Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain

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
27. March 2013

Motivation: STAMP/STPA Application Areas

- **STAMP and STPA have been successfully applied to different systems in different areas:**

High Speed Train Accident in China (2011).

Space Shuttle Operation (2008)

Darlington Shutdown System (2012).

- **In the automotive domain:**
  - ❑ **There is only little experience with STAMP/STPA.**
  - ❑ **They still use the traditional hazard analysis techniques for complex system.**
  - ❑ **Safety analysis is not obvious in complex systems.**

Outline

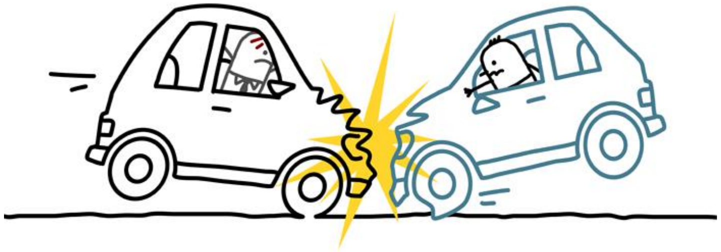
- Motivation ✓
- Overview ◎
- Experiences with Applying STPA to the Automotive Domain
- A Comparison between Safety Cases and STPA
- Issues and Conclusion

Overview

- **The research is performed based on published knowledge from a case study with MAN Truck & Bus AG.**

