STPA Applied to Automotive Automated Parking Assist

Massachusetts Institute of Technology

John Thomas

Megan France

APA Collaboration with General Motors

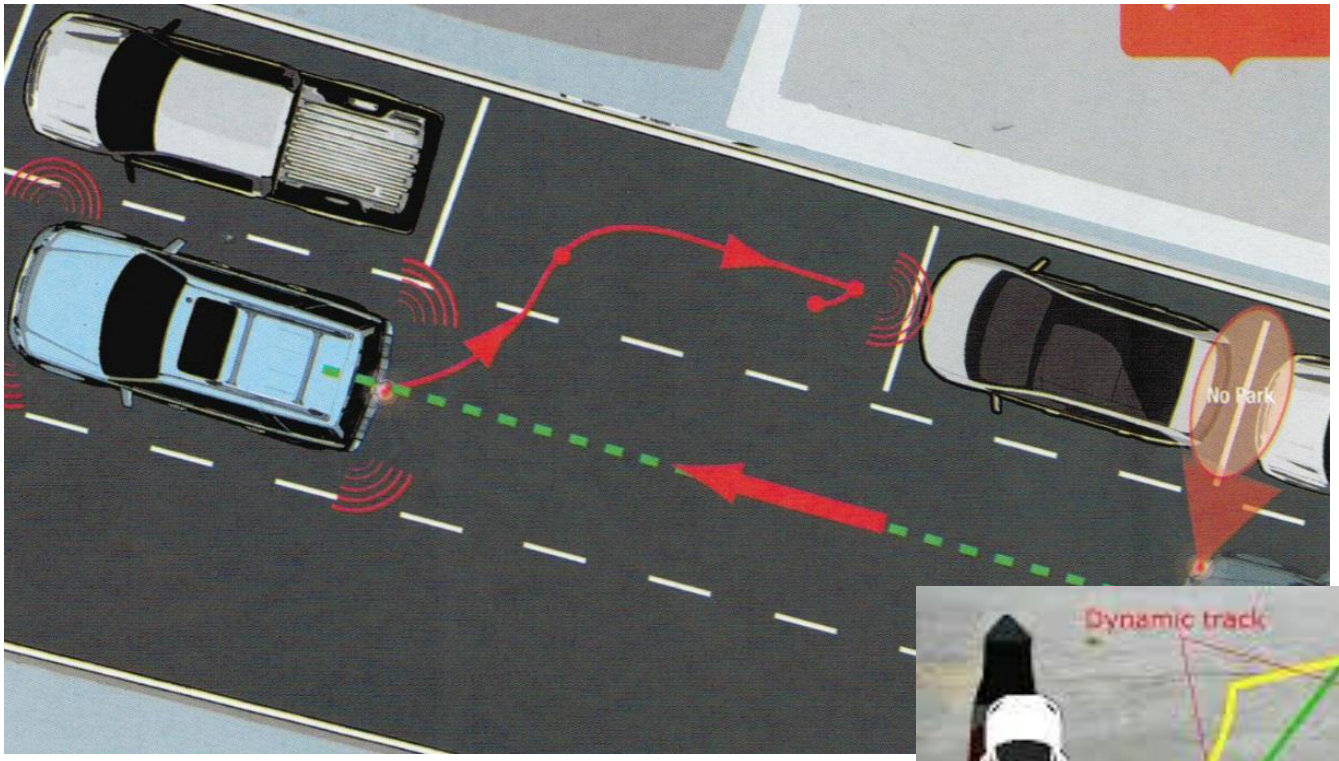
