ENGINEERING FOR HUMANS
Human-Automation Interaction in STPA

MEGAN FRANCE
Massachusetts Institute of Technology
March 27, 2017

ABOUT ME

- 2nd year Master's student under Dr. Nancy Leveson
- B.S. in Human Factors Engineering from Tufts University
- Worked ~3 years as an intern at the Volpe National Transportation Systems Center in Cambridge, MA in the Surface Transportation Human Factors Division
- Received the ASSE Liberty Mutual Safety Research Fellowship for Summer 2016 to study applications of STPA to workplace safety in a rail environment

SPECIAL THANKS TO:

Dr. Nancy Leveson, thesis advisor

Dr. John Thomas, project advisor

General Motors, project sponsor

Charles A. Green, Mark A. Vernacchia, Padma Sundaram, & Joseph D'Ambrosio, collaborators

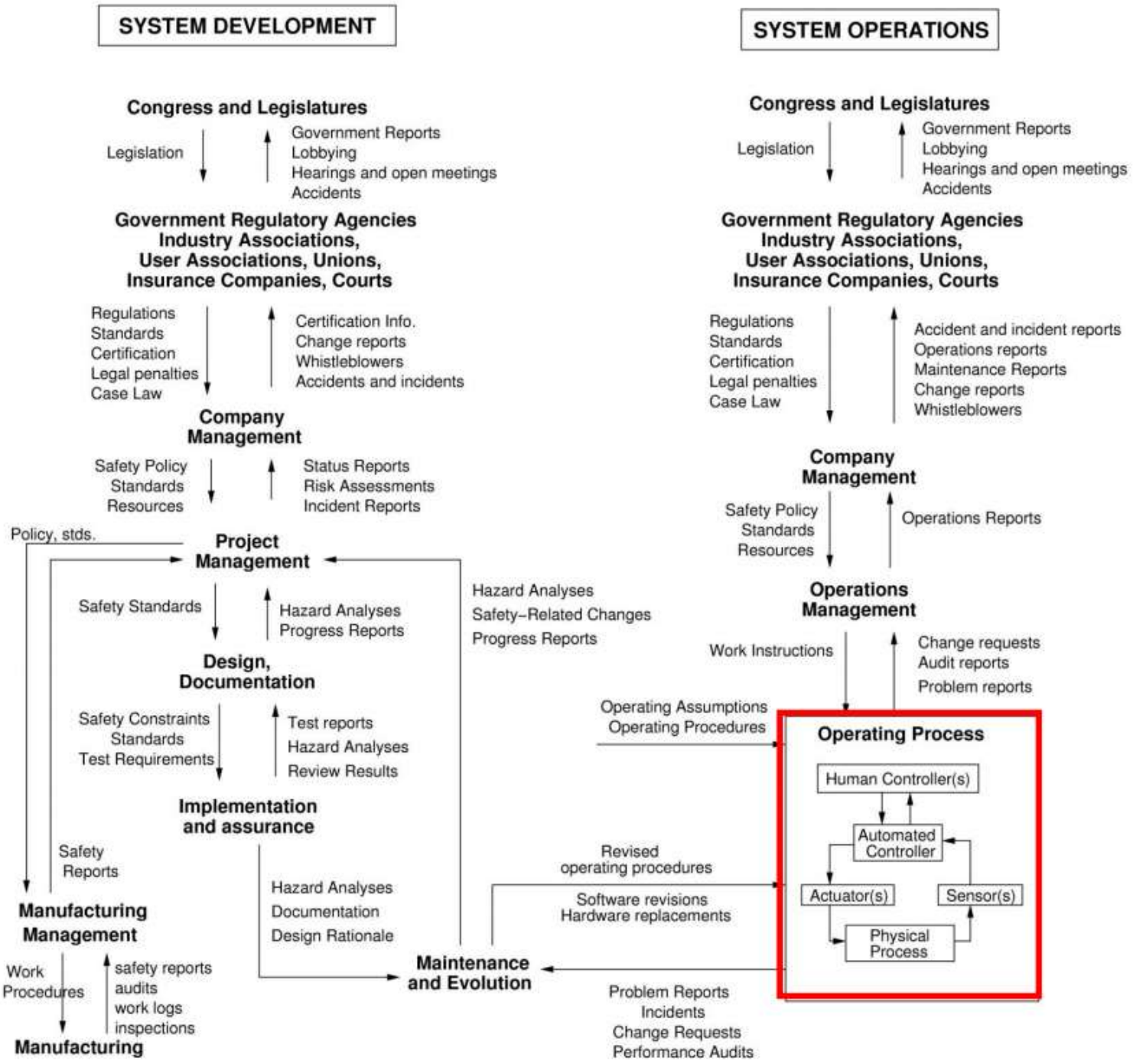
OUTLINE

- Introduction
- Engineering for Humans Extension

- Example Applications
  - Railway grade crossing
  - Aircraft pitch and speed control
  - Automated Parking Assist (APA)

- Q&A

TODAY'S SOCIOTECHNICAL SYSTEMS ARE COMPLEX!



WHAT'S WRONG WITH CURRENT APPROACHES?

Without considering the operator's process model in the actual operational context, we can fall victim to:

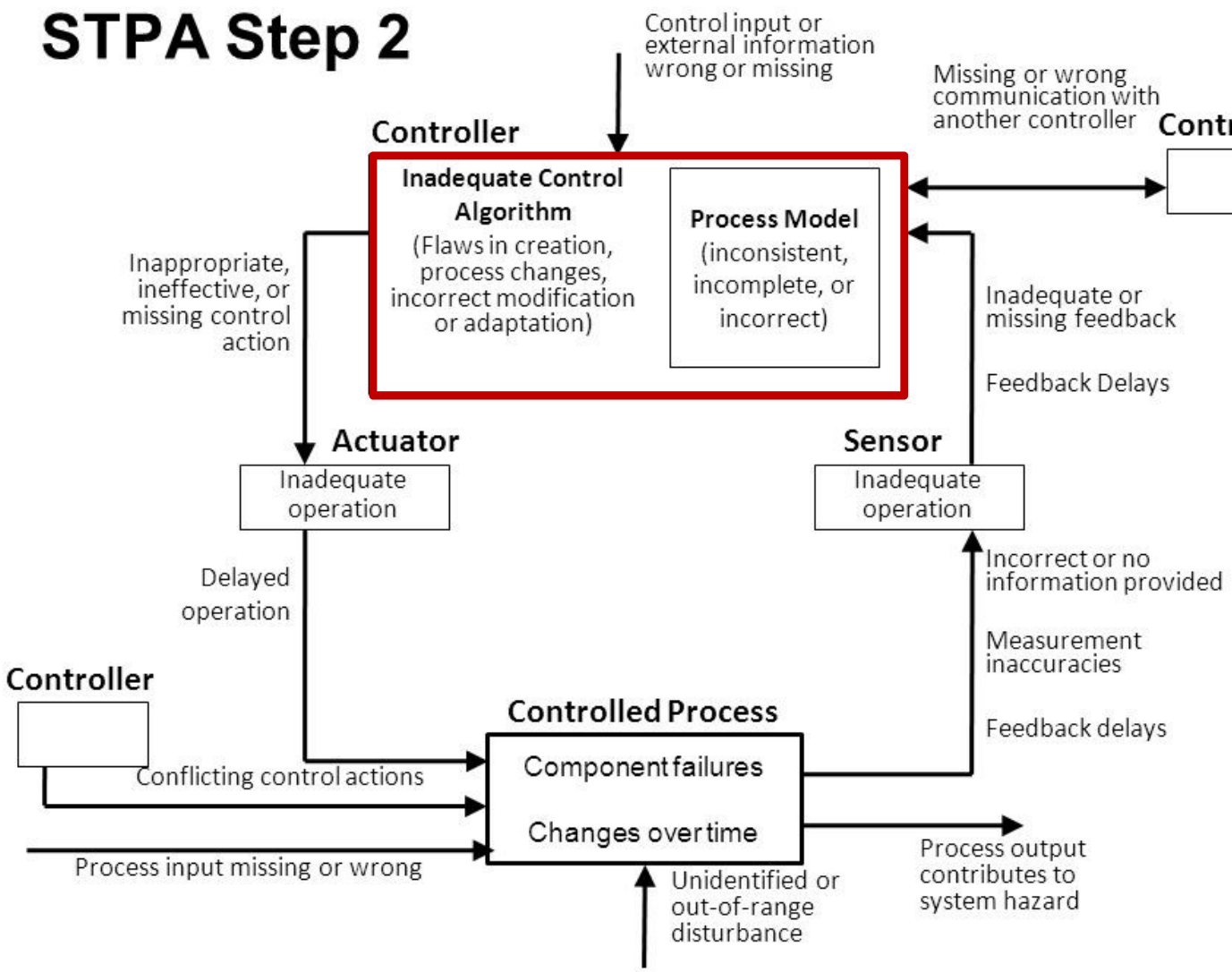
- ***"Root cause seduction"*** – it's appealing to find a single root cause that can be easily changed, but it's not going to fix underlying systemic problems!
- ***Hindsight bias*** – tendency to see what "could" or "should" have been done after the fact.

STPA helps us avoid these common pitfalls.

THE CHANGING ROLE OF HUMAN OPERATORS

- Many tasks now involve **supervisory control** of automation, or **human-machine collaboration**
- Operators may be required to **monitor more information with less direct interaction** with the controlled process
- As system complexity increases, so do risks for **mode confusion and automation surprises**
- Operator's actions are driven by **mental models** of the controlled process and environment

WHY WE NEED AN EXTENSION



While STPA is well-suited to studying issues of human-automation interaction, it does not yet provide specific guidance in this area!