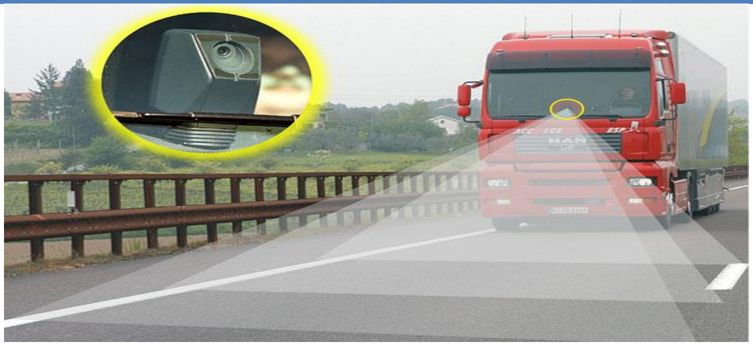
Applying STPA to Automotive Domain

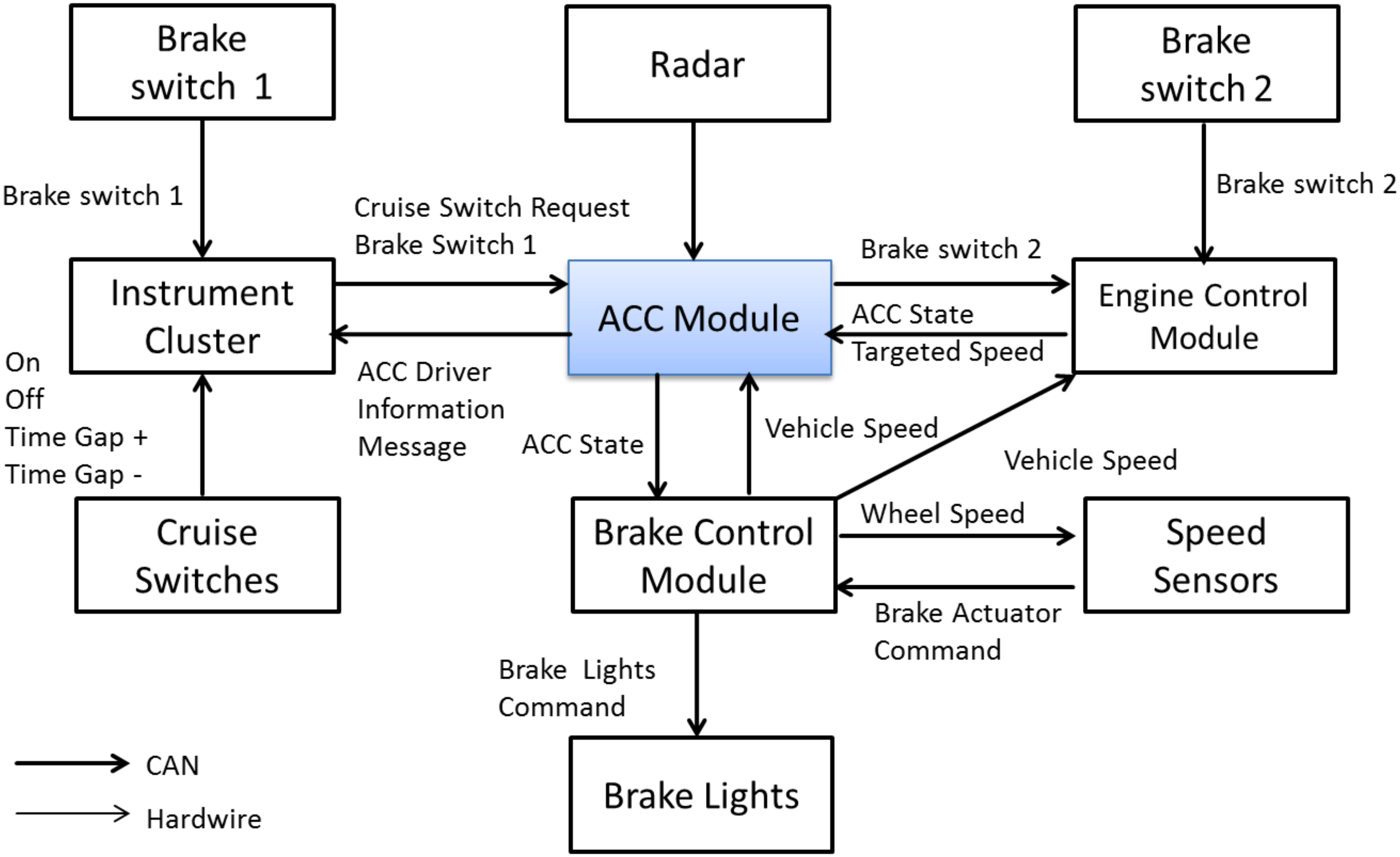
- **Research Objectives:**
  - ❑ To investigate the benefits of applying STAMP/STPA in industry to get an understanding of their effect and problems in the applications.
  - ❑ To understand how these approaches can be useful for automotive safety.
  - ❑ To provide an assessment of the usage of these approaches.
- **Research Questions:**
  - ❑ How can STPA improve the safety in the automotive domain?
  - ❑ What are potential problems of applying STPA to automotive safety?
  - ❑ What are the differences between STPA and safety cases?



Study Object: Adaptive Cruise Control (ACC)

- **The ACC system** is able to automatically adjust the driving speed as well as the distance to the vehicle ahead in accordance with the pre-settings.





[source: Szuszman, P. 2005]

Hazard Analysis for the ACC System

- **Step 1.a: Establish fundamentals:** Accidents, hazards, design requirements and design constraints.

http://www.autoblog.com

System Accidents:

