ENGINEERING FOR HUMANS
STPA ANALYSIS OF AN AUTOMATED PARKING SYSTEM

Massachusetts Institute of Technology

John Thomas

Megan France

General Motors

Charles A. Green

Mark A. Vernacchia

Padma Sundaram

Joseph D'Ambrosio

PROJECT GOALS

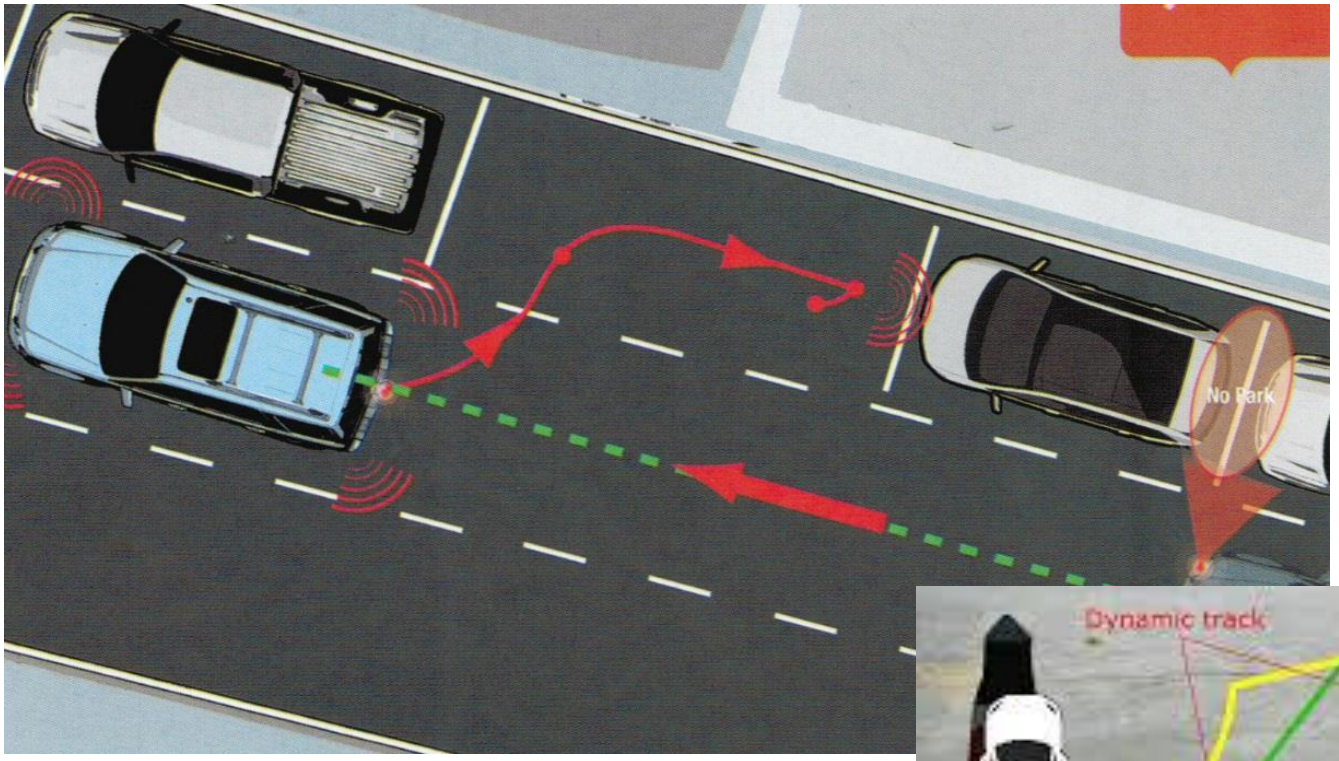
- To **examine the role of humans** in the safety of complex, automated human machine systems from a systems-theoretic perspective
- To **develop a human engineering extension** to STPA that assists us in understanding human process models and capturing additional causal scenarios
- To **use automated parking as a test case** for an STPA analysis to validate our human engineering extension

MOTIVATION

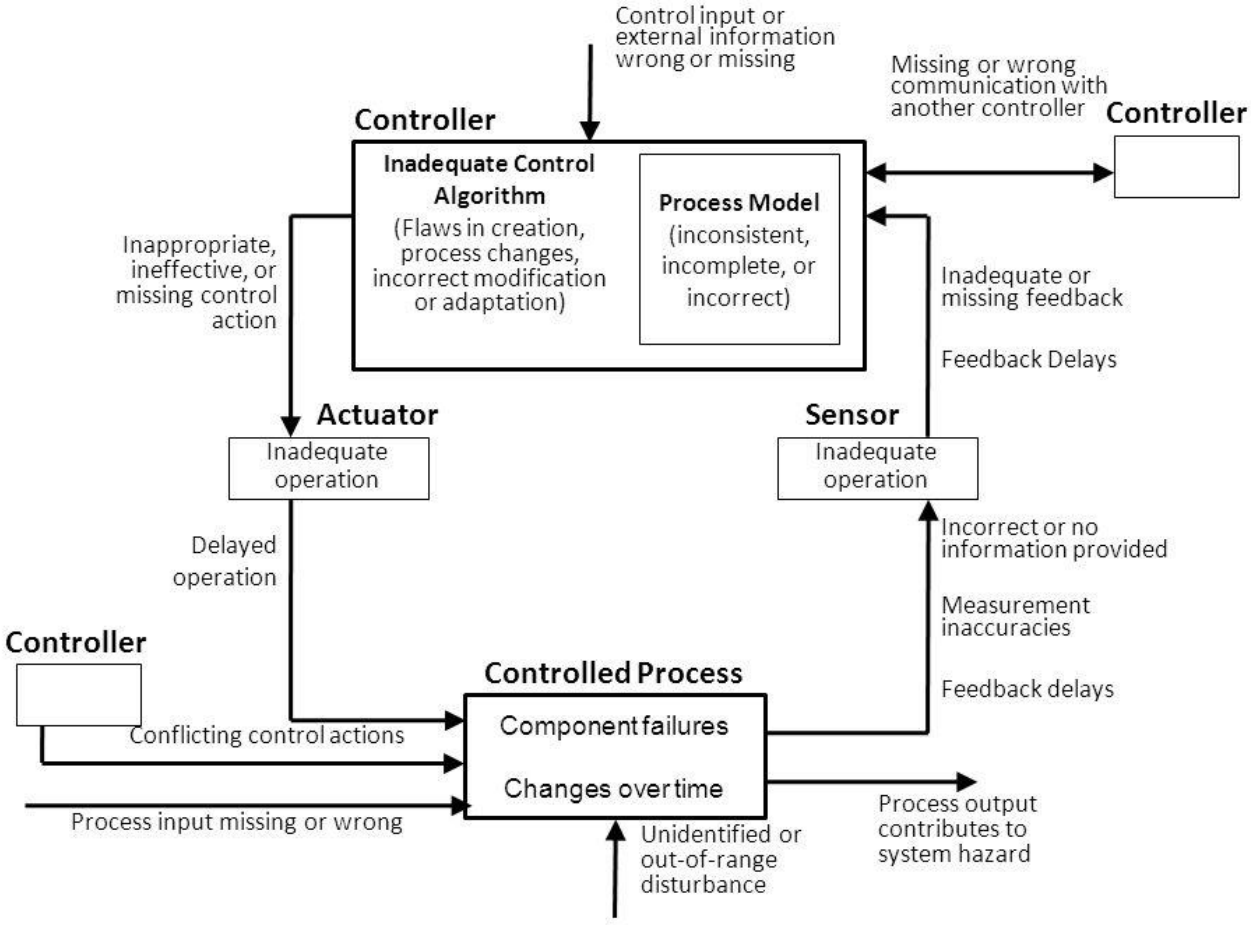
Why use automated parking as a case study for interactions in complex human machine systems?

- Interactions between driver and automation
  - Changes in driver role, increased complexity
  - Importance of human process model
- Complexity of the parking task
  - Rich environment
  - Requires multiple driver control types

