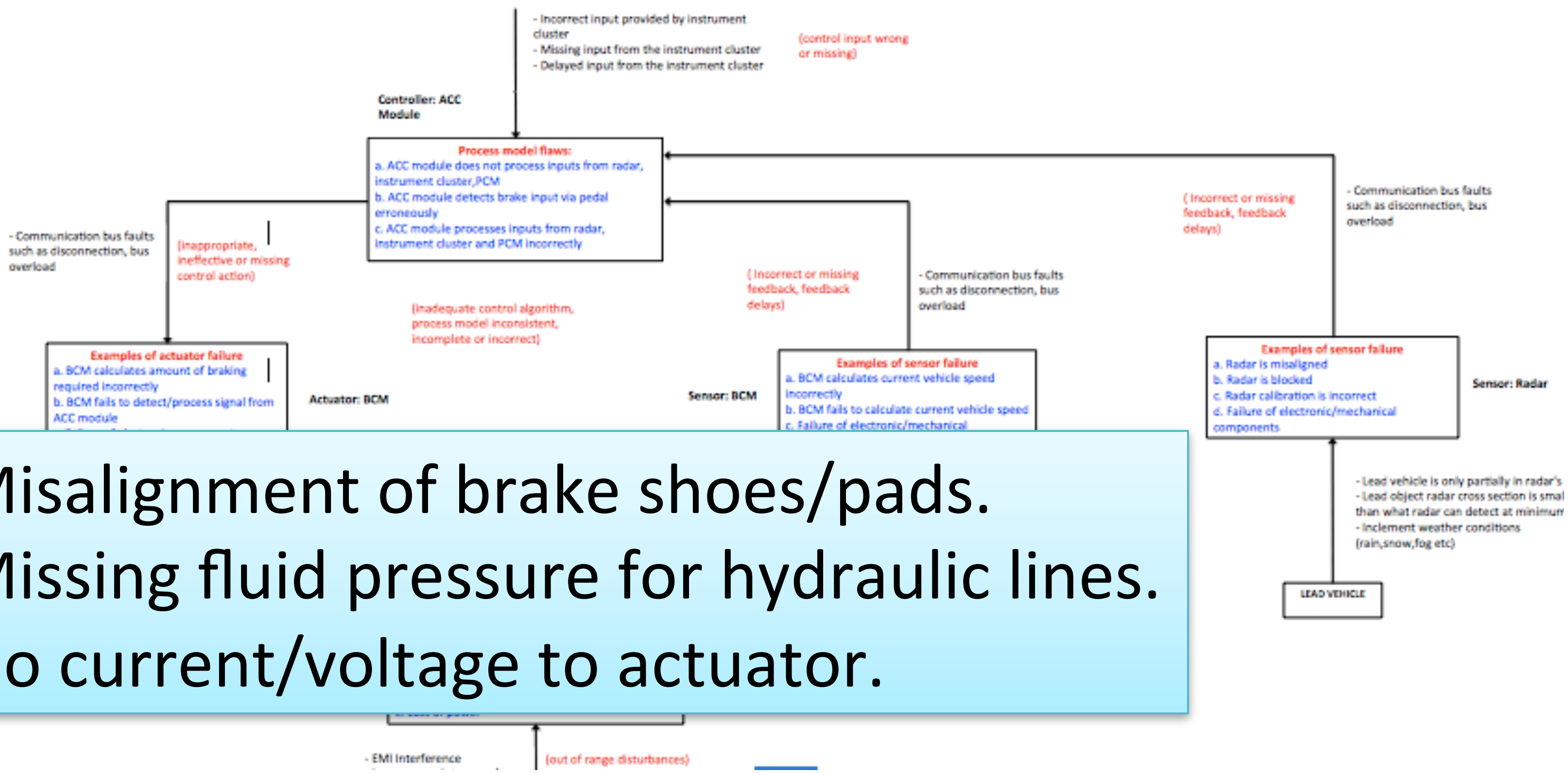
Causal Analysis Results (2)

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.



Causal Analysis Results (3)