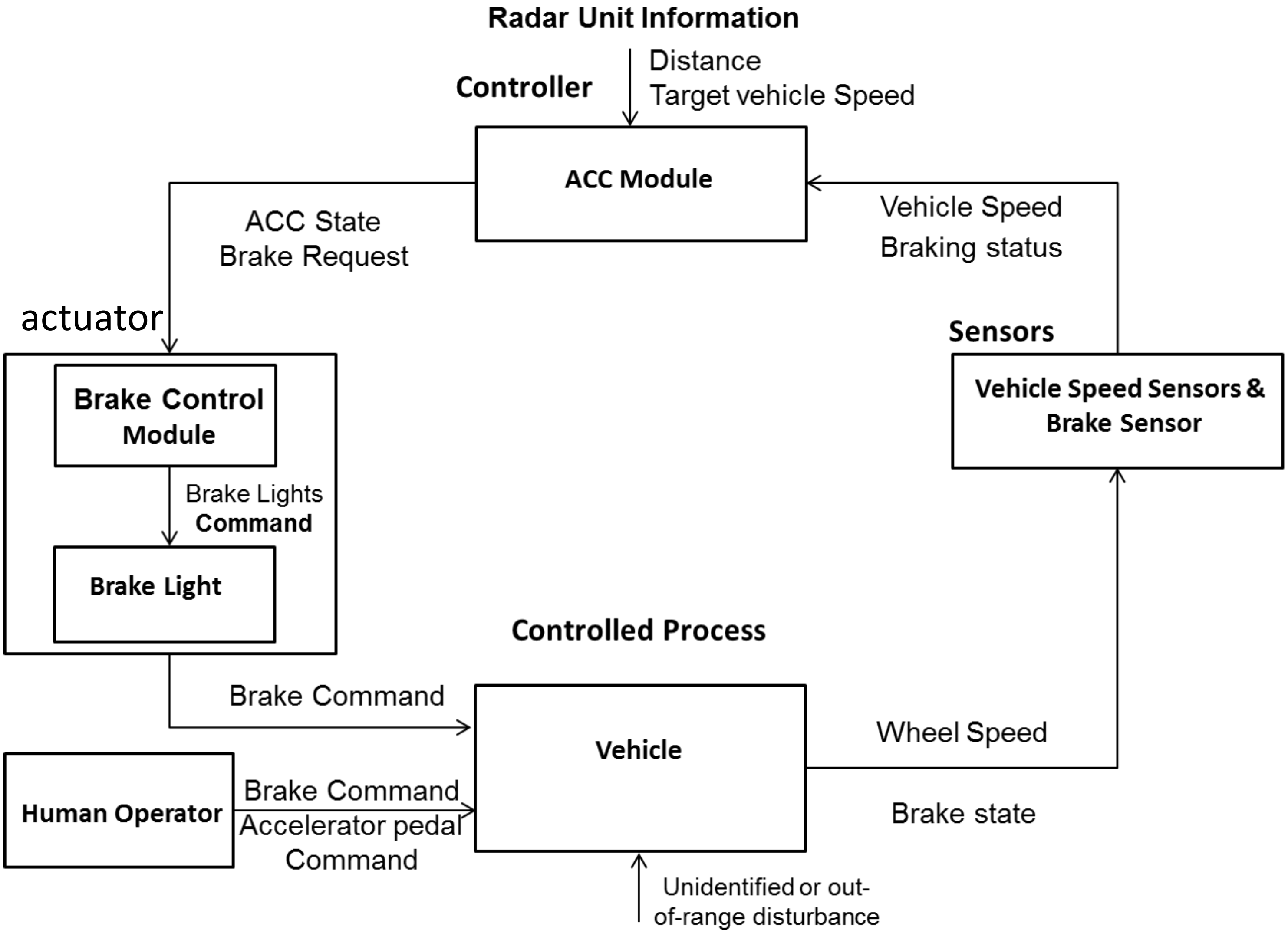
- **Accident 1:** The ACC vehicle crashes with a vehicle in front when the ACC system is in active mode **(Forward Collision vehicle to vehicle)**
- **Accident 2:** The vehicle behind crashes the ACC vehicle when the ACC system detects an object in the vehicle path **(Backward Collision vehicle to vehicle)**

System hazards:

- **H.1:** ACC violates the safe distance between ACC vehicle and vehicle in front.
- **H.2:** ACC did not illuminate brake light to warn vehicle in the behind.
- **H.3:** ACC does not reduce throttle and apply the braking force to maintain safe distance as preset by driver when vehicle catches up with a slower preceding vehicle.
- **H.4:** ACC estimates wrong values of distance and speed of vehicle ahead.
- **H.5:** The driver is able to override the ACC system at any time by activating the brake or accelerator pedal.

