CASCAD

(**C**ausal **A**nalysis using **S**TAMP for **C**onnected and **A**utomated **D**riving)

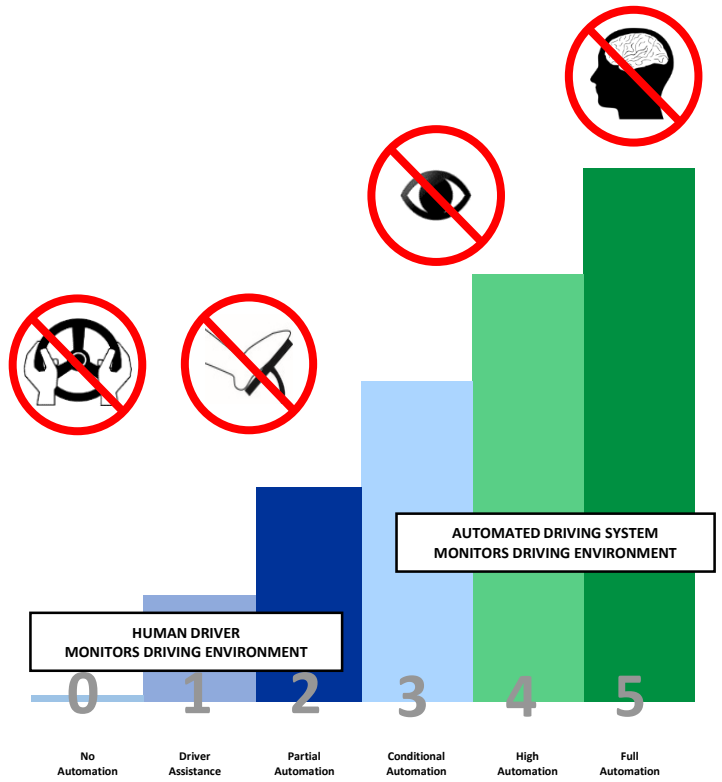
Stephanie Alvarez, Yves Page & Franck Guarnieri

MINES ParisTech

PSL RESEARCH UNIVERSITY PARIS

DACIA

Introduction:



SAE levels of vehicle automation

Vehicle automation will introduce changes into the road traffic system and bring new causal factors

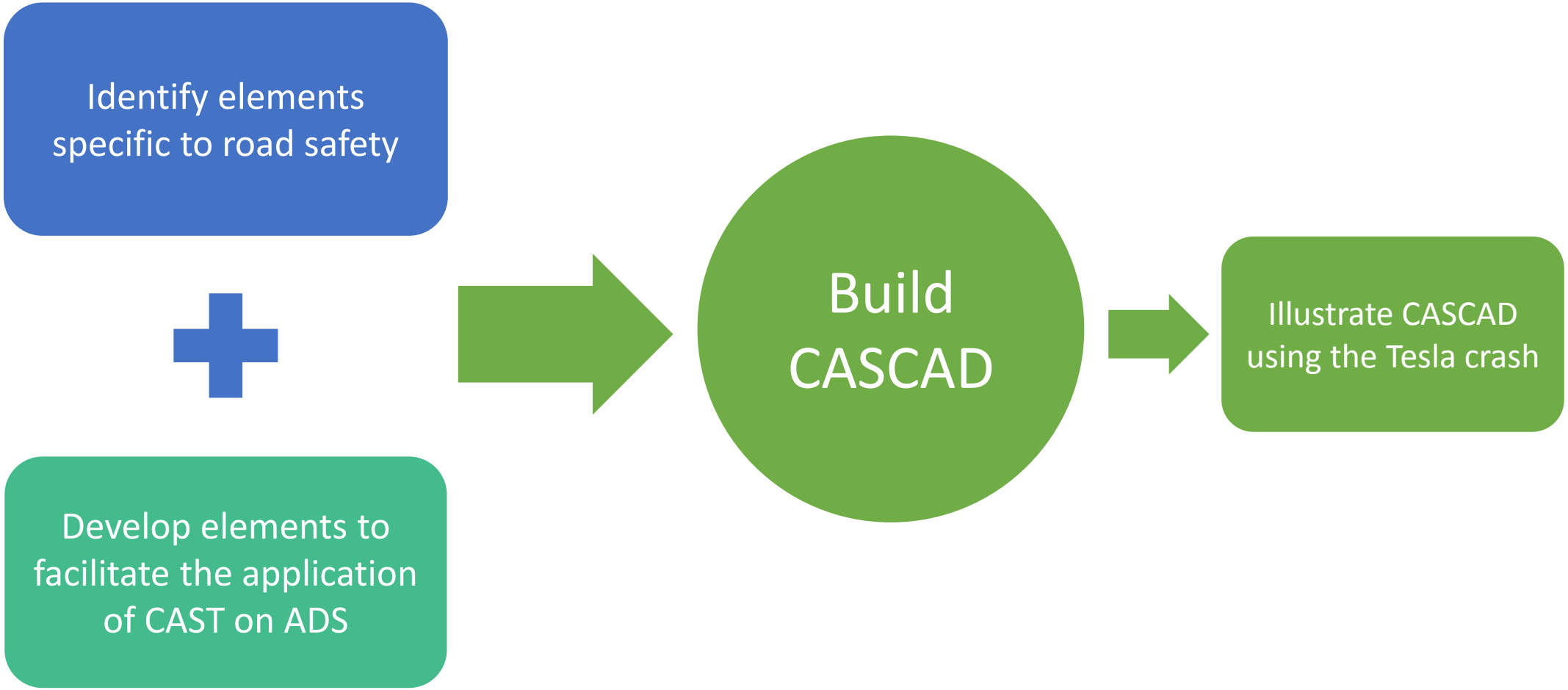
The road safety community must prepare for the analysis of crashes involving automated driving by finding appropriate accident analysis methods

CAST is appropriate for the analysis of these crashes but it is not specific to road safety and may not meet practitioner's needs

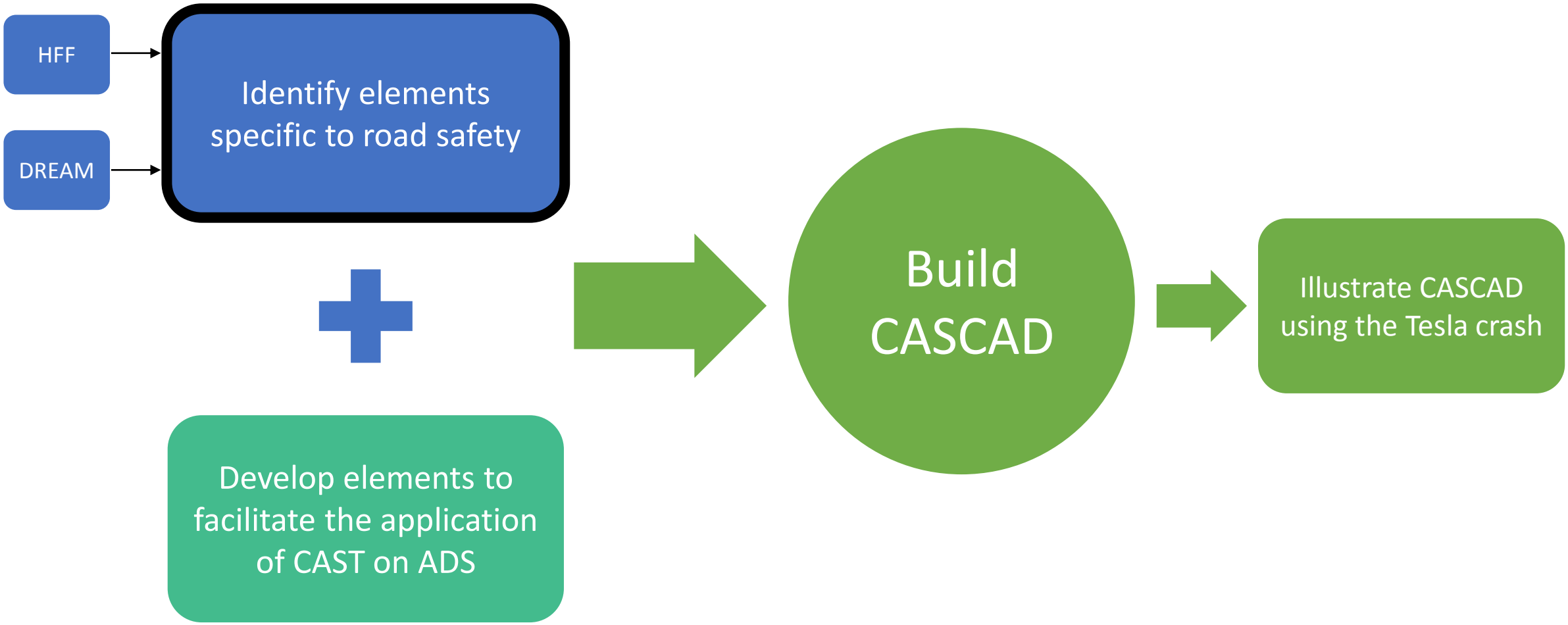
Aim:

- The aim of this work was to extend CAST into a method called CASCAD which incorporates road safety-specific elements and automated driving, to assist a more complete analysis of crashes involving vehicle automation

Approach:


Identify elements specific to road safety
Develop elements to facilitate the application of CAST on ADS
Build CASCAD
Illustrate CASCAD using the Tesla crash

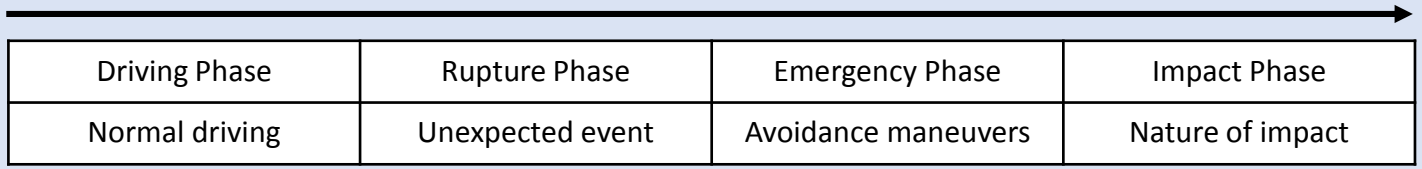
Elements specific to road safety:



Elements specific to road safety:

	HFF	DREAM
Crash Description		
Taxonomy for human failures/ errors		
Contributory factors		
Degree of involvement		

Elements specific to road safety:

	HFF	DREAM
Crash Description		
Taxonomy for human failures/ errors		
Contributory factors		
Degree of involvement		

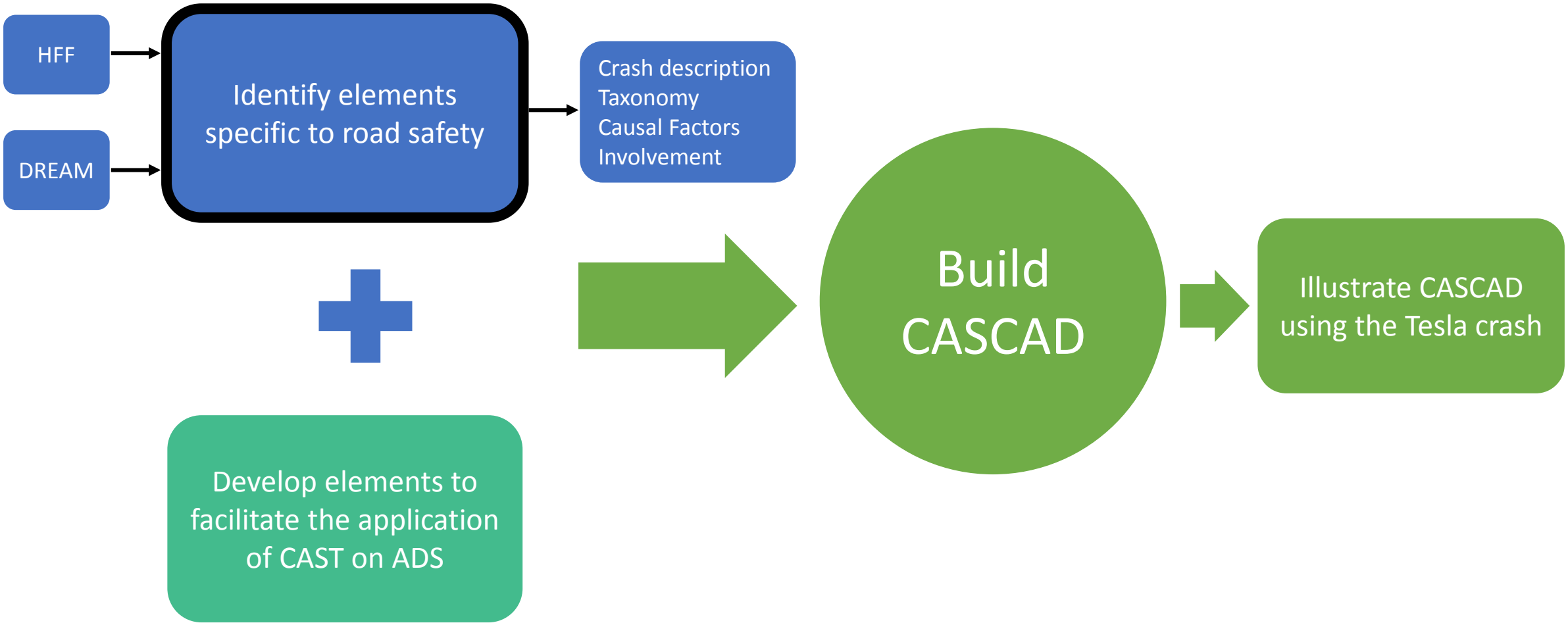
Elements specific to road safety:

<table>
<tr><th></th><th>HFF</th><th>DREAM</th></tr>
<tr><td>Crash Description</td><td colspan="2"><table><tr><td>Driving Phase</td><td>Rupture Phase</td><td>Emergency Phase</td><td>Impact Phase</td></tr><tr><td>Normal driving</td><td>Unexpected event</td><td>Avoidance maneuvers</td><td>Nature of impact</td></tr></table></td></tr>
<tr><td>Taxonomy for human failures/ errors</td><td>6 types of general failures
20 types of specific failures</td><td rowspan="2">Classification scheme
<table><tr><th>Phenotypes</th></tr><tr><td>Timing
Speed
Distance
Direction
Force</td></tr></table><table><tr><th colspan="3">Genotypes</th></tr><tr><td>Human</td><td>Technology</td><td>Organization</td></tr><tr><td>Observation
Interpretation
Planning</td><td rowspan="2">Vehicle
Traffic environment</td><td rowspan="2">Organization
Maintenance
Vehicle design
Road design</td></tr><tr><td>Personal factors</td></tr></table></td></tr>
<tr><td>Contributory factors</td><td>List of explanatory factors related to the human driver, the road, the traffic and the vehicle</td></tr>
<tr><td>Degree of involvement</td><td></td><td></td></tr>
</table>

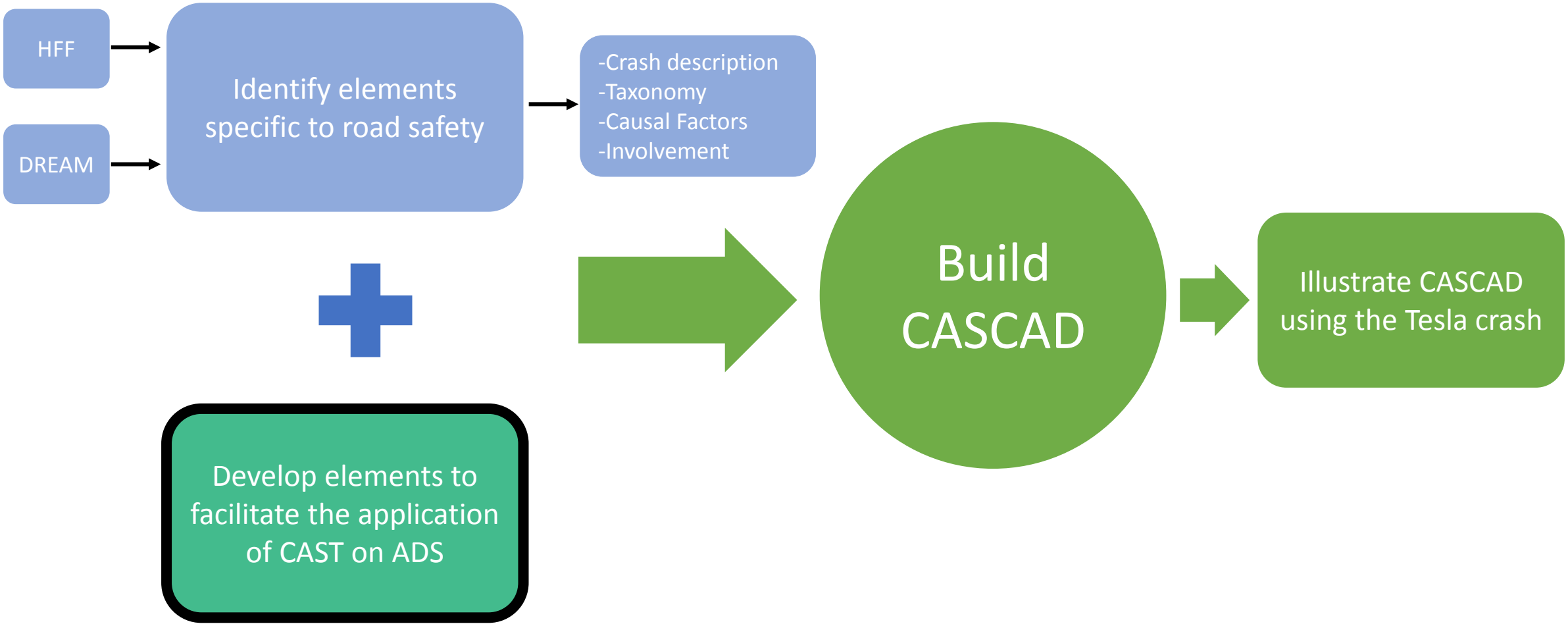
Elements specific to road safety:

<table>
<tr><th></th><th>HFF</th><th>DREAM</th></tr>
<tr><td>Crash Description</td><td colspan="2"><table><tr><td>Driving Phase</td><td>Rupture Phase</td><td>Emergency Phase</td><td>Impact Phase</td></tr><tr><td>Normal driving</td><td>Unexpected event</td><td>Avoidance maneuvers</td><td>Nature of impact</td></tr></table></td></tr>
<tr><td>Taxonomy for human failures/ errors</td><td>6 types of general failures
20 types of specific failures</td><td rowspan="2">Classification scheme
<table><tr><th>Phenotypes</th></tr><tr><td>Timing
Speed
Distance
Direction
Force</td></tr></table><table><tr><th colspan="3">Genotypes</th></tr><tr><td>Human</td><td>Technology</td><td>Organization</td></tr><tr><td>Observation
Interpretation
Planning</td><td rowspan="2">Vehicle
Traffic environment</td><td rowspan="2">Organization
Maintenance
Vehicle design
Road design</td></tr><tr><td>Personal factors</td></tr></table></td></tr>
<tr><td>Contributory factors</td><td>List of explanatory factors related to the human driver, the road, the traffic and the vehicle</td></tr>
<tr><td>Degree of involvement</td><td>a) Primary active
b) Secondary active
c) Non-active
d) Passive</td><td>NA</td></tr>
</table>