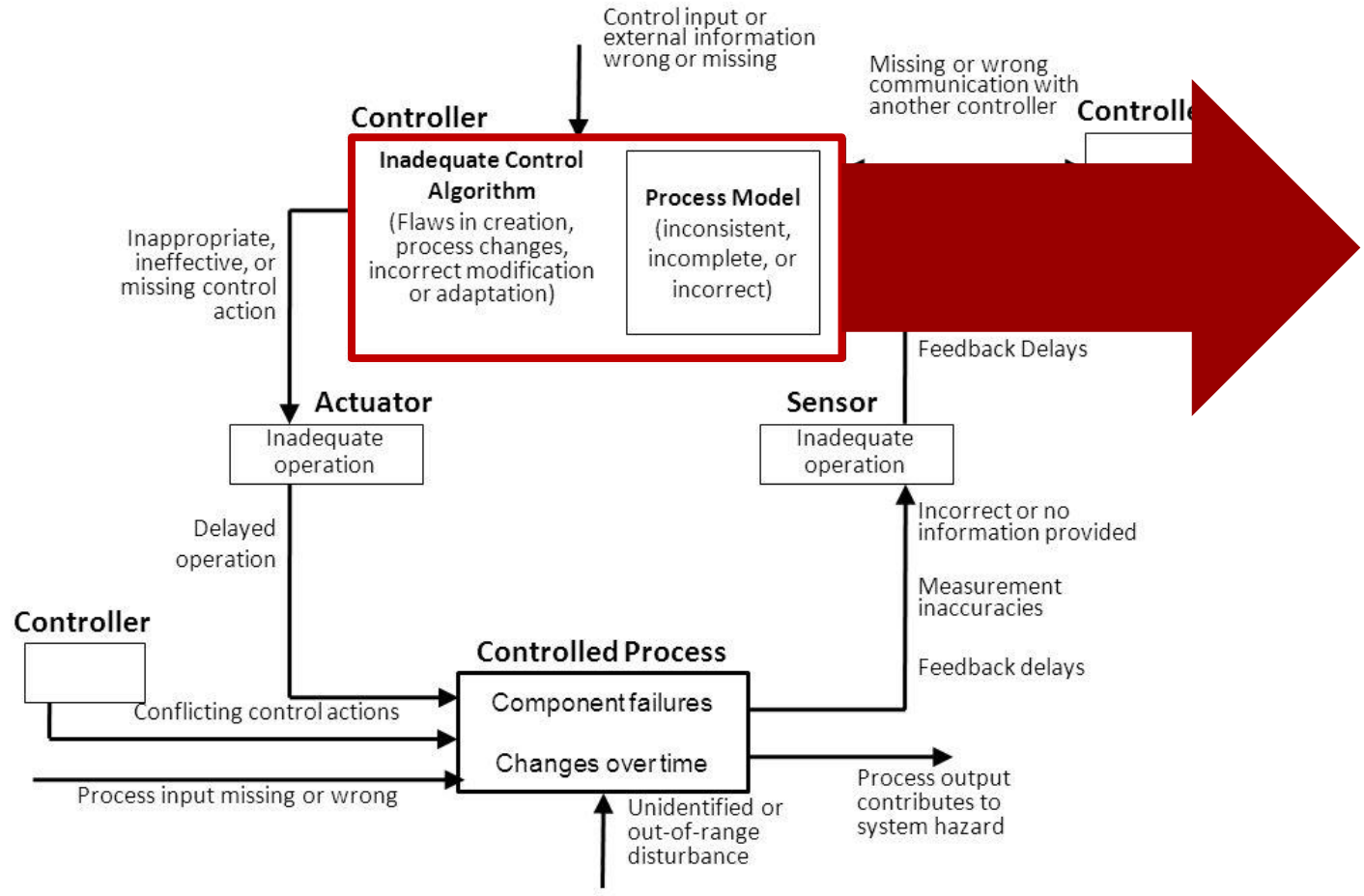
AUTOMATED PARKING ASSIST



CONTROL LOOP



CONTROL LOOP



Existing systems-theoretic controller model

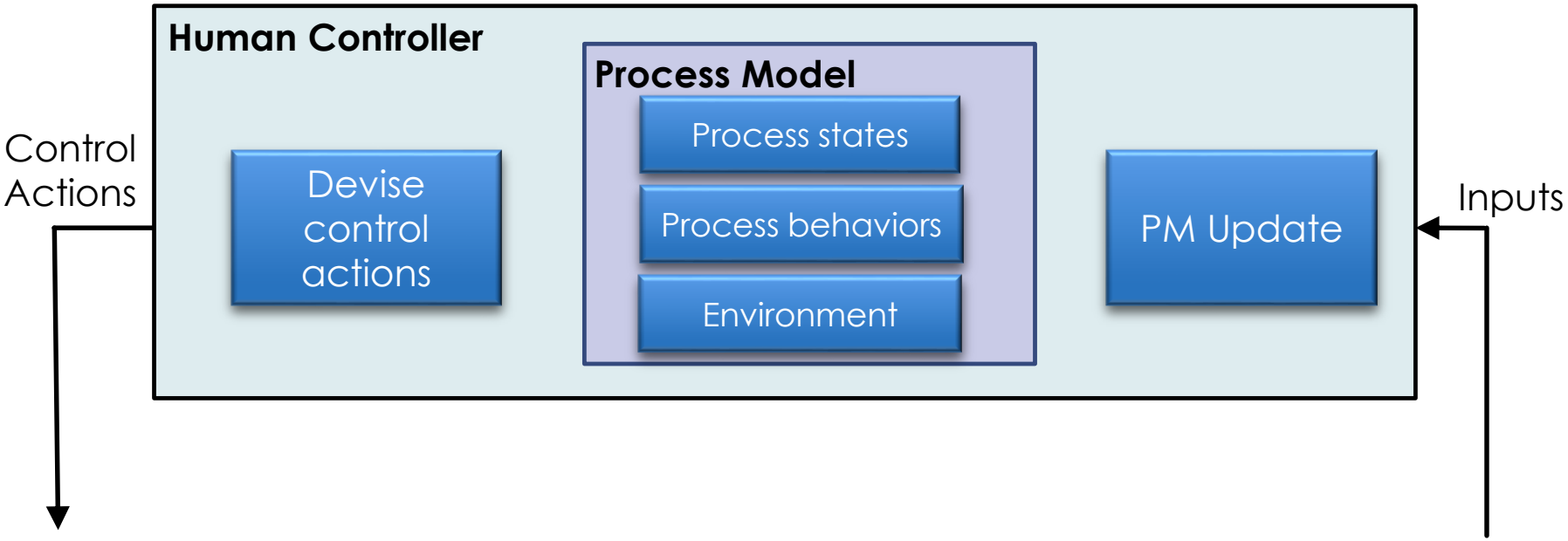
- Generic
- Not specific to humans

Developing a human model and analysis process

John Thomas

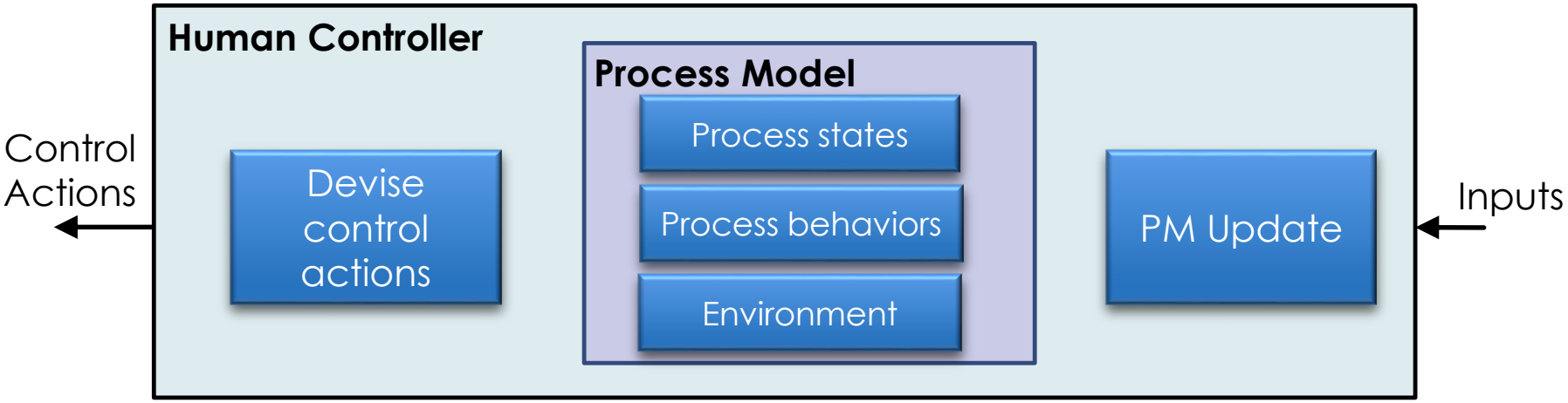
HUMAN CONTROL MODEL

HUMAN CONTROL MODEL



NEW HUMAN ENGINEERING APPROACH

- Identify UCAs
- Identify Process Model variables
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe decisions (Control Action Selections)

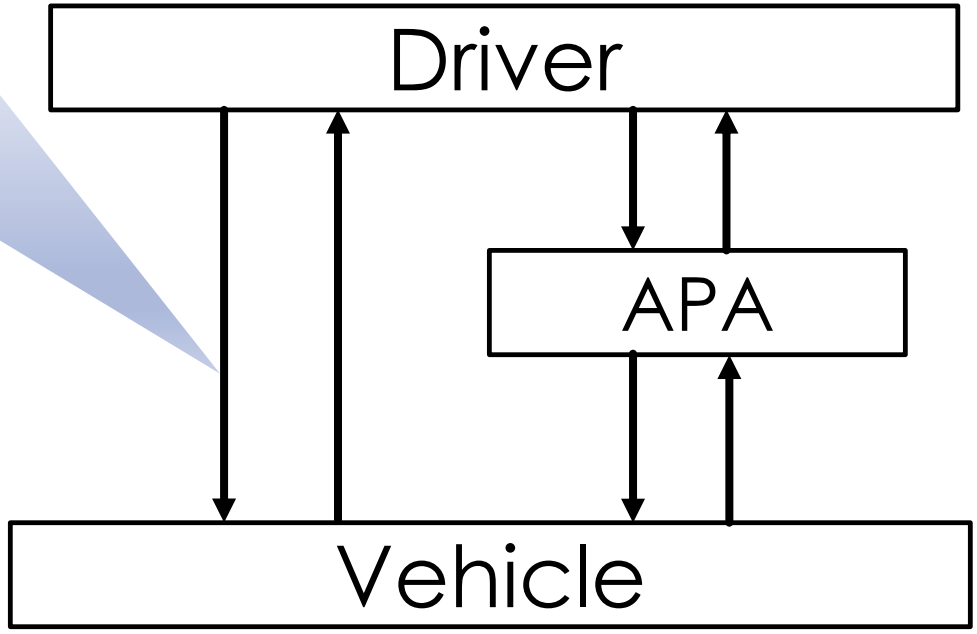


NEW HUMAN ENGINEERING PROCESS

- Identify UCAs
- Identify Process Model variables
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe decisions (Control Action Selections)

