The Second European STAMP Workshop 2014

STPA in Automotive Domain Advanced Tutorial

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

Joint work with:
Prof. Dr. Stefan Wagner

ESW 2014, Stuttgart, Germany
22. September, 2014

University of Stuttgart
Germany

Technische Universität Braunschweig

Massachusetts Institute of Technology

Agenda

- Automotive Domain ◎
- STAMP/STPA Background ✔
- STPA Steps in Practice
- STPA Group Exercise
- Wrap-Up
  - Participants Questions
  - Current Research Trends

Systems Approach to Safety Engineering

STAMP Model

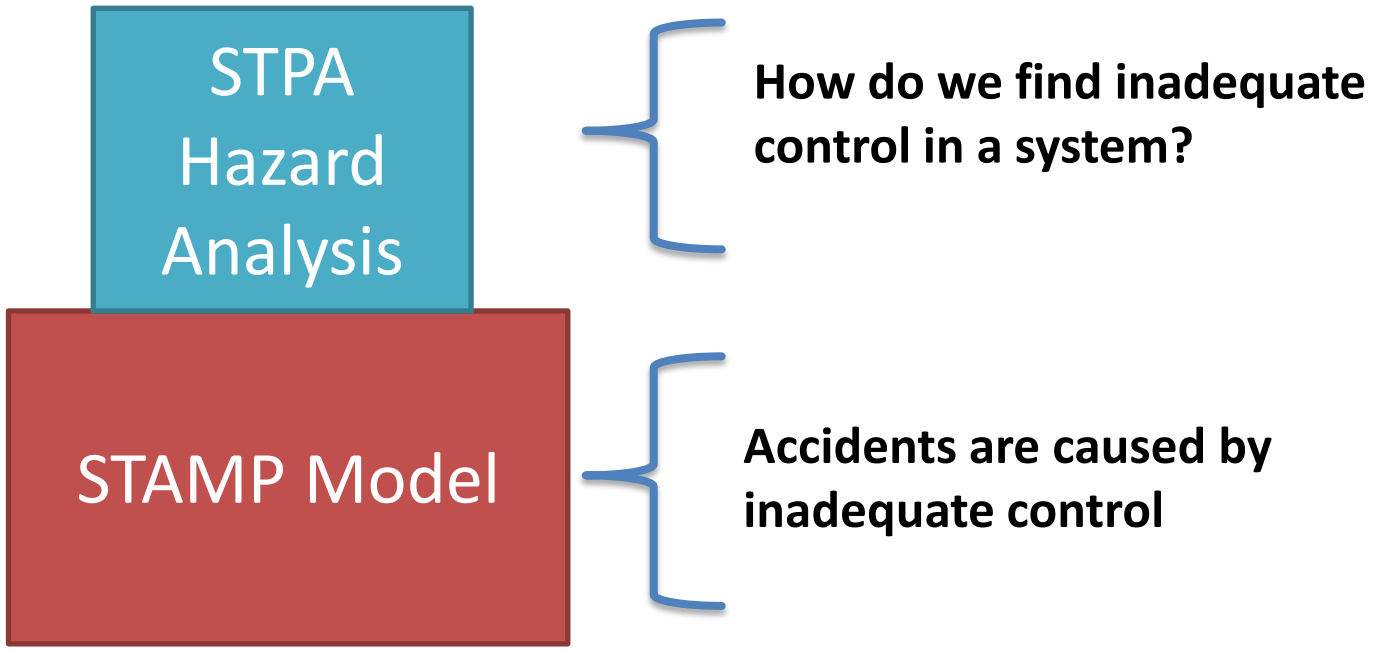
- **Accidents are more than a chain of events, they involve complex dynamic processes.**
- **Treat accidents as a control problem, not a failure problem.**
- **Prevent accidents by enforcing constraints on component behaviour and interactions.**
- **Captures more causes of accidents:**
  - **Component failure accidents**
  - **Unsafe interactions among components**
  - **Complex human, software behaviour**
  - **Design errors**
  - **Flawed requirements**

esp. software-related accidents.

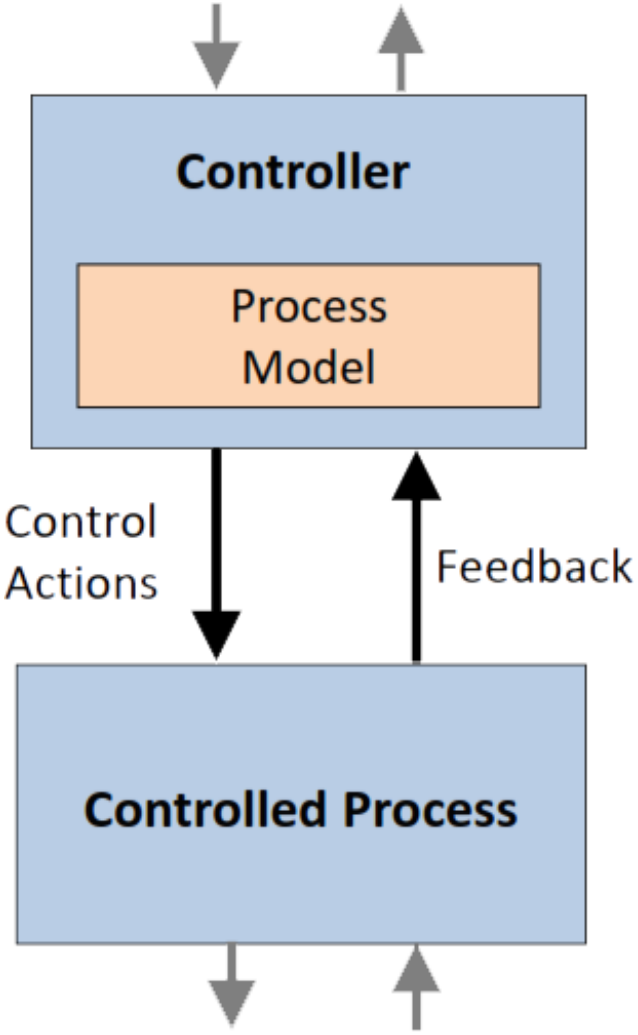
Leveson (2003); Leveson (2011)

STPA (Systems-Theoretic Process Analysis)

