RENESAS
BIG IDEAS FOR EVERY SPACE

ZENUITY

Model-Based Certification of Automated Vehicles

Michael Schmid

July 31, 2020

Goal of this presentation

Provide an answer to the question …

How can we certify vehicle automation?

Please contact schmidm@mit.edu for any questions!

Outline

> Motivation: Safety Problem with AVs

> Model-Based Approach to Safety and Certification

> Implementation of Model-Based Certification

Please contact schmidm@mit.edu for any questions!

Outline

> **Motivation: Safety Problem with AVs**

> Model-Based Approach to Safety and Certification

> Implementation of Model-Based Certification

Please contact schmidm@mit.edu for any questions!

The Age of AVs is right in front of us!

“highly and fully automated driving into series production by 2021.”

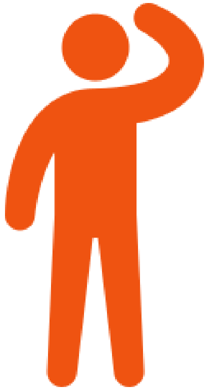
“deploy ‘thousands’ of self-driving cars in 2018”

“Level 4 vehicle in 2021, no gas pedal, no steering wheel, and the passenger will never need to take control of the vehicle in a predefined area.”

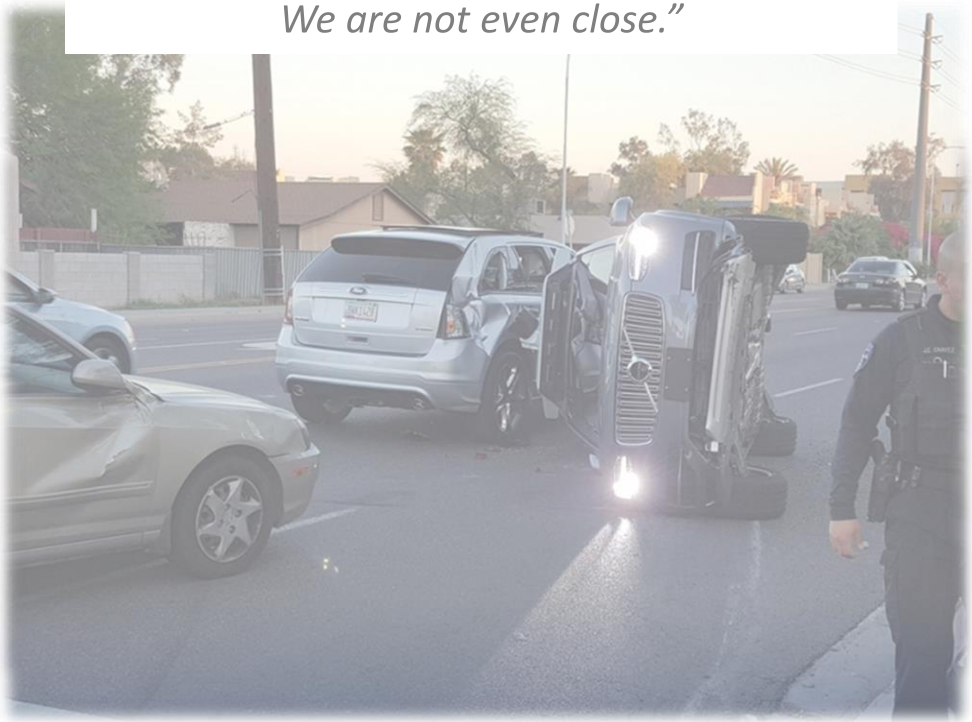
Please contact schmidm@mit.edu for any questions!

The age of AVs is right in front of us!

Is it?



“none of us in the automobile or IT industries are close to achieving true Level 5 autonomy. We are not even close.”



What is holding back progress?

- Legal challenges
- Lack of social acceptance
- High complexity is a challenge
- Strong economic competition vs. safety
- Security?

>>> many blocking points are <u>safety-related</u>!

Pending Safety-Related Questions

Safety compared to a human driver?
Trustworthiness?

AV insurance?

How safe is safe enough?

→

Guidance through Certification?

Perception dependable?

How to manage complexity?

Outline

> Motivation: Safety Problem with AVs

> Model-Based Approach to Safety and Certification

> Implementation of Model-Based Certification

Please contact schmidm@mit.edu for any questions!

What are the challenges?

“Driverless cars will require one billion lines of code”

Overwhelming amount of software

High complexity

nuTonomy

WAYMO

cruise

TESLA

ARGO AI

Technical variety
&
changes over time

>>> no space for looking at details – abstraction needed!

Please contact schmidm@mit.edu for any questions!

[4] [5]

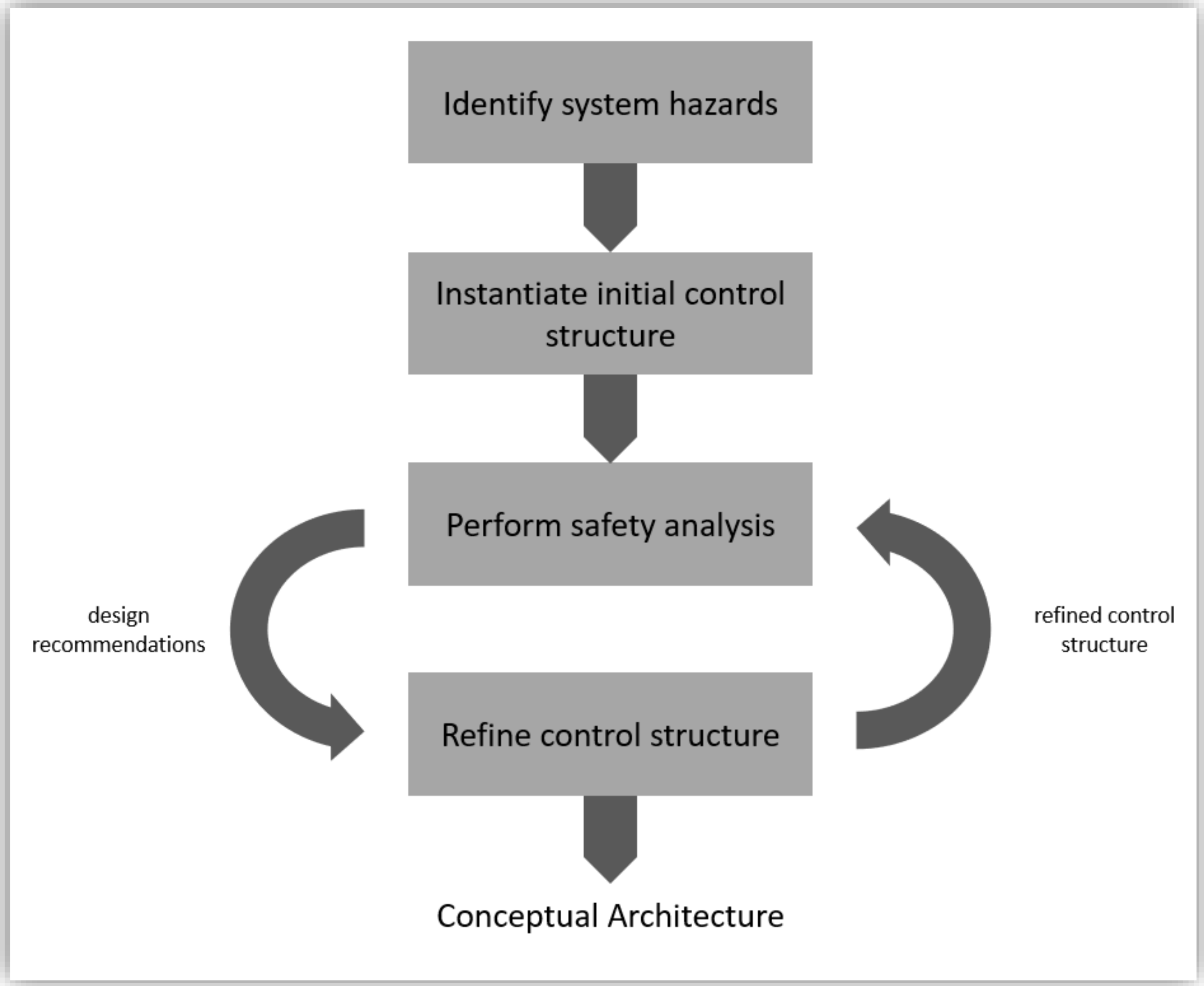
How to abstract?