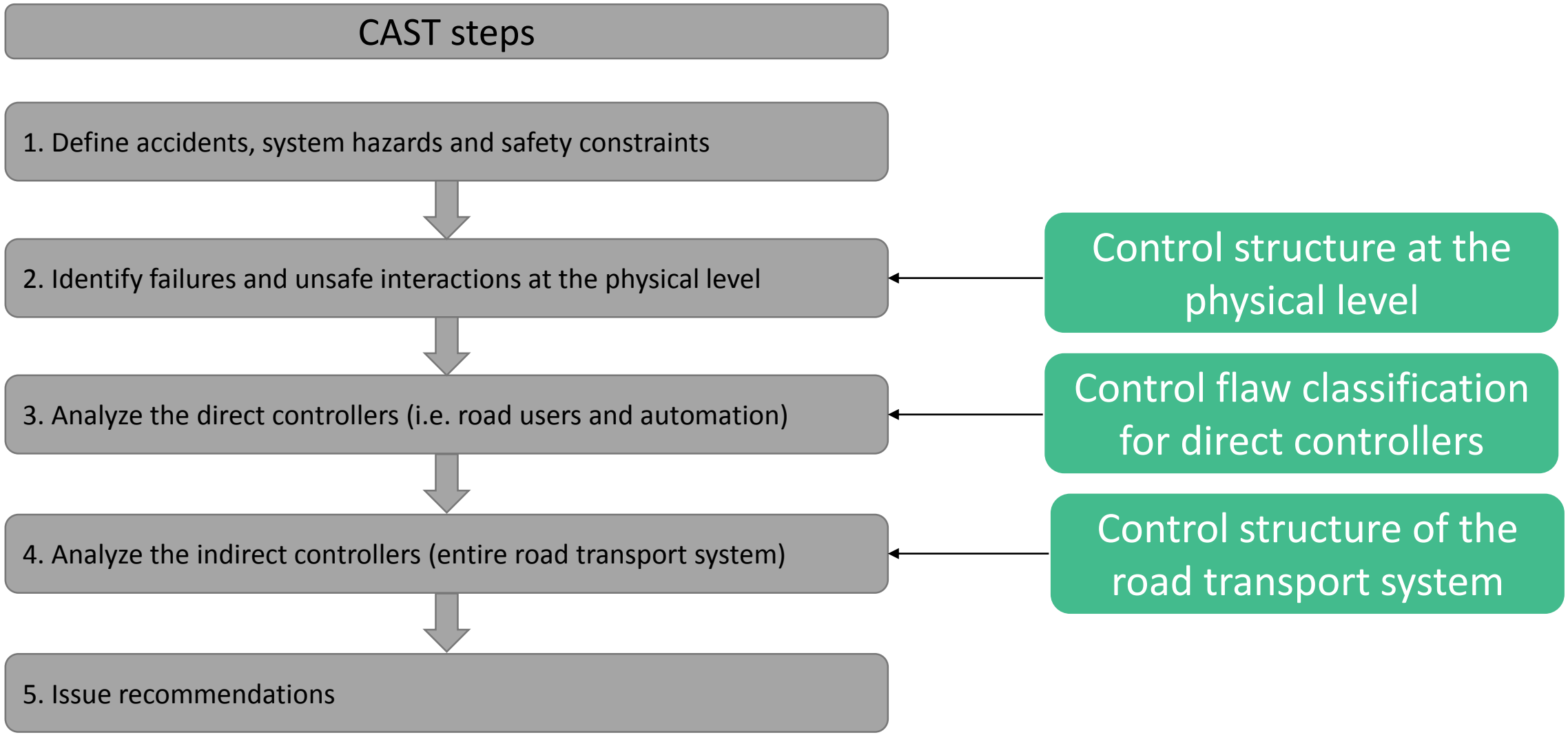
Elements to facilitate the application of CAST:



Elements to facilitate the application of CAST:

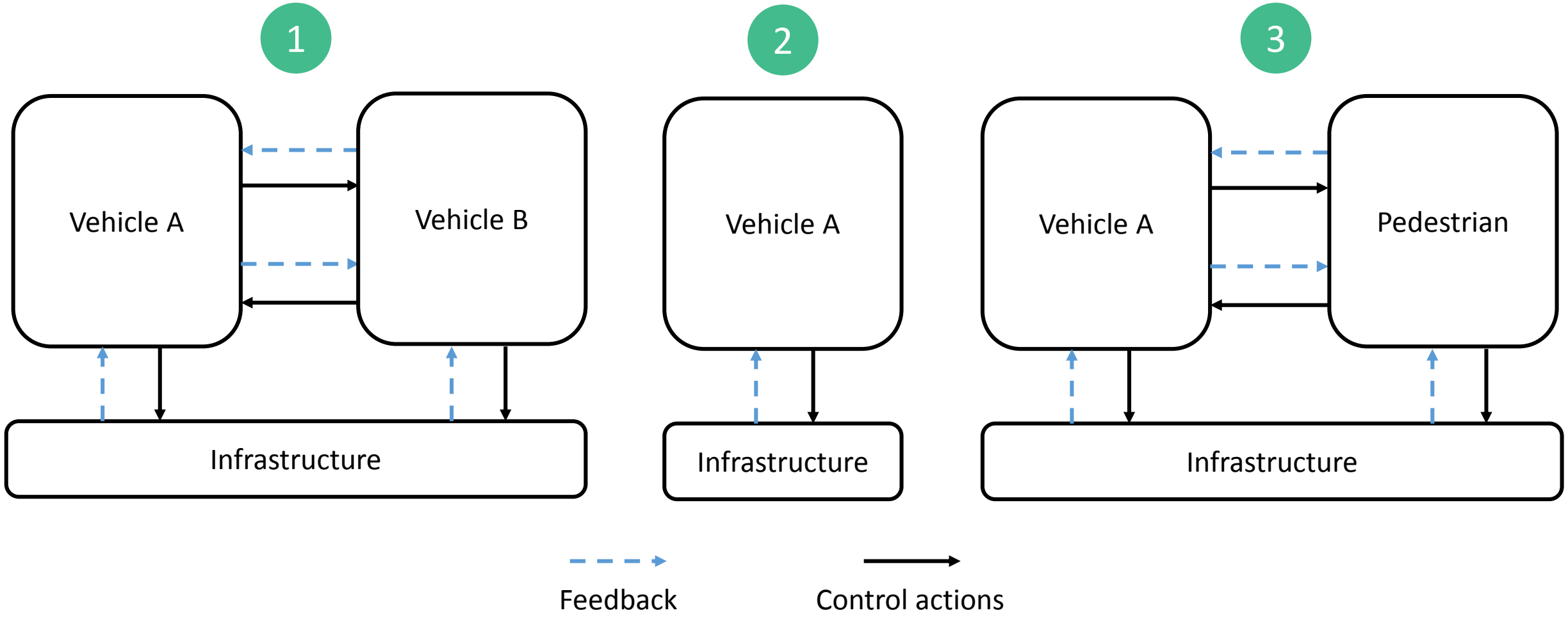


Elements to facilitate the application of CAST:



Elements to facilitate the application of CAST:

Control structure at the physical level



Elements to facilitate the application of CAST:

Control flaw classification for direct controllers

Control structure of an automated vehicle an a non-automated vehicle

→

Examine the interactions of direct controllers

→

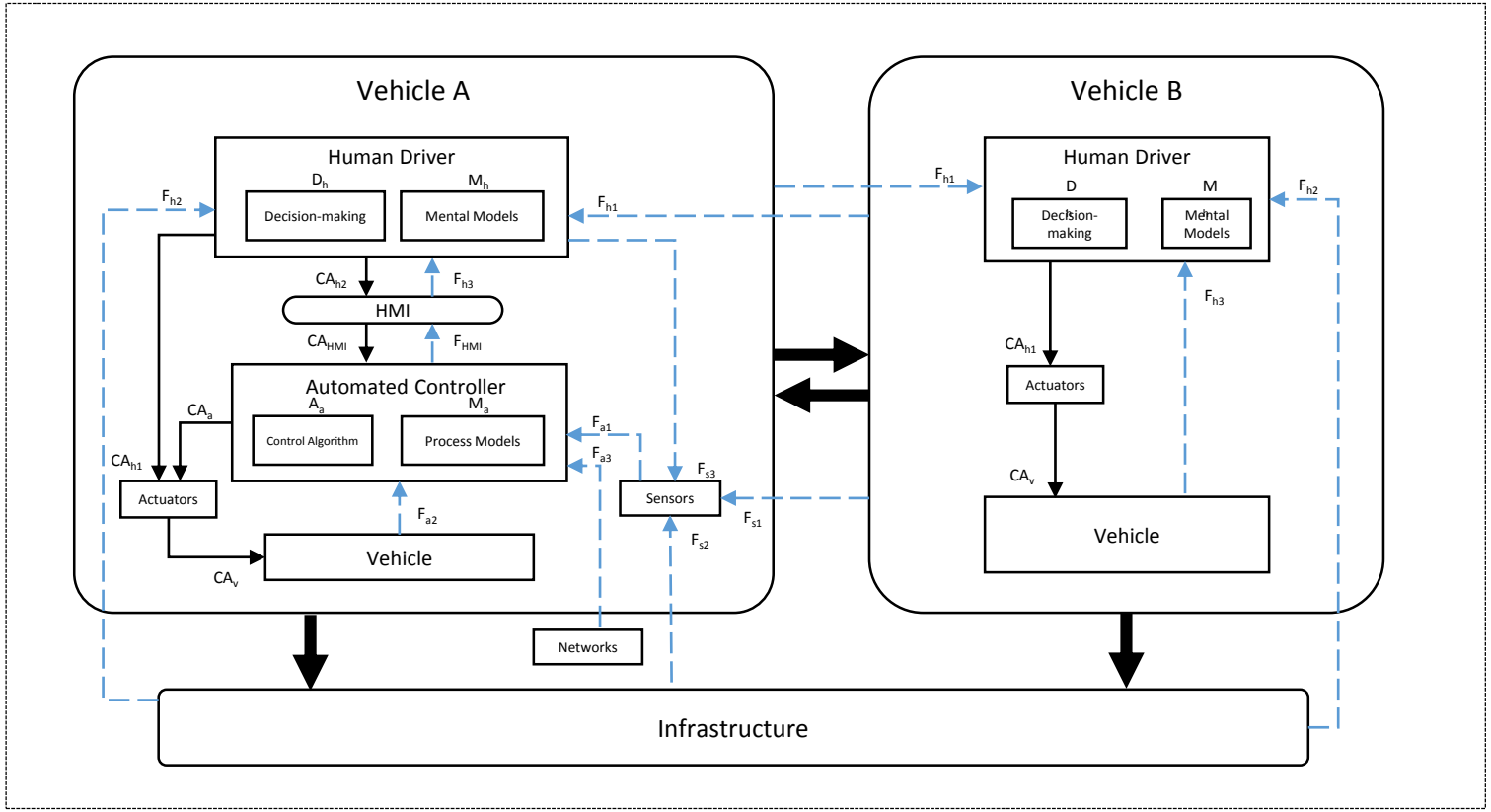
Identify control flaws:

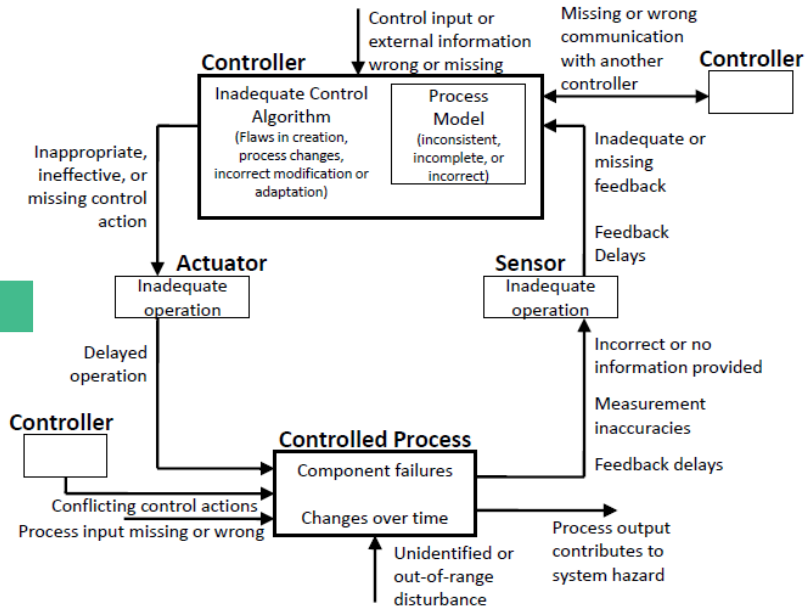
- Perception (feedback)
- Mental Models
- Decision-making
- Action Execution

(Leveson, 2011; Leveson et al. 2013)

Elements to facilitate the application of CAST:

Control flaw classification for direct controllers





(Leveson, 2011; Leveson et al. 2013)

Elements to facilitate the application of CAST:

Control flaw classification for direct controllers

Control structure of an automated vehicle and a non-automated vehicle

→

Examine the interactions of direct controllers

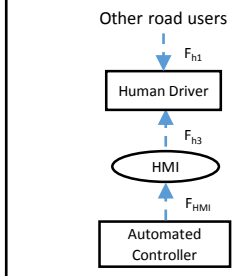
→

Identify control flaws:

- Perception (feedback)
- Mental Models
- Decision-making
- Action Execution

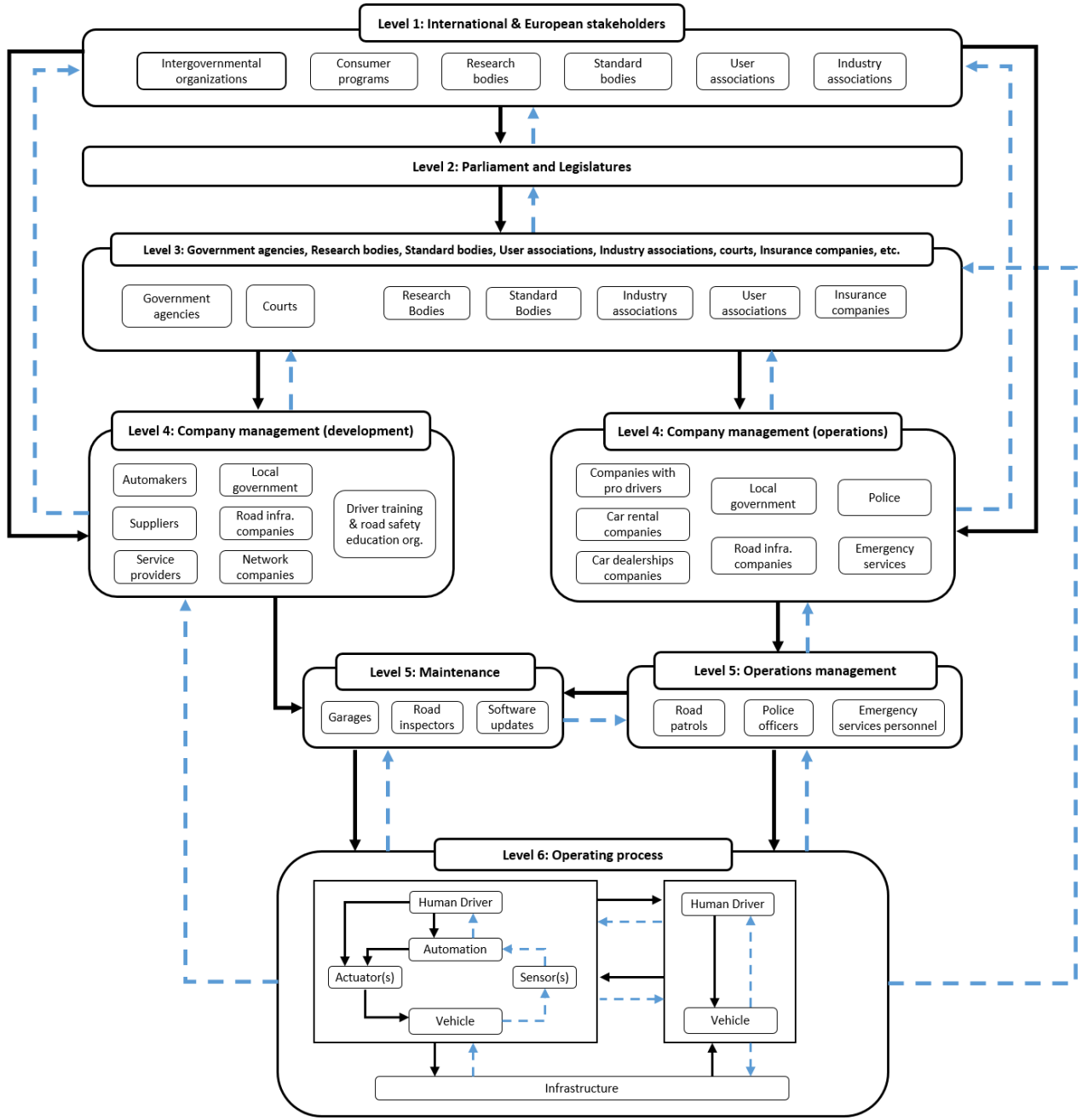
→ 58 control flaws for the human driver controller

→ 48 control flaws for the automated controller

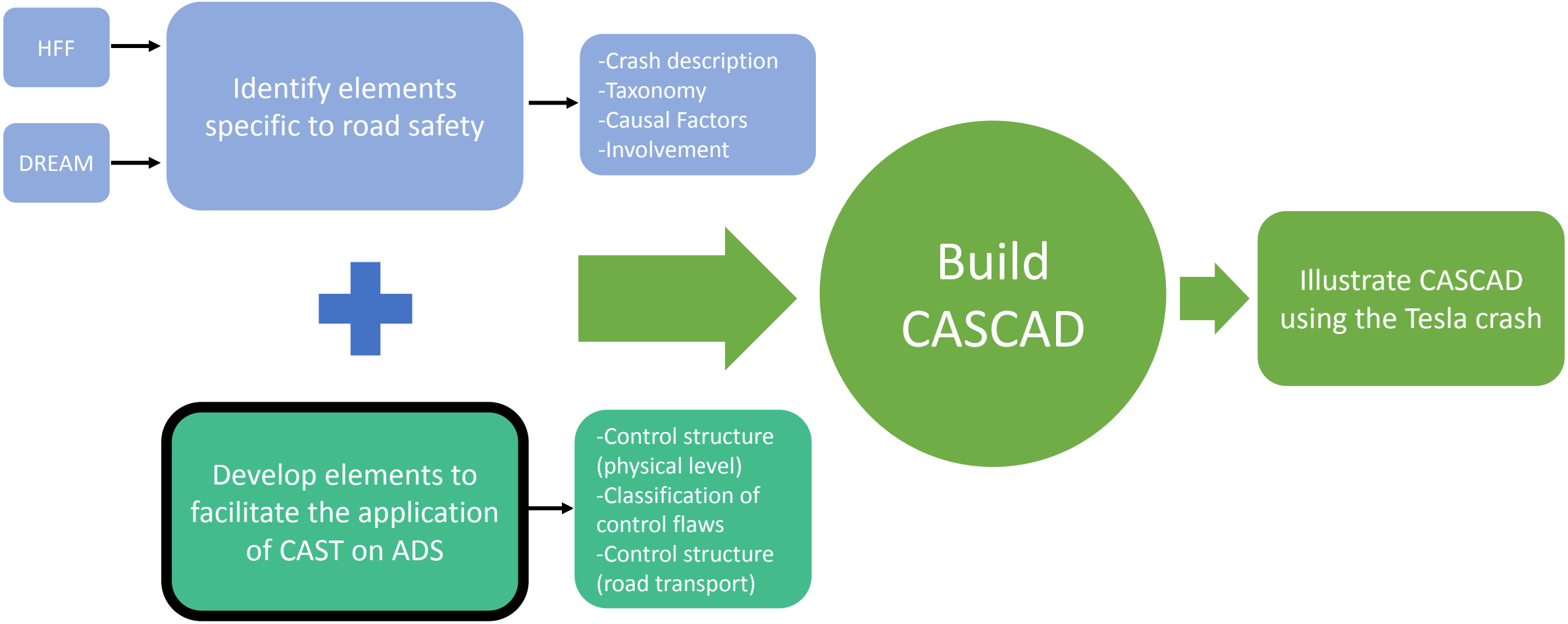
Human Driver Controller							
Category		Control flaw	Example	SAE level			
				0	1-2	3	4
Perception		Missing human perception of feedback on another road user (F_{h1})	The human driver does not perceive a road user in the adjacent lane	x	x	x	
		Incorrect information provided by automation (F_{HMI})	Automation provides the HMI with incorrect info relative to the speed of another vehicle		x	x	x
		Missing human perception of HMI feedback (F_{h3})	A human driver does not perceive a takeover request			x	x