UNSAFE CONTROL ACTIONS

	Not Provided	Provided	Too early, too late, out of order	Stopped too soon, applied too long
Brake	**UCA-1: Driver does not brake when auto-parking and computer doesn't react to an obstacle**			



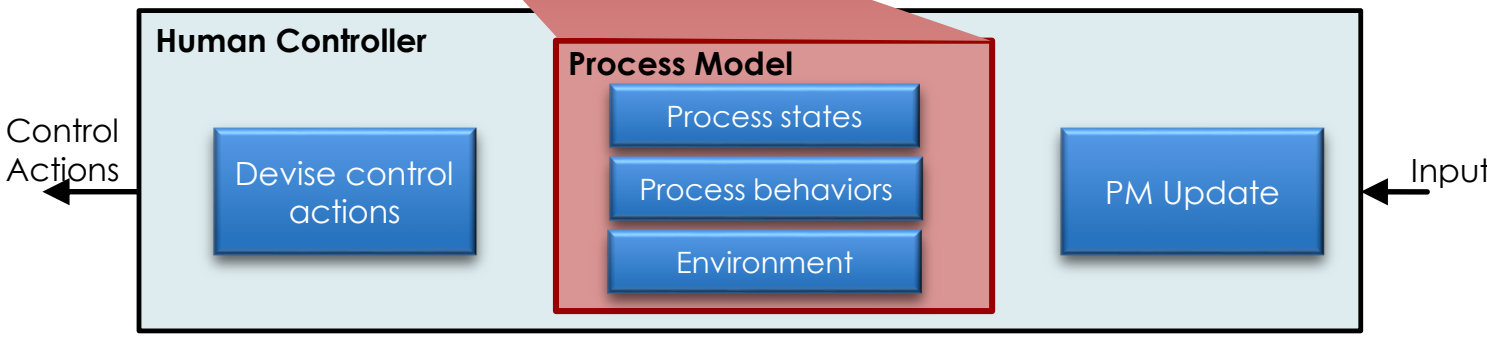
NEW HUMAN ENGINEERING PROCESS

- Identify UCAs
  - UCA-1: Driver does not brake when auto-parking and computer doesn't react to an obstacle

- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe Control Action Selections

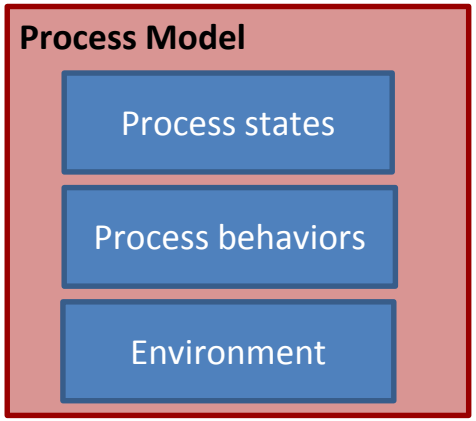
NEW HUMAN ENGINEERING PROCESS

- Identify UCAs
  - UCA-1: Driver does not brake when auto-parking and computer doesn't react to an obstacle
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify flaws in Process Mode dates
- Identify unsafe Control Action Se



NEW HUMAN ENGINEERING PROCESS

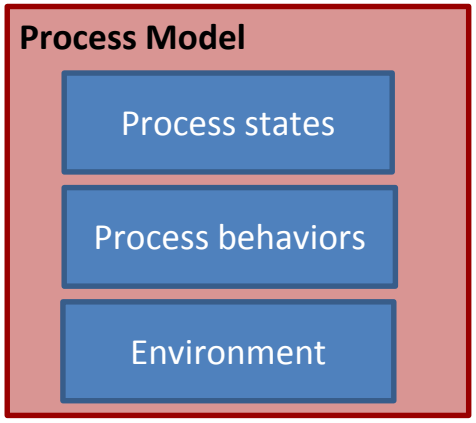
- Identify UCAs
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify unsafe decisions (Control Action Selections)
- Identify inadequate Process Model Updates



Type of PM flaw	Examples
Incorrect beliefs about process state (including modes)	
Incorrect beliefs about process behaviors	
Incorrect beliefs about environment	

NEW HUMAN ENGINEERING PROCESS

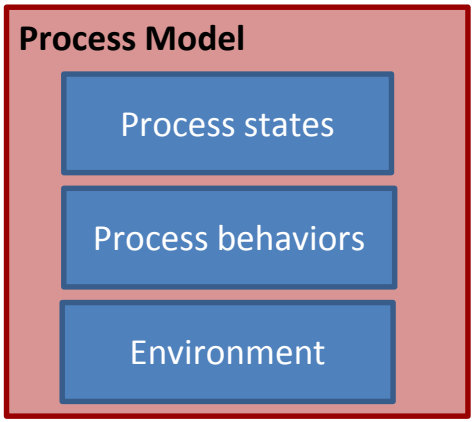
- Identify UCAs
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify unsafe decisions (Control Action Selections)
- Identify inadequate Process Model Updates



Type of PM flaw	Examples
Incorrect beliefs about process state (including modes)	Driver thinks APA is enabled when APA is really disabled
Incorrect beliefs about process behaviors	Driver thinks APA is reacting properly and will brake automatically
Incorrect beliefs about environment	Driver thinks there is no obstacle when there is one Driver knows there is an obstacle but doesn't know it's on a collision path

NEW HUMAN ENGINEERING PROCESS

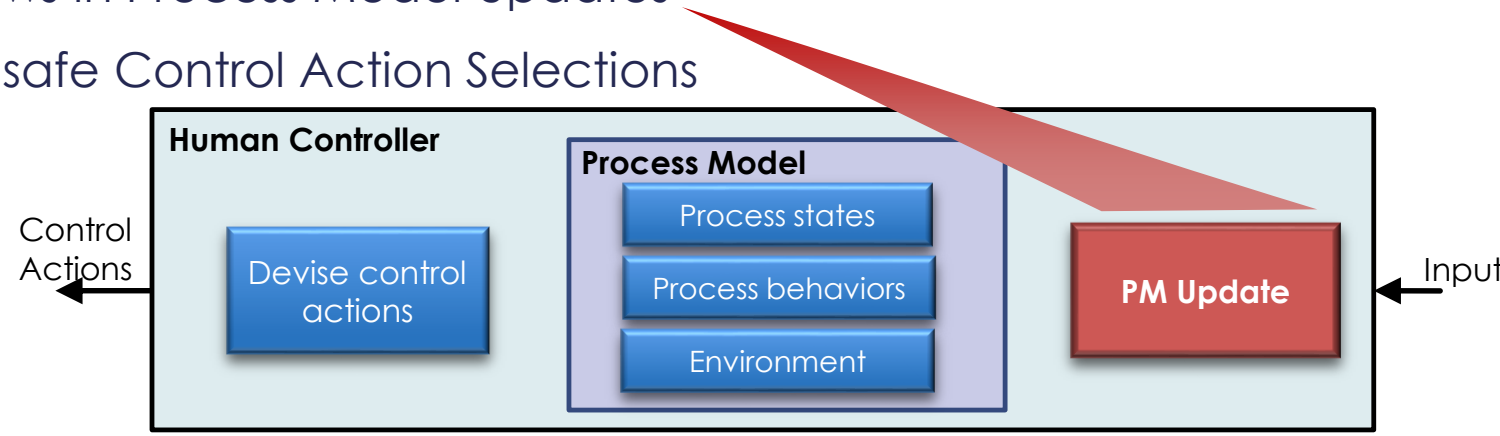
- Identifying Process Model Flaws
  - Incorrect beliefs about process state
    - Consider modes, automatic mode changes, phases of operation
  - Incorrect beliefs about Process behaviors
    - Consider perceived effect of control actions, behavior in other modes, past experiences, etc.
  - Incorrect beliefs about environment
    - Consider changes to environment, similar past environments, etc.
  - "Known Unknown" and "Unknown Unknowns"
    - Believes there is a pedestrian in the way
    - Believes there is no pedestrian
    - Believes they don't know if there is a pedestrian (may trigger a check)
    - Consider inadequate feedback, driver may know something changed but doesn't know the new state, etc.