- Effectiveness in early stages of development
- Ability to account for problems beyond mechanical failures
- Provide guidance on measures to achieve desired properties (e.g. safety)

>>> Abstraction based on Control Theory >>> STPA!

Please contact schmidm@mit.edu for any questions!

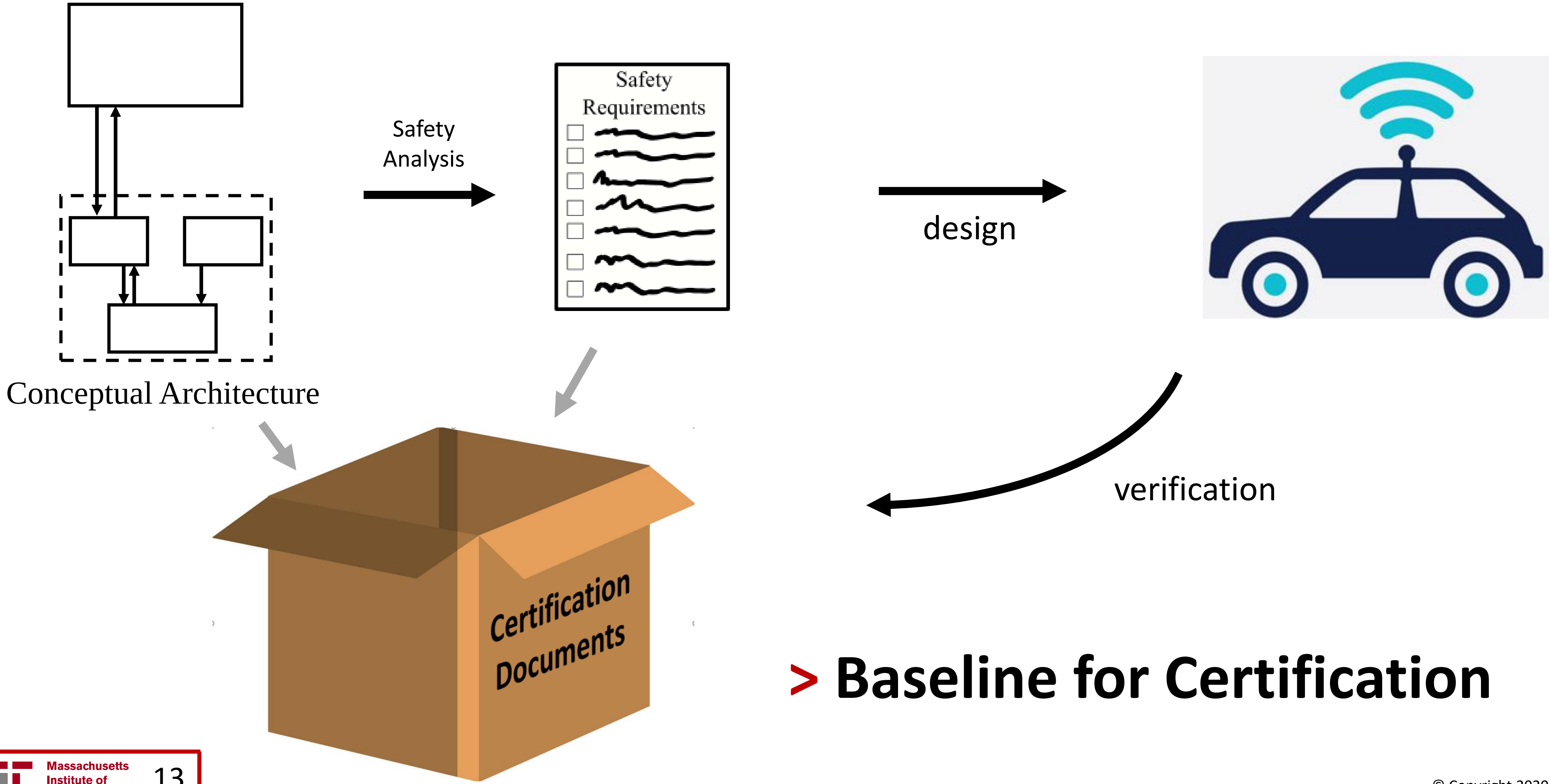
How can we create this abstraction?



Conceptual Architecture: a control-theoretic abstraction of a system that serves as a concept for physical design

Please contact schmidm@mit.edu for any questions!

How can we use this for certification?