HUMAN ENGINEERING EXTENSION

(Thomas & France, 2016)

STPA – ENGINEERING FOR HUMANS EXTENSION

- Define system accidents and hazards
- Draw the safety control structure
- Write Unsafe Control Actions (UCAs)
- Write scenarios as usual for control actions performed by software controllers

Traditional STPA

- Write scenarios for actions performed by the human operator, using the new Human Controller Model for guiudance

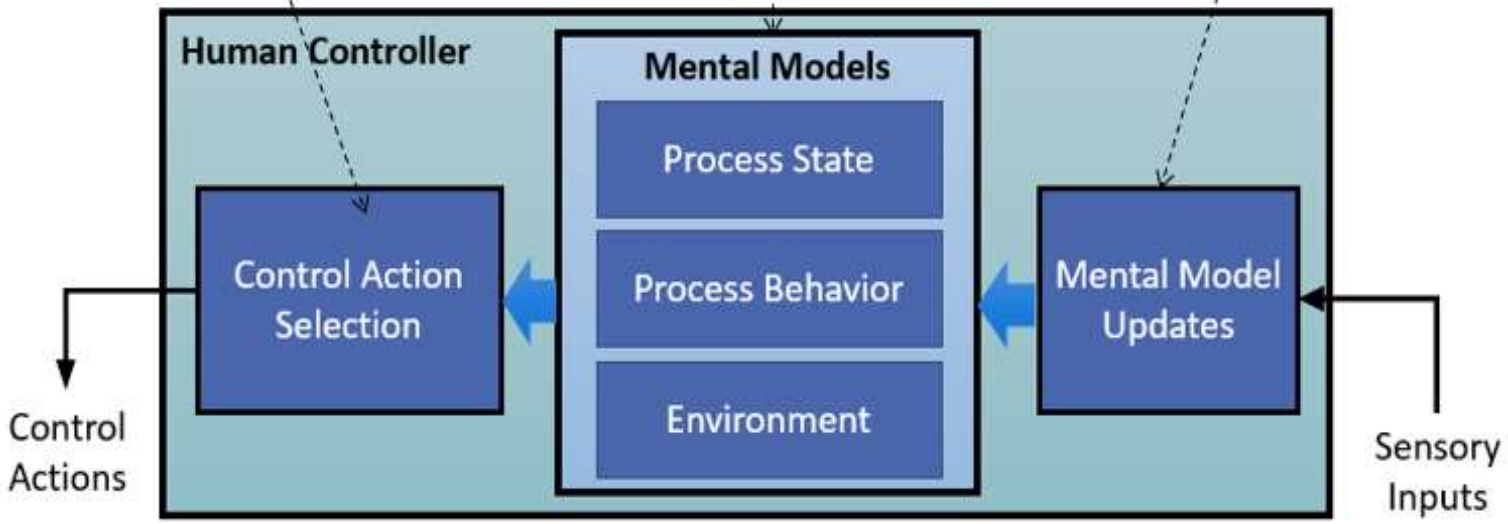
NEW

A NEW MODEL FOR HUMAN CONTROLLERS

Captures the controller's goals and how decisions are made based on the mental models

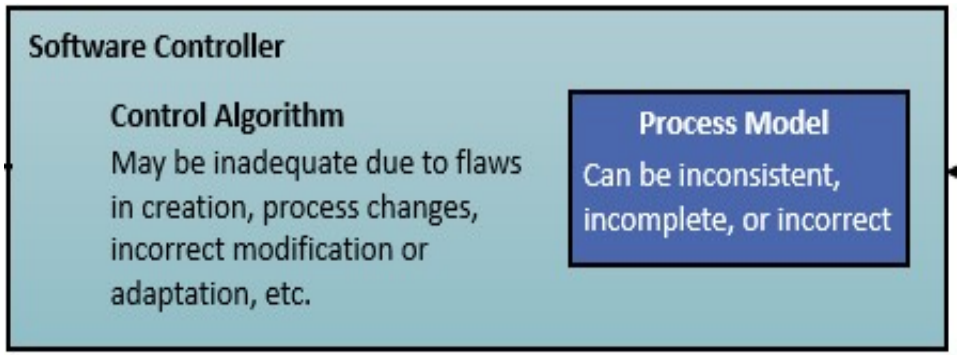
Captures specific types of flaws in the way the human controller conceptualizes the system and environment

Captures the influence of human experiences, and expectations on the processing of sensory input



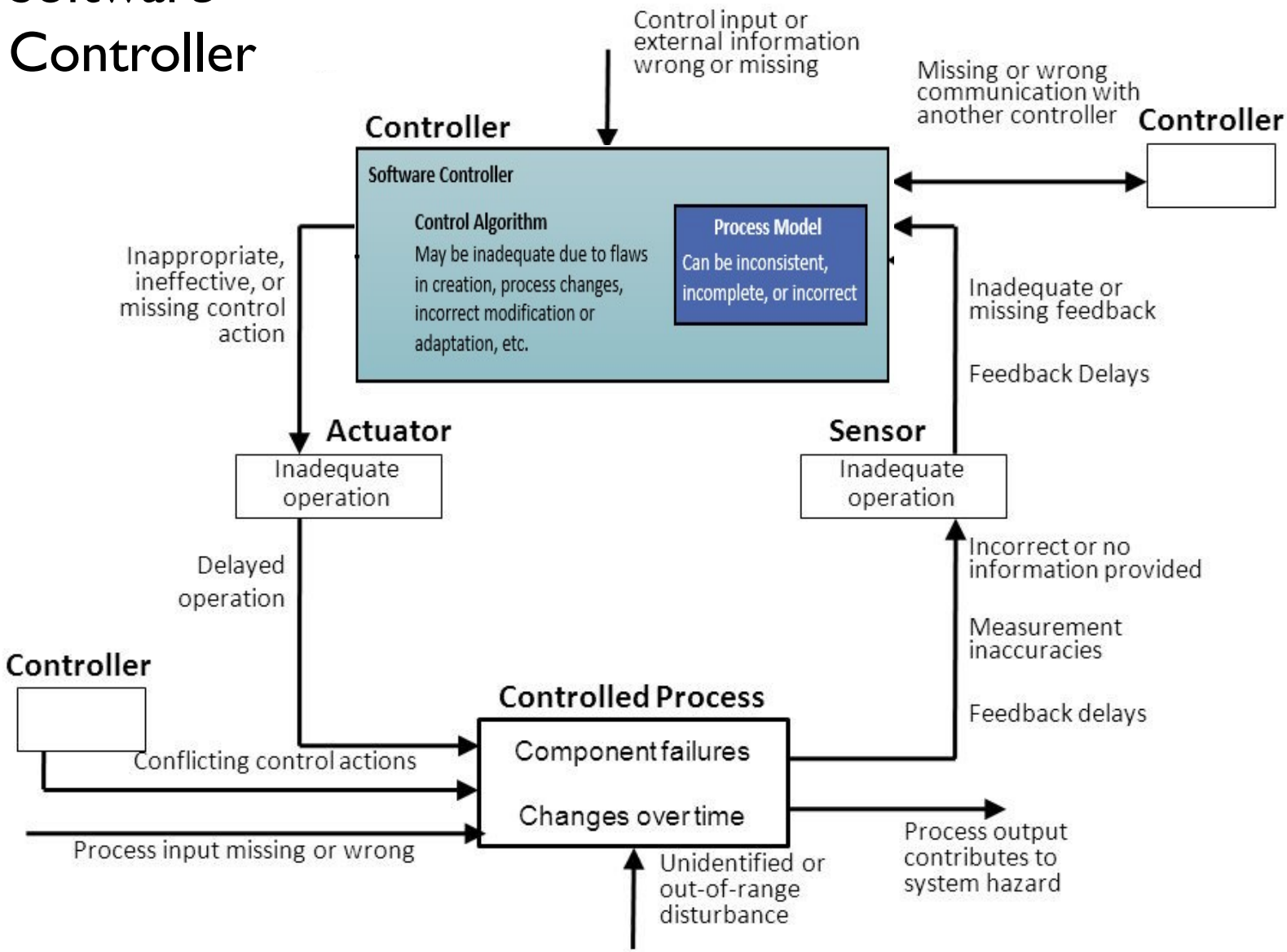
(Thomas & France, 2016)

Provides an alternative to the existing controller model which is better suited for software controllers