Providing guidance to ensure coverage

NEW HUMAN ENGINEERING PROCESS

- Identify UCAs
  - UCA-1: Driver does not brake when auto-parking and computer doesn't react to an obstacle
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe Control Action Selections

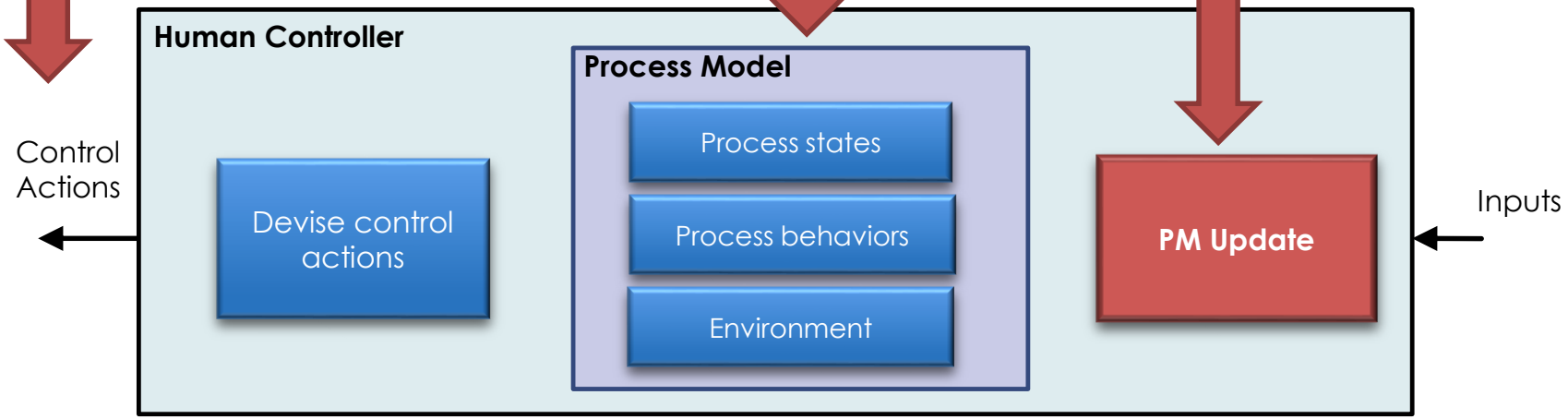


NEW HUMAN ENGINEERING PROCESS

Driver does not brake when auto-parking and computer doesn't react to an obstacle (UCA-1)

Driver thinks APA is enabled when APA is really disabled (PM-1)

APA automatically disabled itself but driver didn't notice the change

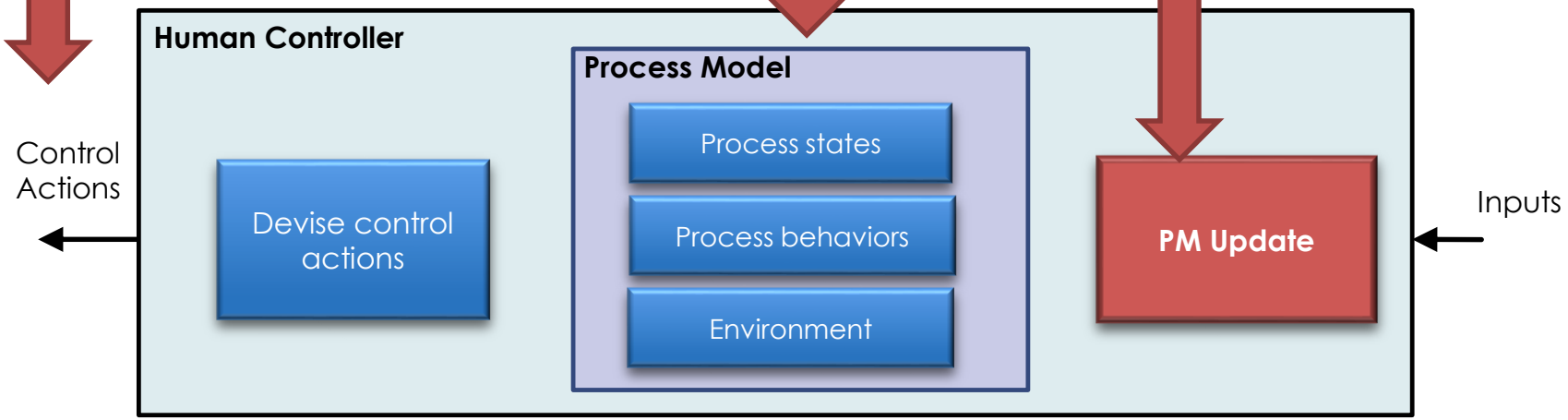


NEW HUMAN ENGINEERING PROCESS

Driver does not brake when auto-parking and computer doesn't react to an obstacle (UCA-1)

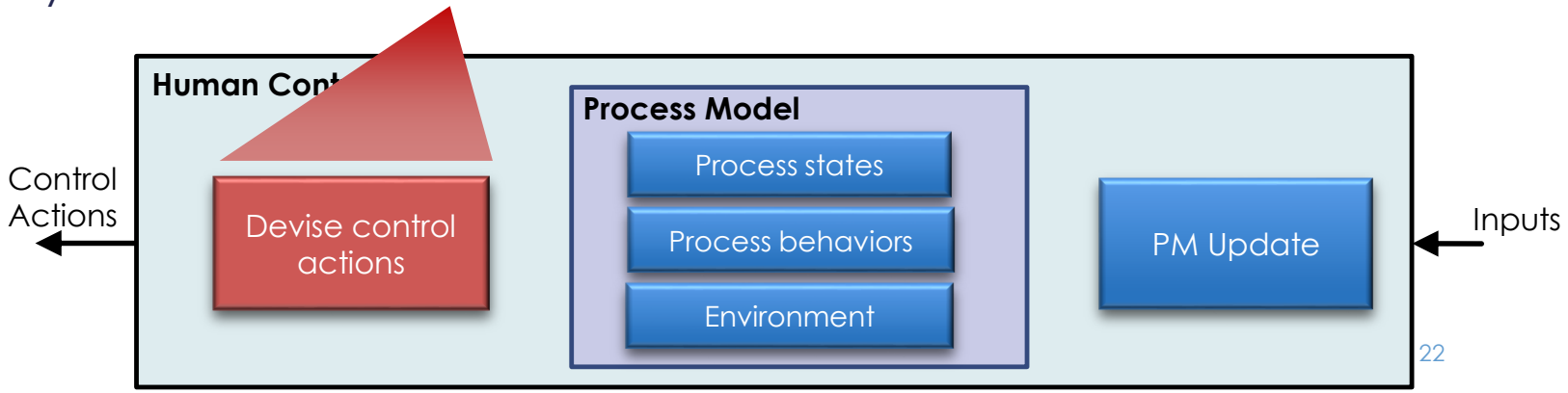
Driver thinks APA is enabled when APA is really disabled (PM-1)

APA automatically disabled itself, driver noticed the change but didn't understand it



NEW HUMAN ENGINEERING PROCESS

- Identify UCAs
  - UCA-1: Driver does not brake for an obstacle when computer does not react appropriately to the obstacle
- Identify Process Model variables
  - PM-1: APA reacting appropriately/inappropriately
  - PM-2: Obstacle on collision path
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe Control Action Selections

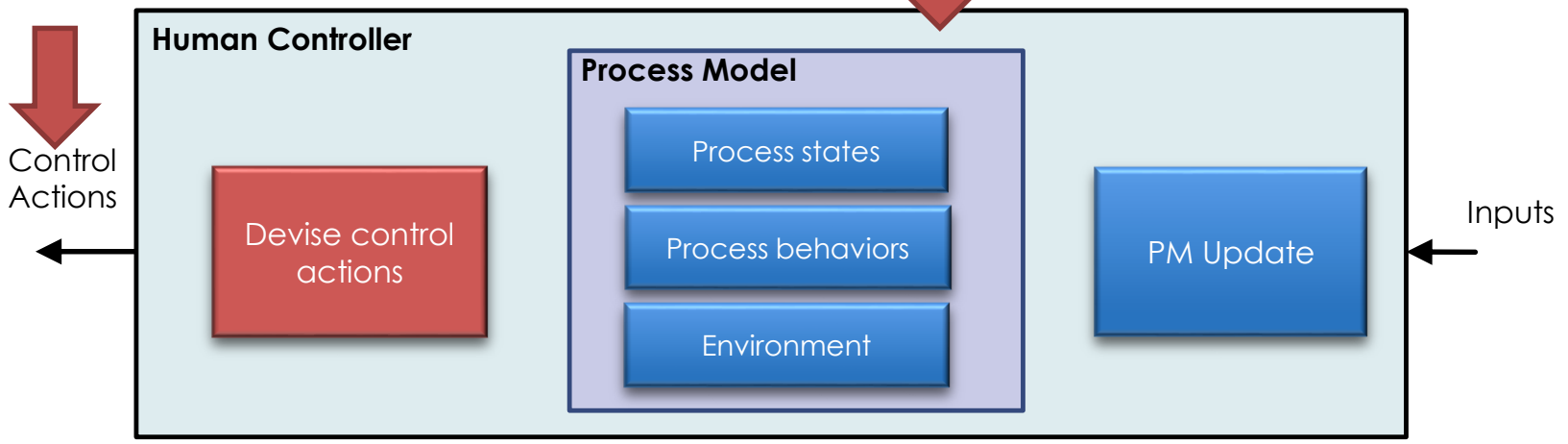


NEW HUMAN ENGINEERING PROCESS

- Identify unsafe Control Action Selections

Driver does not intervene to brake (UCA-1)

Driver knows APA is on
Driver knows APA hasn't reacted yet
Driver knows there is an obstacle in the way