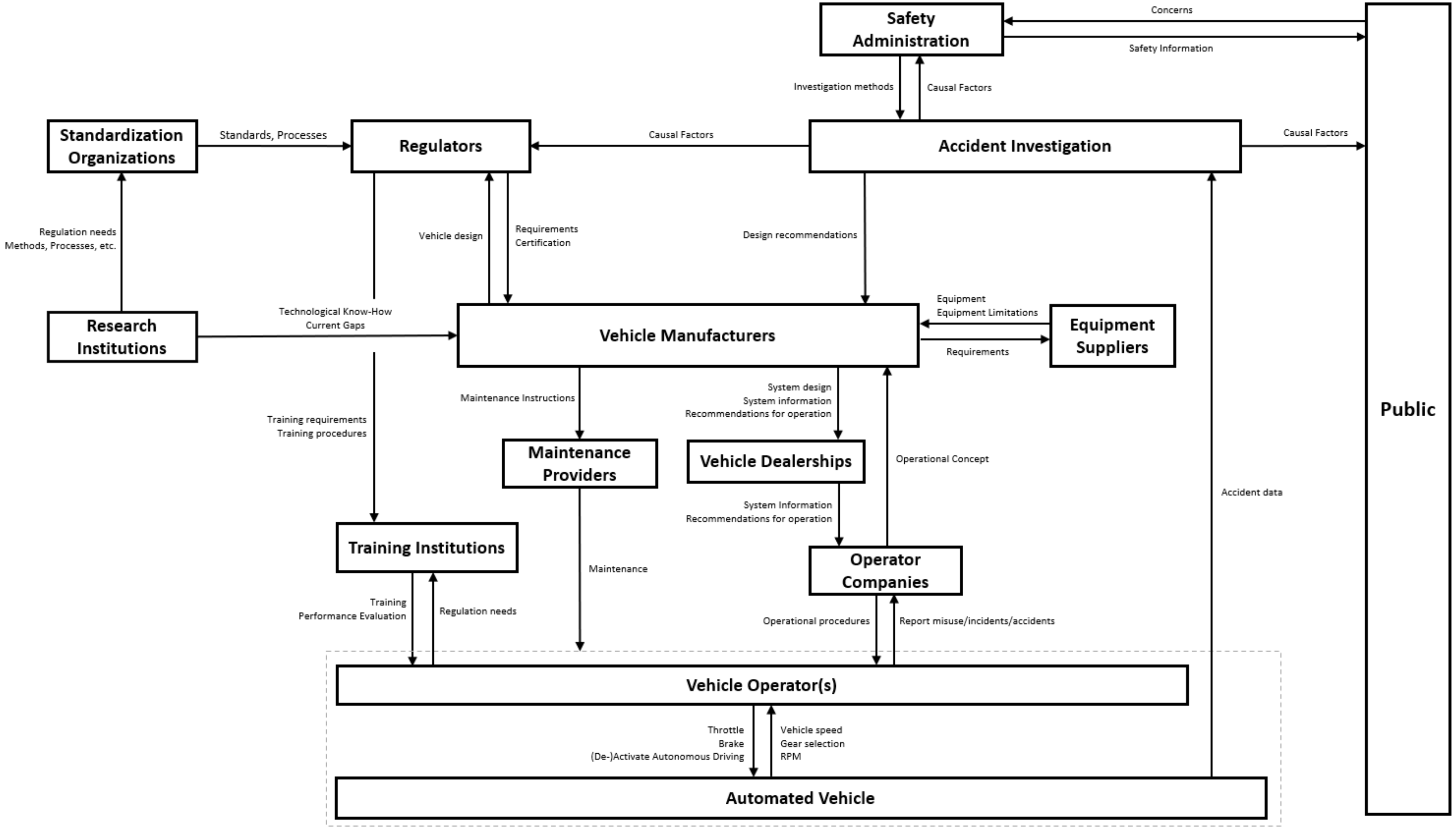
> Baseline for Certification

Please contact schmidm@mit.edu for any questions!

Some Results …

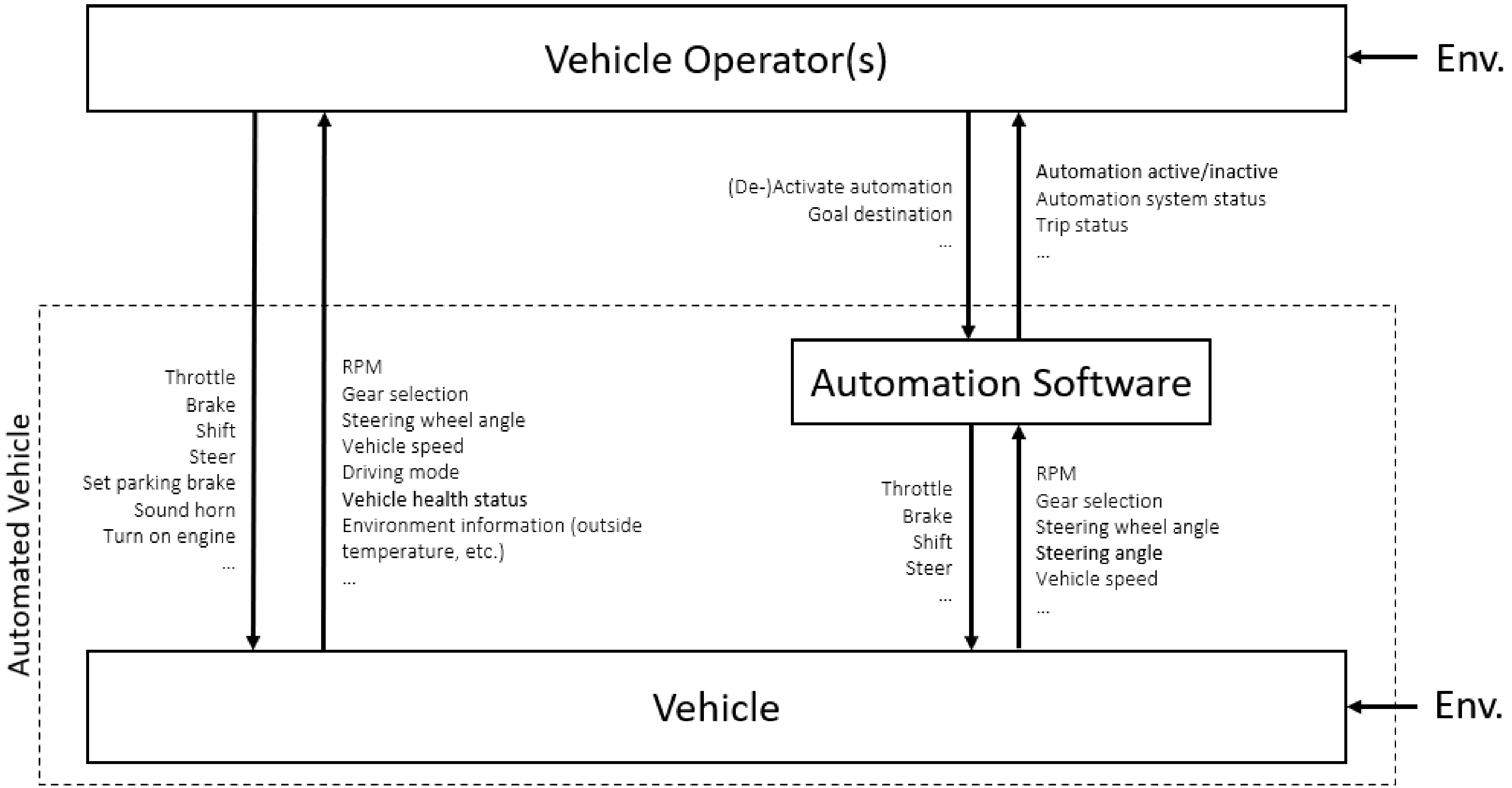
Please contact schmidm@mit.edu for any questions!