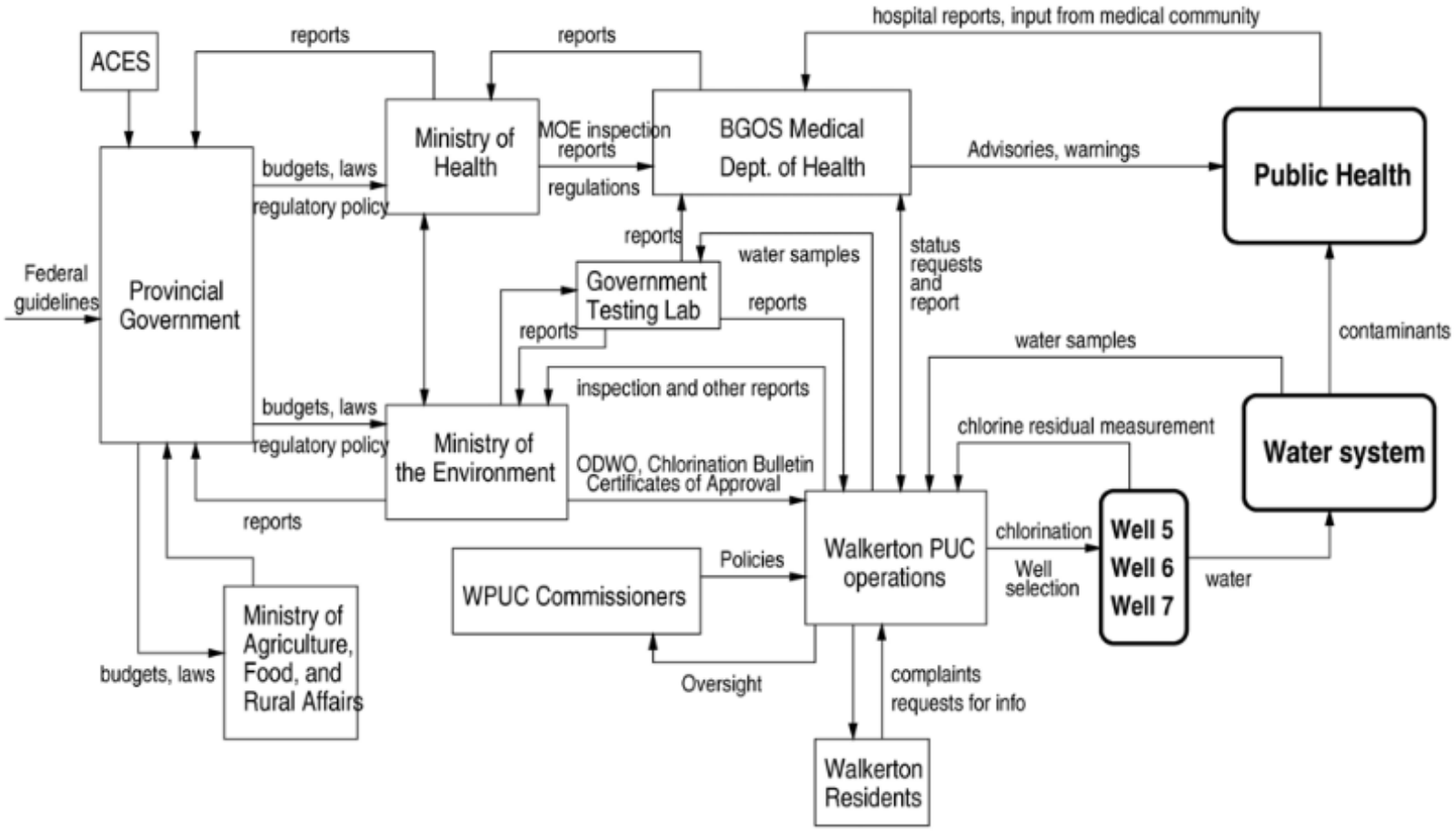
- **STPA:**
  - A new hazard analysis technique built on STAMP.
  - The same goal as fault trees or any other hazard analysis techniques but
    - starts from hazards and looks at more than component failures and
    - finds more types of accident scenarios.



Basic Control Loop



Example: Water Safety Control Structure



Leveson et al. (2011)

STPA Steps in Practice

- **Identify fundamentals (accidents, hazards, safety constraints, etc.)**
- **Construct the control structure**
  - Identify major components and controllers
  - Label the control/feedback arrows
- **Step 1: Identify Unsafe Control Actions (UCAs)**
  - Create Control Table: Action required but not provided, Unsafe action provided, wrong timing or order, stopped too soon/applied too long
  - Create corresponding safety constraints
- **Step 2: Identify causal factors**
  - Identify controller process models
  - Analyze controller, control path, feedback path, process.

Step1: Identify Unsafe Control Actions

Unsafe Control Action Table:

Each control action should be documented with four hazardous action types.

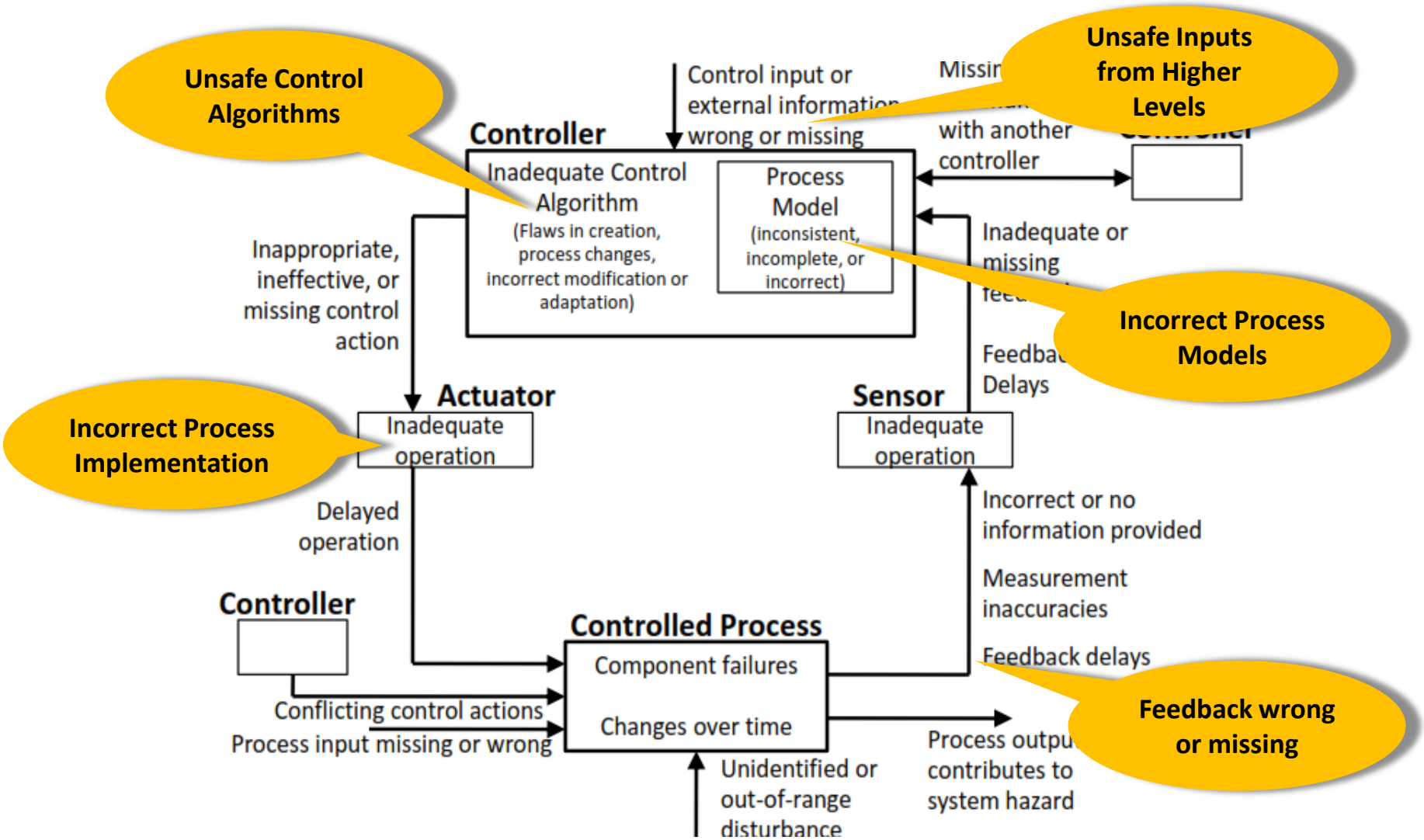
Control Actions	Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped too soon/Applied too long

Step 1: Identify Unsafe Control Actions

A more rigorous approach by John Thomas

Control Actions	Process Model Variable 1	Process Model Variable 2	Process Model Variable 3	Hazardous?