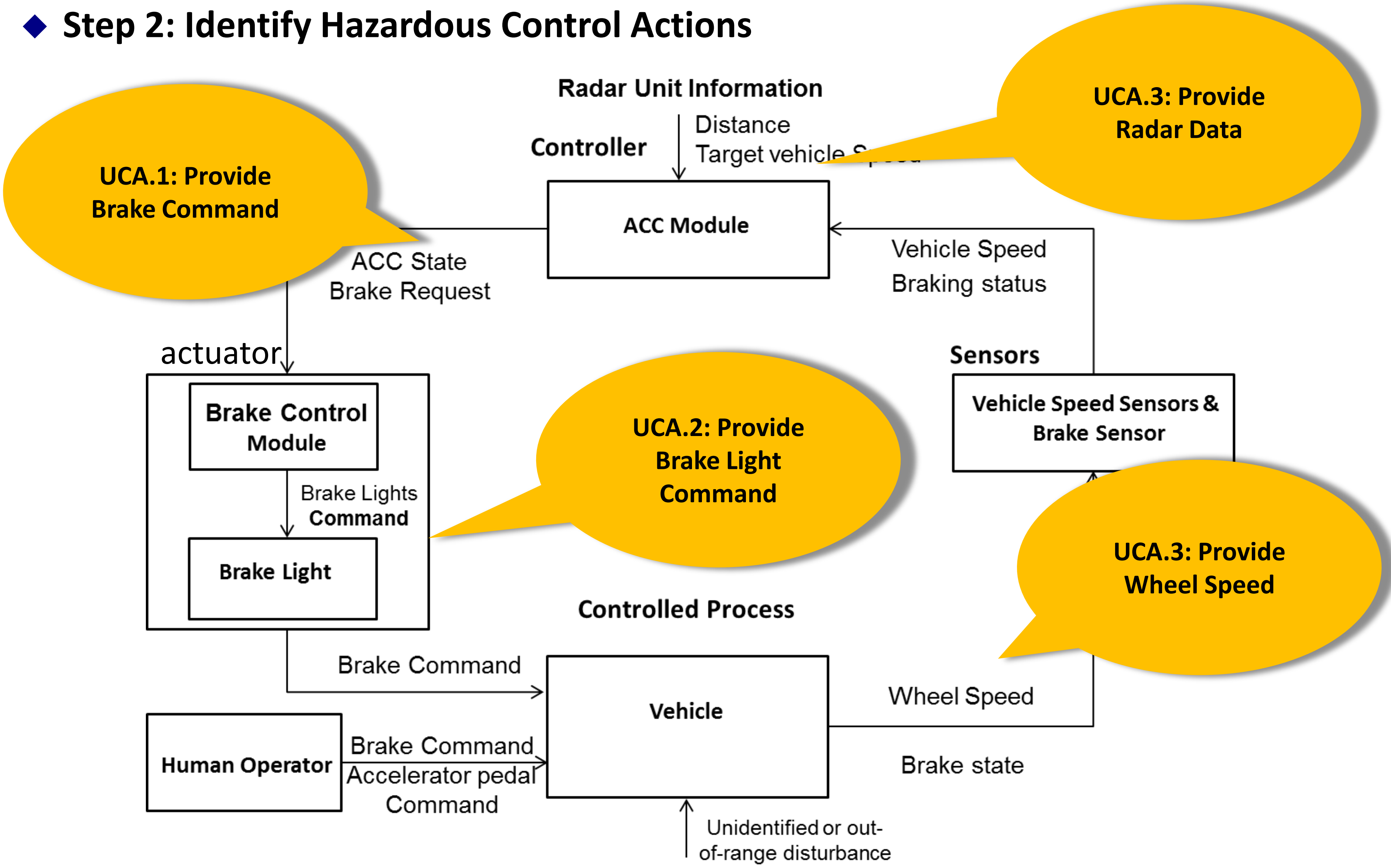
Safety-Control Structure Diagram

- **Step 1.b: Draw the control structure**



Unsafe Control Actions

- **Step 2: Identify Hazardous Control Actions**



Control Actions Table

- **Step 2: Examples of potentially inadequate control actions of ACC system:**

Control Actions	Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped too soon
Brake Command (A1)	Vehicle does not brake when the vehicle has detected a slowed or stopped object in its path **[H1, H3]** Vehicle does not brake because the driver has ignored all the warnings **[H5]**	Braking is commended when there is no a slowed or stopped object in the vehicle path **[H2, H3]**	Early: Braking is commanded to early when the distance to the target vehicle is too far **[H1].** Late: Braking is commended too late when the distance to the target vehicle is too close **[H1, H3]**	Braking stops too soon before the safety distance to target vehicle reached **[H1, H3]**
Brake Light Command (A2)	Vehicle does not illuminate Brake to warn vehicle in the behind **[H1]**	Brake light command illuminate light while ACC does not request brake command.	Brake light command illuminate late, after the vehicle has stopped **[H2]**	Brake light illuminate stopped too soon during braking situation
Radar Data	Radar Sensor does not provide relative speed and distance of objects ahead of vehicle **[H4]**	Radar sensor provides incorrect data of target vehicle speed **[H1, H4]**	The data of radar sensor comes too late when the distance to a forward vehicle is too close **[H1,H4]**	Radar sensor is stopped too soon that the ACC module does not get the relative data signal.