Excerpt from the control flaws table associated to the human driver controller

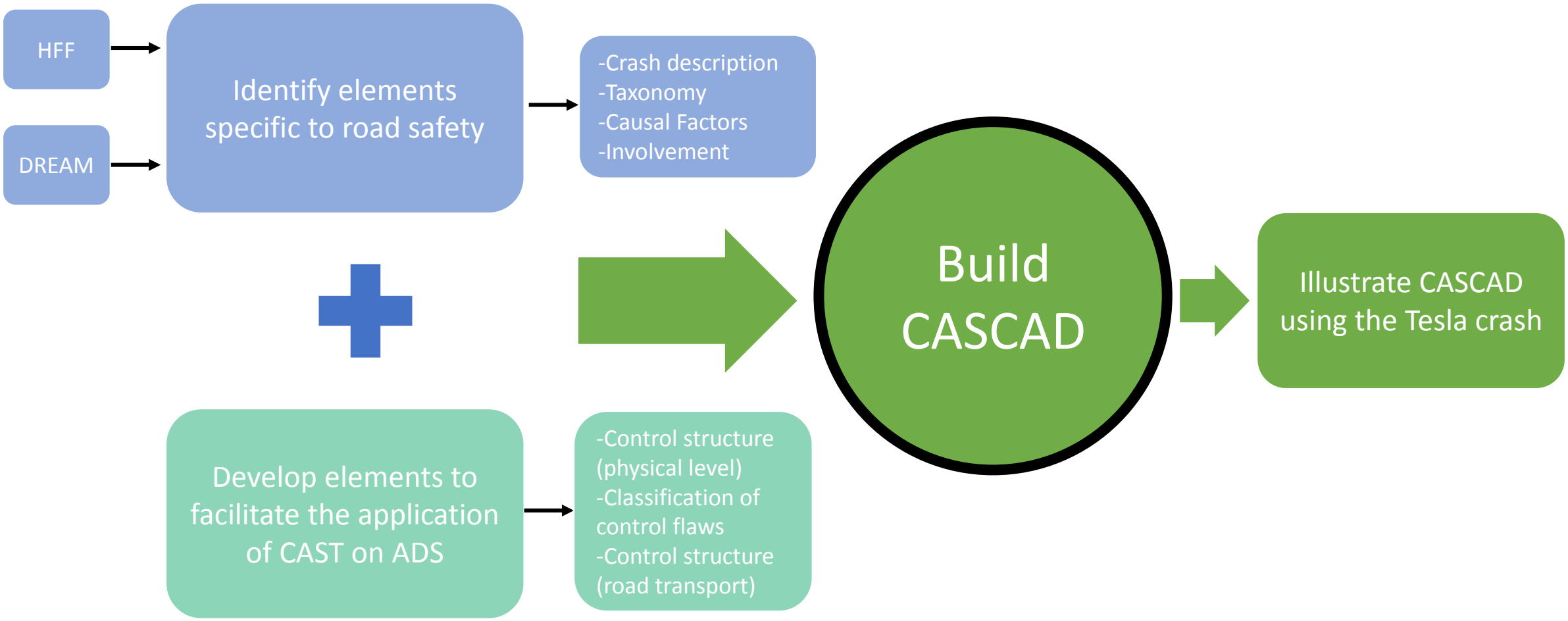
Control structure of the road transport system



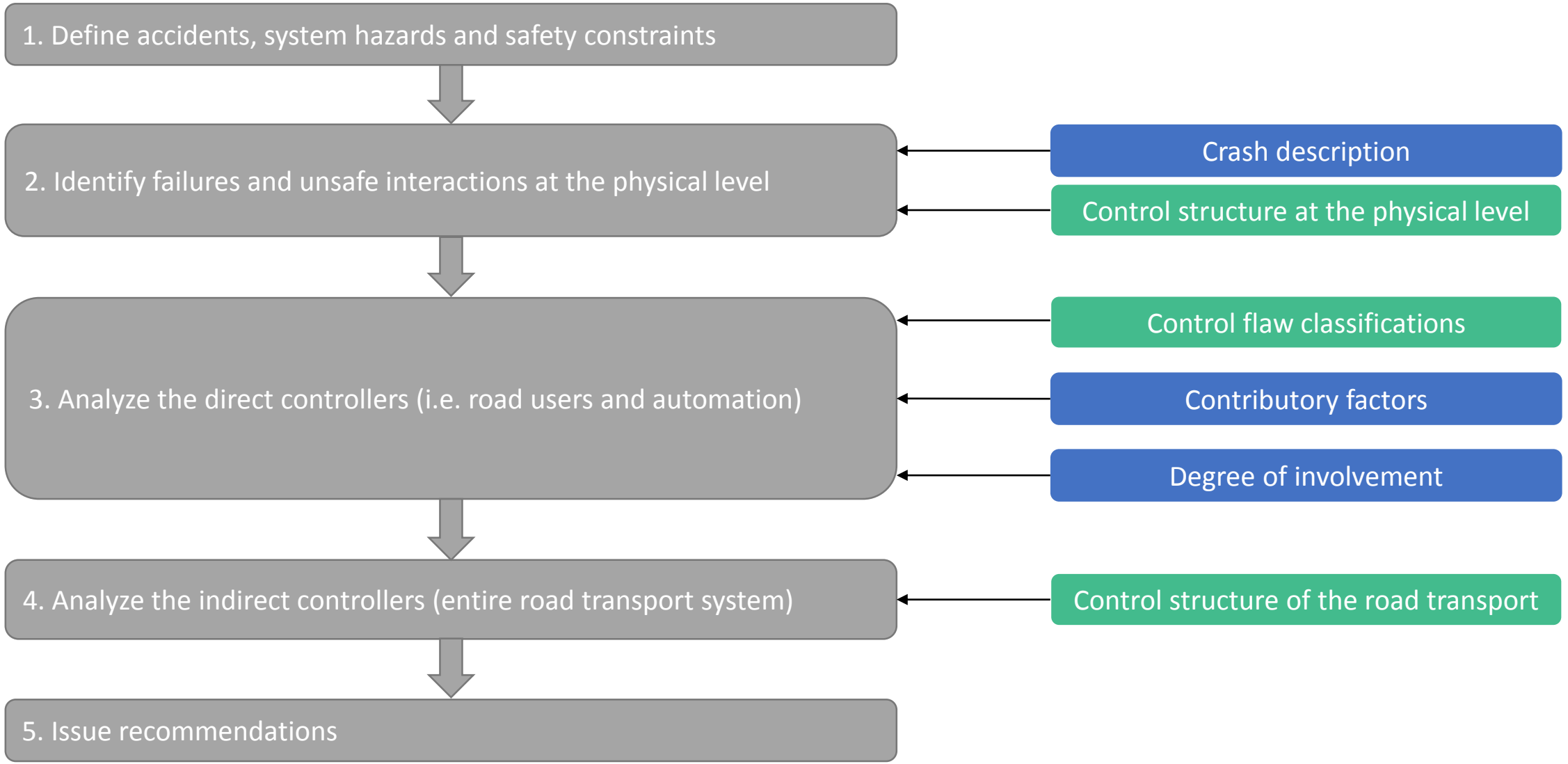
Elements to facilitate the application of CAST:



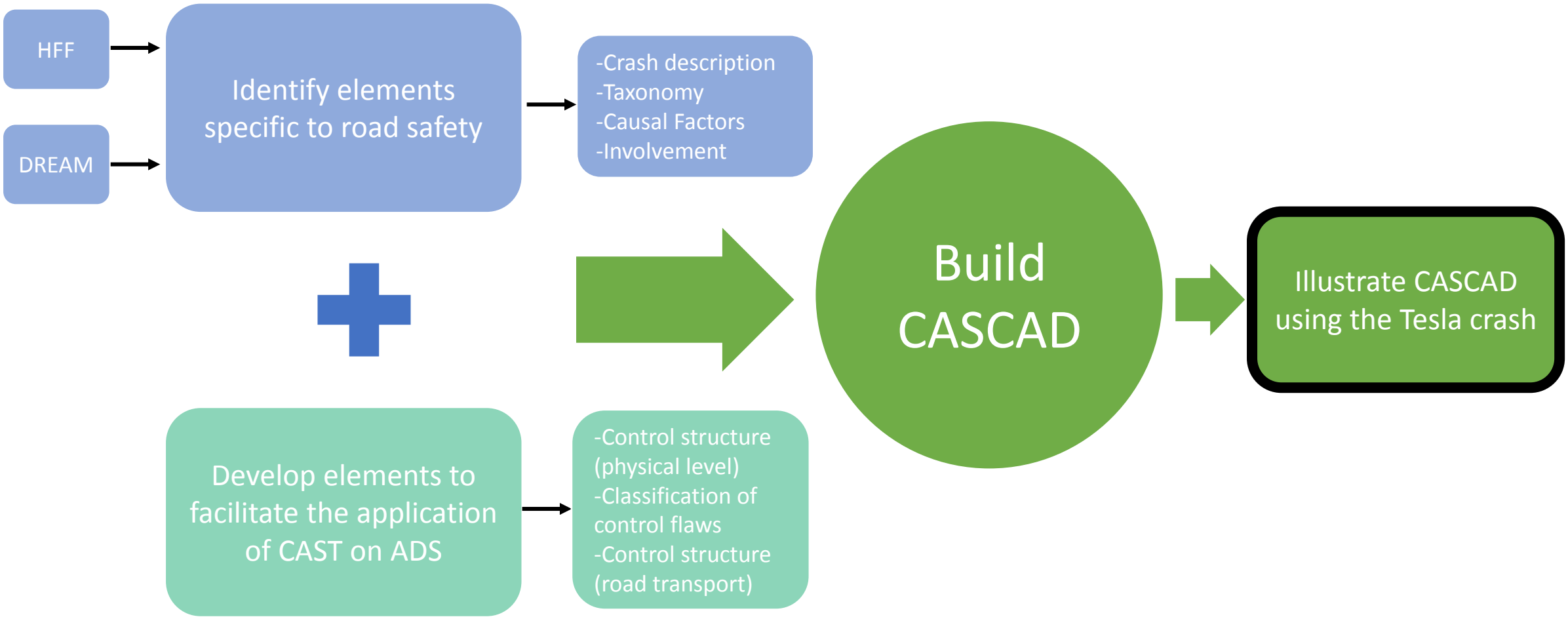
Building CASCAD:



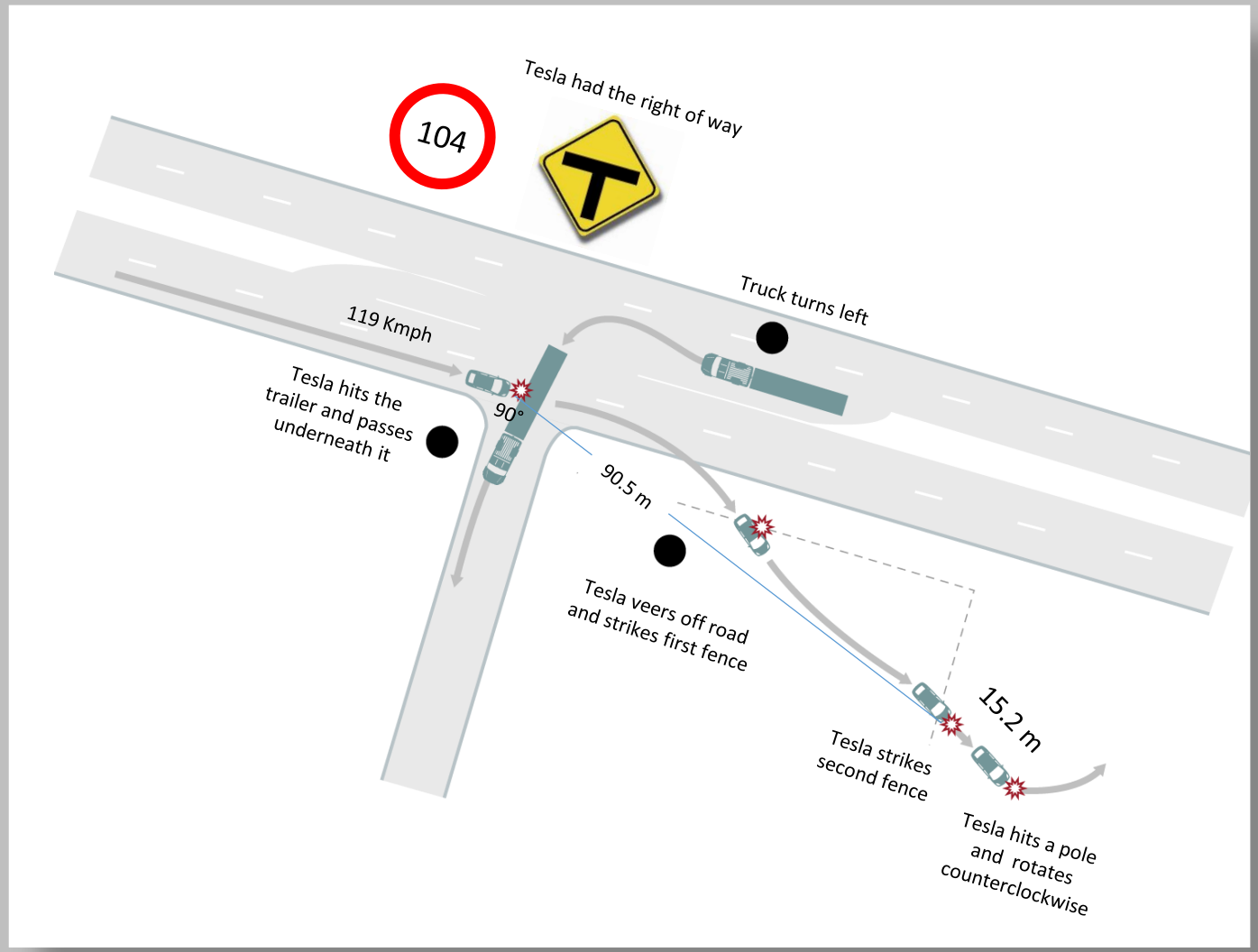
Building CASCAD:



Illustrating CASCAD:



Tesla crash description



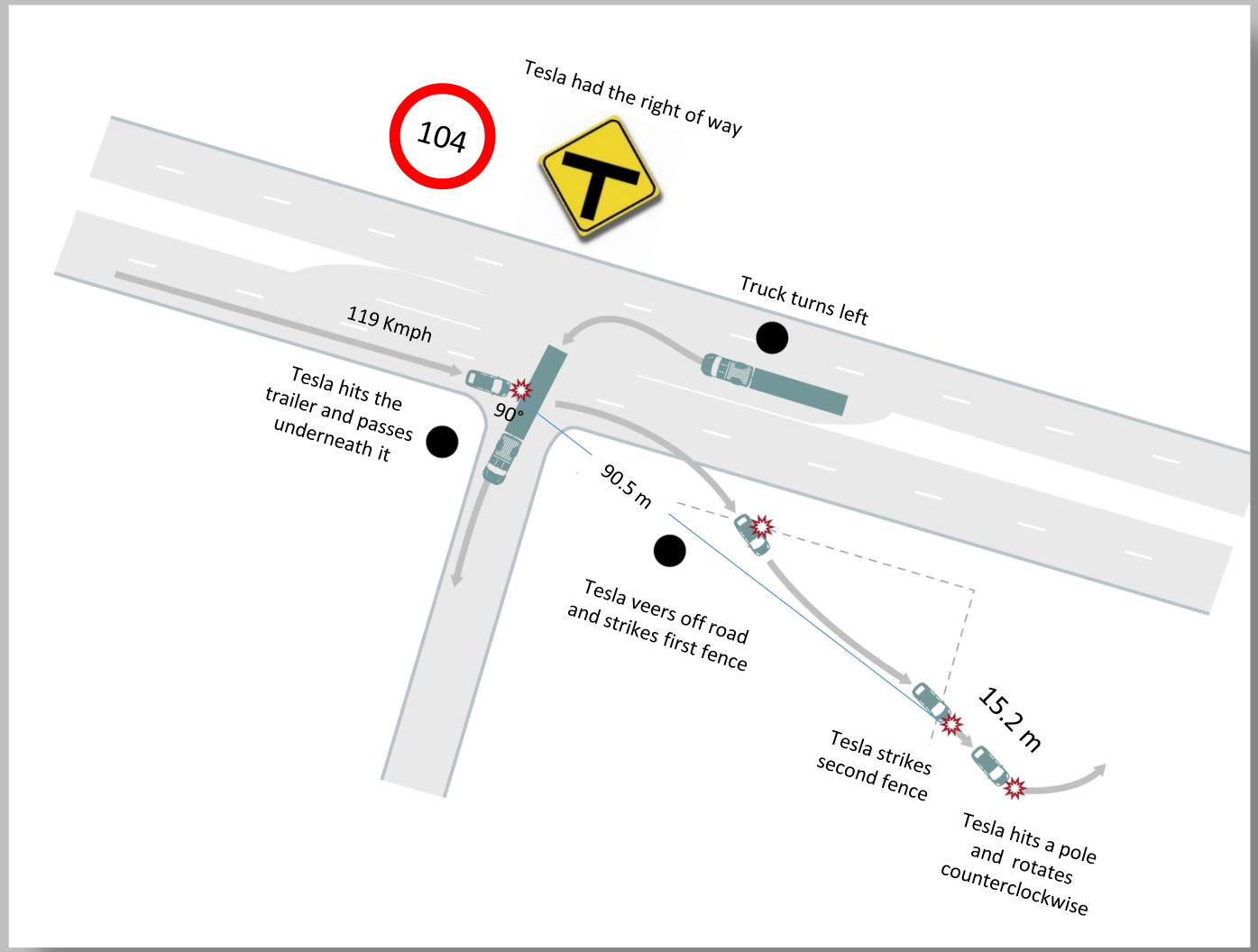
(A. Singhvi & K. Russell 2016)

- 16h40 on Saturday May 7th in central Florida (US27A)
- Daylight with clear and dry weather conditions

Tesla	
2015 Tesla S	
40 year old male	
Autopilot was engaged	AEB did not brake

Truck
2014 Freightliner Cascadia truck + semitrailer
63 year old male (Okemah Express)
Manual driving mode

Tesla crash description

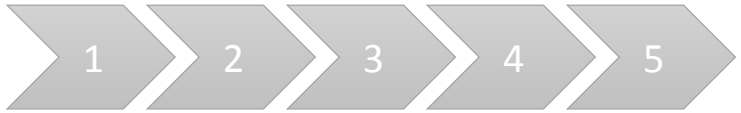


(A. Singhvi & K. Russell 2016)

(National Transportation Board 2016)

(National Transportation Board 2016)

Illustrating CASCAD:



1. Define accidents, system hazards and safety constraints

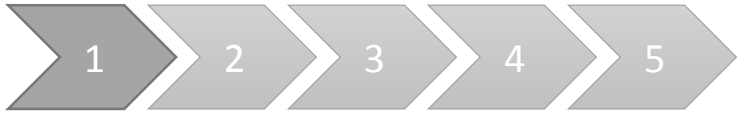
2. Identify failures and unsafe interactions at the physical level
   - Crash description
   - Control structure at the physical level

3. Analyze the direct controllers (i.e. road users and automation)
   - Control flaw classifications
   - Contributory factors
   - Degree of involvement

4. Analyze the indirect controllers (entire road transport system)
   - Control structure of the road transport

5. Issue recommendations

Illustrating CASCAD:



1. Define accidents, system hazards and safety constraints

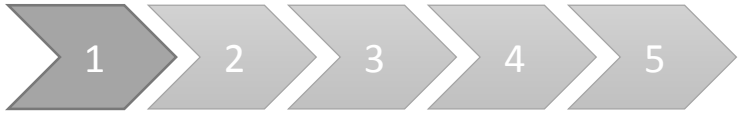
2. Identify failures and unsafe interactions at the physical level
   - Crash description
   - Control structure at the physical level

3. Analyze the direct controllers (i.e. road users and automation)
   - Control flaw classifications
   - Contributory factors
   - Degree of involvement