Step 2: STPA Control Flaws



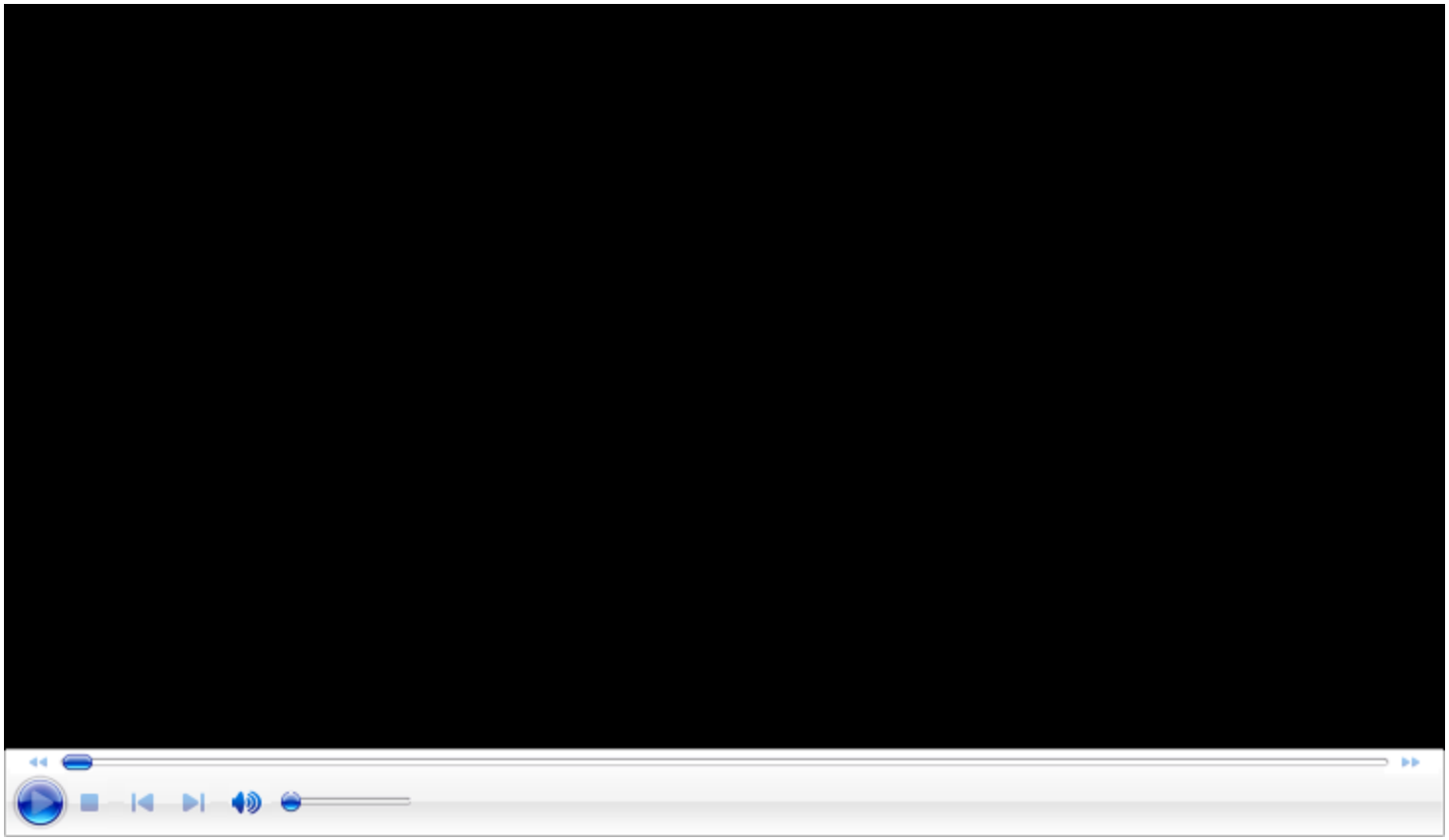
Agenda

- STAMP/STPA Background ✔
- STPA Steps in Practice ◎
- STPA Group Exercise
- Wrap-UP
  - Participant Questions
  - Current Research Trends

Adaptive Cruise Control System

Definition:

ACC is a radar-based system that can monitor the vehicle in front (up to 600 feet) and adjust the speed of the vehicle to keep it at a preset distance behind the lead vehicle, even in most fog and rain conditions. [http://corporate.ford.com/]



STPA Steps in Practice

- **Identify fundamentals (accidents, hazards, safety constraints, etc.)**
- **Construct the control structure**
  - Identify major components and controllers
  - Label the control/feedback arrows
- **Step 1: Identify Unsafe Control Actions (UCAs)**
  - Create Control Table: Not given, given incorrectly, wrong timing, stopped too soon
  - Create corresponding safety constraints
- **Step 2: Identify causal factors**
  - Identify controller process models
  - Analyze controller, control path, feedback path, process.

Identifying Accidents and Hazards

- **Accidents: ?**

  The ACC vehicle crashes with a vehicle in front when the ACC system is active.

- **Hazards: ?**
  - **H.1**: ACC did not keep 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 estimated wrong values of distance and speed of vehicle ahead.
  - **H.4**: ACC slow down the vehicle too suddenly, and vehicle is rear-ended.
  - **H.5**: The driver is able to override the ACC system at any time by activating the brake or accelerator pedal.

Qi (2012), Abdulkhaleq et al. (2013)

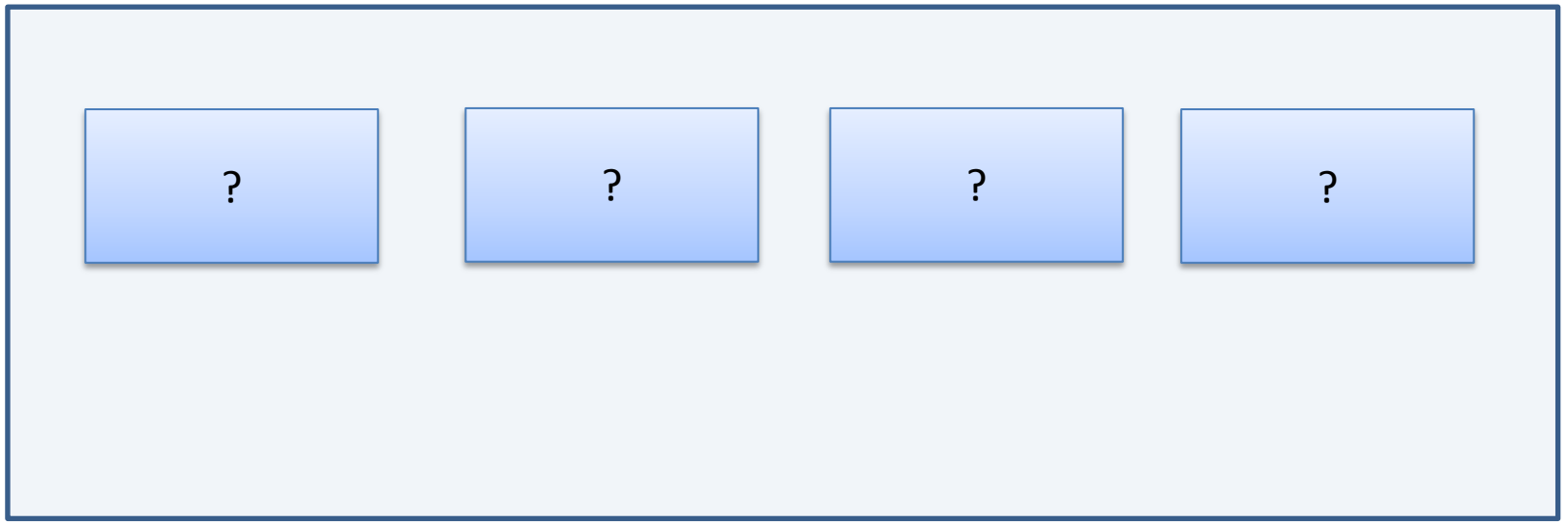
STPA Steps in Practice

- **Identify fundamentals (accidents, hazards, safety constraints, etc.)**
- **Construct the control structure**
  - Identify major components and controllers
  - Label the control/feedback arrows
- **Step 1: Identify Unsafe Control Actions (UCAs)**
  - Create Control Table: Not given, Given incorrectly, wrong timing, stopped too soon.
  - Create corresponding safety constraints
- **Step 2: Identify causal factors**
  - Identify controller process models
  - Analyze controller, control path, feedback path, process.