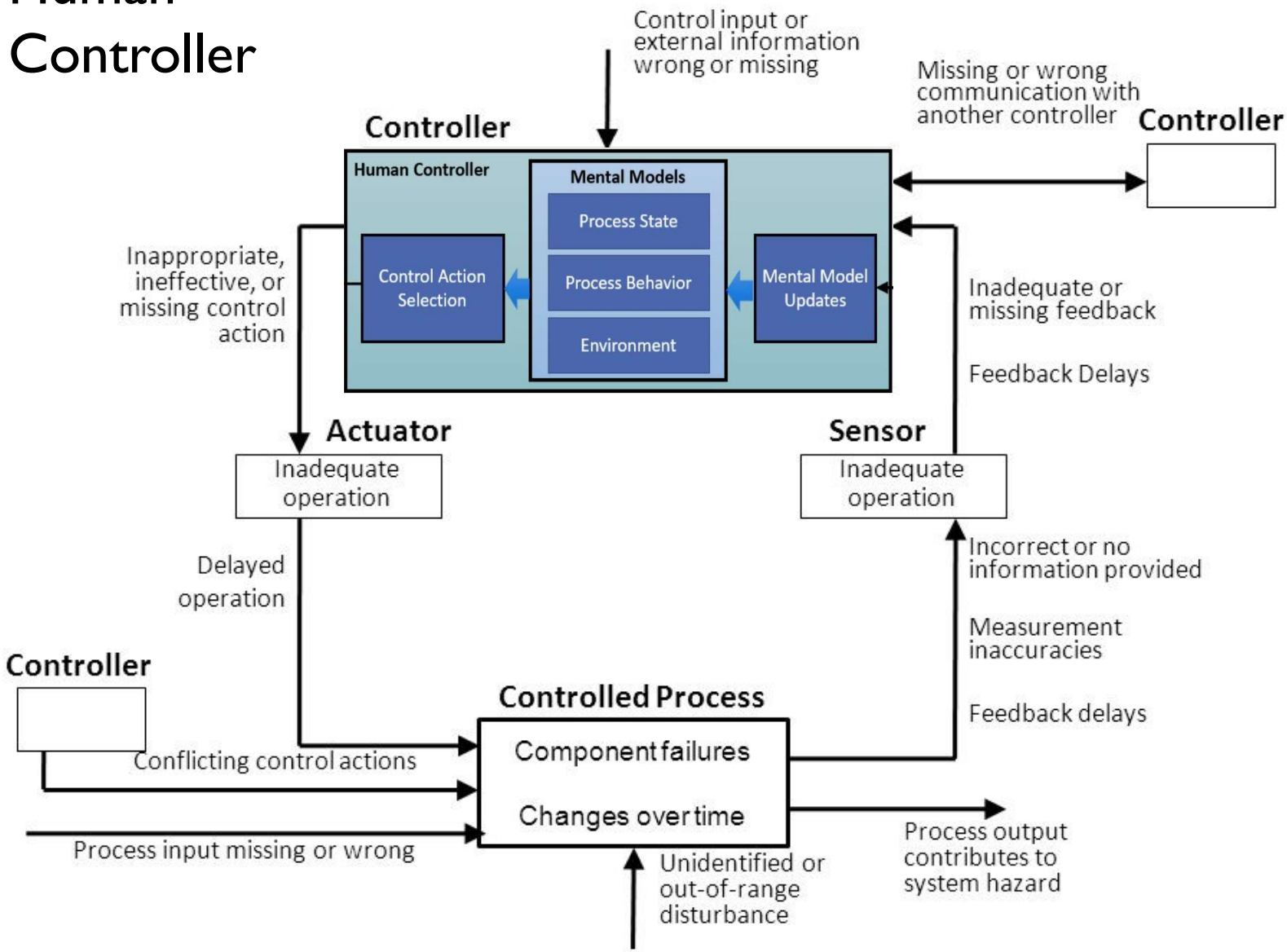
TREAT SOFTWARE AND HUMANS DIFFERENTLY

Software Controller

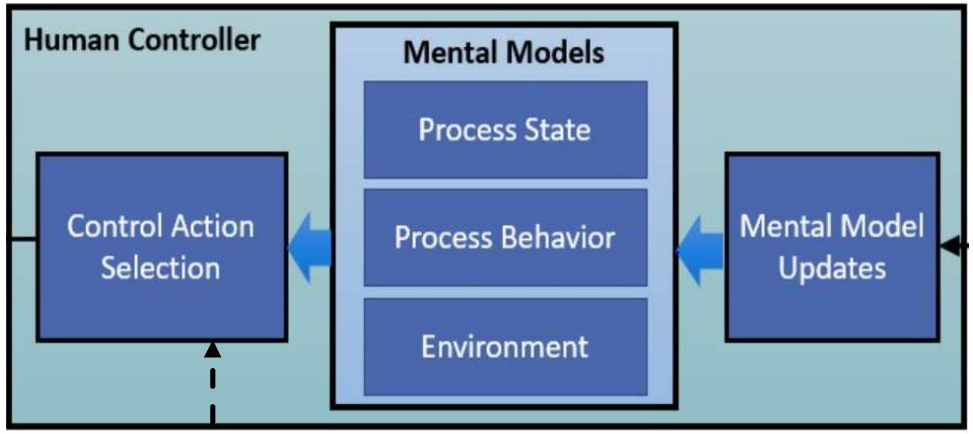


TREAT SOFTWARE AND HUMANS DIFFERENTLY

Human Controller



CONTROL ACTION SELECTION



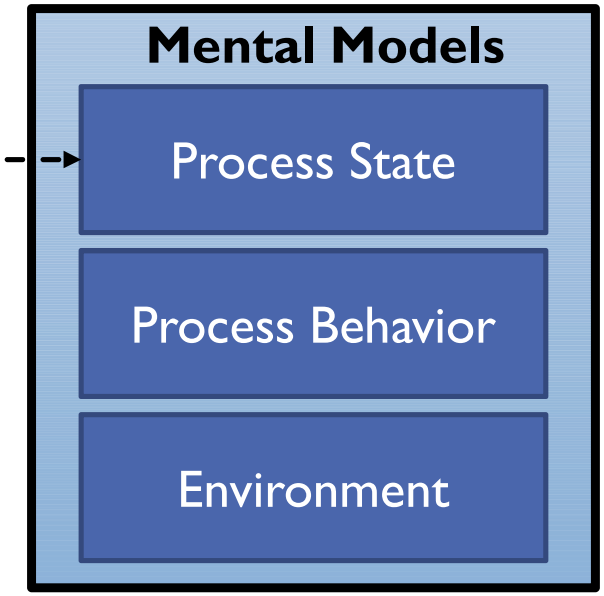
How did the operator choose which control action to perform?

Control Action Selection

- What were the operator's goals?
- What alternatives was the operator choosing between?
- How automatic or novel was the behavior?
- How might the operator's mental models affect their decision?
- What external factors (*eg. time pressure)* might affect their decision?

MENTAL MODELS

"Small-scale models of external reality"
– Kenneth Craik, 1943



Mental models are ***partial representations.***

- *Information may be purposefully omitted*
- *"Unknowns" may be known or unknown*
- *Information may be incorrect or outdated*

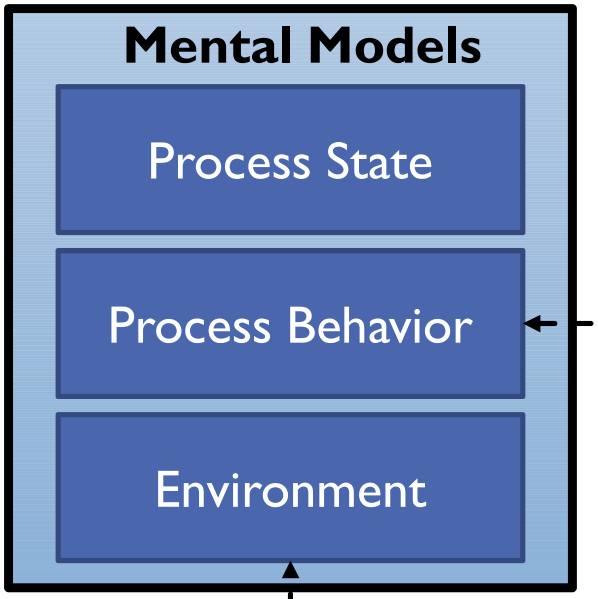
What does the operator believe about the system?

Mental Model of Process State

- Beliefs about modes and mode changes
- Believes about the current process stage, for processes with multiple stages
- Beliefs about system variables (eg. true/false)

MENTAL MODELS

What does the operator believe about the system?



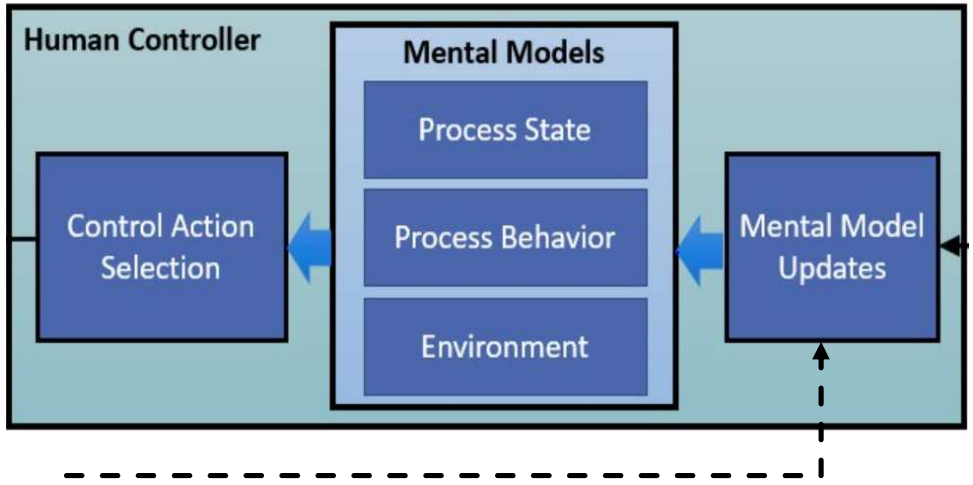
Mental Model of Process Behavior

- Beliefs about what the system can do
- Beliefs about how the system will behave in a particular mode or stage of operation
- Beliefs about if-then relationships between operator input and system output

Mental Model of the Environment

- Changes in environmental conditions
- Familiar or unfamiliar environments
- State and behavior of other controllers
- Social and organizational relationships

MENTAL MODEL UPDATES

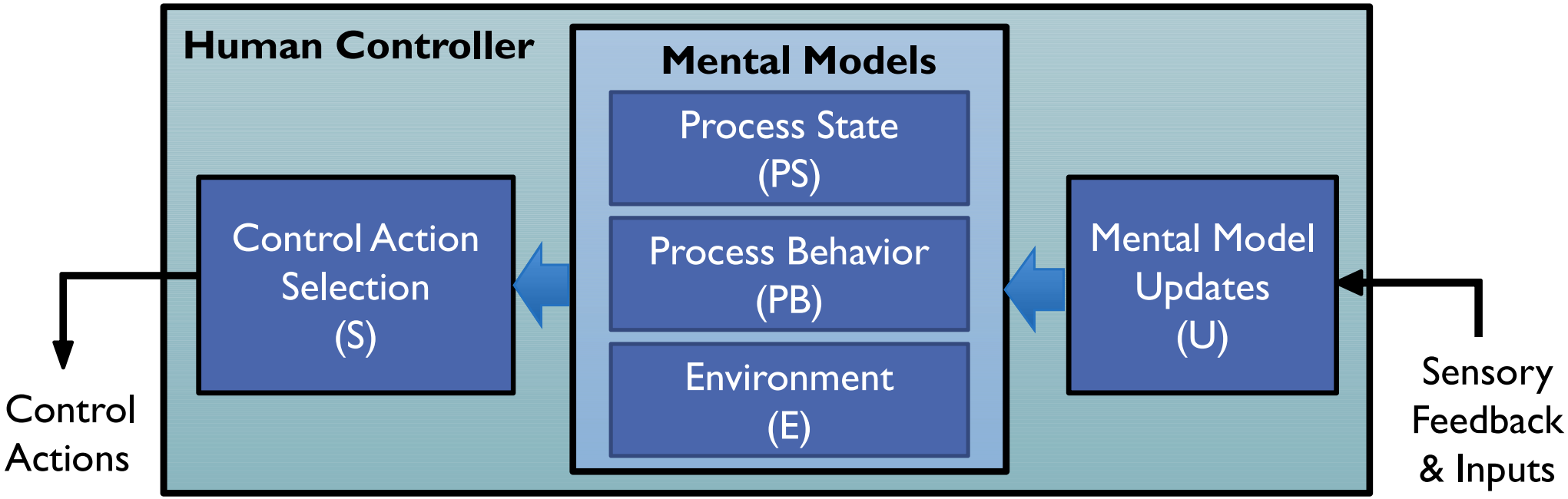


How did the operator come to have their current beliefs?

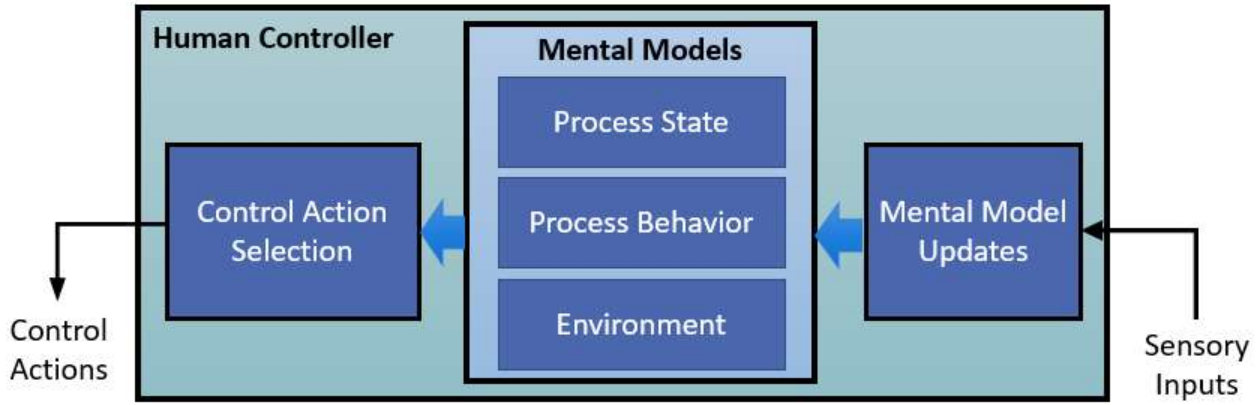
Mental Model Updates (and Initial Formation!)