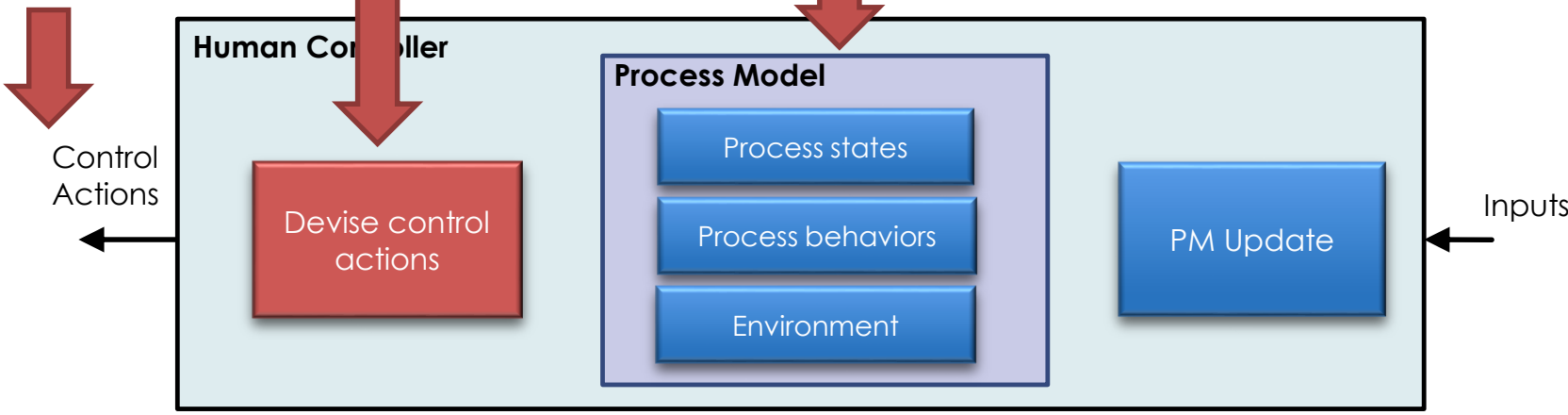
NEW HUMAN ENGINEERING PROCESS

- Identify unsafe Control Action Selections

Driver does not intervene to brake (UCA-1)

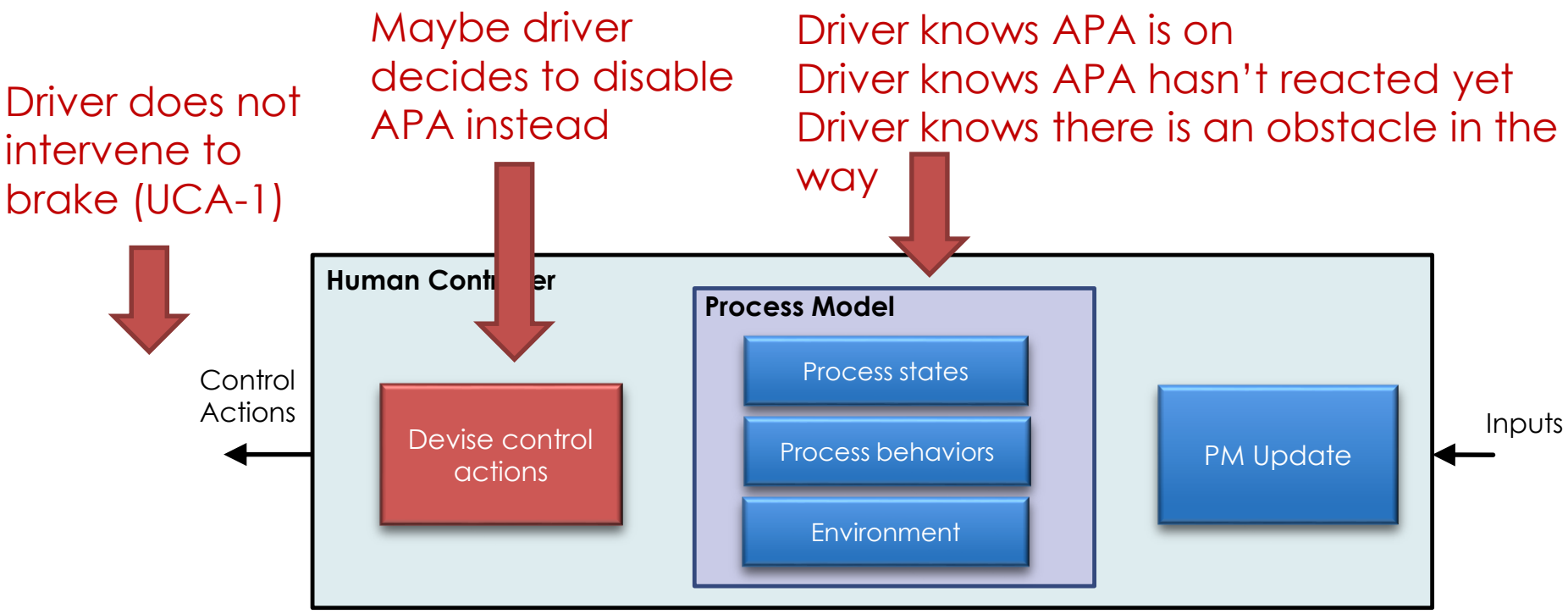
Maybe driver does not know they can control brake with APA on

Driver knows APA is on
Driver knows APA hasn't reacted yet
Driver knows there is an obstacle in the way



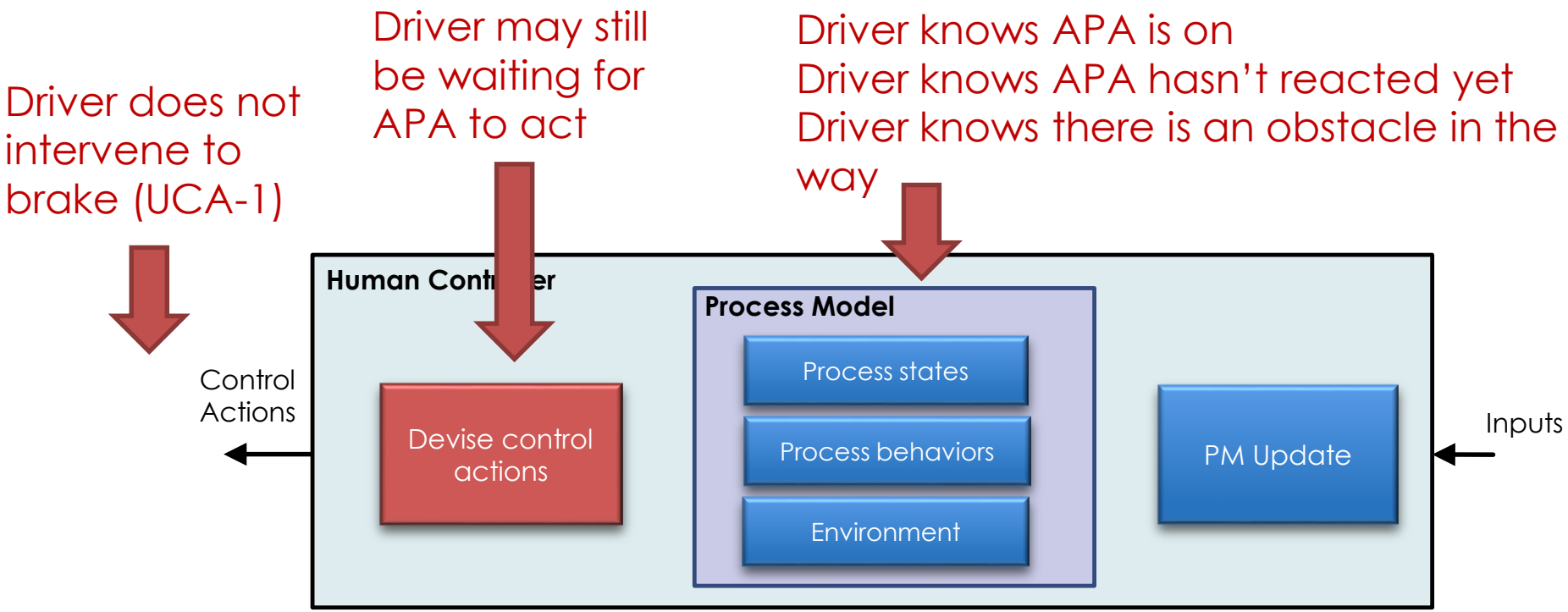
NEW HUMAN ENGINEERING PROCESS

- Identify unsafe Control Action Selections



NEW HUMAN ENGINEERING PROCESS

- Identify unsafe Control Action Selections

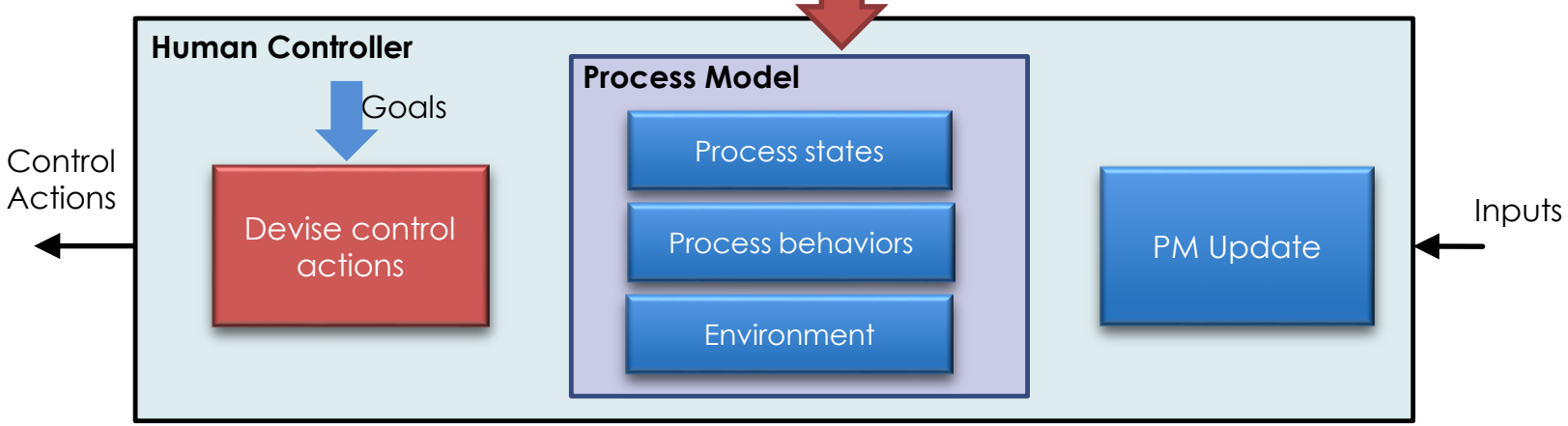


NEW HUMAN ENGINEERING PROCESS

- Identify unsafe Control Action Selections
  - Consider whether the driver is aware they can control X
  - Consider alternative driver controls/actions
  - Consider other driver goals