Control Structure

High-level (simple) Control Structure

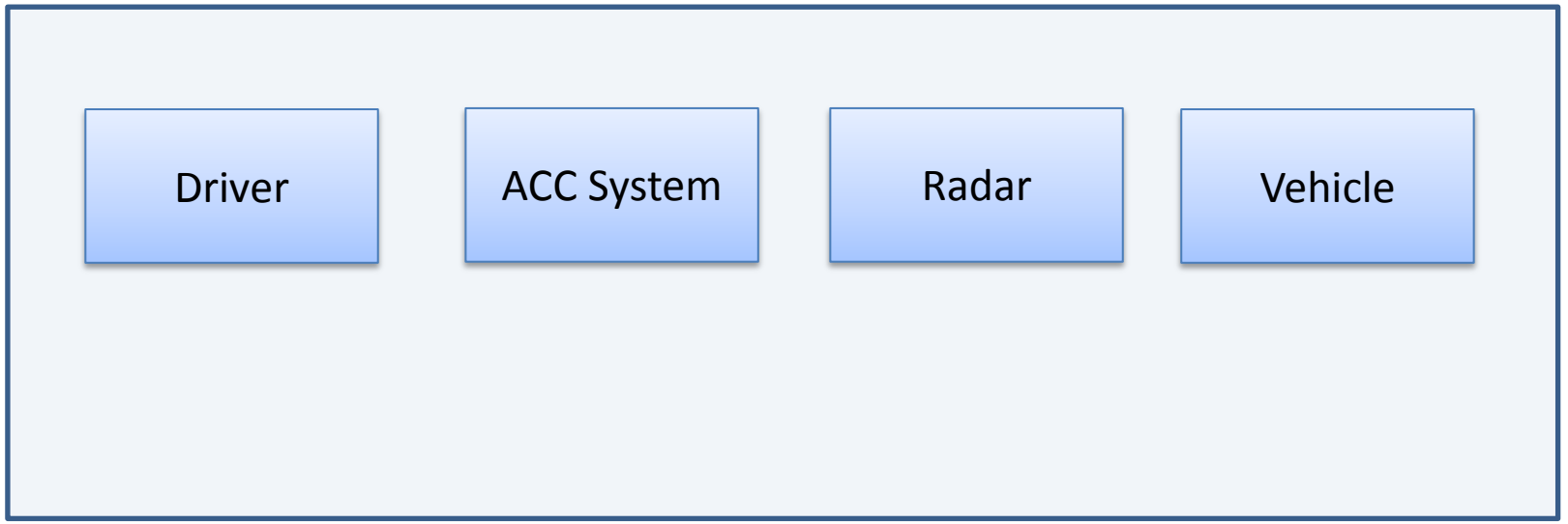
Main components and controllers?



Control Structure

High-level (simple) Control Structure

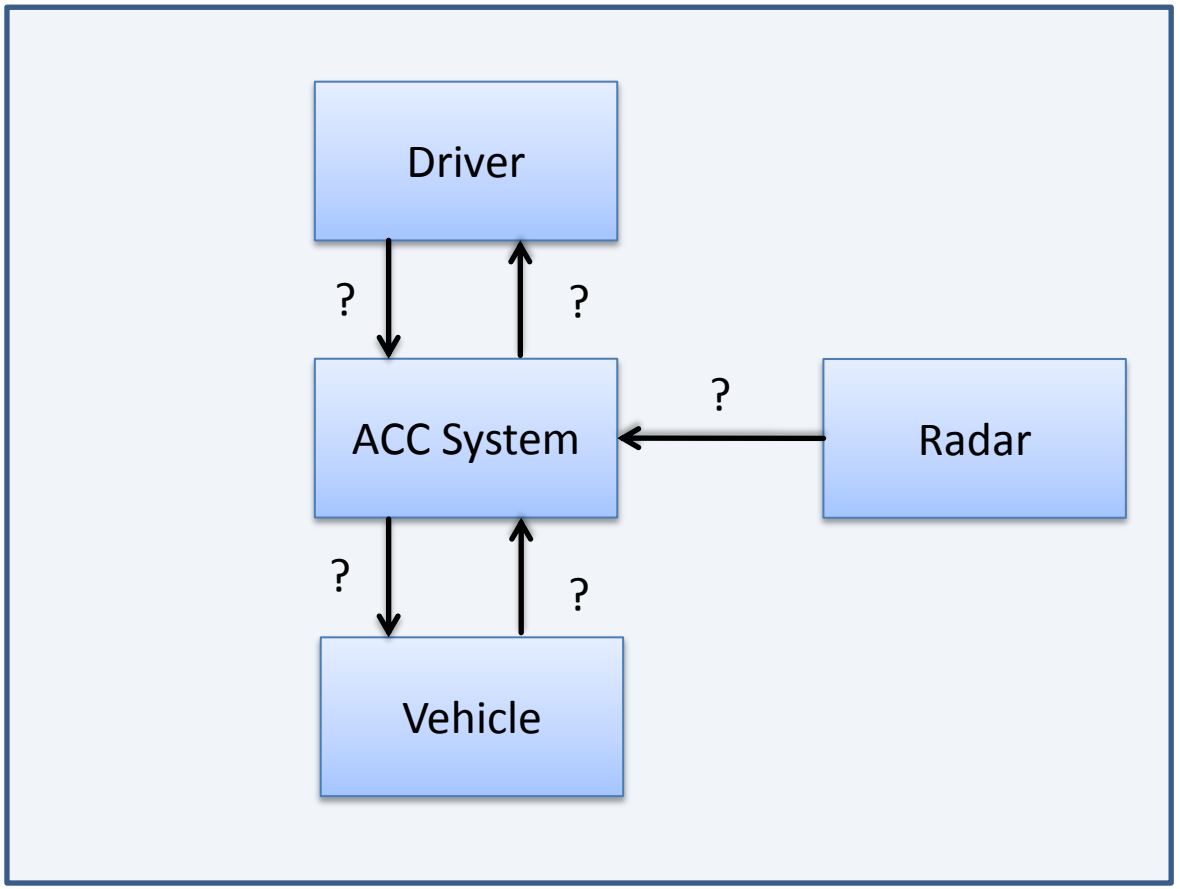
Main components and controllers?



Control Structure

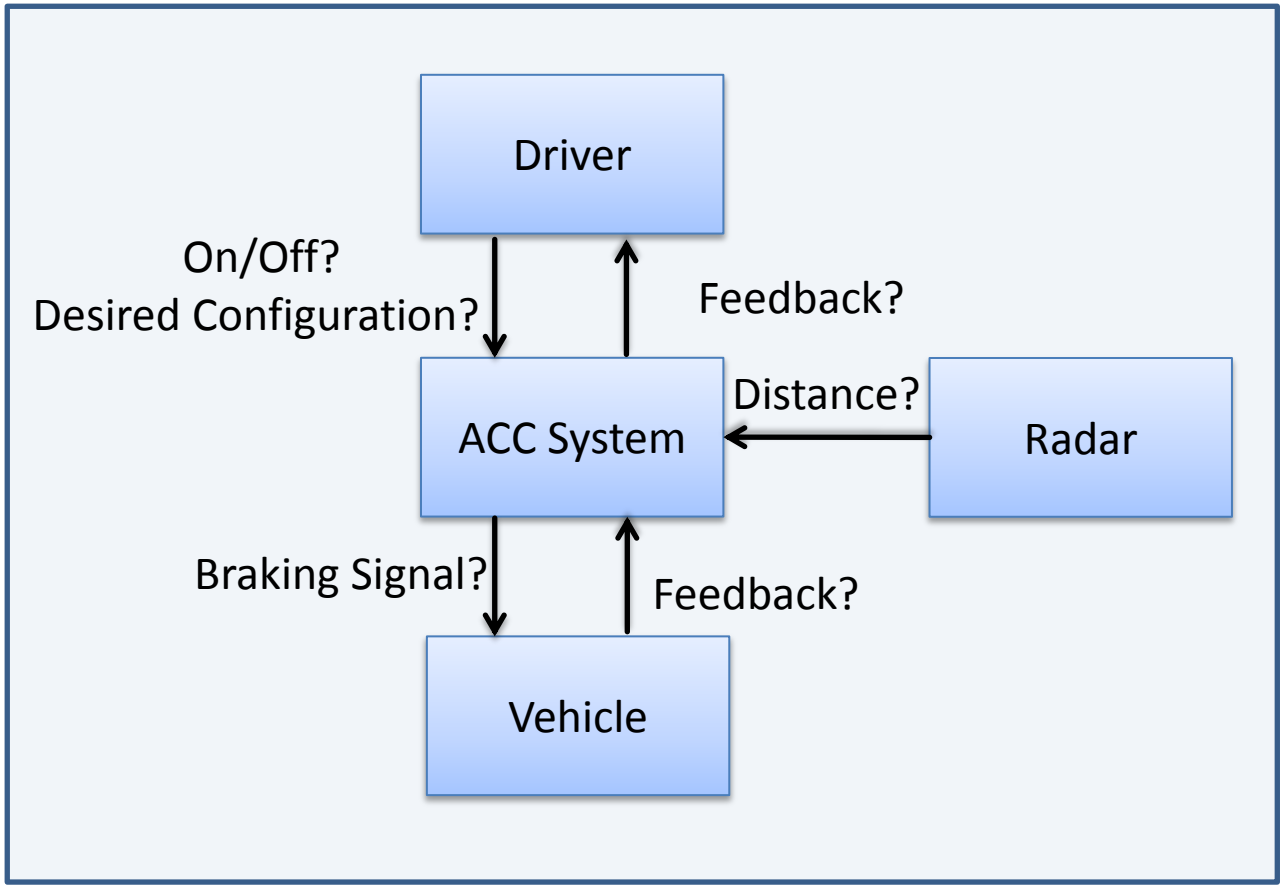
High-level (simple) Control Structure

What commands are sent?