- Consider initial formation of mental model vs. later updates
- Consider non-feedback inputs such as training programs and documentation
- Consider whether input/feedback was observed (*salience, expectations)*
- Consider whether input/feedback was correctly perceived & interpreted

ABBREVIATIONS TO LINK MODEL TO SCENARIOS



BENEFITS



- The new Engineering for Humans approach is **simple to apply**, and each part of the new model provides important insight into human behavior
- It **provides additional guidance** for STPA, and can be used **early in the design process**
- Most importantly, it fits well into existing processes and provides a **"common language"** for engineers to discuss issues across disciplines

OUTLINE

- Introduction
- Engineering for Humans Extension

- Example Applications
  - Railway grade crossing
  - Aircraft pitch & speed control
  - Automated Parking Assist (APA)

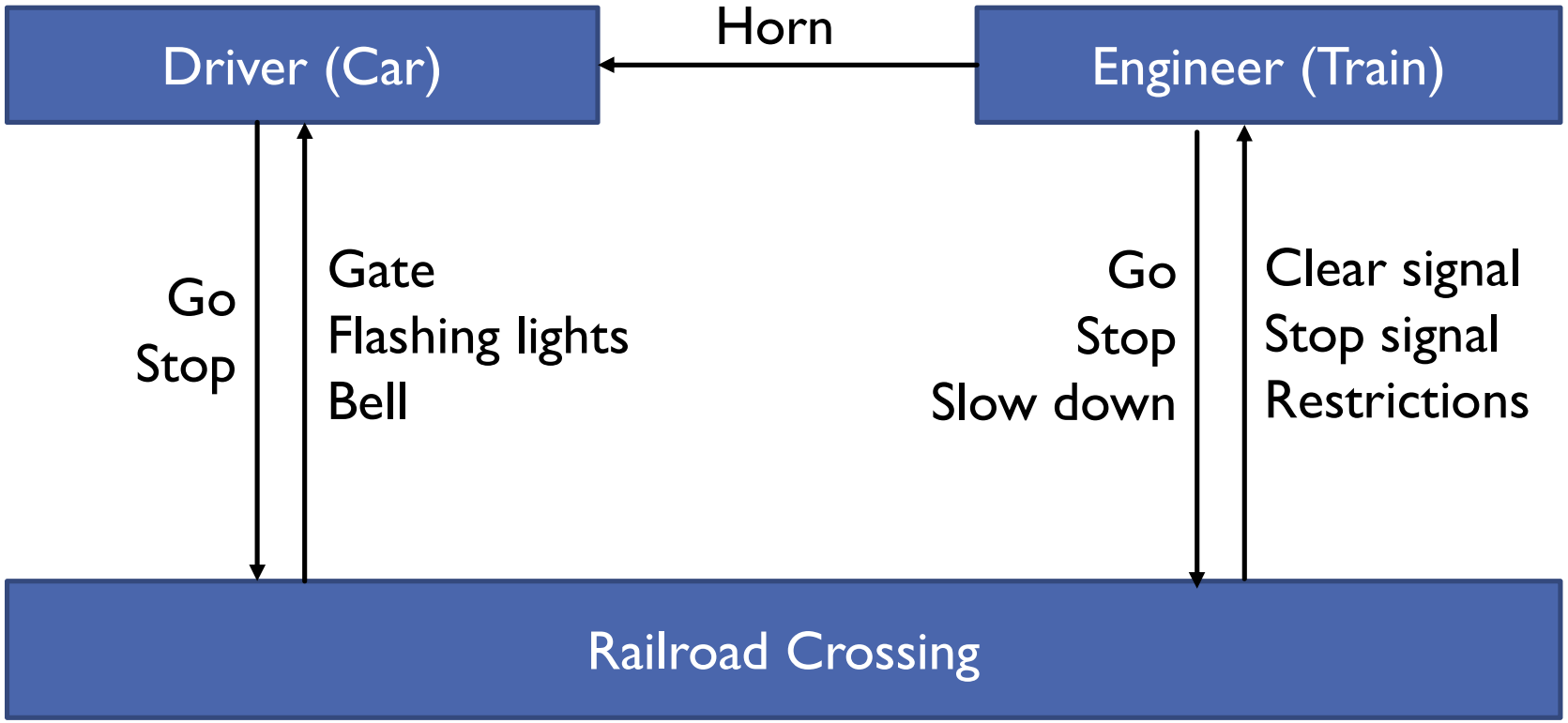
- Q&A

RAIL EXAMPLE

RAILROAD CROSSING EXAMPLE

Accidents	A1: A car and train collide at a railroad crossing.
Hazards	H1: A car is stopped in the path of a train. H2: A car is moving in front of the path of a train.

SAFETY CONTROL STRUCTURE [SIMPLIFIED]



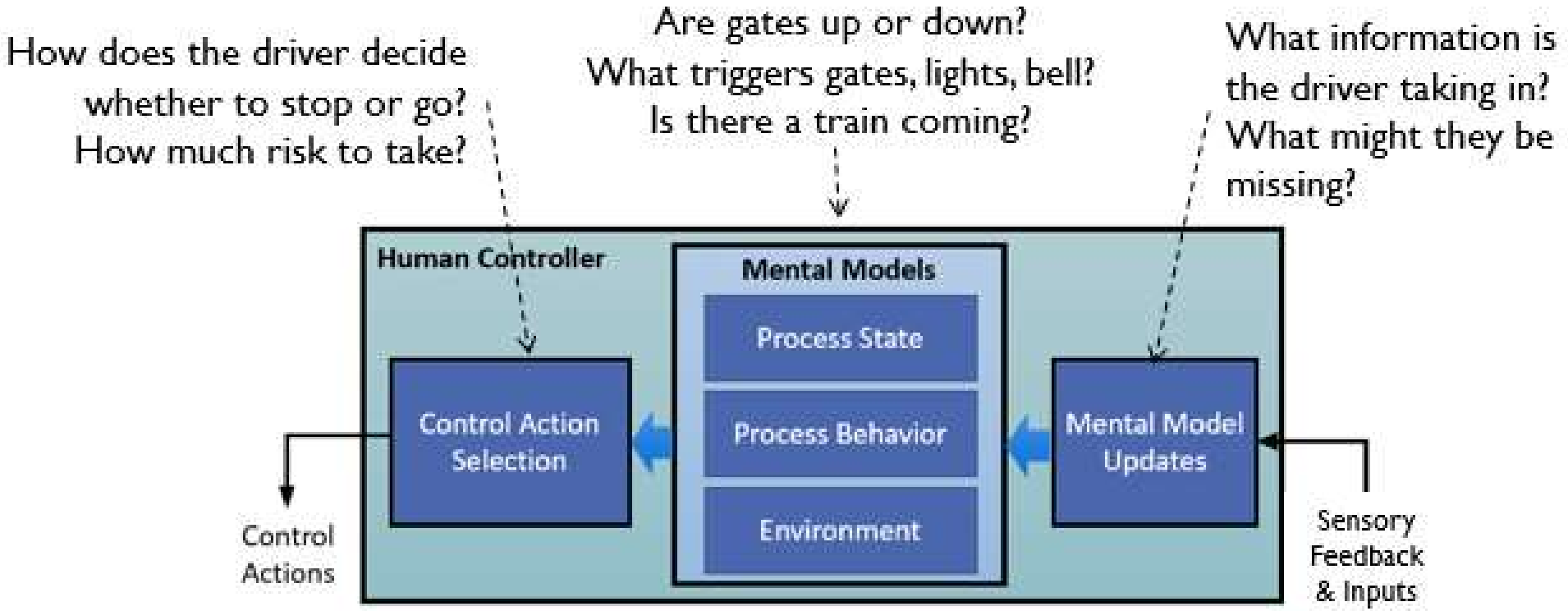
DRIVER UNSAFE CONTROL ACTIONS

Control Action	Applying causes Hazard	Not applying causes hazard	Wrong timing or order	Stopped too soon or applied too long
Stop	**UCA-1:** Driver stops over the tracks when a train is approaching. [H1]	**UCA-2:** Driver does not stop before the crossing when a train is approaching. [H2]	-	-

Reminder-
H1: A car is stopped in the path of a train.
H2: A car is moving in front of the path of a train.

DEVELOPING CAUSAL SCENARIOS

New model gives us additional information to consider…



DEVELOPING CAUSAL SCENARIOS

UCA-1: Driver stops over the tracks when a train is approaching. [H1]

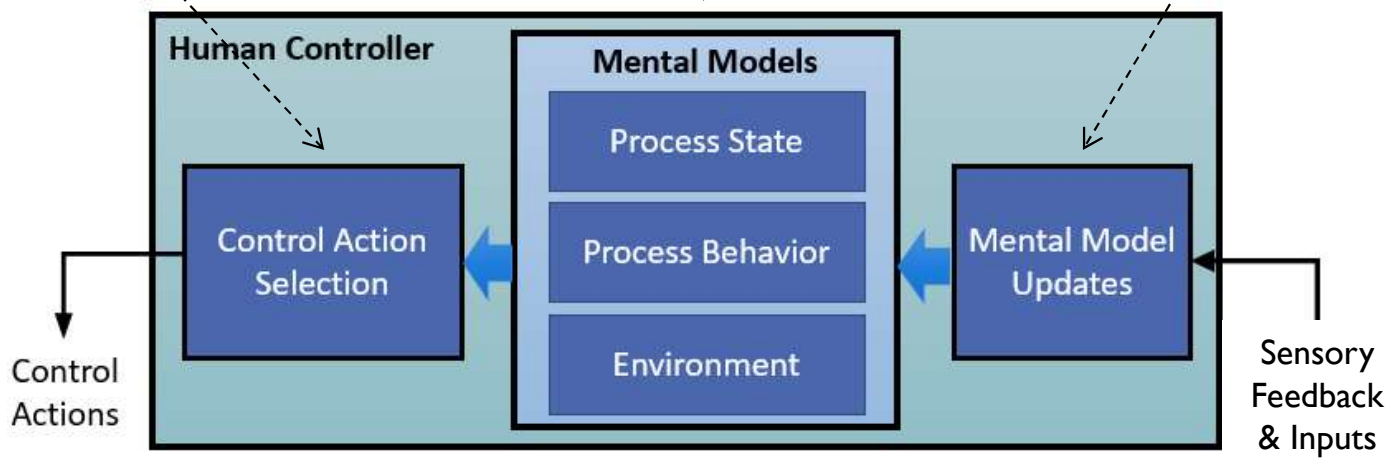
Driver incorrectly believes there is no train / it is safe to cross (PS),

Because a gate would come down if it were not safe (PB).