Safety Constraints

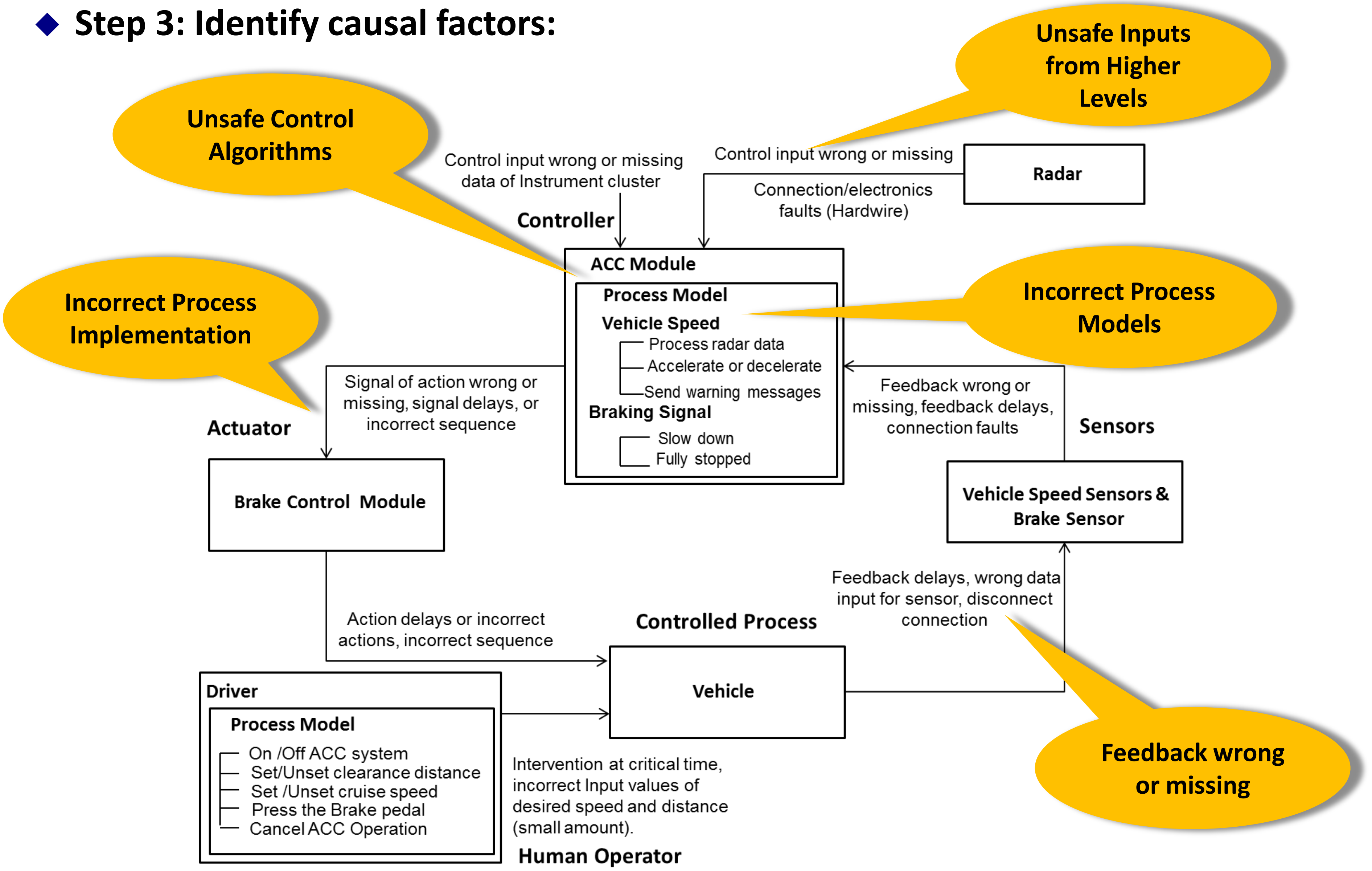
- **Step 2: Examples of the corresponding safety constraints :**

Unsafe Control Action	**Safety Constraints**
Vehicle does not illuminate the brake light to warn vehicle behind.	Vehicle must illuminate the brake light to warn vehicle in the back.
Brake light command illuminate late after vehicle has stopped.	Brake light command must illuminate early within X-seconds before stopping vehicle.
Vehicle does not brake when the vehicle has detected a slowed or stopped object in its path.	Vehicle must brake when vehicle detected slowed or stopped object (at a few X-meters within the preset value of the safety distance) in its path.
Vehicle does not brake due to the driver has ignored all of the warnings.	The intervention between ACC system and driver should be limited to the traffic environment and conditions.