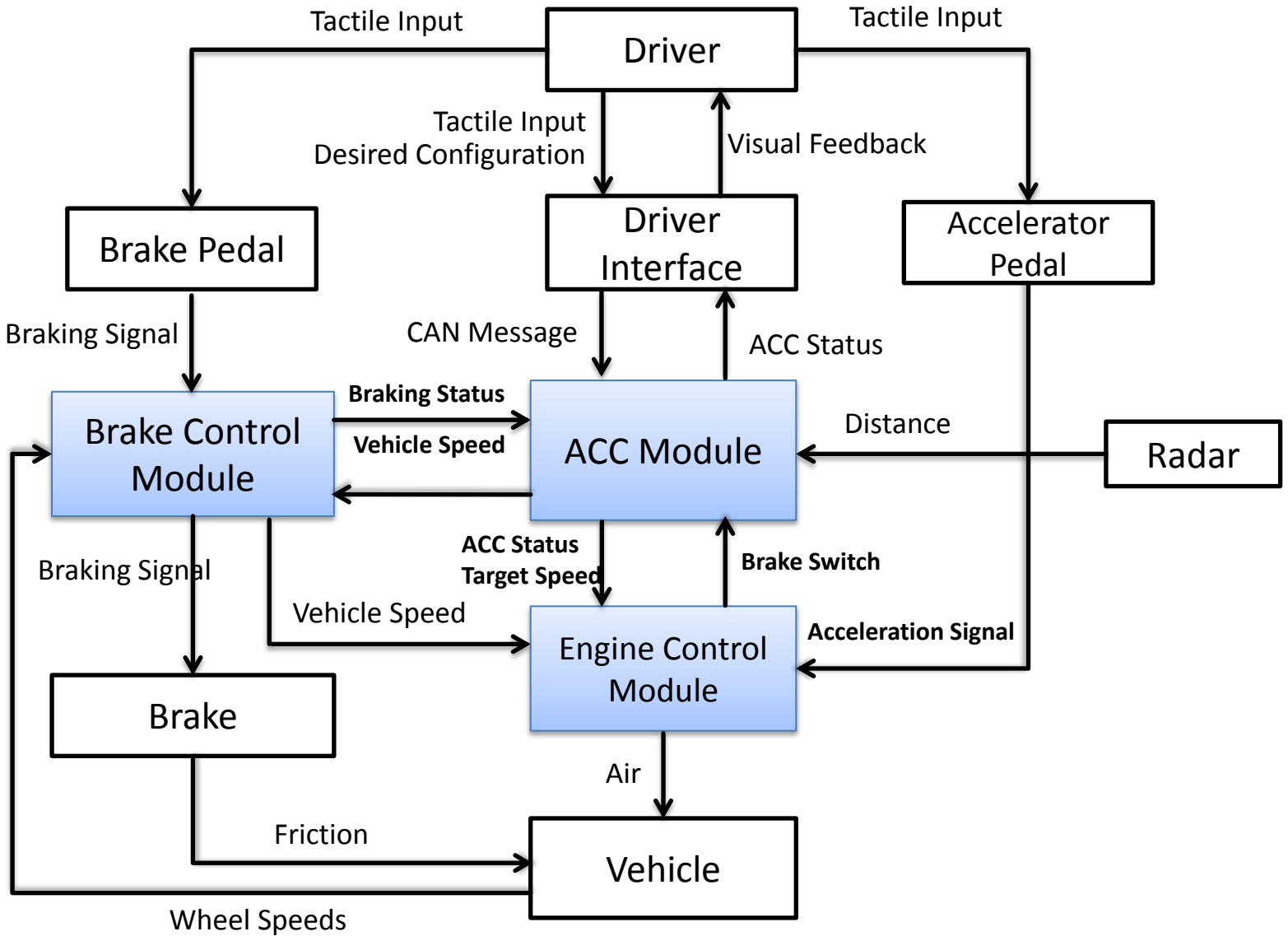
Control Structure

High-level (simple) Control Structure



Control Structure

More Complex Control Structure



STPA Steps in Practice

- **Identify fundamentals (accidents, hazards, safety constraints, etc.)**
- **Construct the control structure**
  - Identify major components and controllers
  - Label the control/feedback arrows
- **Step 1: Identify Unsafe Control Actions (UCAs)**
  - Create Control Table: Not given, Given incorrectly, wrong timing, stopped too soon.
  - Create corresponding safety constraints
- **Step 2: Identify causal factors**
  - Identify controller process models
  - Analyze controller, control path, feedback path, process.

Identify Unsafe Control Actions

Unsafe Control Table

Control Actions	Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped too soon
Radar Data	Radar Sensor does not provide relative speed and distance of objects ahead of vehicle **[H3]**	Radar sensor provides incorrect data of target vehicle speed **[H1, H3]**	The data of radar sensor comes too late when the distance to a forward vehicle is too close **[H1,H3]**	Radar sensor is stopped too soon that the ACC module does not get the relative data signal **[H1].**
Brake Signal from ACC to BCM				

Identify Unsafe Control Actions

Unsafe Control Table

Control Actions	Action required but not provided	Unsafe action provided	Incorrect Timing/Order	Stopped too soon
Radar Data	Radar Sensor does not provide relative speed and distance of objects ahead of vehicle **[H3]**	Radar sensor provides incorrect data of target vehicle speed **[H1, H3]**	The data of radar sensor comes too late when the distance to a forward vehicle is too close **[H1,H3]**	Radar sensor is stopped too soon that the ACC module does not get the relative data signal **[H1].**
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 driver **[H1, H2]**	Braking is commented when the distance to the lead vehicle is larger than the set value **[H1, H2]**	Early: Braking is commanded to early when the distance to the target vehicle is too far **[H1, H4].** Late: Braking is commended too late when the distance to the target vehicle is too close **[H1]**	Braking stops too soon before the safety distance to target vehicle reached **[H1]**