Initial Socio-Technical Control Structure



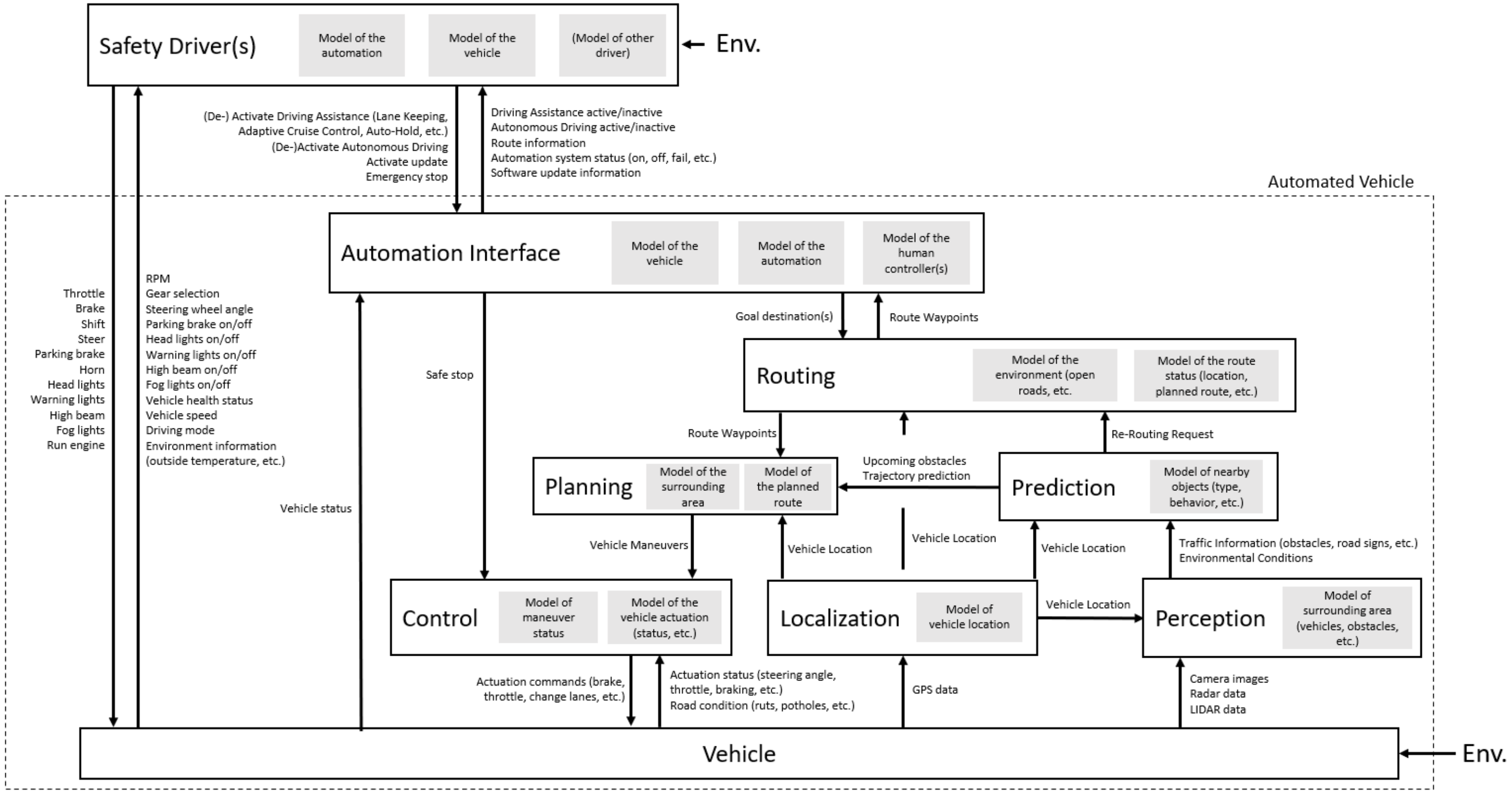
Please contact schmidm@mit.edu for any questions!

Zoom-in: Initial Operational Control Structure



Please contact schmidm@mit.edu for any questions!

Conceptual Architecture and Safety Requirements



R-8: The driver must be informed whenever the vehicle is in automated mode.

R-9: The automation must not allow re-activation after a collision until the vehicle has been checked by maintenance.

R-10: The communication channel between the automation and the braking system must never prevent braking.

R-11: Braking must never be prevented by a compromised braking system (including brake actuators).

Please contact schmidm@mit.edu for any questions!

Outline

> Motivation: Safety Problem with AVs

> Model-Based Approach to Safety and Certification

> Implementation of Model-Based Certification

Please contact schmidm@mit.edu for any questions!

Organizational Implementation

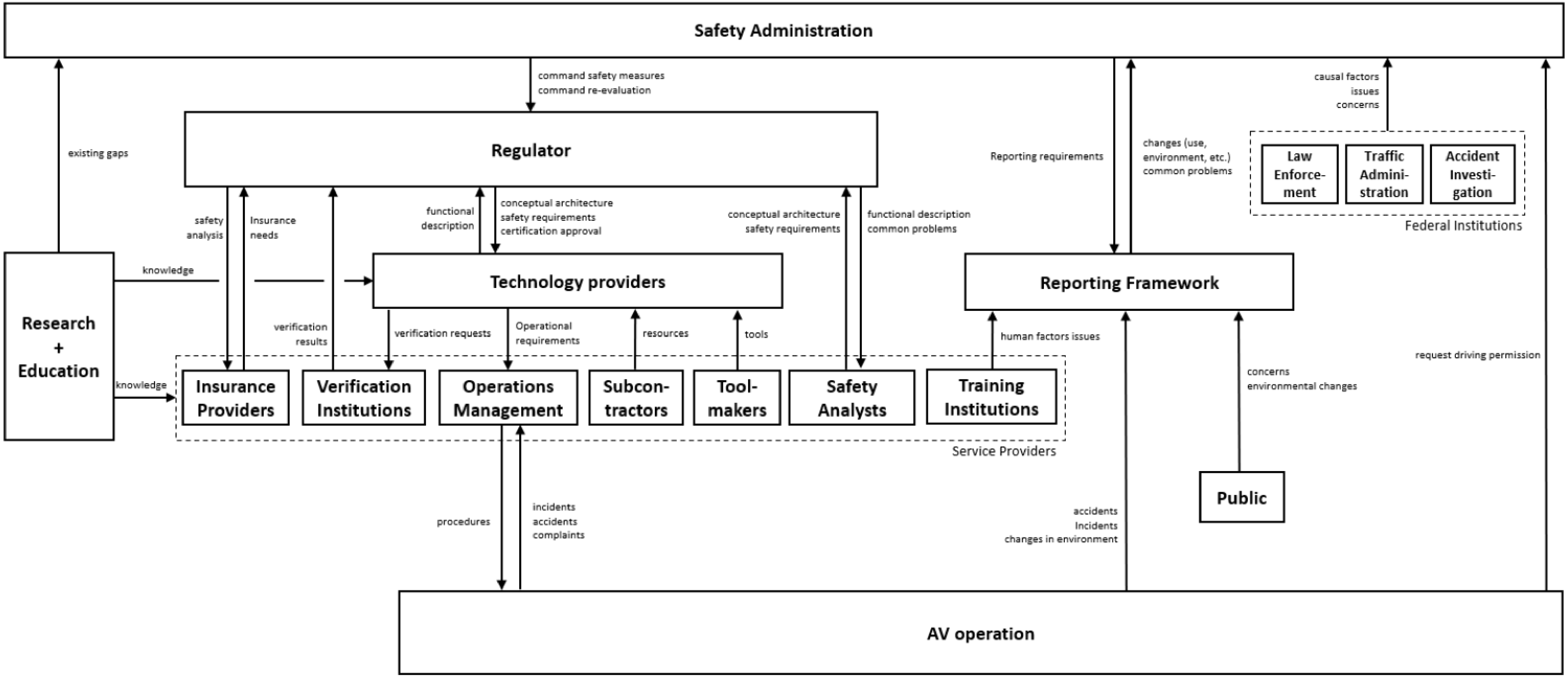


Figure 4-1: Organizational structure for model-based certification.

Please contact schmidm@mit.edu for any questions!