Charles A. Green

Mark A. Vernacchia

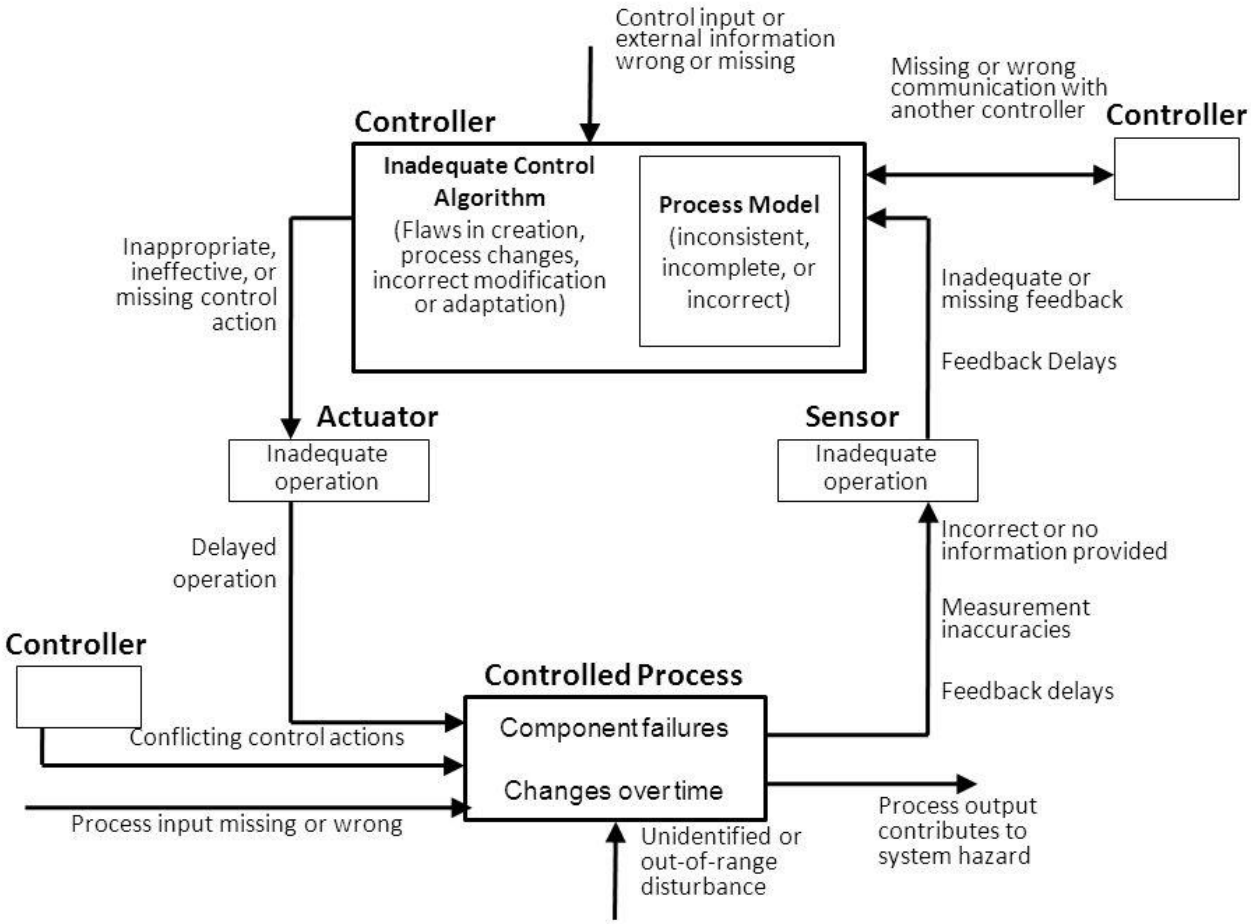
Padma Sundaram

Joseph D'Ambrosio

AUTOMATED PARKING ASSIST