Defining Safety Constraints

Safety Constraints Table

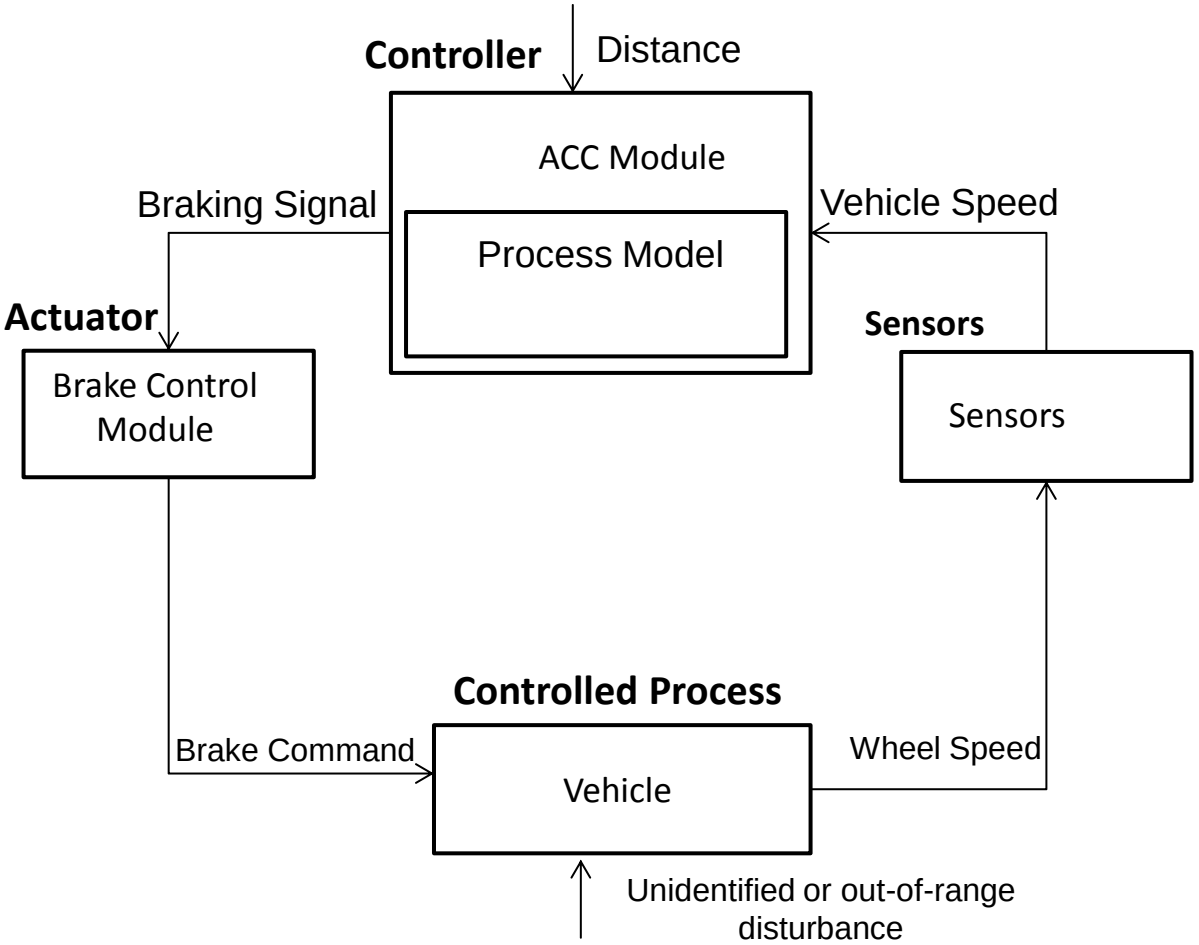
Unsafe Control Action	Safety Constraints
Vehicle does not illuminate the brake light to warn vehicle behind.	Vehicle must illuminate the brake light to warn vehicle in the back.
Brake light command illuminate late after vehicle has stopped.	Brake light command must illuminate early within X-seconds before 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.

STPA Steps in Practice

- **Identify fundamentals (accidents, hazards, safety constraints, etc.)**
- **Construct the control structure**
  - Identify major components and controllers
  - Label the control/feedback arrows
- **Step 1: Identify Unsafe Control Actions (UCAs)**
  - Create Control Table: Not given, Given incorrectly, wrong timing, stopped too soon.
  - Create corresponding safety constraints
- **Step 2: Identify causal factors**
  - Identify controller process models
  - Analyze controller, control path, feedback path, process.

Causal Factors

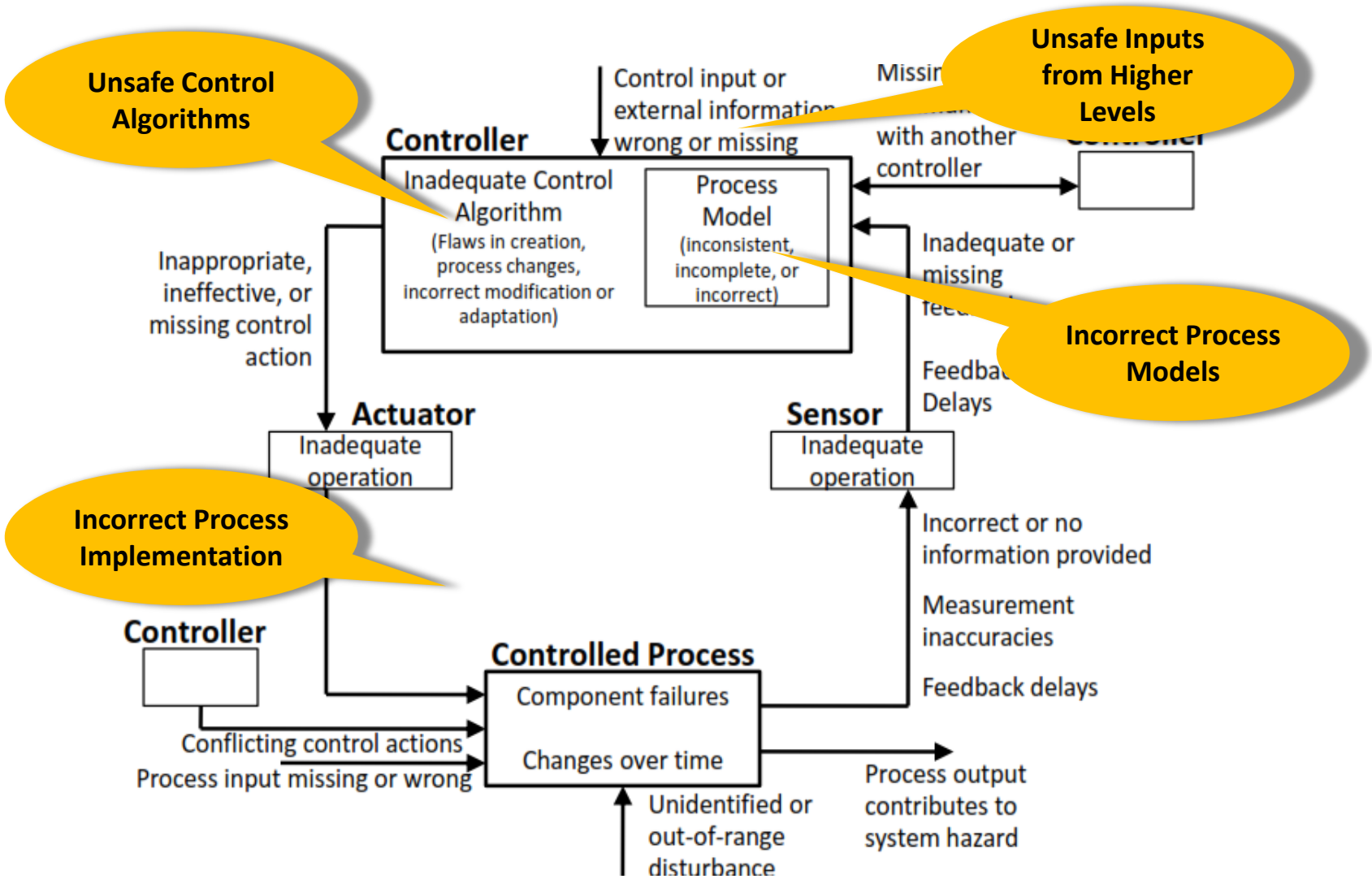
- **Hazard:** ACC did not keep safe distance between ACC vehicle and vehicle in front.
- **Unsafe Control Action:** Vehicle does not brake when the distance to the object in front is less than preset value



How could this action be caused by:

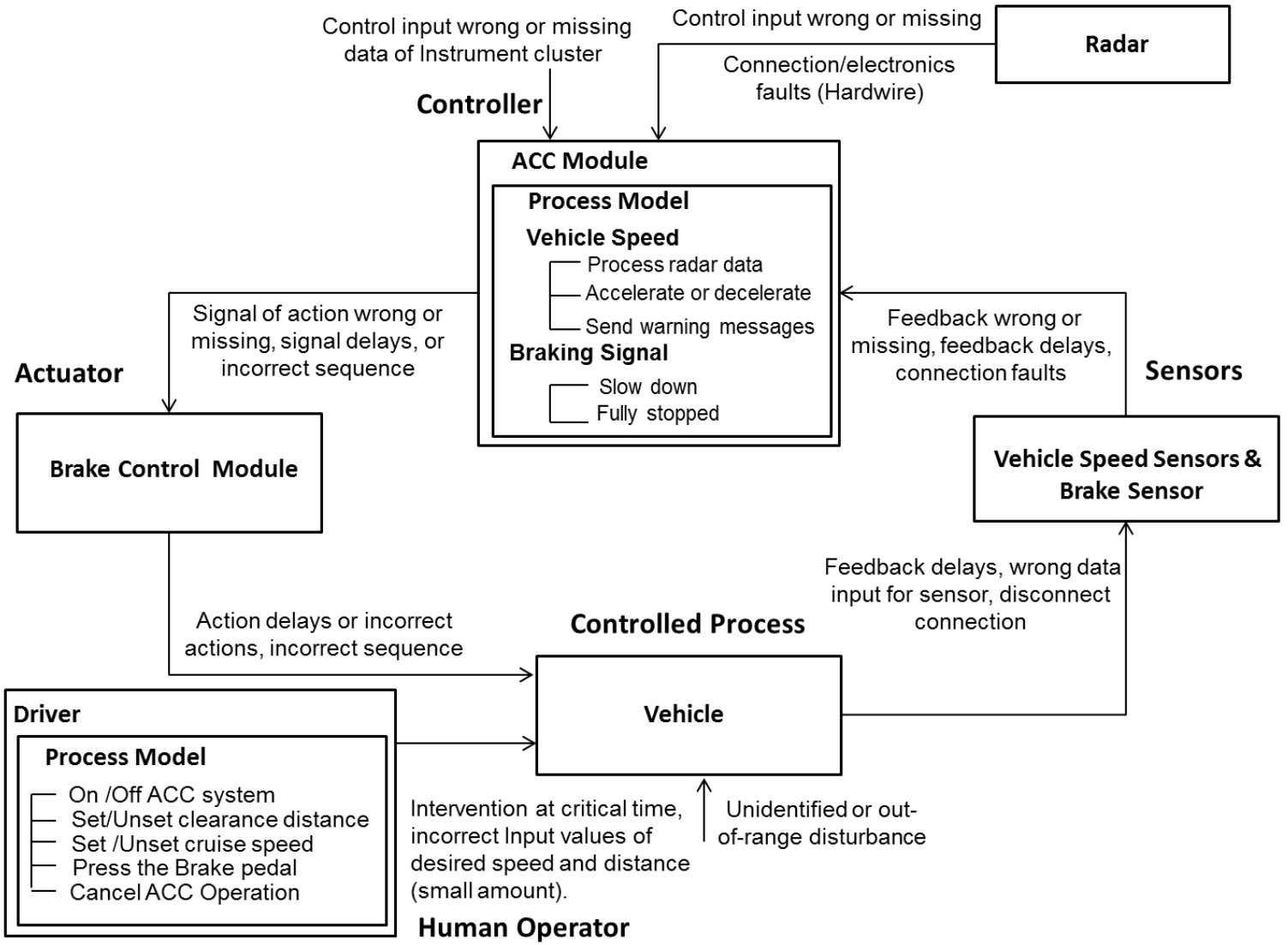
- Process Model
- Feedback
- Sensors
- Etc?

Hint: Causal Factors



Causal Factors

Hazard: ACC did not keep safe distance between ACC vehicle and vehicle in front.



Agenda

- Automotive Domain ✔
- STAMP/STPA Background ✔
- STPA Steps in Practice ✔
- STPA Group Exercise ◎
- Warp-Up
  - Participants Questions
  - Current Research Trends

A-STPA Tool Support (Automated STPA)

- **A-STPA is:**
  - implemented in Java as an open-source tool based on the Eclipse platform to assess safety analysts in performing STPA.
  - developed as a student project in the software engineering programme of the university of Stuttgart. The project started in April 2013 and finished in 28th February 2014. Our team consisted of 9 students and 3 teaching assistants.
  - supports different operating systems: Windows (32bit, 64bit), Linux and Mac OS X.

- **To download A-STPA Tool:**
  - **Fill out the form on A-STPA website:**

http://www.iste.uni-stuttgart.de/en/se/werkzeuge/a-stpa.html

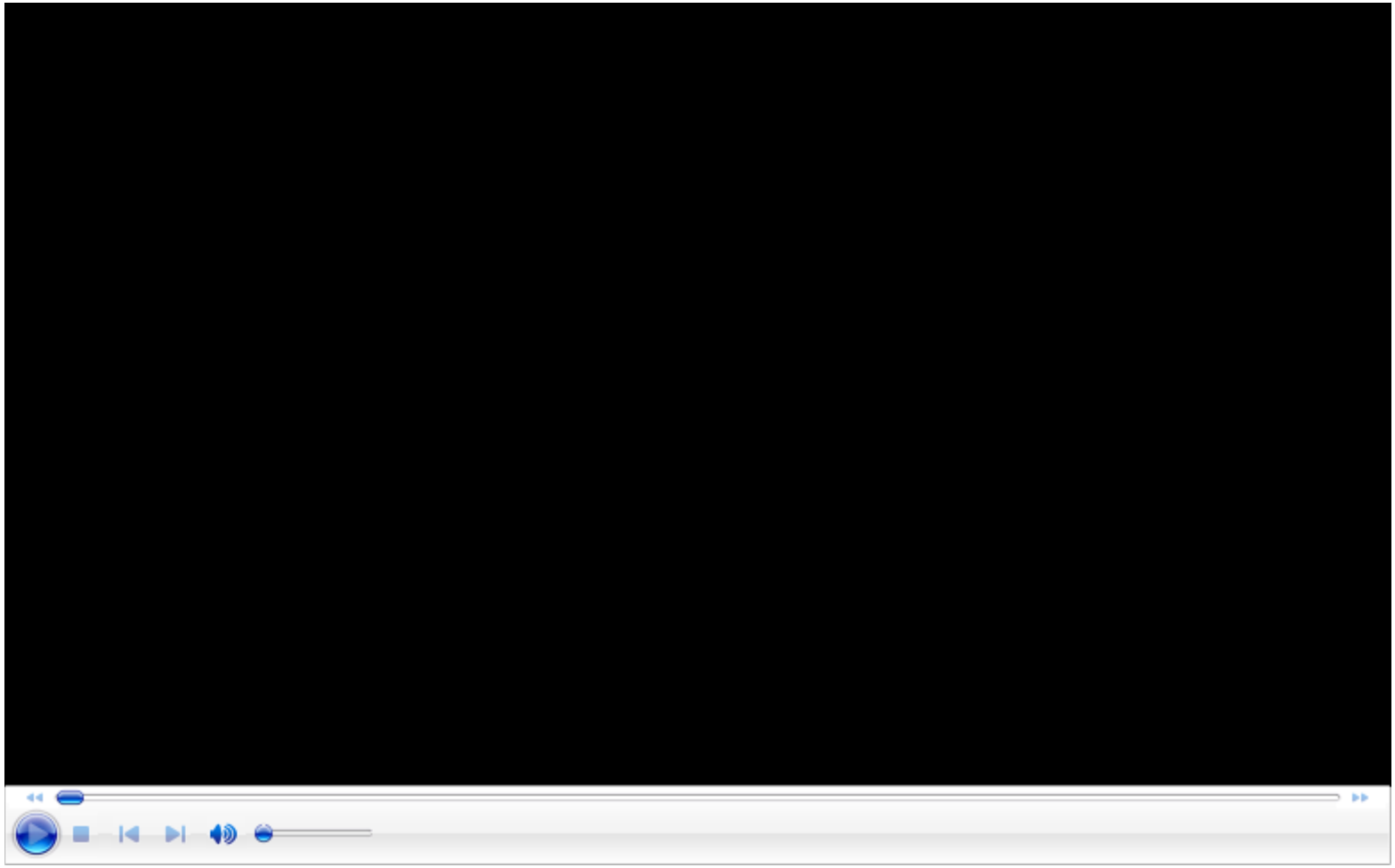
STPA Group Exercise

- **Analysing the Anti-Lock Braking System.**

  ABS is a safety system on motor vehicles which prevents the wheels from locking while braking

- **The ABS Architecture:**
  - Electronic Control Unit (ECU)
  - Hydraulic Control Unit (HCU)
  - Modulator Valves
  - Wheel speed Sensors (up to 4)
- **How does it work?**
  - The controller monitors the speed sensors all the times.
  - When the controller detects rapid decelerations in the wheel, the controller reduces the pressure to that brake until it sees an acceleration, then it increases the pressure until it sees the deceleration again.