Driver is at an intersection in traffic (E).

Driver decides to cross intersection because he is in a hurry & believes it is safe (but gets stuck on track).

Driver is familiar with gated crossings & did not notice this crossing has no gate.



DEVELOPING CAUSAL SCENARIOS

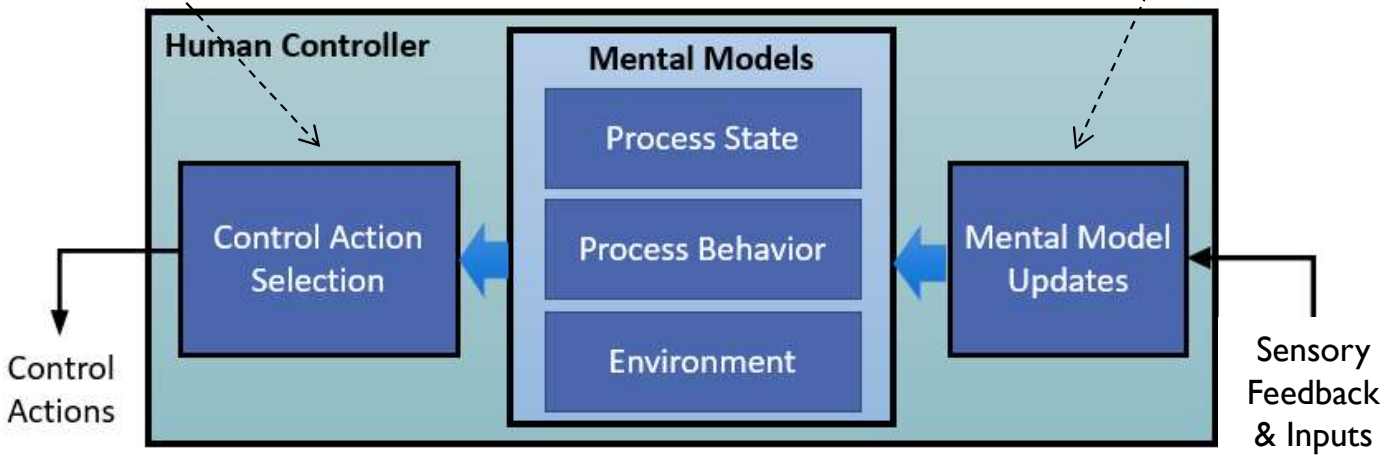
UCA-2: Driver does not stop before the crossing when a train is approaching. [H2]

Driver decides to go around the gate, believing the risk is low.

Driver knows that gates sometimes come down when there is no train (PB).

Driver believes there is no train (PS).

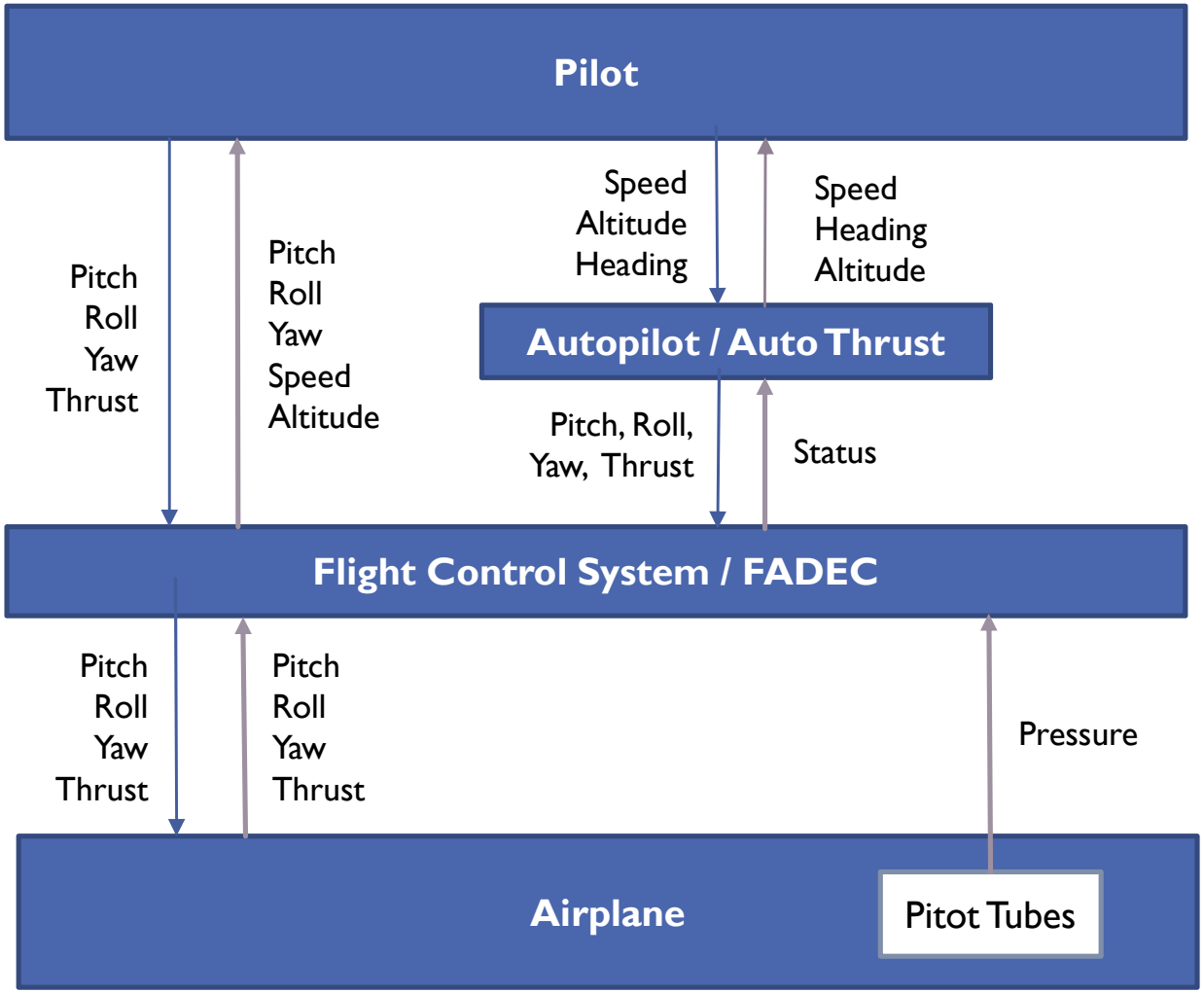
Driver has waited for gates in the past when no train was coming.



AVIATION EXAMPLE

ACCIDENTS AND HAZARDS

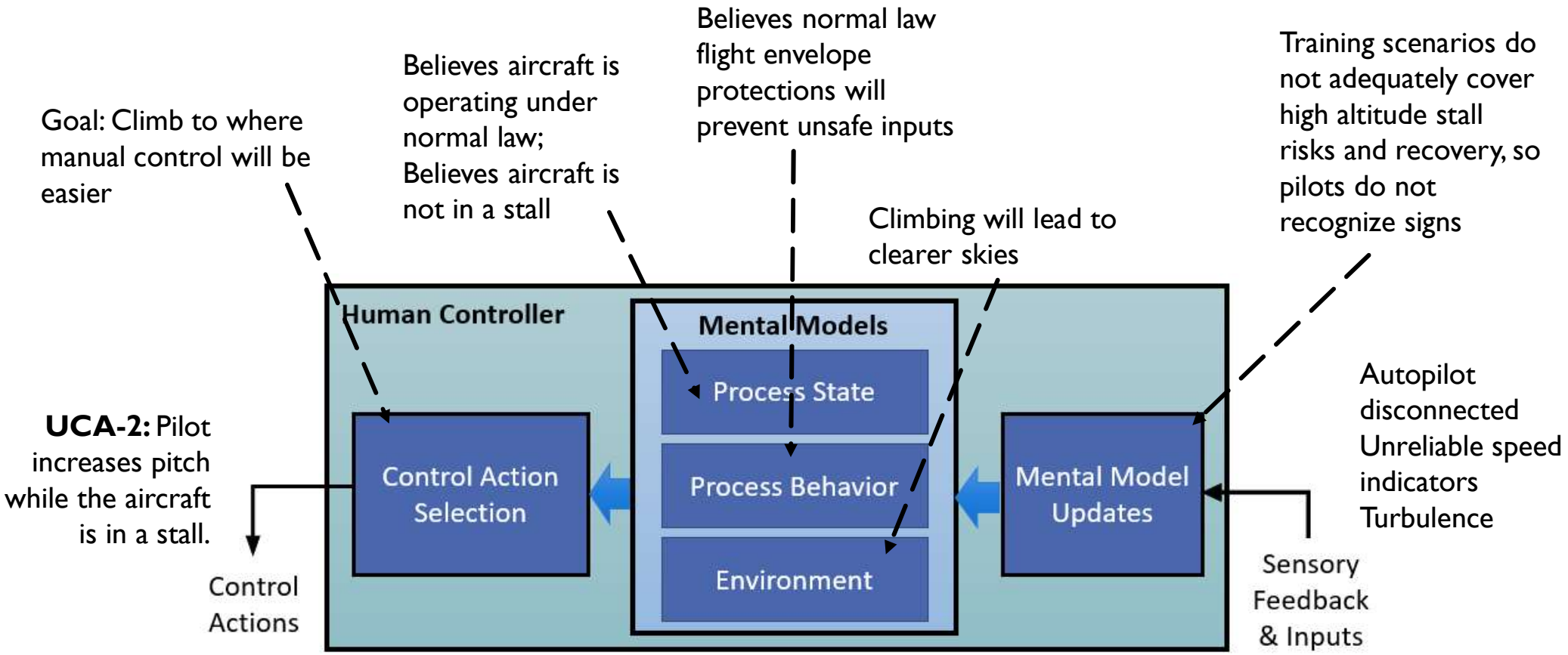
- A-1: Aircraft collision with terrain
- H-1: Loss of lift during flight
  - H-1.1: Angle of attack (pitch) is too great
  - H-1.2: Aircraft speed is too low


Pilot
Pitch
Roll
Yaw
Thrust
Pitch
Roll
Yaw
Speed
Altitude
Speed
Altitude
Heading
Speed
Heading
Altitude
Autopilot / Auto Thrust
Pitch, Roll,
Yaw, Thrust
Status
Flight Control System / FADEC
Pitch
Roll
Yaw
Thrust
Pitch
Roll
Yaw
Thrust
Pressure
Airplane
Pitot Tubes

UCAS– PITCH CONTROL

Control Action	Not Provided	Provided	Too Late / Too Soon / Wrong Order	Stopped too soon / Applied too long
Increase Pitch	Pilot does not increase pitch when aircraft is at risk of collision with terrain.	**Pilot increases pitch while the aircraft is in a stall.**	-	Pilot increases pitch, but stops too soon before reaching the target pitch. Pilot continues to increase pitch too long when doing so exceeds the safe flight envelope.