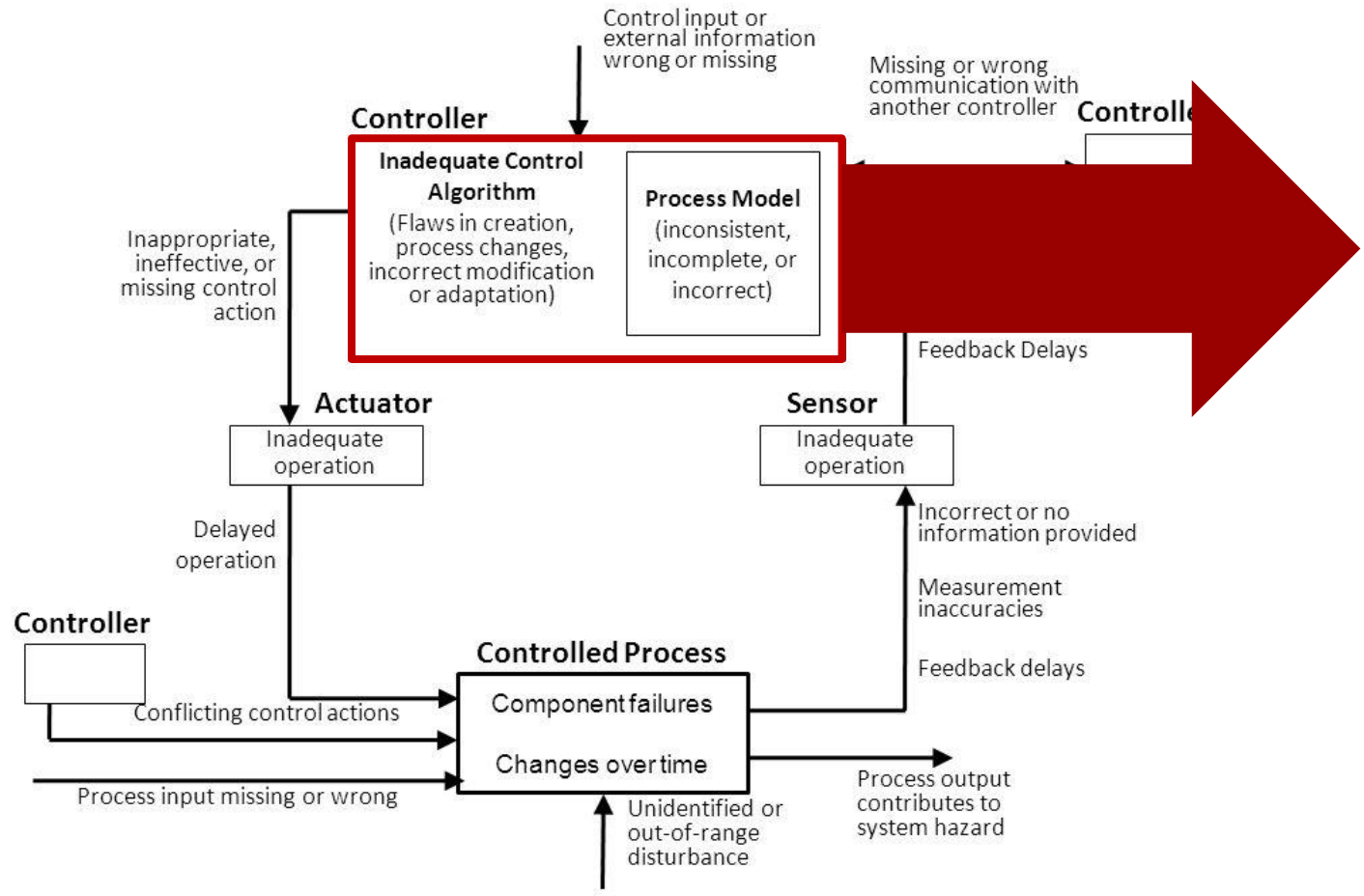


CONTROL LOOP



Leveson, 2012

CONTROL LOOP



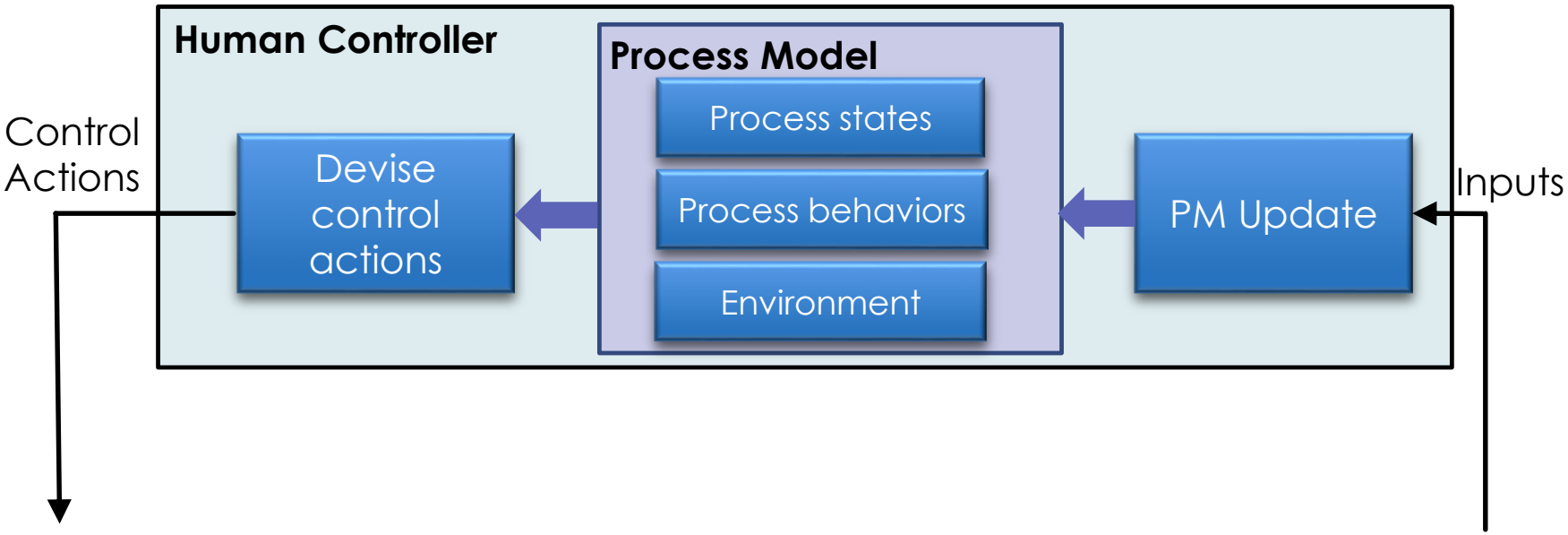
Existing systems-theoretic controller model

- Generic
- Not specific to humans