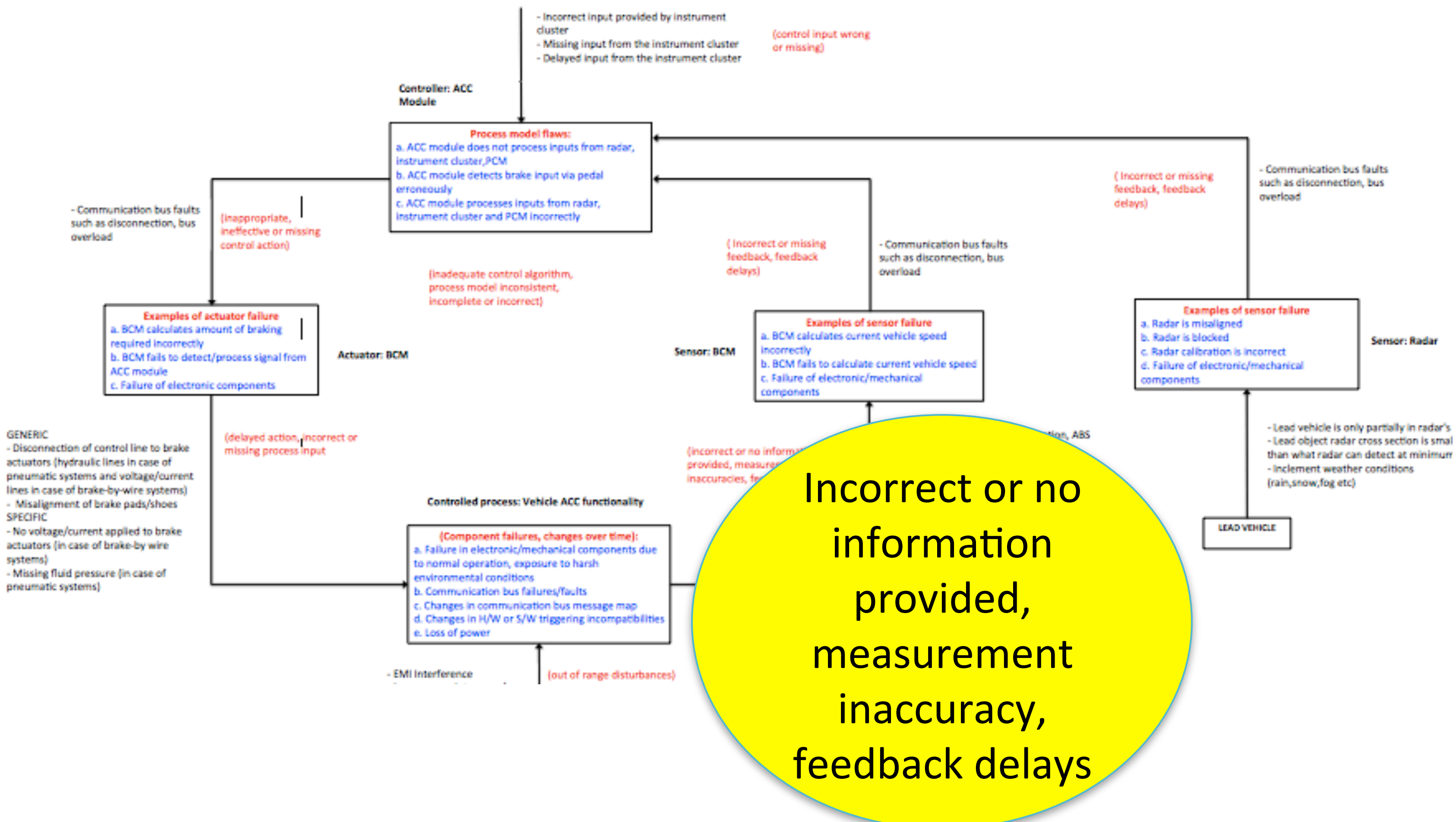
Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.



- Misalignment of brake shoes/pads.
- Missing fluid pressure for hydraulic lines.
- No current/voltage to actuator.