4. Analyze the indirect controllers (entire road transport system)
   - Control structure of the road transport

5. Issue recommendations

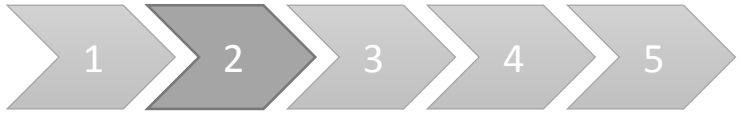
Illustrating CASCAD:



1 Define accidents, system hazards and safety constraints

Accident	Human loss due to a vehicle collision
System Hazard	Violation of minimal safety distance between the Tesla and the truck
System Safety Constraint	The safety control structure must prevent the violation of minimal distance between a vehicle and a truck

Illustrating CASCAD:



1. Define accidents, system hazards and safety constraints

2. Identify failures and unsafe interactions at the physical level
   - Crash description
   - Control structure at the physical level

3. Analyze the direct controllers (i.e. road users and automation)
   - Control flaw classifications
   - Contributory factors
   - Degree of involvement

4. Analyze the indirect controllers (entire road transport system)
   - Control structure of the road transport

5. Issue recommendations

Illustrating CASCAD:

1 2 3 4 5

2 Identify failures and unsafe interactions at the physical level

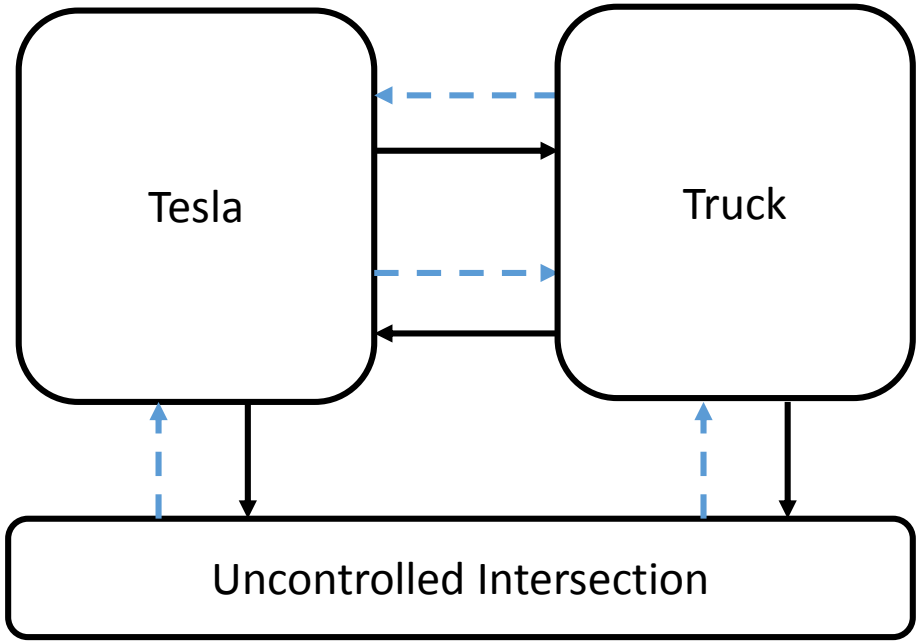
Crash description

Vehicle	Driving phase	Rupture phase	Emergency phase	Crash phase
	The Tesla is travelling on a highway on a Saturday at 4:40 pm.	The Tesla does not slow down as it approaches an uncontrolled intersection	The Tesla violates the minimal safety distance to the truck and does not decrease the speed of the vehicle	The front of the Tesla strikes the trailer of the truck with a 90° angle at 119 km/h, passes underneath the trailer, leaves the road and hits two fences and a pole before rotating counterclockwise and coming to rest
	The truck is travelling on a highway on a Saturday at 4:40 pm to deliver blueberries	The truck estimates that it can engage a left turn maneuver	The truck engages a left turn maneuver and does not have the time to stop as the Tesla approaches at 119 km/h.	The bottom of the truck's semitrailer is hit by the Tesla

Illustrating CASCAD:

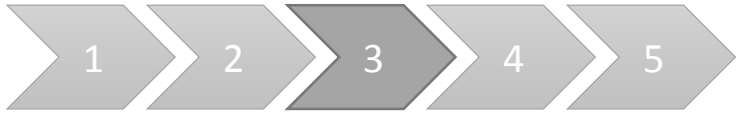
1 2 3 4 5

2 Identify failures and unsafe interactions at the physical level



- **Physical failures?** None
- **Unsafe interactions at the physical level:**
  - The truck made a left turn too soon at a highway intersection when it did not have the right of way
  - The Tesla vehicle did not slow down/stop the car when the safety distance to a truck was violated

Illustrating CASCAD:



1. Define accidents, system hazards and safety constraints

2. Identify failures and unsafe interactions at the physical level
   - Crash description
   - Control structure at the physical level

3. Analyze the direct controllers (i.e. road users and automation)
   - Control flaw classifications
   - Contributory factors
   - Degree of involvement

4. Analyze the indirect controllers (entire road transport system)
   - Control structure of the road transport

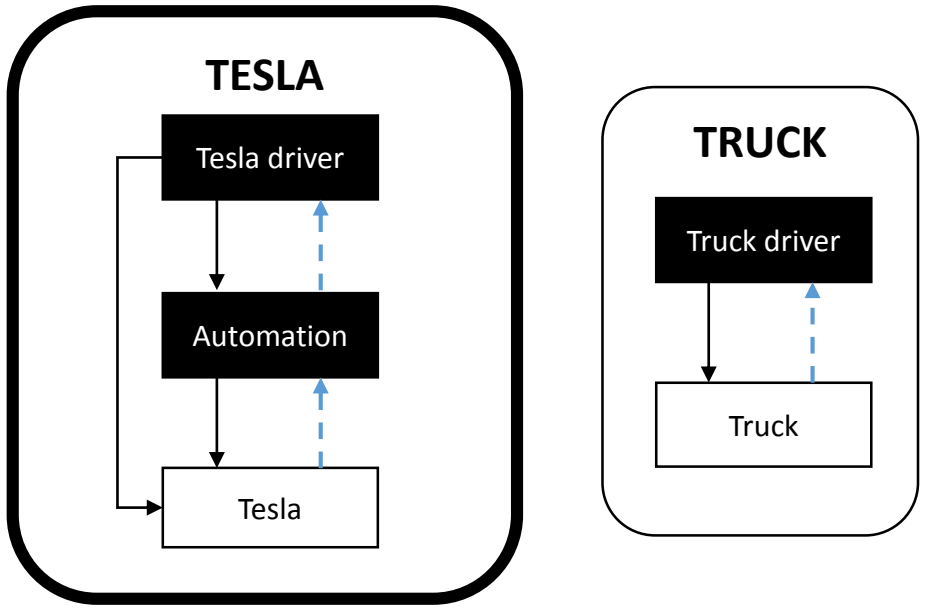
5. Issue recommendations

Illustrating CASCAD:

1 2 3 4 5

3 Analyze the direct controllers (automation and human drivers)

Direct Controllers



Analysis

A. Unsafe Control Action

B. Control flaws

- Control flaw classifications
- Contributory factors

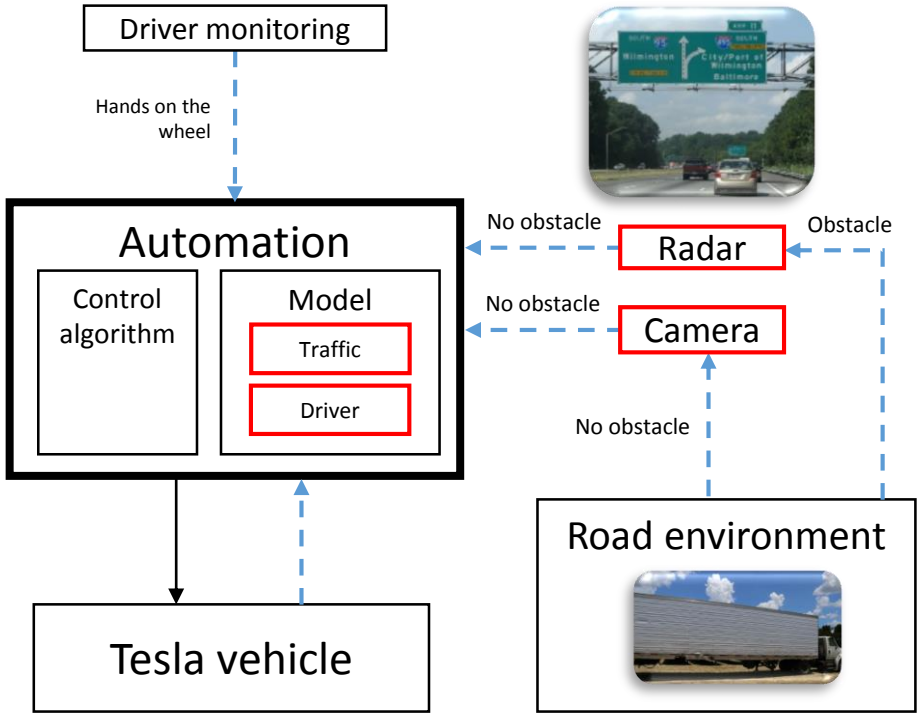
C. Context in which decisions were made

Degree of involvement

Illustrating CASCAD:

1 2 3 4 5

A. UCA: Automation did not apply brakes when the vehicle violated the safety distance to the truck



B. CONTROL FLAWS (Automation)			
Category	**Control flaw**	**Description**	**Contributory factors**
Perception	Measurement inaccuracies on road users' feedback provided by sensors	Camera provided inaccurate measures due to the white trailer being against bright sky	Bright sky influence on camera's detection
	Inadequate or incorrect feedback provided by sensors	The radar provided incorrect feedback because it tuned out the data on the truck obstacle to avoid false braking events (overhead traffic signs).	False positives
Model of process	Inadequate model of the traffic situation	The autopilot and the AEB module were unaware of the presence of the truck due to incorrect feedback	Reliability and performance of the perception system
	Inadequate model of the human driver	Automation was unaware that the driver was distracted because the driver monitoring system does not detect when drivers have their eyes off the road	Design of the driver monitoring system