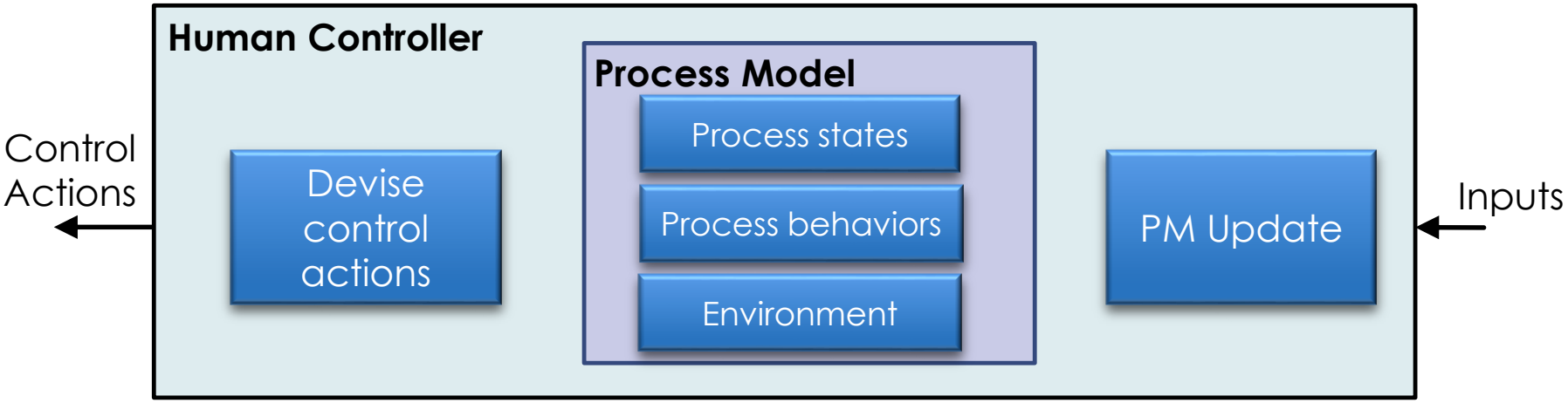
Driver knows APA is on
Driver knows APA hasn't reacted yet
Driver knows there is an obstacle in the way

Driver does not intervene to brake (UCA-1)



NEW HUMAN ENGINEERING APPROACH

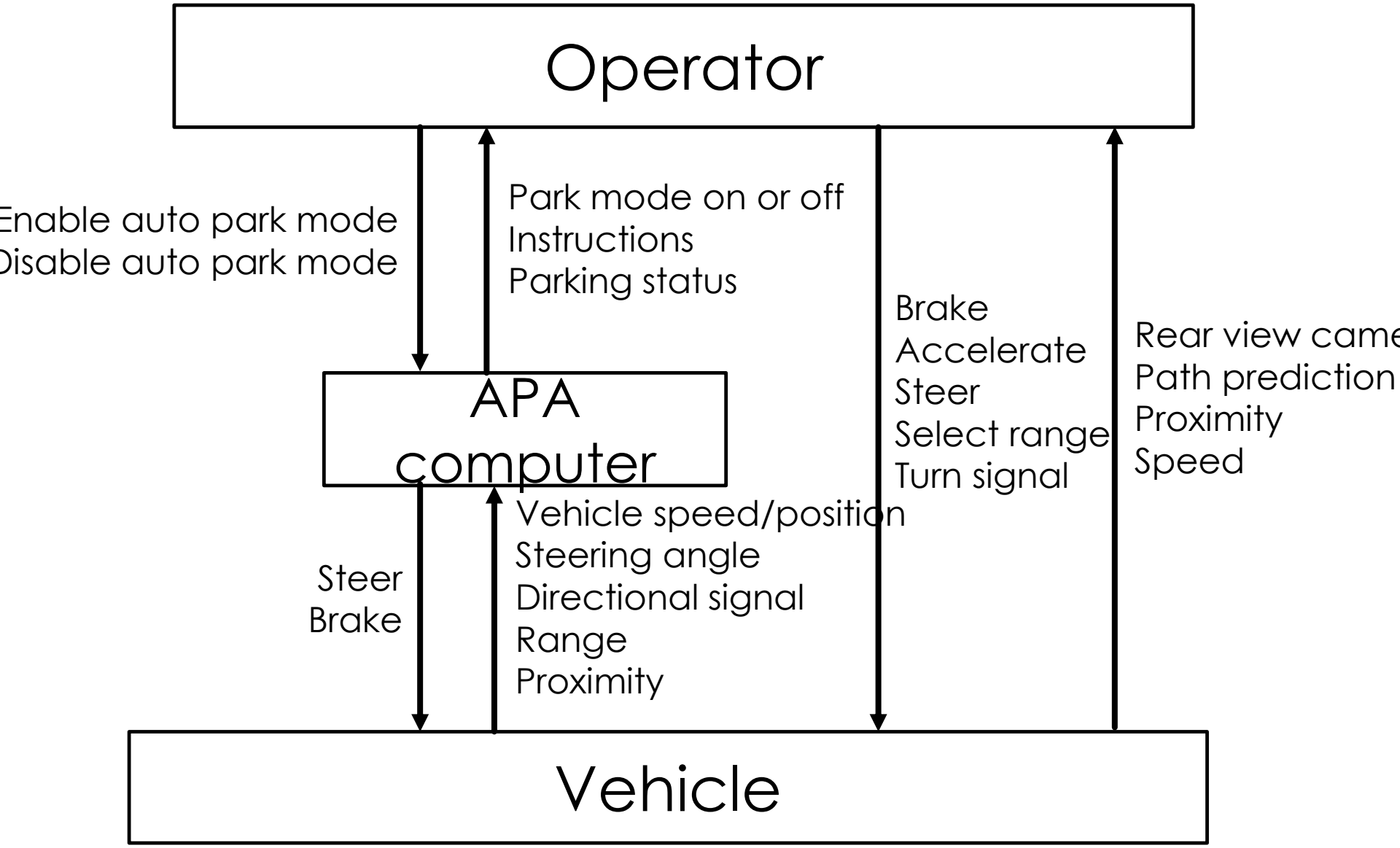
- Identify UCAs
- Identify Process Model variables
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe decisions (Control Action Selections)



Applying the new process to Automated Parking test cases

Presented by Megan France

INITIAL CONTROL STRUCTURE



AUTOMATED PARKING TEST CASES

Summary of features of each system considered for this analysis.

	Manual Operation	Level 1 "Driver Assistance"	Level 2a "Partial Automation"	Level 2b "Partial Automation"	Level 3 "Conditional Automation"
Steering	-	✓	✓	✓	✓
Braking	-	-	✓	✓	✓
Shifting and Acceleration	-	-	-	✓	✓
Object/Event Detection & Response	-	-	-	-	✓

*System numbering is consistent with SAE definitions for levels of automation; "a" and "b" indicate different implementations which are classified within the same SAE level.

UNSAFE CONTROL ACTIONS OVERVIEW

Number of UCAs identified for the driver for steering, braking, shifting, and accelerating.

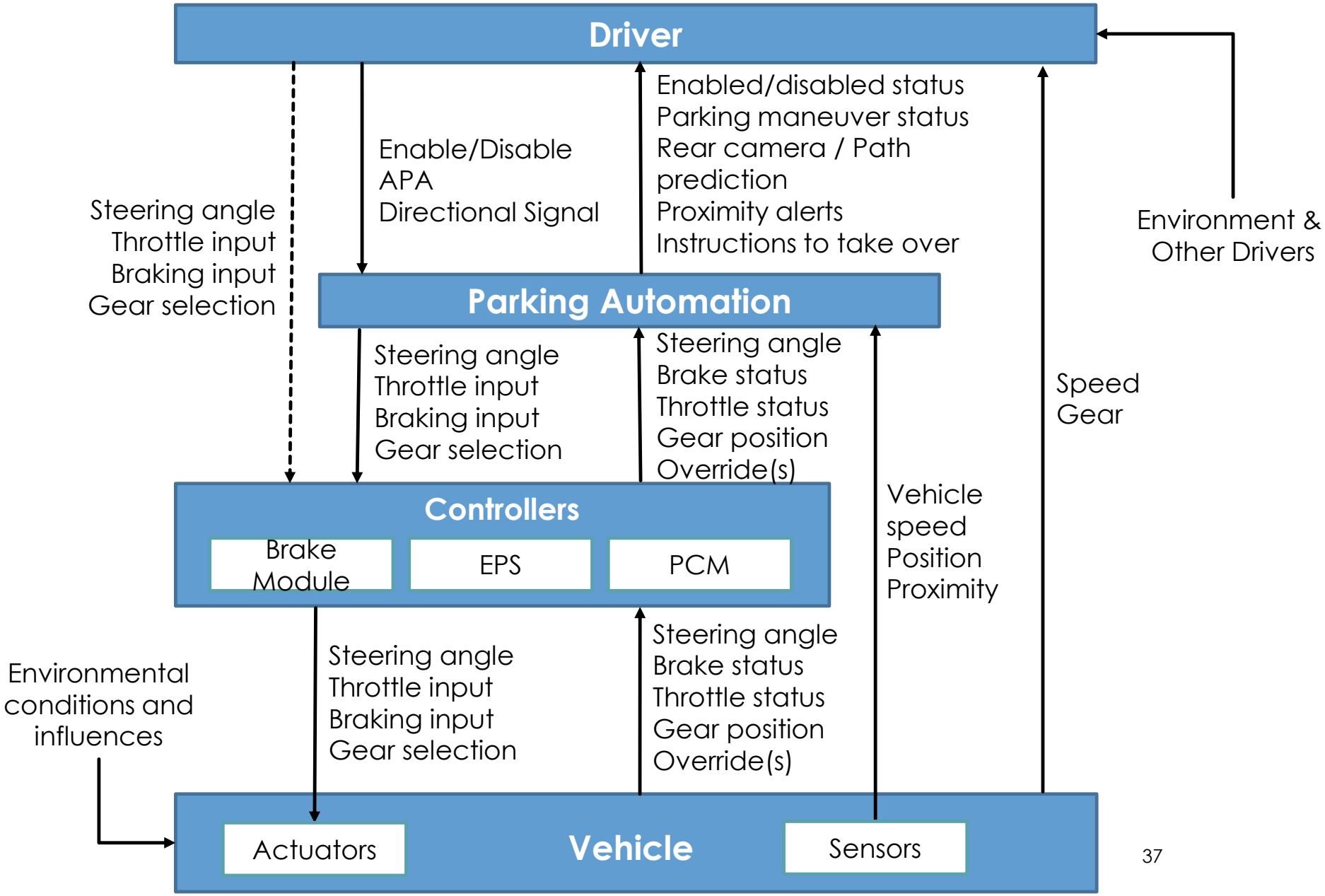
Note: number of UCAs does not indicate how safe each system is!