Certification - New Developments

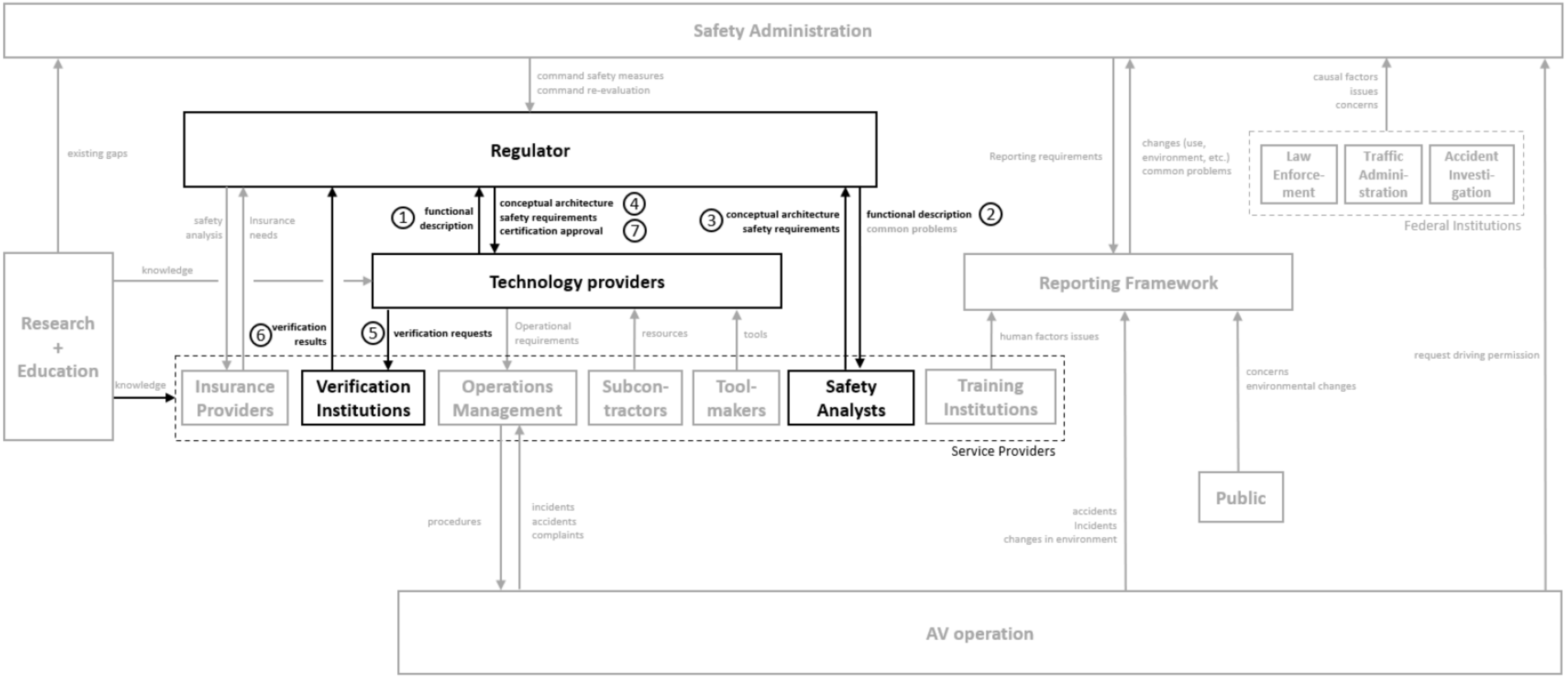


Figure 4-2: Process steps for the certification of new developments.

Please contact schmidm@mit.edu for any questions!

Certification - Changes to Existing Systems

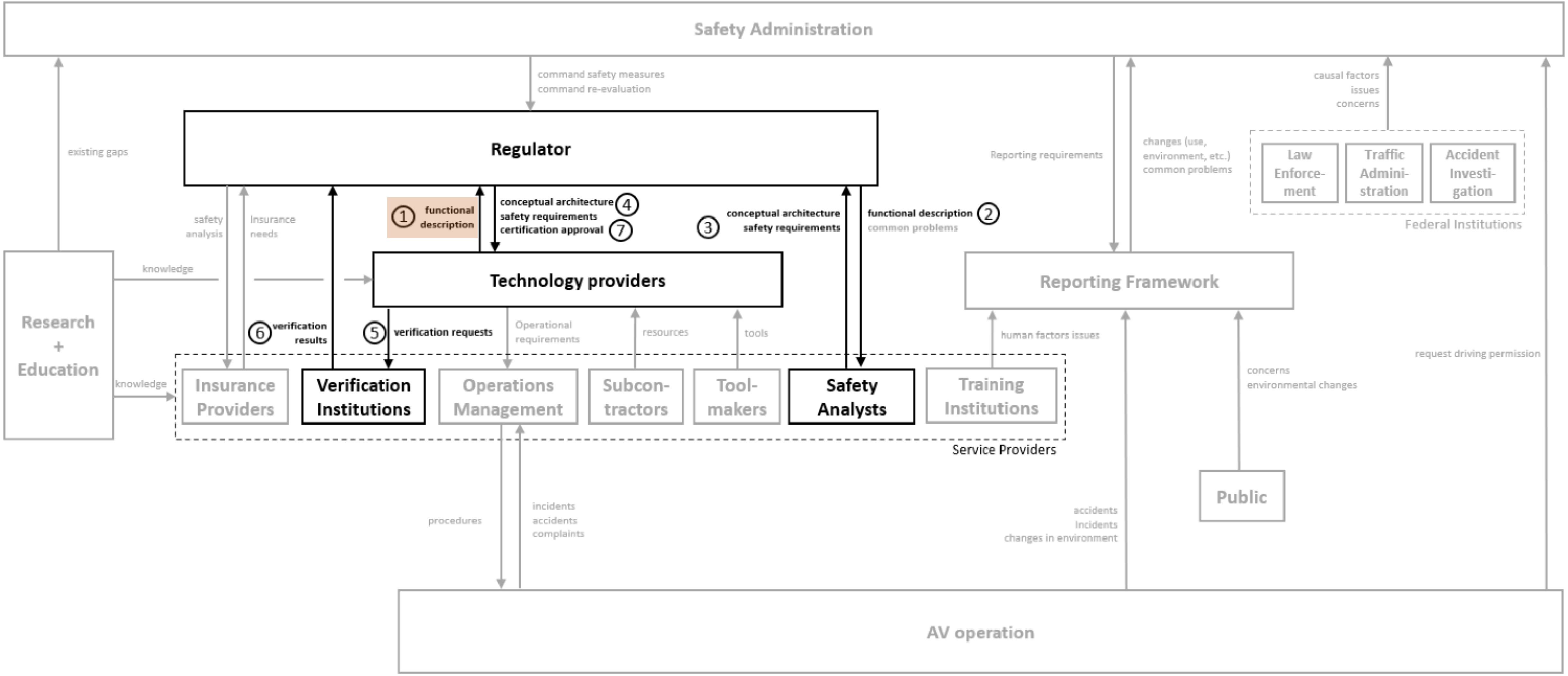


Figure 4-3: Steps for the certification of changes to existing systems.

Please contact schmidm@mit.edu for any questions!