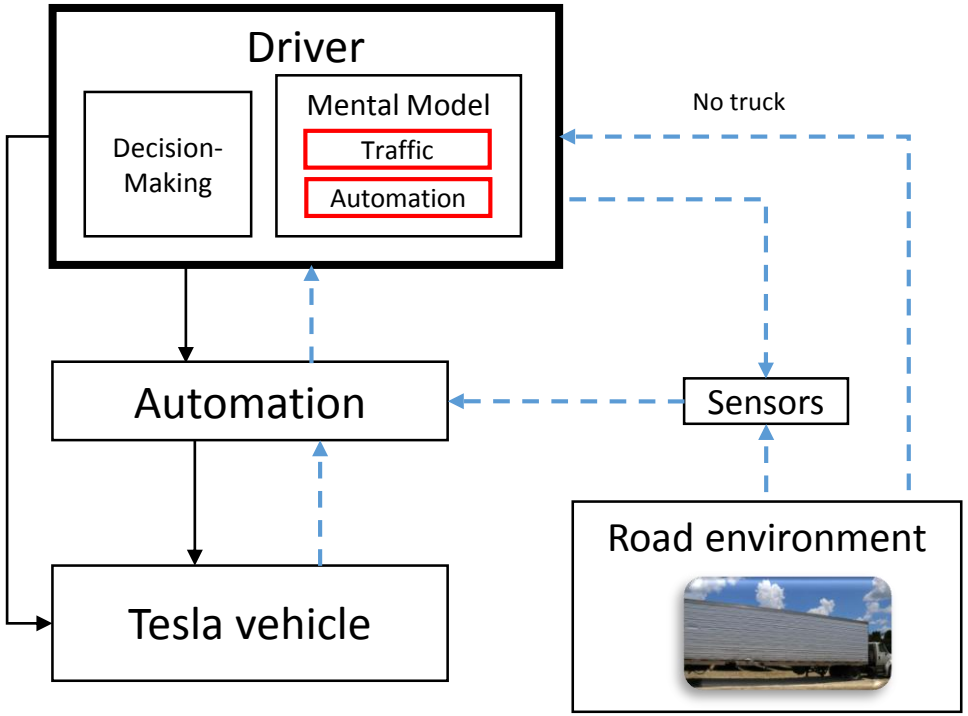
C. Context: Daylight with clear weather conditions, no known problems with truck detection

Degree of involvement: Secondary active

Illustrating CASCAD:

1 2 3 4 5

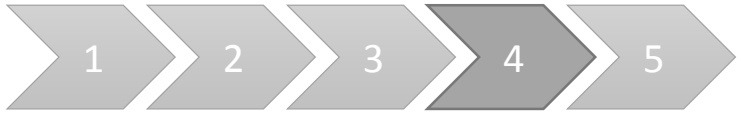
A. UCA: The human driver did not override automation and apply brakes when the vehicle violated the safety distance to the truck



B. CONTROL FLAWS (Human Driver)			
Category	**Control flaw**	**Description**	**Contributory factor**
Perception	Missing human perception of feedback on another road user	The driver did not perceive the truck because he was distracted	-Distraction -Secondary non-driving related task -Misuse
Model of process	Inadequate model of the traffic situation	The driver was unaware of the presence of the truck	-Priority feeling
	Inadequate model of automation	Driver believed that automation's monitoring was enough for safe operation	-Overreliance -Misuse

C. Context: Driver had the right of way, he was a Tesla fan

Illustrating CASCAD:



1. Define accidents, system hazards and safety constraints

2. Identify failures and unsafe interactions at the physical level
   - Crash description
   - Control structure at the physical level

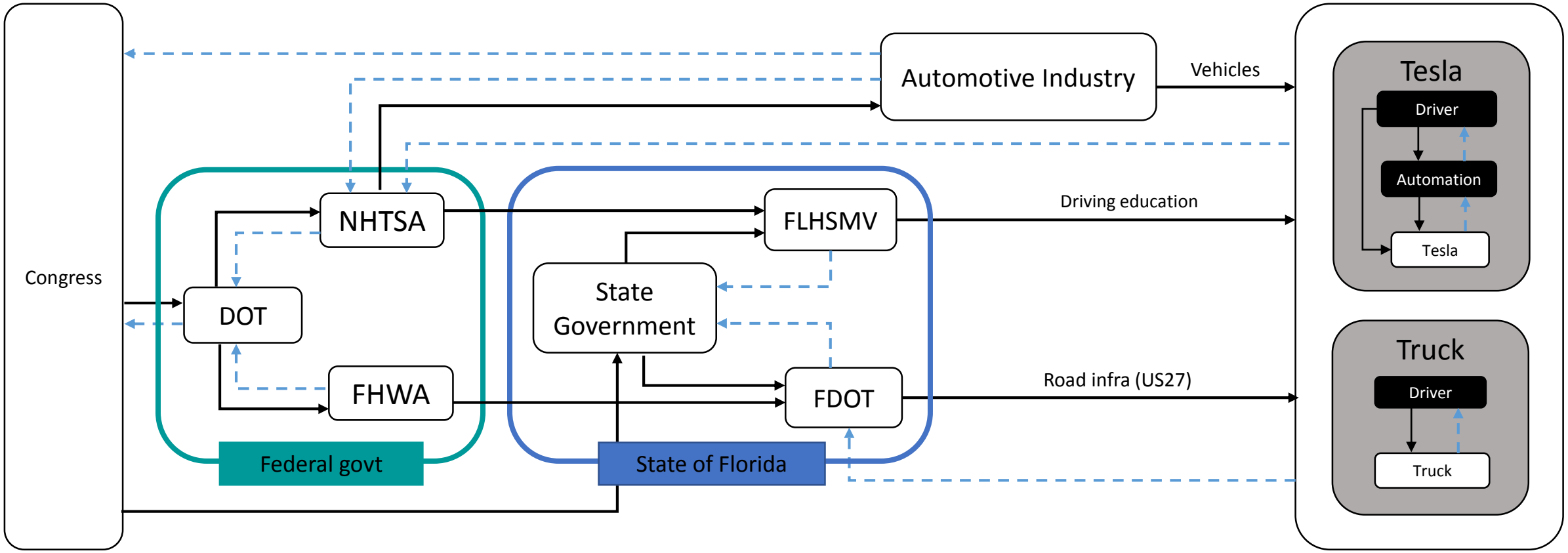
3. Analyze the direct controllers (i.e. road users and automation)
   - Control flaw classifications
   - Contributory factors
   - Degree of involvement

4. Analyze the indirect controllers (entire road transport system)
   - Control structure of the road transport

5. Issue recommendations

Illustrating CASCAD:

Control structure of Florida's Road Transport System



DOT: Department of Transportation

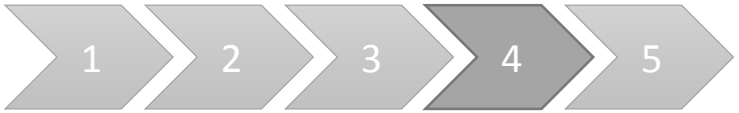
NHTSA: National Highway Traffic Safety Administration

FHWA: Federal Highway Administration

FLHSMV: Florida Highway Safety and Motor Vehicles

FDOT: Florida Department of Transportation

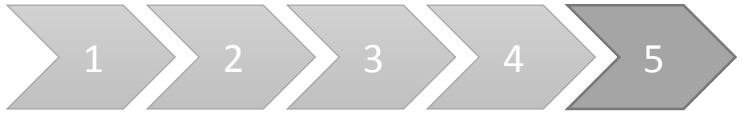
Illustrating CASCAD:



4 Analyze the indirect controllers (entire transport system)

Automotive industry (Tesla)	
Safety requirements	• Design, build and commercialize vehicles that can be safely operated
Unsafe Control actions	• Commercialized a BETA version of an SAE 2 automated driving system that can be (mis)used as an SAE 3 automated driving system, and engaged on highway sections with uncontrolled intersections.
Mental Model Flaws	• Believed that customers were going to monitor the driving environment • Thought that customers' driving info is very valuable for enhancing automation and therefore BETA versions are worth the risk
Context in which decisions were made	• A lot of pressure to be a cutting edge tech company and bring vehicle automation in the market • Legislation and regulatory gaps for vehicle automation

Illustrating CASCAD:



1. Define accidents, system hazards and safety constraints

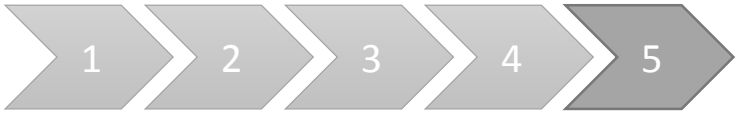
2. Identify failures and unsafe interactions at the physical level
   - Crash description
   - Control structure at the physical level

3. Analyze the direct controllers (i.e. road users and automation)
   - Control flaw classifications
   - Contributory factors
   - Degree of involvement

4. Analyze the indirect controllers (entire road transport system)
   - Control structure of the road transport

5. Issue recommendations

Illustrating CASCAD:



- **Tesla company**
  - Evaluate how design assumptions are being made and validated (radar tuning out info, data fusion choices, etc.)
  - Redesign system to accurately detect when drivers are not monitoring the road environment and to show the driver what automation is perceiving.
  - Redesign autopilot to only be engaged in the environments of its design limits (start to disengage autopilot when it approaches highway sections with intersections/exits)
  - Question the company's Roadmap relative to customers' safety.

Conclusions

- CAST represents a suitable method for the accident analysis of crashes involving automated driving, however its lack of specificity to road safety may prevent practitioners from adopting it.
- CAST was extended into a method called CASCAD which incorporates road safety-specific elements and elements to facilitate the application of CAST to crashes involving automated driving.
- Some elements from traditional crash analysis methods are still relevant for the analysis of automated driving. Also, STAMP can be applied on an automated driving system in order to generate usage guidance elements for road safety practitioners. These elements are able to coexist with CAST.
- The methodology proposed in CASCAD was illustrated using data from the Tesla crash in May 2016.

Perspectives:

- To develop more guidance elements, especially for the contributory factors related to the human behavior in automated driving and the factors that influence automation.
- To apply CASCAD on crash investigations involving automated driving and to compare it with traditional methods in order to validate CASCAD’s contribution to a more complete understanding.
- To talk with road safety practitioners to identify if CASCAD meets their needs and potential improvements.