Each unsafe control action is then translated into a system-level safety constraint

Causal Analysis

- **Step 3: Identify causal factors:**



Unsafe Inputs from Higher Levels
Unsafe Control Algorithms
Control input wrong or missing data of Instrument cluster
Control input wrong or missing
Radar
Connection/electronics faults (Hardwire)
Controller
ACC Module
Process Model
Vehicle Speed
Process radar data
Accelerate or decelerate
Send warning messages
Braking Signal
Slow down
Fully stopped
Incorrect Process Models
Incorrect Process Implementation
Signal of action wrong or missing, signal delays, or incorrect sequence
Actuator
Feedback wrong or missing, feedback delays, connection faults
Sensors
Brake Control Module
Vehicle Speed Sensors & Brake Sensor
Feedback delays, wrong data input for sensor, disconnect connection
Action delays or incorrect actions, incorrect sequence
Controlled Process
Vehicle
Driver
Process Model
On /Off ACC system
Set/Unset clearance distance
Set /Unset cruise speed
Press the Brake pedal
Cancel ACC Operation
Intervention at critical time, incorrect Input values of desired speed and distance (small amount).
Human Operator
Feedback wrong or missing

The classification of control flaws leading to hazards (Leveson 2011)

The Causal Factors of Hazard H1.

Part of loop.	**Examples of causal factors leading to hazard H1**	
ACC Module	Control input (from Radar sensor) wrong or missing	Radar sensor should be developed further to detect the small object (e.g. Motorcycle) and vehicle driving far off center.
	Control input (from Instrument Cluster) wrong or missing	ACC module processes input from instrument cluster incorrectly (Transmission failure).
	Control algorithm inadequate	Process model of ACC-module incorrect e.g. display warring message to drive and accelerate speed of vehicle.
	Feedback inadequate	Missing or spurious feedback of current vehicle speed and brake sensor status that may lead to a miscalculation from ACC module for time gap (time gap= clearance/ACC vehicle speed).
	Feedback delays	Sensor signal from radar sensor or instrument cluster or vehicle speeds sensors or a brake sensor is lost during transmitting.

- **Improvement Potentials:**
  - The radar sensor in the front shall detect small objects (e.g. motorcycle) or a vehicle driving far off center.
  - An extra radar sensor should be added in the back of the vehicle to detect the speed of vehicles behind.

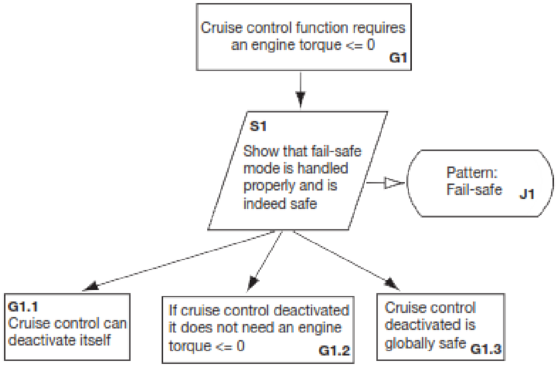
Outline

- Motivation ✓
- Overview ✓
- Experiences with Applying STPA to the Automotive Domain ✓
- A Comparison between Safety Cases and STPA ◎
- Issues and Conclusion

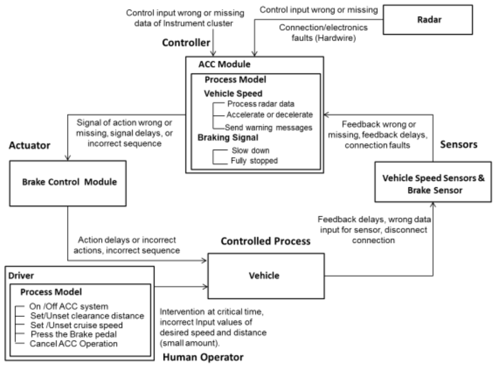
A Comparison between STPA and Safety Cases

- **We conducted a case study applying safety cases for the same ACC system**

Safety case


Cruise control function requires an engine torque <= 0
G1
S1
Show that fail-safe mode is handled properly and is indeed safe
Pattern: Fail-safe
J1
G1.1
Cruise control can deactivate itself
If cruise control deactivated it does not need an engine torque <= 0
G1.2
Cruise control deactivated is globally safe
G1.3