	Level 1 "Driver Assistance"	Level 2a "Partial Automation"	Level 2b "Partial Automation"	Level 3 "Conditional Automation"
Driver UCAs	26	24	20	17
Computer UCAs	5	12	25	25
Total UCAs	*31*	*36*	*45*	*42*

EXAMPLE SYSTEM OVERVIEW

- Automation is responsible for steering, braking, shifting & acceleration
  - Does not actively monitor the environment
- Driver is responsible for monitoring the environment and responding to unexpected events
  - Driver may override the actions of the automation by braking, steering, etc.
- Key assumption: while automation is on…
  - Driver can brake for <2 seconds in contributory mode
  - Braking >2s will shut off the automation

DETAILED SAFETY CONTROL STRUCTURE



DRIVER UNSAFE CONTROL ACTIONS

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing or Order	Stopped Too Soon or Applied Too Long
Braking	**Driver does not brake when the computer does not react appropriately to an obstacle [UCA-1].**	Driver provides insufficient brake command when computer does not react appropriately to the obstacle. Driver provides too much brake when doing so puts other traffic on collision course or causes passenger injury. Driver brakes for long enough to disable automation when doing so puts the vehicle on a collision path.	Driver waits too long to brake after the automation does not react appropriately to an obstacle.	Driver continues override braking for too long and disables automation when doing so puts the vehicle on a collision path. Driver does not brake for long enough to avoid collision when automation is not reacting appropriately to an obstacle.

DRIVER UNSAFE CONTROL ACTIONS

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing or Order	Stopped Too Soon or Applied Too Long
Steering	Driver does not steer when auto park is disabled. Driver does not steer when the vehicle is on a collision path.	Driver attempts to steer when wheel is turning quickly. Driver provides steering override that puts vehicle on a collision path.	Driver takes control of the wheel too late after disabling auto park.	-
Accelerating	Driver does not provide accelerate command when necessary to override the automation and avoid an approaching vehicle. **Driver does not resume accelerating after braking long enough to disable automation [UCA-2].**	Driver provides accelerate command to override automation when doing so puts the vehicle on a collision path. Driver accelerates too quickly, subjecting driver to extreme forces.	Driver accelerates before shifting into the proper gear, putting the vehicle on a collision path. Driver provides accelerate command to override automation too late to avoid obstacles.	Driver continues accelerating too long, putting the vehicle is on a collision path. Driver does not accelerate long enough to clear an obstacle safely.

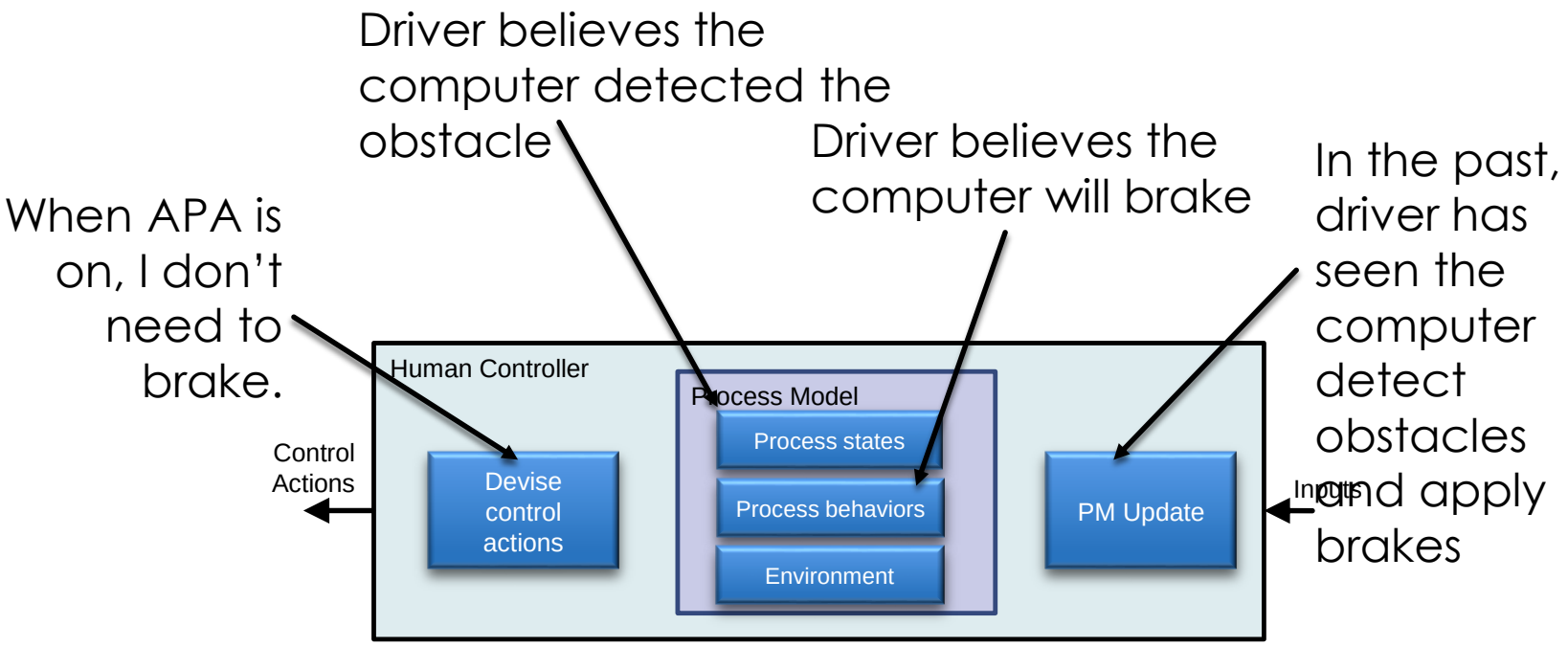
CAUSAL SCENARIOS USING NEW EXTENSION

UCA-1: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.

Scenario 1-1: 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-1: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.



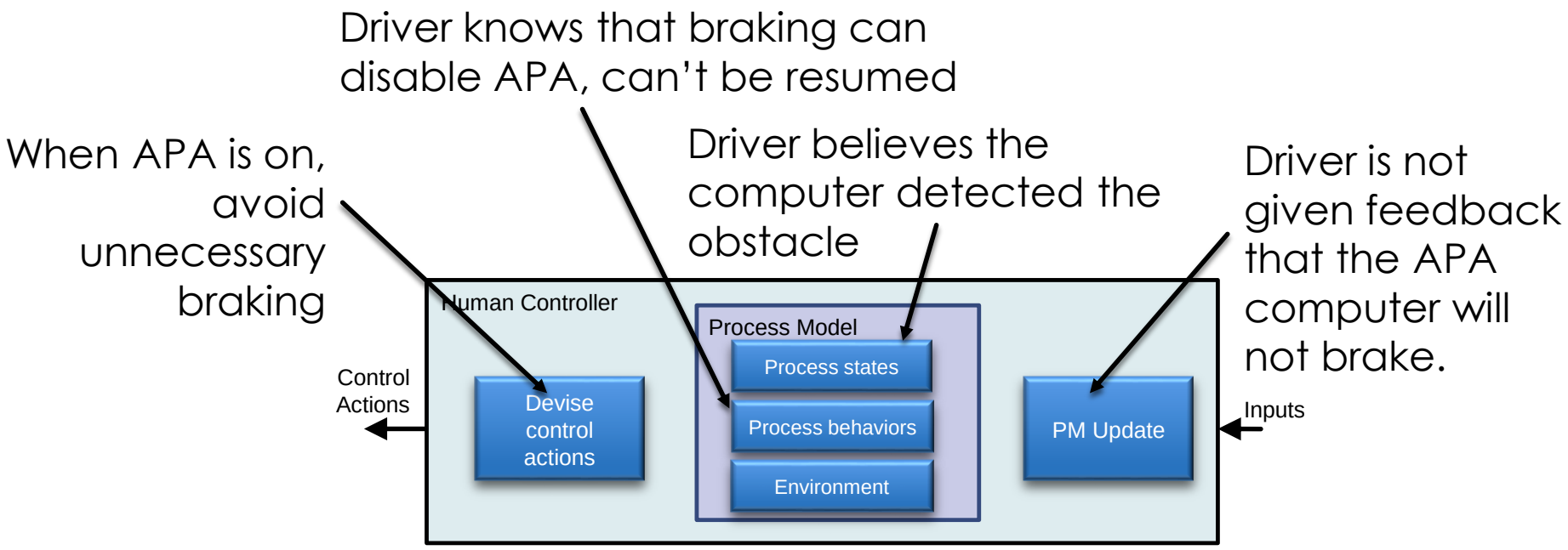
CAUSAL SCENARIOS USING NEW EXTENSION

UCA-1: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.