Certification - Changes in the Operating Environment

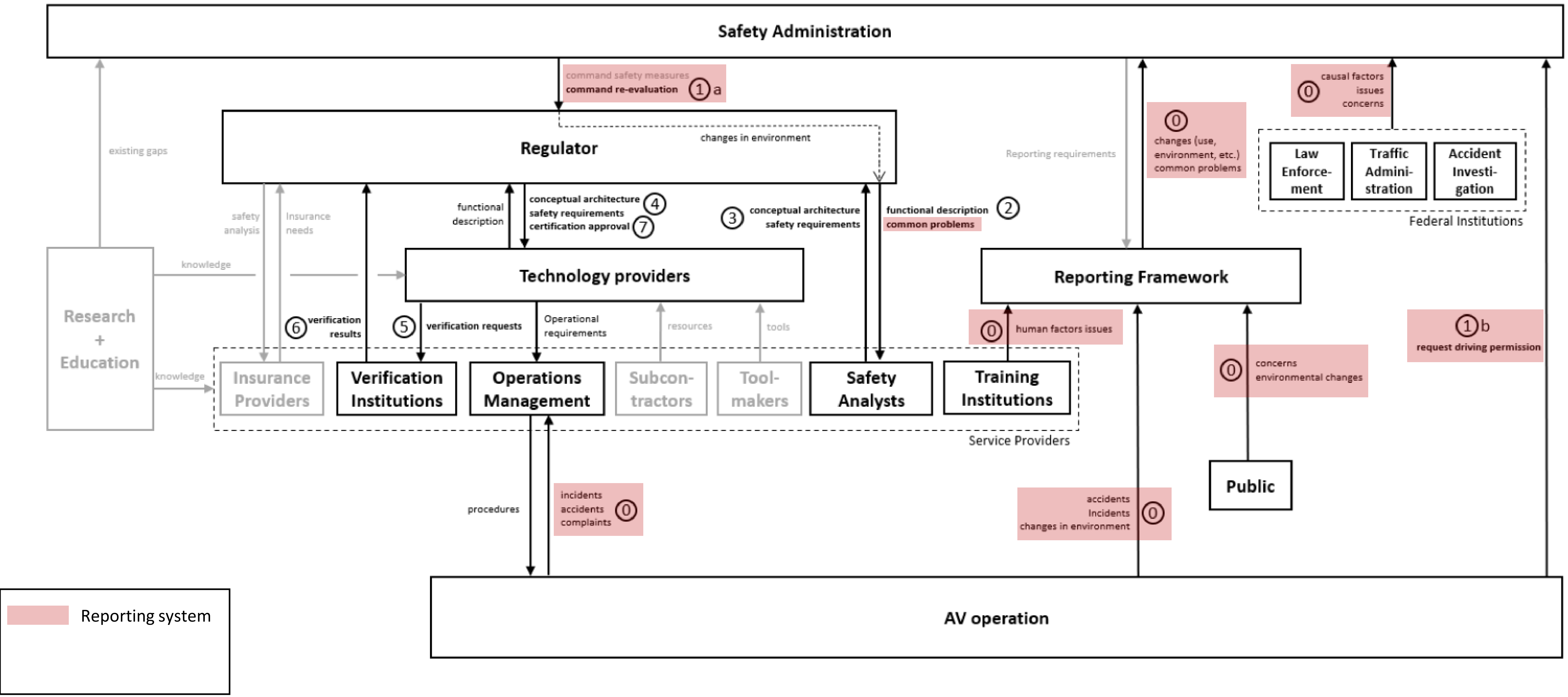


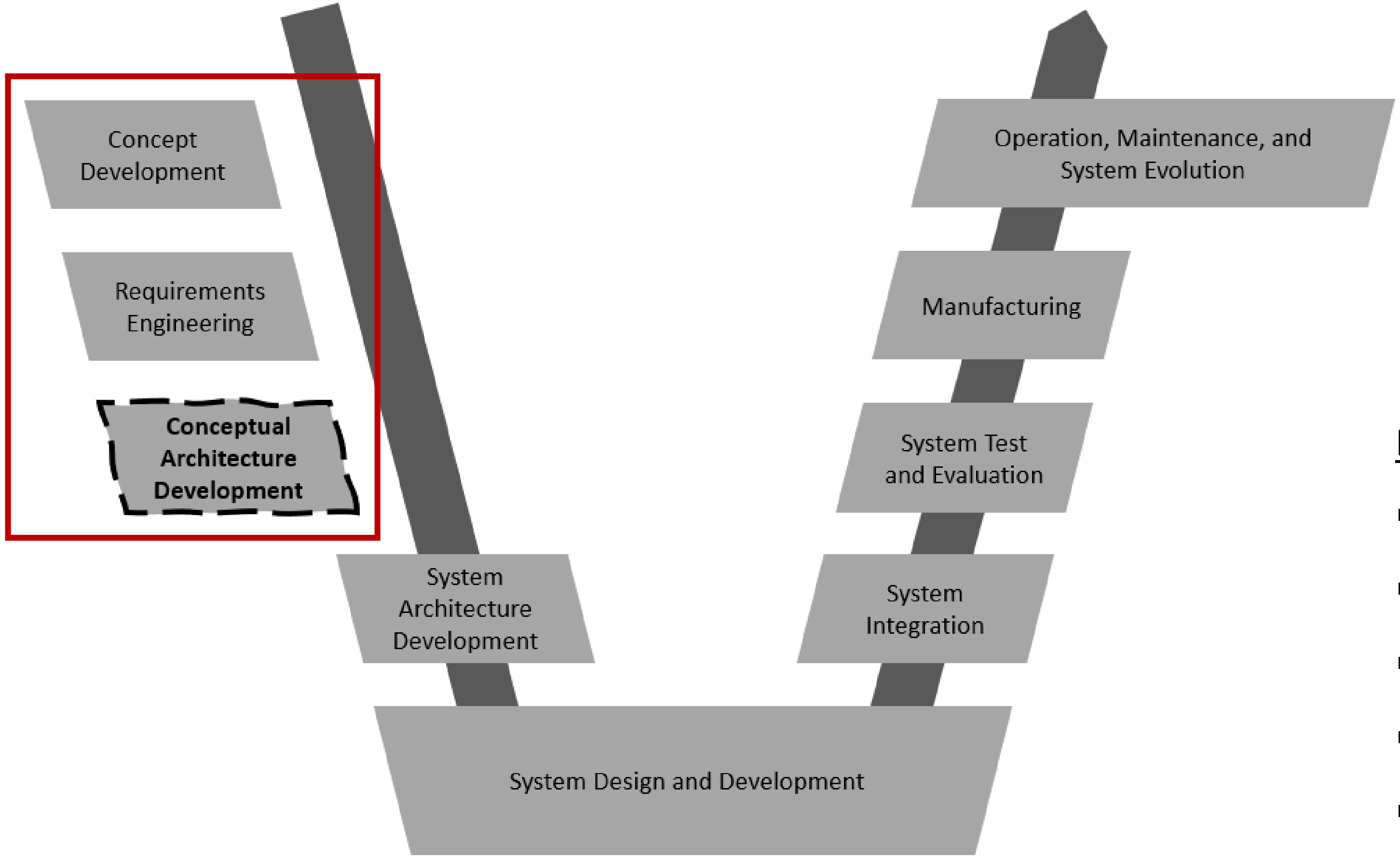
Figure 4-4: Steps for the certification within a changing environment.

Please contact schmidm@mit.edu for any questions!

Conclusion

<u>Regulators</u>: Analysis

<u>Manufacturers</u>: Design



<u>Benefits</u>

- separation of concerns
- reduced effort (regulators & OEMs), cost
- guidance in liability questions
- basis for new insurance concepts
- support for OEM-supplier interactions, etc.
- …

Please contact schmidm@mit.edu for any questions!

Questions?