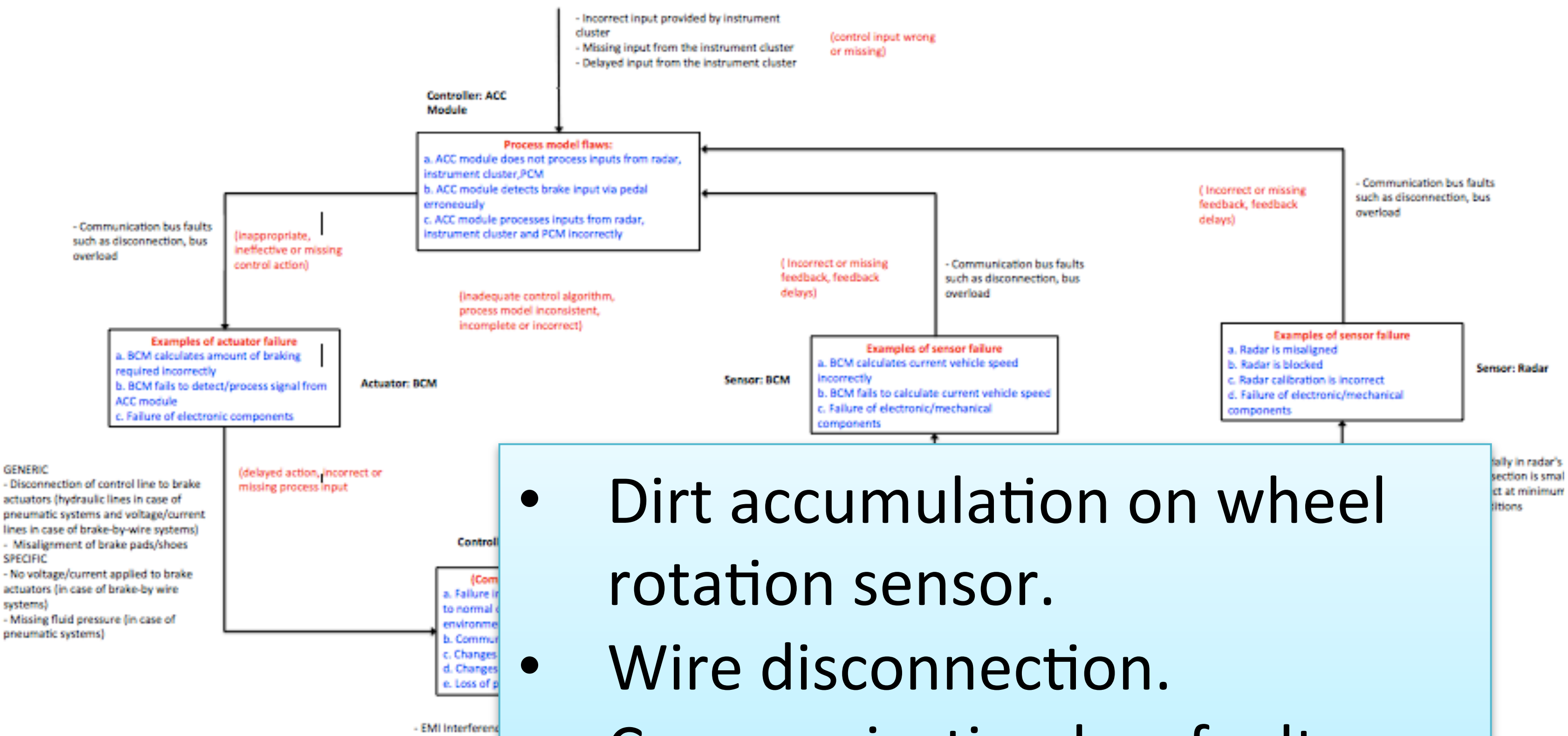
Causal Analysis Results (4)

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.



Causal Analysis Results (5)

Unsafe Control Action:
Vehicle does not brake when the distance to the object in front is less than preset value.



- Dirt accumulation on wheel rotation sensor.
- Wire disconnection.
- Communication bus faults, overload, message priority.

Assess the Effectiveness of STPA

- The outcome of STPA was a list of component design requirements that will ensure top level safety goal.
- Compare with actual industry design specifications.
  - Unable to do so because of proprietary nature of the design specifications.

Assess STPA (2)

- Compared with ISO 22179 and SAE J2399.
  - Many more detailed requirements than what is in the standards.
  - Industry standards are the lowest common denominators among the manufacturers.
  - **Can only compare with categories of requirements.**
- **Compared with actual implementation in production vehicles.**
  - **Warning signals among manufacturers**
  - **Warnings in driver's manual**

Categories of Requirements Missing in Industry Standards

- Driver control authority vs. computer automation authority
  - The importance of vehicle state feedback information (warning lights/sounds/icons) for driver
  - Driver mental model inconsistency with vehicle state (complacency and distracted driving)
- Sensor and actuator
  - Hardware quality
  - Degradation

Categories of Requirements Missing in Industry Standards (2)

- Communication bus
  - Delays
  - Signal priority
- Controls software errors
  - Delay in processing inputs
  - Parameter calibration errors
  - Control software algorithm process model
  - Software handling of signal priority
- Service and maintenance requirements

Comparison with Implementation

1. Significant difference in the implementation of warning messages and signals among OEM's and across models.

Example: ACC Malfunction Lights (Credit: Zoepf)

Porsche   Toyota   Volvo   Nissan

2. Leaving a lot of the limitations of ACC in the drivers' manual.
   – NISSAN INFINITI EX 2010, 21 pages (ACC feature), 16 warnings and 1 caution.
   – Ford Lincoln MKX 2010, 7 pages (ACC feature), 10 warnings.

Summary

- This was our first attempt to apply STPA to a modern automotive electronics feature.
- The method works.
- The analysis identified many more safety critical requirements than what is identified in the industry standards.
- STPA can be a very powerful method to identify safety critical design requirements, and prevent accidents in the first place.
- Industry collaboration will further improve our understanding of the effectiveness of the method, and how to integrate it with the current product development process.

Thank you!
Question?

Qi D. Van Eikema Hommes
qhommes@mit.edu