Scenario 1-2: The driver does not brake for an obstacle because the driver incorrectly believes that the computer detects and will brake for the obstacle ahead. She is concerned that if she brakes unnecessarily, she will cancel the automation and need to restart the parking maneuver. She does not receive any feedback that the computer is unaware of the obstacle.

CAUSAL SCENARIOS USING NEW EXTENSION

UCA-1: Driver does not brake for an obstacle when the APA computer does not react appropriately to the obstacle.



STARTING POINTS FOR SOLUTIONS

Scenario details:

- The driver is concerned that braking would cancel the automation and require her to restart the parking maneuver.
- The driver incorrectly believes that the computer detects and will brake for the obstacle ahead. She does not receive any feedback that the computer is unaware of the obstacle.

Some possible solutions:

- Make it easy to resume auto parking with minimal steps for the driver.
- Provide feedback about automation's status (obstacles detected or not) and next actions in the form of a prominent display.
- Consider whether it is appropriate to require driver monitoring of the system or whether automation should be designed to handle such events.

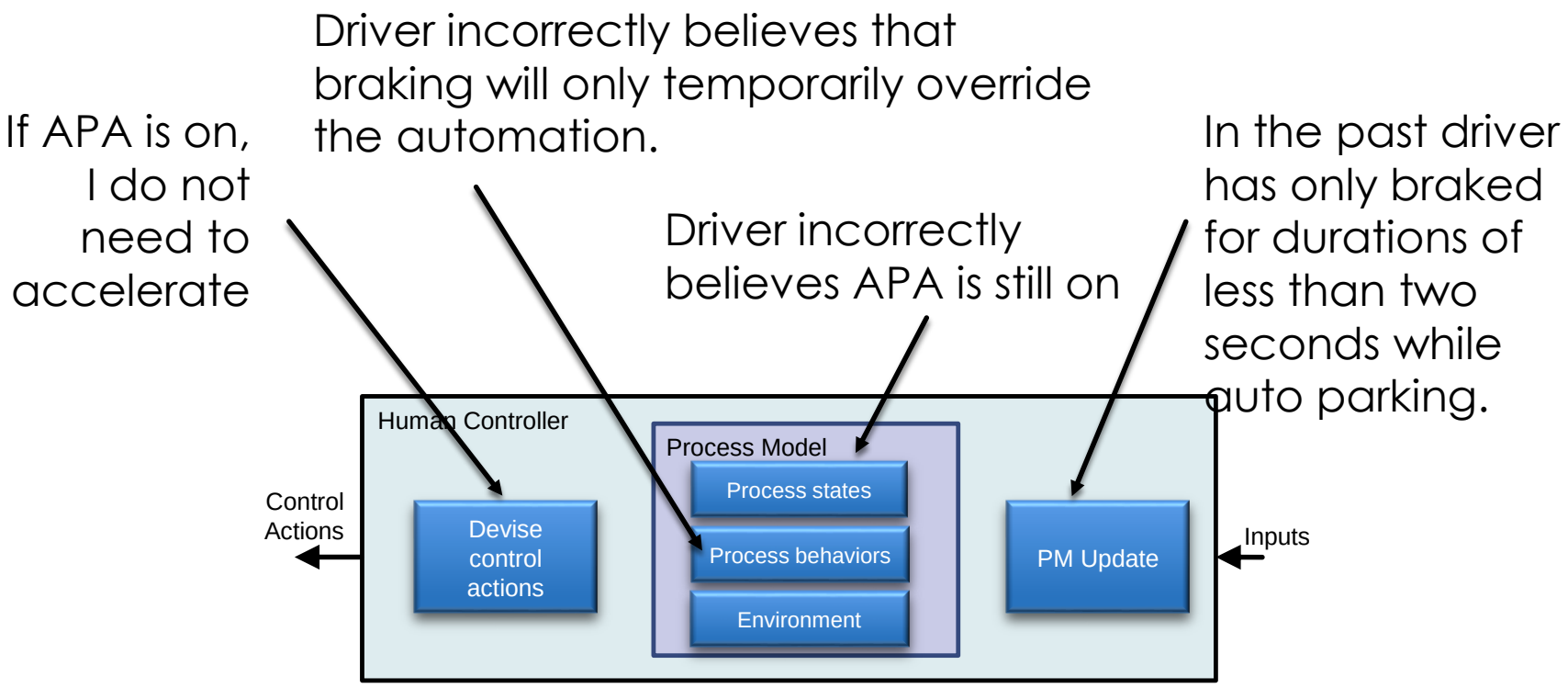
CAUSAL SCENARIOS USING NEW EXTENSION

UCA-2: Driver does not resume accelerating after braking long enough to disable automation.

Scenario 2-1: The driver does not resume accelerating after braking long enough to disable the automation because the driver incorrectly believes that APA is on. She incorrectly believes that braking will not disable the automation because in the past, she has not applied the brakes for long enough to trigger automation to shut off. The driver is not given feedback that automation is about to be disabled.

CAUSAL SCENARIOS USING NEW EXTENSION

UCA-2: Driver does not resume accelerating after braking long enough to disable automation.



STARTING POINTS FOR SOLUTIONS

Scenario details:

- Driver expected to cause a temporary override.
- Driver incorrectly believes that braking will not disable the automation, since in the past she has only braked for durations of less than two seconds while auto parking.

Some possible solutions:

- Provide explicit feedback when APA is disabled during a driver override – warn the driver to monitor the environment and continue manual driving.
- Avoid situations where the same control is used for multiple control actions – do not use brake pedal for both contributory braking and APA shutoffs.

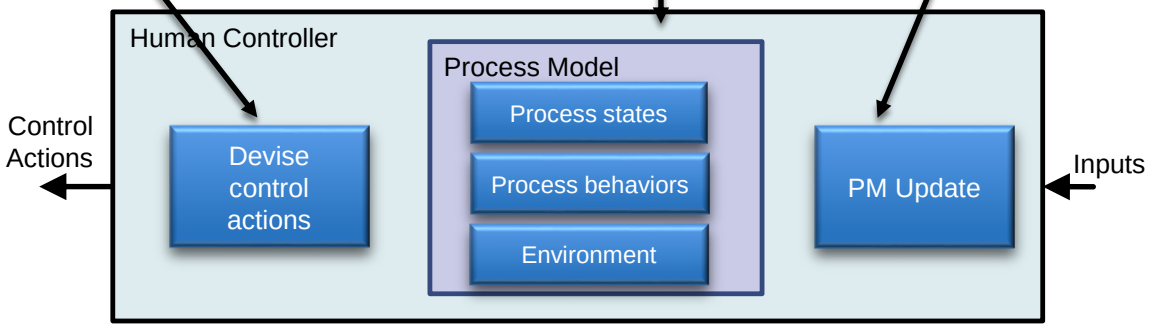
SUMMARY OF NEW MODEL BENEFITS

The new model scenarios incorporate additional context to explain ***why*** the driver may have certain beliefs and how those beliefs influence the driver's control actions.

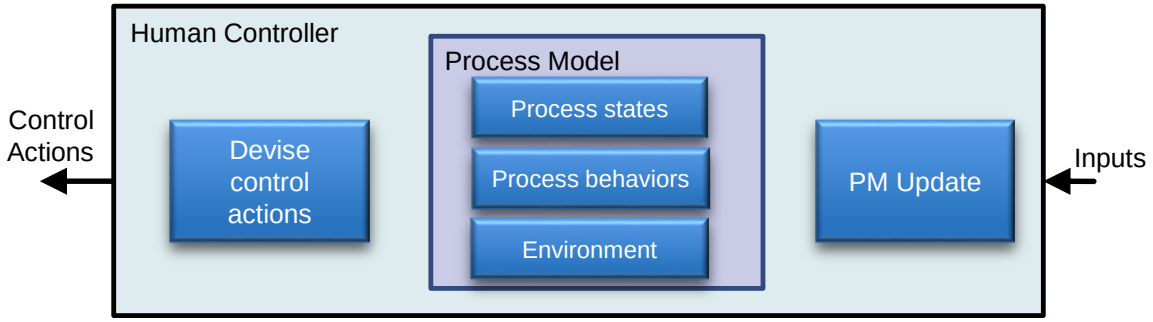
Captures goals and prioritization; how UCAs are selected based on PM

Captures specific types of flaws which may call for different solutions

Captures influence of past experience and expectations on processing of inputs



CONCLUSIONS



New human engineering extension strengths:

- Provides additional guidance for human process model flaws
- Can help suggest *engineering solutions*, not just human problems
- Can be used earlier in design process than detailed simulations or prototypes