Demo



STPA Group Exercise

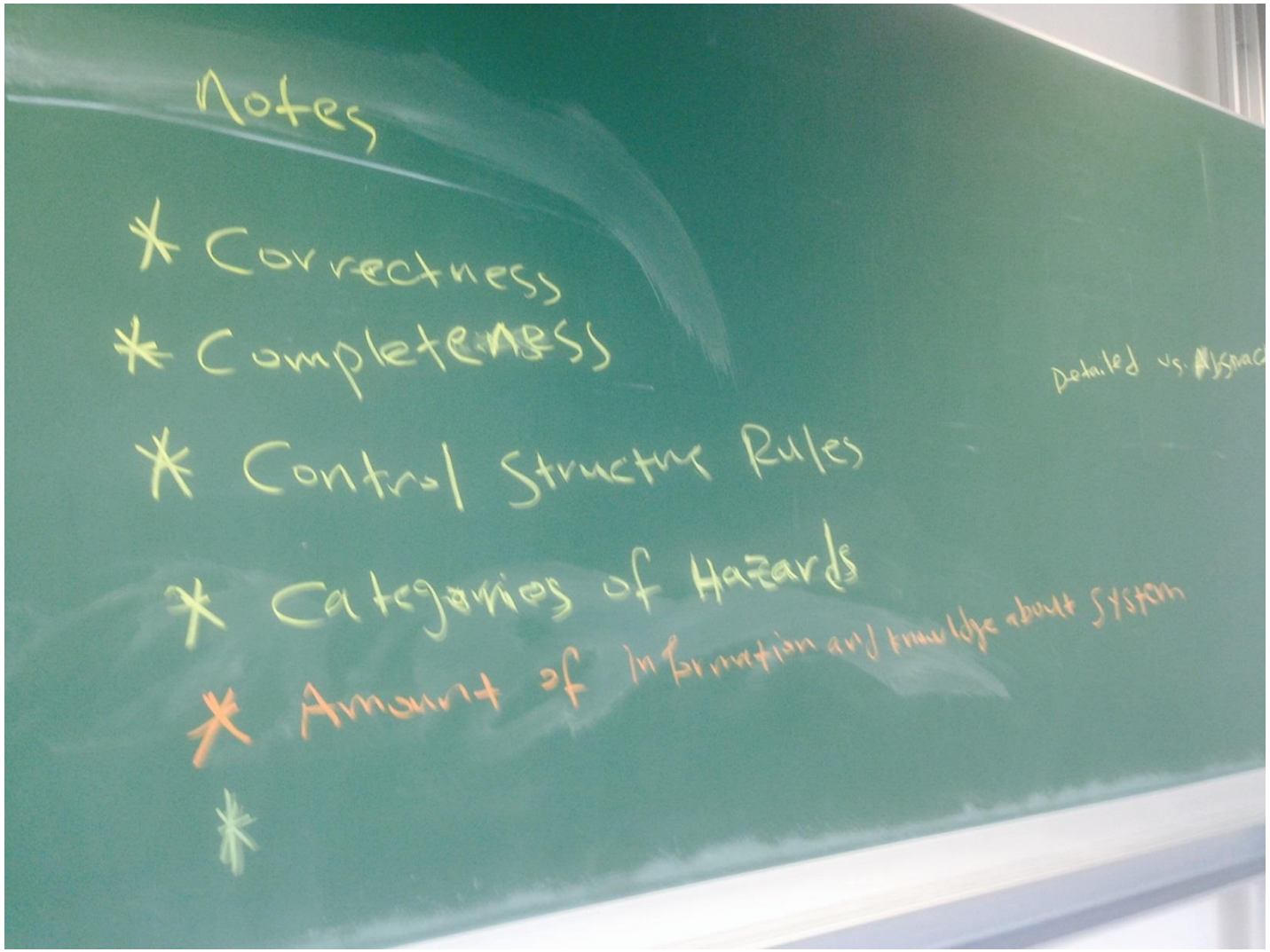
- **Identify fundamentals (accidents, hazards, safety constraints, etc.) « 15 minutes**
- **Construct the control structure « 15 minutes**
  - Identify major components and controllers
  - Label the control/feedback arrows
- **Step 1: Identify Unsafe Control Actions (UCAs) « 30 minutes**
  - Create Control Table: Not given, Given incorrectly, wrong timing, stopped too soon.
  - Create corresponding safety constraints
- **Step 2: Identify causal factors « 30 minutes**
  - Identify controller process models
  - Analyze controller, control path, feedback path, process.

Discussion & Questions

Notes of Discussion

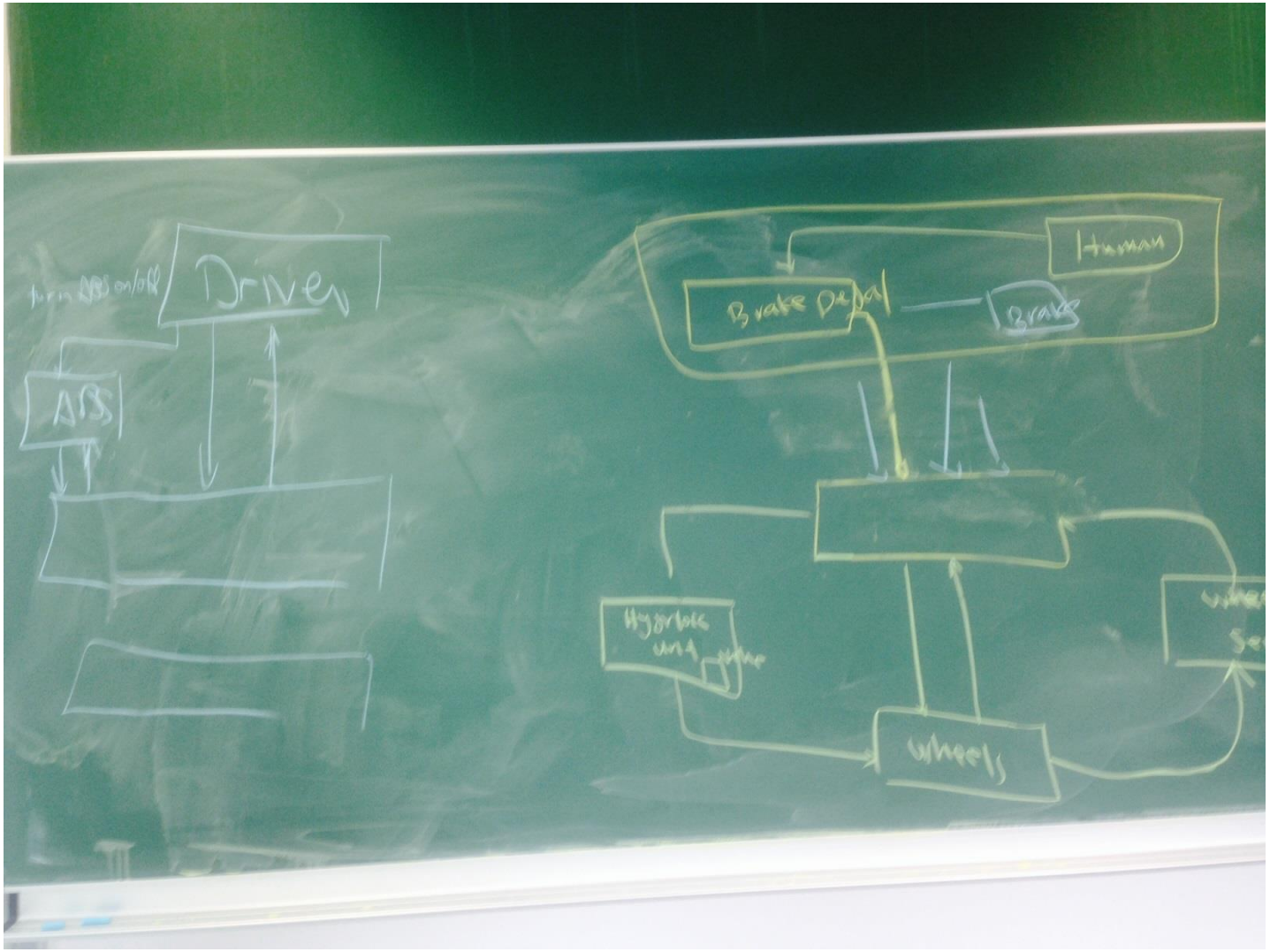
- **Main notes about Step 1:** **Correctness, Completeness, Control Structure diagram**

Rules, Categories of hazards, Amount of information and knowledge of system



Notes of Discussion

- **Issue: The level of control structure of system in automotive domain**



Detailed diagram **vs.** **Abstract diagram**