The thesis on this topic can be downloaded from https://michael.systems

or

https://www.linkedin.com/in/michael-schmid-b72027100/

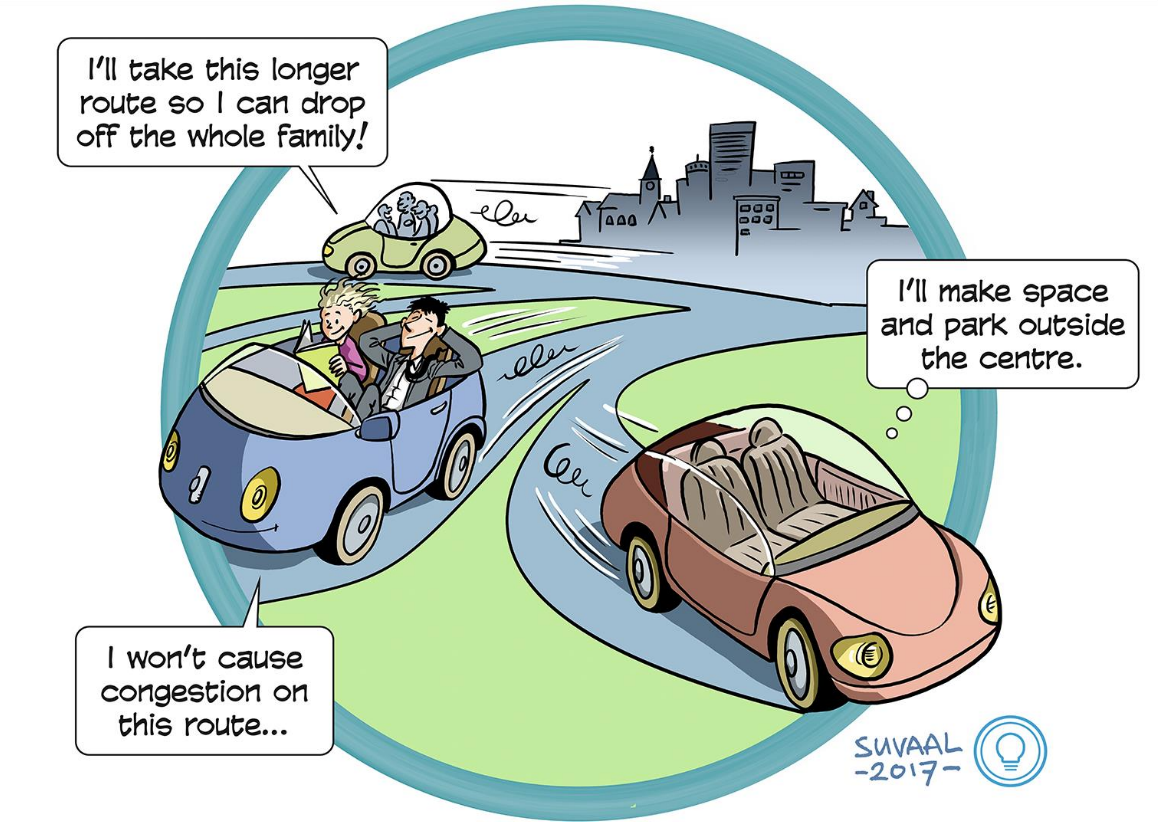
or

http://psas.scripts.mit.edu/home/

Please contact schmidm@mit.edu for any questions!

Appendix

Expected Benefits of Automated Vehicles



- Increased mobility & comfort
- Less parking problems
- Less traffic congestion
- Better fuel economy
- Faster transportation
- Higher level of safety

[3]

Conceptual Architecture Generation Process – Step 1: Losses & System Hazards

Losses

L-1: Loss of Life or Injury of People

L-2: Loss of or Damage to Vehicle

…

Hazards

H-1: Vehicle does not maintain a safe distance to other vehicles or objects [L-1,2,3,4,5,6]

H-2: Vehicle leaves authorized or designated roadway [L-1,2,3,4,5]

…

Please contact schmidm@mit.edu for any questions!

Conceptual Architecture Generation Process – Step 3: Perform Safety Analysis (UCAs)

UCAs >>>

Table 3.1: Design constraints generated from UCAs.

DC-1: The Safety Driver must not activate the automation when the vehicle controls have not been calibrated[4]. [UCA-40]	
DC-2: The Safety Driver must provide braking when the vehicle's path is not clear[5]. [UCA-27]	
DC-3: The Safety Driver must provide steering when automated steering is inconsistent with vehicle speed[6]. [UCA-35]	

Please contact schmidm@mit.edu for any questions!

Conceptual Architecture Generation Process – Step 3: Perform Safety Analysis (Scenarios)

UCA-74: Automation provides throttle when the vehicle's path is not clear (e.g. at a traffic light or junction). [H-1,4]

Scenario-1: The automation does not recognize that the vehicle's path is not clear. This flawed process model may be due to:

a) The automation does not receive information about obstacles around the vehicle.

b) The automation identifies a pedestrian that is about to enter the vehicle's path but interprets it as a dummy (e.g. because the person is not moving and is interpreted as a mock-up).

c) The feedback that the vehicle's path is not clear is provided only once the vehicle is close enough to the obstacles in the path (e.g. detection distance limitations of sensors).

DC-16: The automation must receive information about the vehicle's environment.

DC-17: The automation must always provide the most conservative estimate of its detections (obstacle type, speed, etc.).

Conceptual Architecture Generation Process – Step 4: Refine Control Structure

“*The automation must receive information about the vehicle‘s environment*” (DC-16)
“*The automation must account for all potential future positions of obstacles around the vehicle‘s planned path*” (DC-18)

>>> need control structure elements for perception and prediction

see Conceptual Architecture next page

Model-Based Safety Analysis (STPA) – Unsafe Control Actions

Table 3.2: Unsafe Control Actions – Automation.

Control Action	Not Providing	Providing	Provided Too Early / Too Late	Provided For Too Long / Stopped Too Soon
brake	Automation does not provide a brake command after the vehicle has suffered a collision and the vehicle must stop. (UCA-1) [H-1,2,3]	Automation provides excessive braking when a following vehicle cannot decelerate in time. (UCA-2) [H-1]	Automation stops providing brake command too early when vehicle speed is still above speed limits (e.g traffic flow limit). (UCA-3) [H-1,2,3,4]	Automation stops providing brake command too soon when a collision is imminent. (UCA-4) [H-1]
throttle	Automation does not provide throttle when a speed increase is required to avoid a rear or side collision. (UCA-5) [H-1]	Automation provides throttle when vehicle is under maintenance. (UCA-6) [H-1,3]	Automation provides throttle too early before the vehicle's path has become clear (e.g. dynamic obstacles slower than anticipated, etc.). (UCA-7) [H-1,4]	Automation provides throttle for too long until forward collision becomes imminent. (UCA-8) [H-1]
steering	Automation does not provide steering when the vehicle's lane is about to end. (UCA-9) [H-1]	Automation provides steering when it steers the vehicle into a collision (e.g. lane keeping feature). (UCA-10) [H-1]	Automation provides steering too late after merging is no longer possible (e.g. gap closed by another vehicle). (UCA-11) [H-1,4]	Automation stops providing steering too early before the maneuver is finished. (UCA-12) [H-1,4]

Model-Based Safety Analysis (STPA) – Scenarios & Safety Requirements

UCA-1: Automation does not provide a brake command after the vehicle has suffered a collision and the vehicle must stop. [H-1,2,3]

Scenario-6: The automation recognizes the collision but decides that it is safer to keep travelling. This flawed control algorithm may occur because:

a) The automation software is programmed to evaluate risk and to transition to a minimal risk condition after a collision. As a result, the vehicle decides that it is safer to travel to the next safe stopping point off the highway rather than stopping on the highway and continues to the next exit.

b) The automation software was programmed to forego providing brake commands after detecting a collision in order to prevent false positives, e.g. on highways when there is no collision, but the vehicle detects a collision. However, as collision detection systems mature and achieve higher dependability, this behavior is no longer justified.

c) The automation software was programmed incorrectly and there is an error in the automation software.

R-4: The automation must never make decisions based on estimated risk after the vehicle has suffered a collision.

R-5: The vehicle must never continue moving after it has suffered a collision except to the side of the road.

R-6: The automation must never forego brake commands to slow down after a collision has been detected.

R-7: The certification of automation software must ensure that adequate development practices were used to minimize software errors.