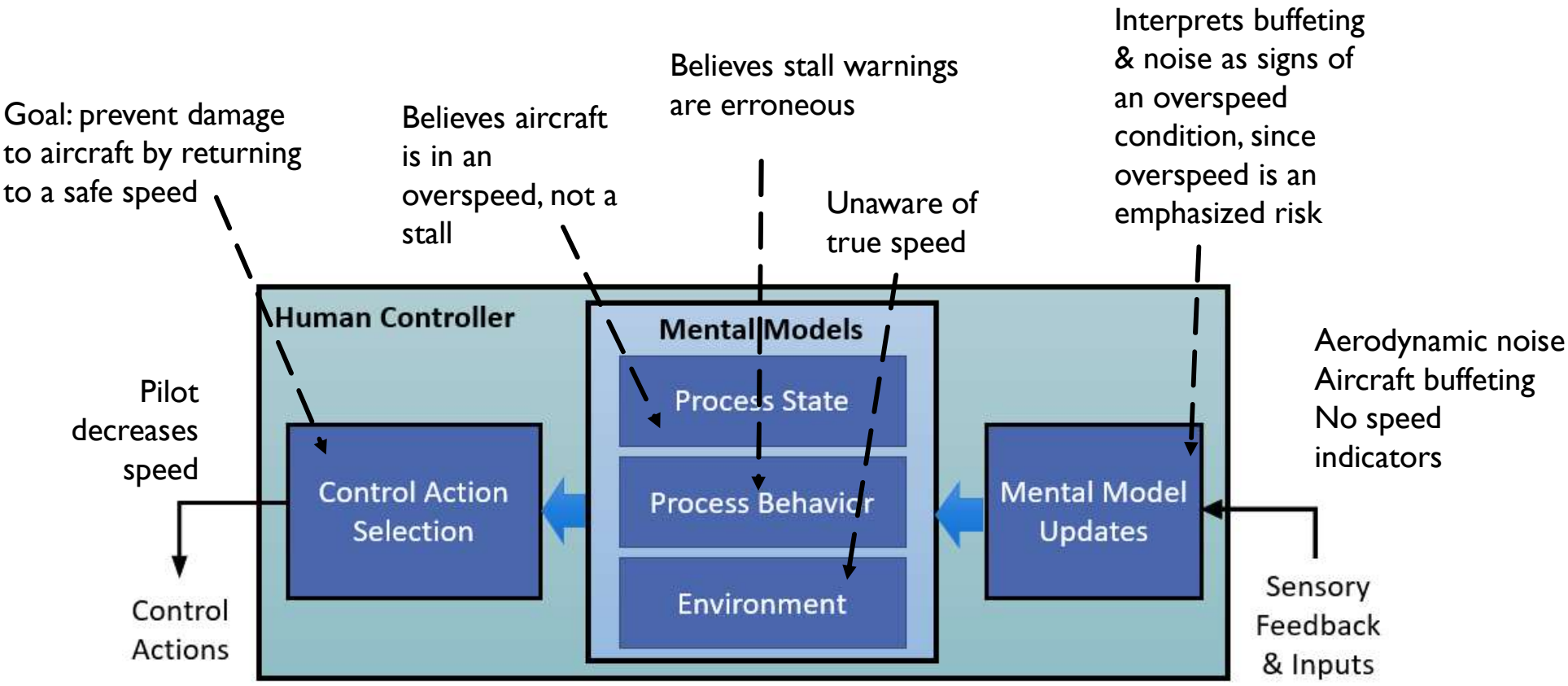
UCA: PILOT INCREASES PITCH WHILE THE AIRCRAFT IS IN A STALL.



UCAS– SPEED CONTROL

Control Action	Not Provided	Provided	Too Late / Too Soon / Wrong Order	Stopped too soon / Applied too long
Decrease Speed	Pilot does not decrease speed when aircraft is in an overspeed condition.	**Pilot decreases speed while the aircraft is in a stall.**	-	-

UCA: PILOT DECREASES SPEED WHILE THE AIRCRAFT IS IN A STALL.



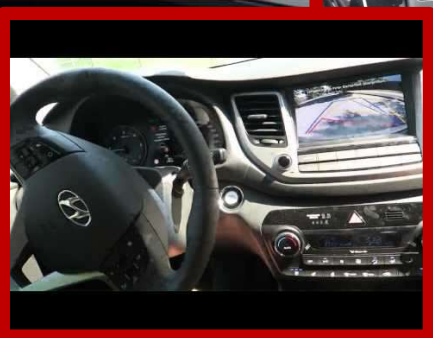
CONCLUSION

- New extension is effective, offers benefits of STPA plus new guidance
- Can be used to examine pilot interactions with cockpit automation
- Captures hazardous interactions including those involved in Air France 447 crash

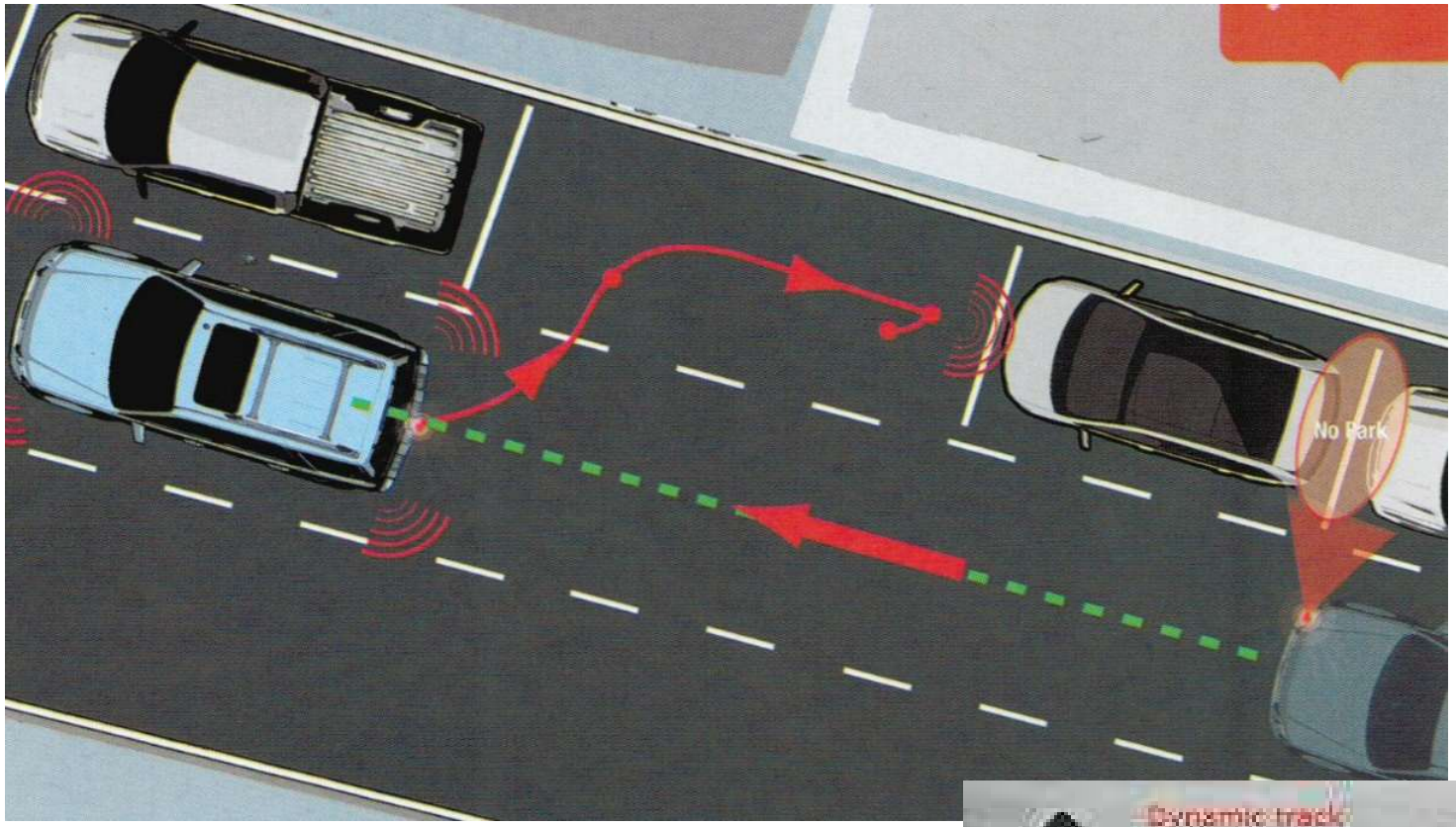
AUTOMATED PARKING ASSIST (APA)

AUTOMATED PARKING

- Nissan Intelligent Park Assist
- Mercedes Active Parking Assist
- BMW Parking Assistant
- Ford Active Park Assist
- Toyota Intelligent Park Assist
- Audi Automatic Parking
- Jaguar Enhanced Parking Assist
- Hyundai Advanced Parking Assistance