STPA hazard analysis


Control input wrong or missing data of Instrument cluster
Control input wrong or missing
Radar
Connection/electronics faults (Hardwire)
Controller
ACC Module
Process Model
Vehicle Speed
Process radar data
Accelerate or decelerate
Send warning messages
Braking Signal
Slow down
Fully stopped
Signal of action wrong or missing, signal delays, or incorrect sequence
Actuator
Brake Control Module
Feedback wrong or missing, feedback delays, connection faults
Sensors
Vehicle Speed Sensors & Brake Sensor
Feedback delays, wrong data input for sensor, disconnect connection
Action delays or incorrect actions, incorrect sequence
Controlled Process
Vehicle
Driver
Process Model
On /Off ACC system
Set/Unset clearance distance
Set /Unset cruise speed
Press the Brake pedal
Cancel ACC Operation
Intervention at critical time, incorrect Input values of desired speed and distance (small amount).
Human Operator

→ **Provides clear means to structure the risk argumentation.**

→ **It is not well suitable for system analysis.**

→ **STPA is a more systematic.**

→ **Step by step process.**

→ **STPA considers safety as a control problem.**

→ **It has no detailed description, however, how to present the final argumentation.**

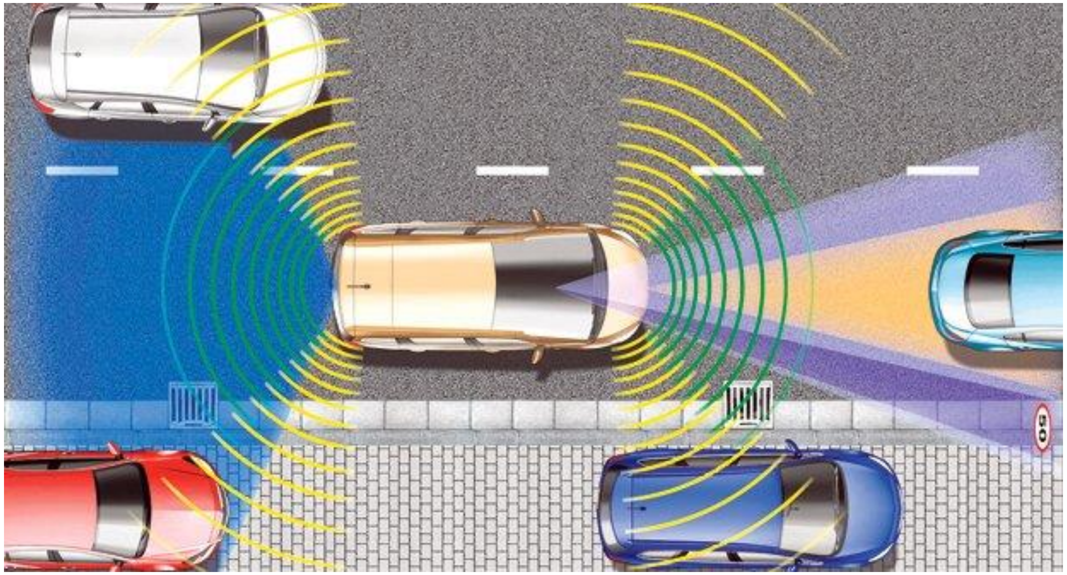
A perfect combination of analysis and argumentation

Issues and Conclusion

- **Issues according to our experiences:**
  - The third step of STPA needs a lot of effort, time and deep knowledge for examining the controllers with process models.
  - There is no systematic way to let the safety analyst know how to evaluate each control actions. Moreover, STPA does not represent operating modes (states) of components, which have an effect on the safety of control action.
  - STPA has limitation for analyzing multiple controllers in the control loop of a system
  - It is not clear how we can provide an action control table and causal factors for multiple controllers with interference among the actions.
  - It is not clear how to address the real-time characteristics of system during STPA.
- **Conclusion**
  - We investigated the application of STAMP/STPA to automotive domain and its difficulties in that domain.
  - We found STPA to be more powerful and useful technique in analyzing accidents and potential controls for software-intensive systems in automotive domain.

Discussion…

Thank You!



[Source: http://www.opel.de]

My Contact Information :

M.Sc. Asim Abdulkhaleq
University of Stuttgart
Institute for Software Technology
Asim.Abdulkhaleq@informatik.uni-stuttgart.de