Please contact schmidm@mit.edu for any questions!

Standards and Practices

> Establish practices for AV development:

- ISO 26262: Road vehicles – Functional safety
- ISO 21448: Safety of the Intended Functionality
- UL 4600: Standard for Safety for the Evaluation of Autonomous Products
- DO-178C, MIL-STD-882E, Federal Motor Vehicle Safety Standards (FMVSS)

- Inadequate for software, human factors, etc.
- Based on quantification of risk
- Assumption of complete set of requirements
- Simulation, testing, and statistics used as means to demonstrate safety
- …

… still accidents > learn from them?

March 23, 2018 / Mountain View, California

Smart? Summon

- Technical limitations
- Reliance on human supervision
- Misuse of automation features
- Misleading marketing
- Awareness of limitations
- …

>>> gaps in practices & not enough accidents!

Please contact schmidm@mit.edu for any questions!

Existing Standards and Practices

- ISO 26262 and ISO 21448 (SOTIF)
- UL-4600
- AUTOSAR
- DO-178C
- MIL-STD-882E
- MISRA-C
- Safety First For Automated Driving [Aptiv, Audi, BMW et al.]
- Measuring Automated Vehicle Safety [RAND Corporation]
- Federal Motor Vehicle Safety Standards (FMVSS)
- …

Limitations

- Inadequate for software, human factors, etc.
- Based on quantification of risk
- Assumption of complete set of requirements
- Simulation, testing, and statistics used as means to demonstrate safety
- …

Please contact schmidm@mit.edu for any questions!

Learning from Accidents

Common factors:

- Driver inattentiveness & over-reliance
- Insufficient feature functionality & maturity, e.g.
  - Smart Summon feature and accidents in
  - Accidents in Williston (FL), China, Mountain View (CA), and Delray Beach (FL)
- Misleading marketing (see Tesla "Autopilot")
- Invalid assumptions (see Uber accident in Tempe, AZ)
- …

Please contact schmidm@mit.edu for any questions!

Other Attempts

Approaches by component suppliers

- Mobileye: Responsibility-Sensitive Safety
- NVIDIA: Safety Force Field (SFF)

Please contact schmidm@mit.edu for any questions!

References I

Slide 1:

- https://zenprospect-production.s3.amazonaws.com/uploads/pictures/5dd3e07c376d300001f8b1e0/picture
- https://wp.technologyreview.com/wp-content/uploads/2018/11/003-av-miami02222018ford0583-edit-9.jpg
- https://media-exp1.licdn.com/dms/image/C4E0BAQGFNL7t1x8Qjg/company-logo_200_200/0?e=2159024400&v=beta&t=FuFpIJMzwSDNuHlKd7KWLmD0y31KvwL5b6Qymv9qnQI

Slide 5:

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Ficon-logo-template-sun-over-horizon-vector-16432791&psig=AOvVaw3XwmqHy-dWAClM0Lmyc2tN&ust=1594994892368000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMCI1pP80eoCFQAAAAAdAAAAABAa
- https://medium.com/self-driving-cars/gm-to-deploy-thousands-of-self-driving-cars-in-2018-4bfd3f7ecdc9
- https://www.bodyshopbusiness.com/bmw-intel-mobileye-fully-autonomous-driving-2021/
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Ftwo-color-driverless-autonomous-car-icon-from-vector-25693439&psig=AOvVaw3TYdGEvXcBATR0_oClyUTJ&ust=1594994643505000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMDdlp340eoCFQAAAAAdAAAAABAD
- https://currentev.com/blog/the-self-driving-car-what-is-it-when-will-it-happen-plans-of-top-11-global-automakers/
- https://www.stockio.com/free-icon/scanning-horizon

References II

Slide 6:

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Ficon-logo-template-sun-over-horizon-vector-16432791&psig=AOvVaw3XwmqHy-dWAClM0Lmyc2tN&ust=1594994892368000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMCI1pP80eoCFQAAAAAdAAAAABAa
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Ftwo-color-driverless-autonomous-car-icon-from-vector-25693439&psig=AOvVaw3TYdGEvXcBATR0_oClyUTJ&ust=1594994643505000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMDdlp340eoCFQAAAAAdAAAAABAD
- https://www.stockio.com/free-icon/scanning-horizon
- https://media.consumeraffairs.com/files/cache/news/uber-accident-twitter_large.jpg
- https://www.businessinsider.com/self-driving-cars-not-feasible-in-5-years-automakers-say-2017-1
- https://cdn.vox-cdn.com/thumbor/UMjM1S7Ncpiw6On67KEd0wJo8YE=/0x0:2822x2117/1200x800/filters:focal(1186x834:1636x1284)/cdn.vox-cdn.com/uploads/chorus_image/image/49794921/wFlcpFG.0.jpg

References III

Slide 7:

- https://www.google.com/url?sa=i&url=https%3A%2F%2Finternetofbusiness.com%2Fopinion-why-driverless-cars-will-force-an-insurance-u-turn%2F&psig=AOvVaw3b_c-fHoWxhh6lGiL30TO1&ust=1586605157879000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCND1r_ri3egCFQAAAAAdAAAAABAj

Slide 10:

- https://www.autoexpress.co.uk/car-news/106617/driverless-cars-will-require-one-billion-lines-of-code-says-jlr
- https://www.bluehomepm.com/wp-content/uploads/2018/11/Complex.png
- https://pbs.twimg.com/media/CzliWIOXgAAzDul.jpg:large
- https://cdn.1min30.com/wp-content/uploads/2019/09/Tesla-logo-1.jpg
- https://www.ocreations.com/wp-content/uploads/2019/02/ocreations-pittsburgh-branding-logos-argo-ai.jpg
- https://d2n4wb9orp1vta.cloudfront.net/cms/brand/ABG/evergreen-images/gm-cruise-logo-2019-o.jpg;width=550;quality=60
- https://michiganvca.org/wp-content/uploads/2018/08/nuTonomy-for-site-300x300.png

Slide 13:

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Fcarton-packing-box-icon-vector-14345961&psig=AOvVaw2QVvL6SiZJrDT_s68oZHKz&ust=1595009194498000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKjPirau0uoCFQAAAAAdAAAAABAD

References IV

Slide 13 (continued):

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Fcarton-packing-box-icon-vector-14345961&psig=AOvVaw2QVvL6SiZJrDT_s68oZHKz&ust=1595009194498000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKjPirau0uoCFQAAAAAdAAAAABAD
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.vectorstock.com%2Froyalty-free-vector%2Ftwo-color-driverless-autonomous-car-icon-from-vector-25693439&psig=AOvVaw3TYdGEvXcBATR0_oClyUTJ&ust=1594994643505000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMDdlp340eoCFQAAAAAdAAAAABAD

Slide 26:

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.tudelft.nl%2Fen%2Ftechnology-transfer%2Fdevelopment-innovation%2Fresearch-exhibition-projects%2Fautomated-vehicles-routing%2F&psig=AOvVaw3afylWhxdRDmedMCpZHWv_&ust=1589378581264000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCND3n5G_rukCFQAAAAAdAAAAABAD

Slide 33:

- https://s.abcnews.com/images/Business/tesla-crash-calif-ap-ps-200212_hpMain_16x9_1600.jpg

References V

Slide 33 (continued):

- https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DcxoEze3UqXQ&psig=AOvVaw1AIPd0b1QKjlOafgsYpeUB&ust=1586606516802000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCMjM5sjo3egCFQAAAAAdAAAAABAD

Please contact schmidm@mit.edu for any questions!