AUTOMATED PARKING

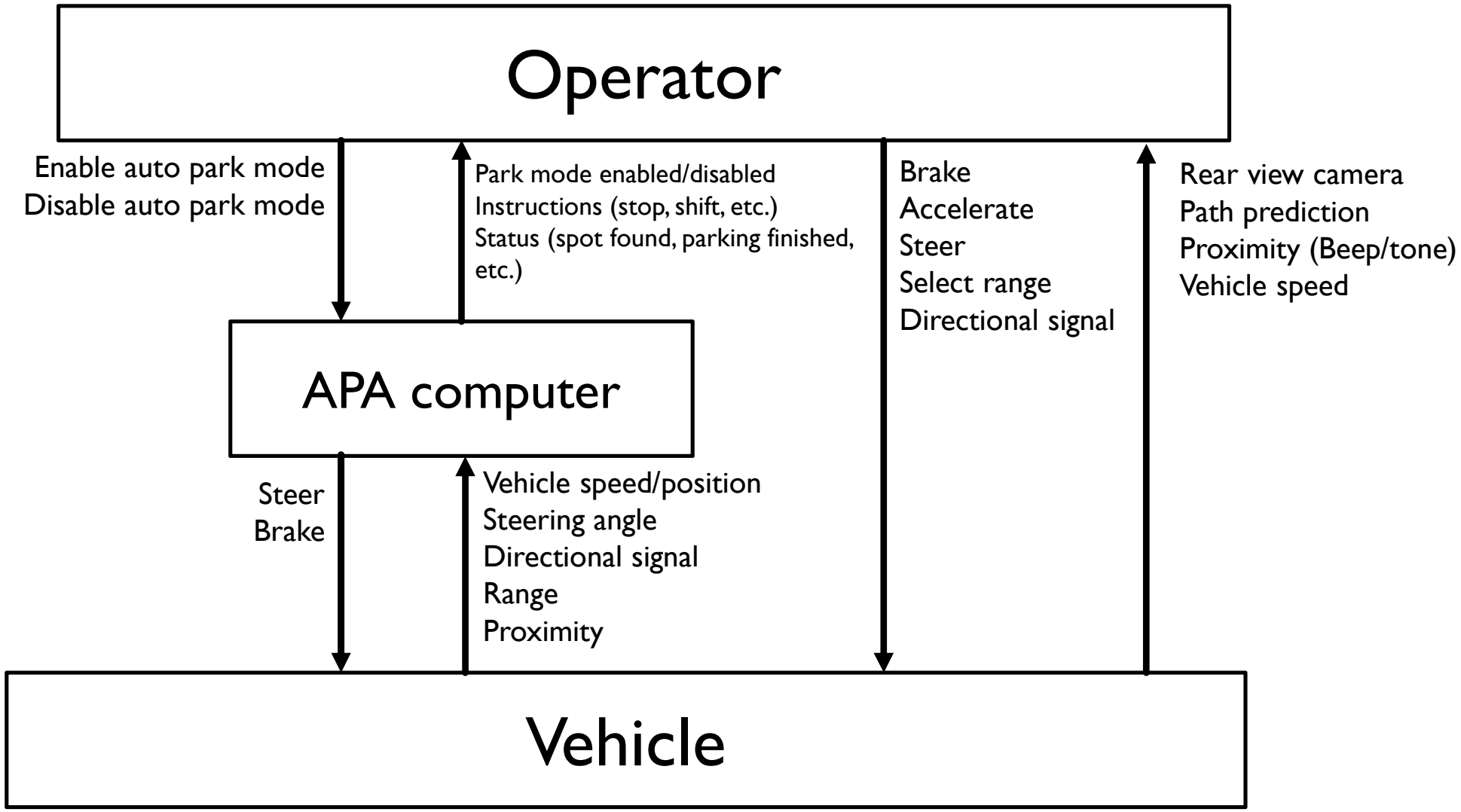


ACCIDENTS AND HAZARDS

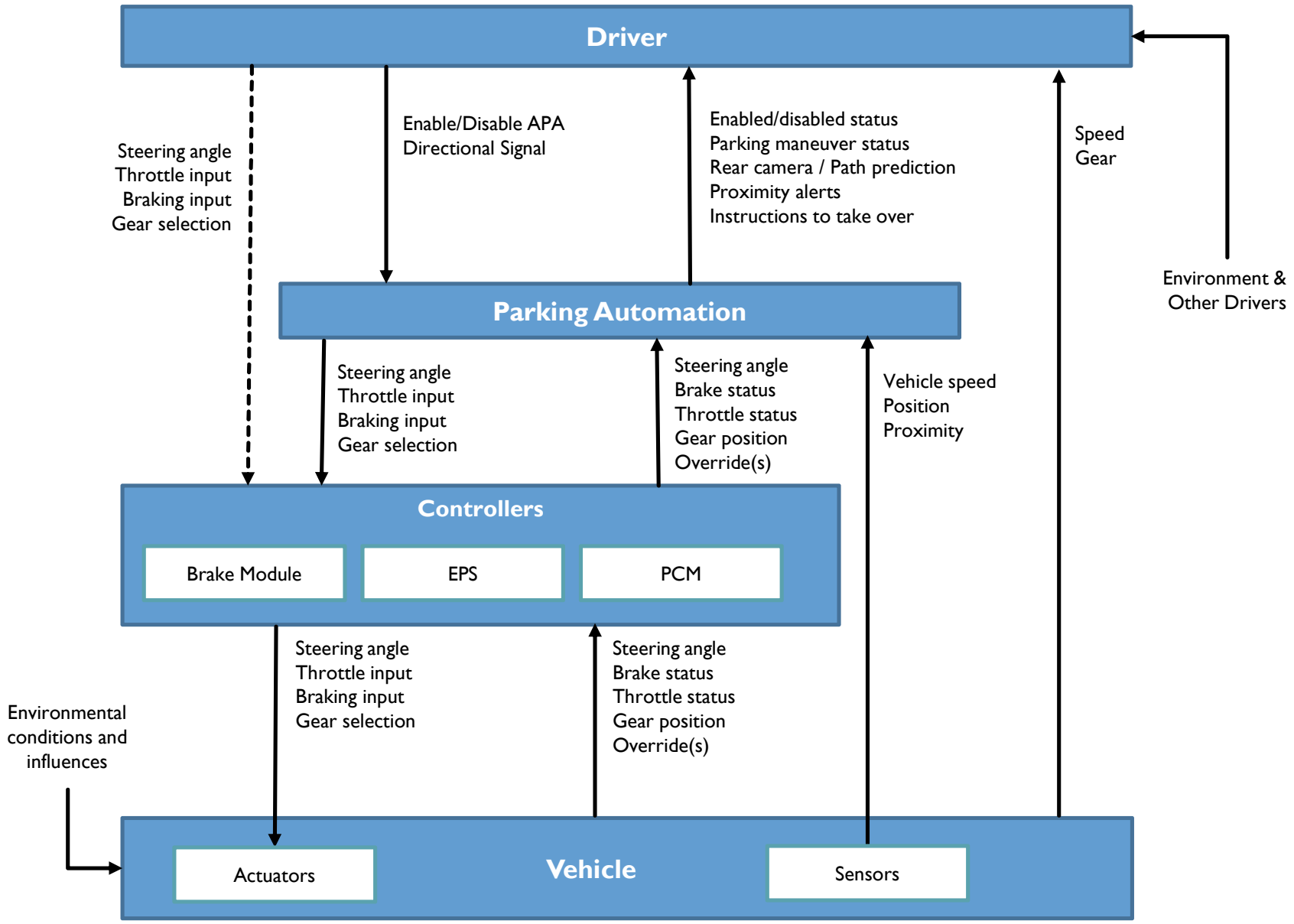
System Level Accidents	
A-1	Death, injury, or property damage resulting from a collision with a person, vehicle, object, or terrain.
A-2	Injury or property damage occurring within the vehicle, without a collision.
A-3	Loss of customer satisfaction with automated parking, without injury or property damage.

System Level Hazards	
H-1	The vehicle does not maintain a safe minimum distance between itself and obstacles such as pedestrians, vehicles, objects, and terrain. [A-1]
H-2	Occupants or cargo are subjected to sudden high forces that may result in injury or property damage. [A-2]
H-3	The vehicle parks inappropriately, either in an unsuitable space (e.g. blocking a fire hydrant) or in violation of parking guidelines (e.g. excessively far from the curb). [A-3]

HIGH-LEVEL CONTROL STRUCTURE



DETAILED CONTROL STRUCTURE



KEY ASSUMPTIONS ABOUT OUR SYSTEM

- The automation is capable of steering, braking, shifting, and accelerating.
- The driver is expected to monitor the system to respond to unexpected events and obstacles.
- The driver may temporarily override the APA computer's actions by braking or accelerating for short periods of time.
- If the driver
  - grabs the wheel
  - accelerates above a given maximum speed
  - brakes for more than 2 seconds
  - or presses the APA button

  the automation will be fully disabled.

UNSAFE CONTROL ACTIONS

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
Brake (Driver)	UCA 2b-33: Driver does not brake when APA is disabled and the vehicle is on a collision path. [H-1] UCA 2b-34: Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle. [H-1]	UCA 2b-35: Driver provides insufficient brake command when APA computer does not react appropriately to the obstacle. [H-1] UCA 2b-36: Driver provides too much brake when doing so puts other traffic on collision course or causes passenger injury. [H-2]	UCA 2b-37: Driver waits too long to brake after the automation does not react appropriately to an obstacle. [H-1] UCA 2b-38: Driver brakes too early before braking is needed, putting the vehicle on a collision path. [H-1]	UCA 2b-39: Driver continues override braking for too long and disables automation when doing so puts the vehicle on a collision path. [H-1] UCA 2b-40: Driver does not brake for long enough to avoid collision when automation is not reacting appropriately to an obstacle. [H-1]

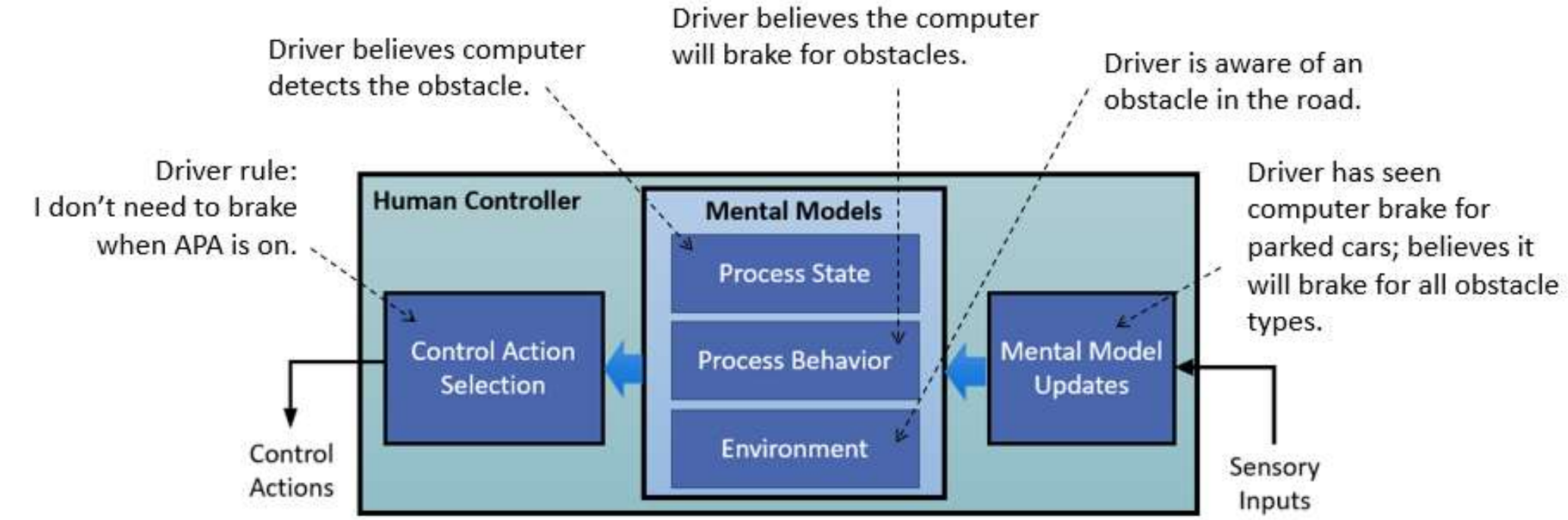
CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.

Scenario: The driver does not brake for the obstacle because the driver incorrectly believes that the computer detects and will brake for the obstacle ahead. This belief stems from past experience in which she has seen the computer apply the brakes to avoid hitting other parked vehicles. She does not receive any feedback that the computer is unaware of the obstacle.

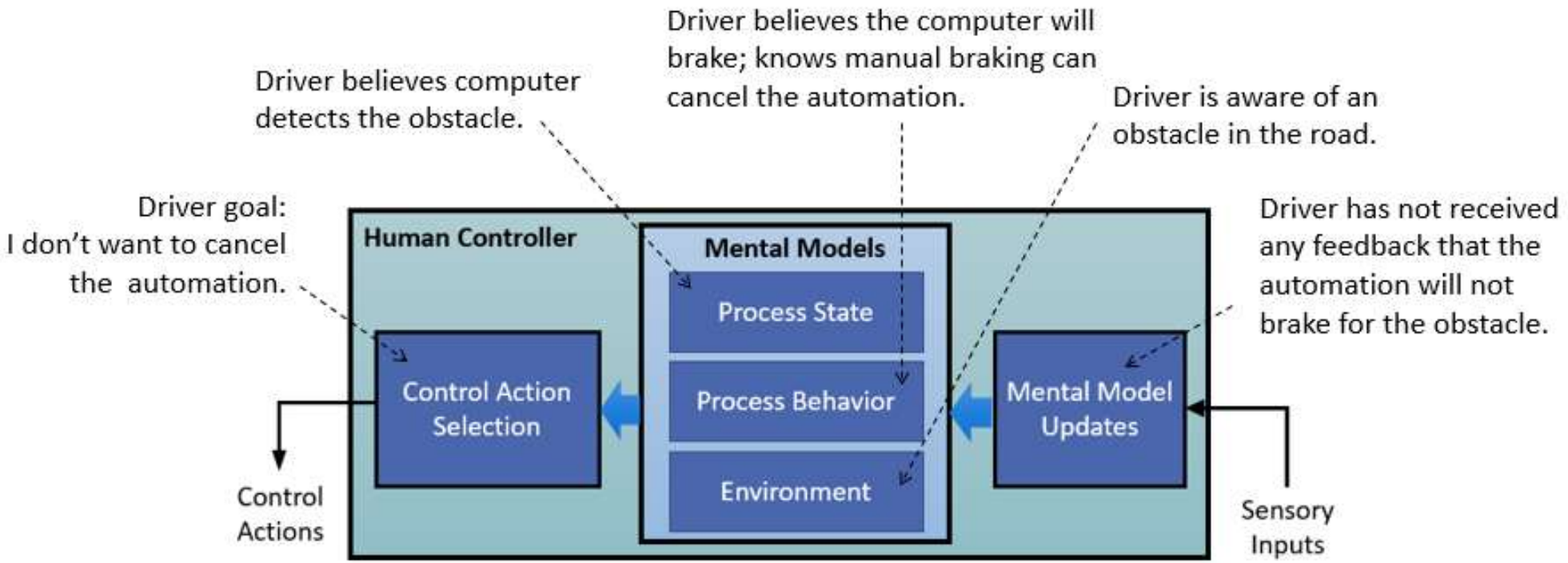
CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.



CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.



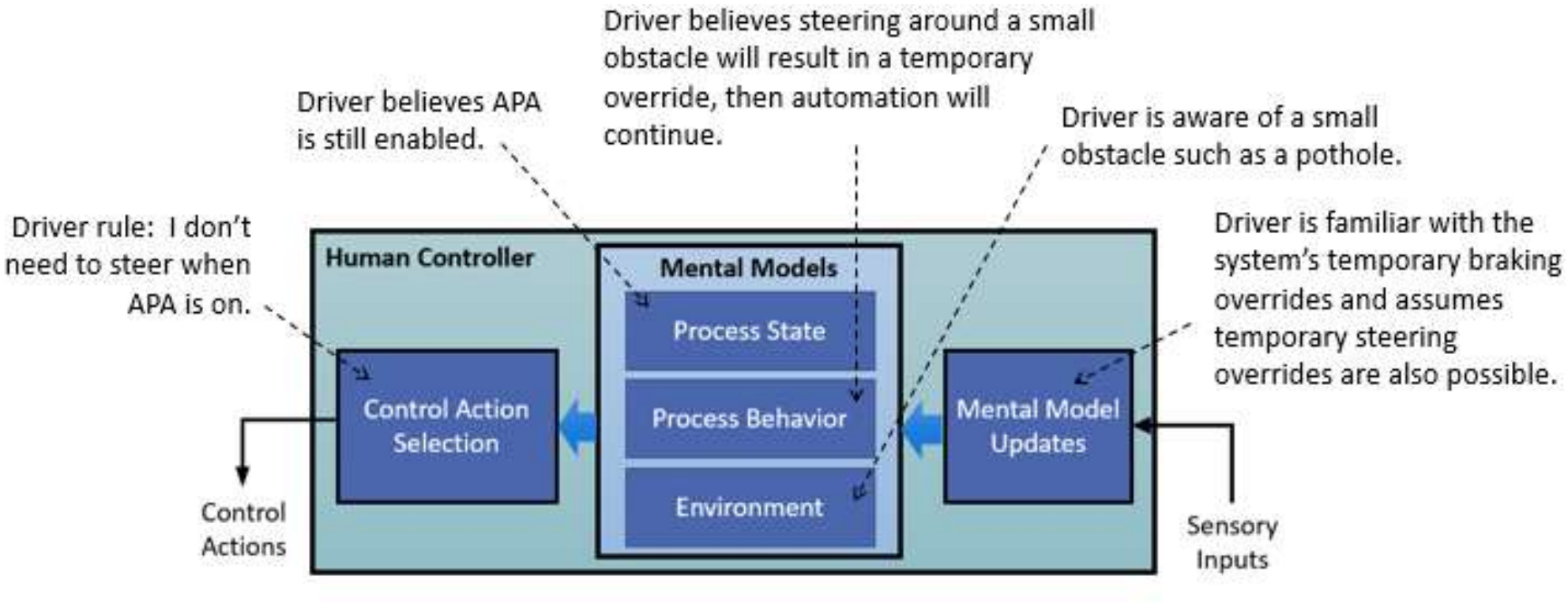
CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver stops providing steering commands after initially disabling the automation.

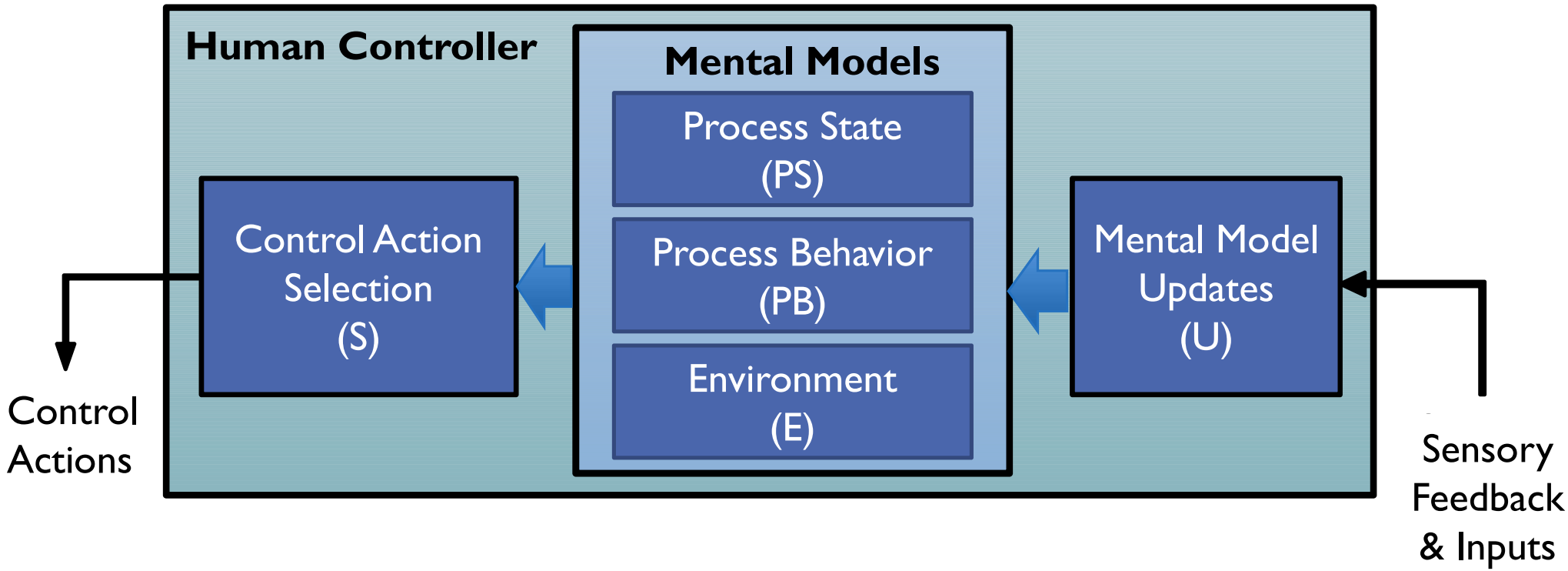
Scenario: The driver acts on the assumption that he does not need to steer when autopark is enabled, and he incorrectly believes it is still enabled because he did not notice or understand the indicator that it disabled. He had grabbed the steering wheel to swerve around a small obstacle and incorrectly assumed this would result in a temporary override because he knows that braking can cause temporary overrides and assumes steering can do the same.

CAUSAL SCENARIOS USING NEW EXTENSION

UCA: Driver stops providing steering commands after initially disabling the automation.



Questions and Discussion



REFERENCES

- Leveson, N. (2012). *Engineering a safer world systems thinking applied to safety*. Cambridge, Mass.: The MIT Press.
- Thomas, John (2013). Systems Theoretic Process Analysis (STPA) Tutorial. http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf
- Thomas, John; France, Megan (2016). Engineering for Humans: Engineering Analysis of an Automated Parking System. http://psas.scripts.mit.edu/home/wp-content/uploads/2016/04/Thomas,France-Engineering_for_Humans.pdf