Leveson, 2012

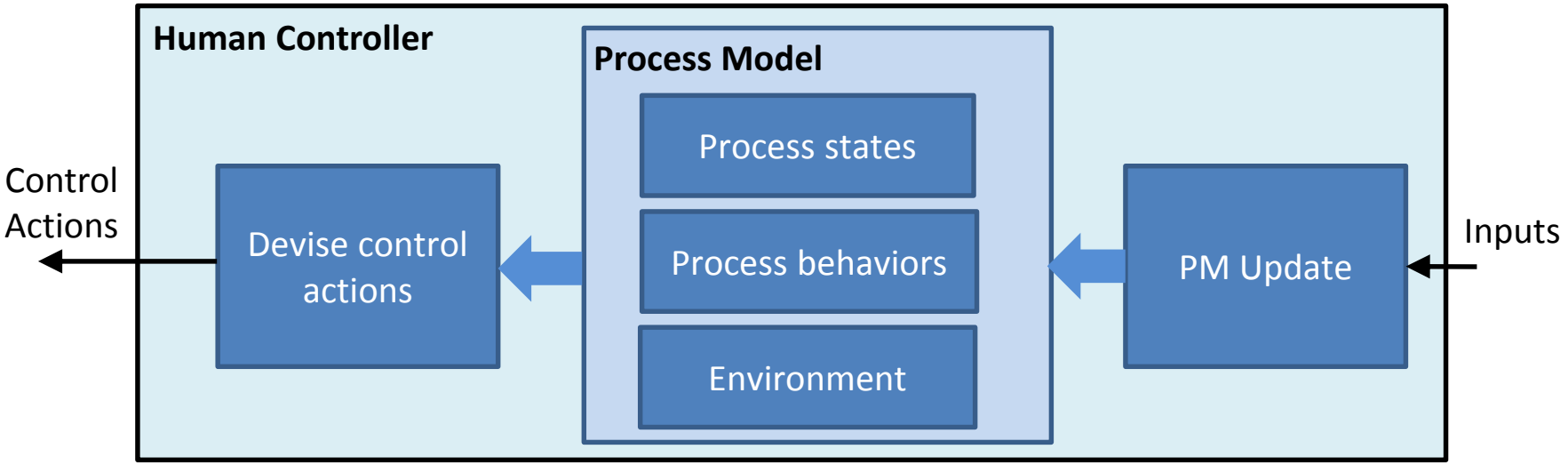
HUMAN CONTROL MODEL

HUMAN CONTROL MODEL



NEW PROCESS

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

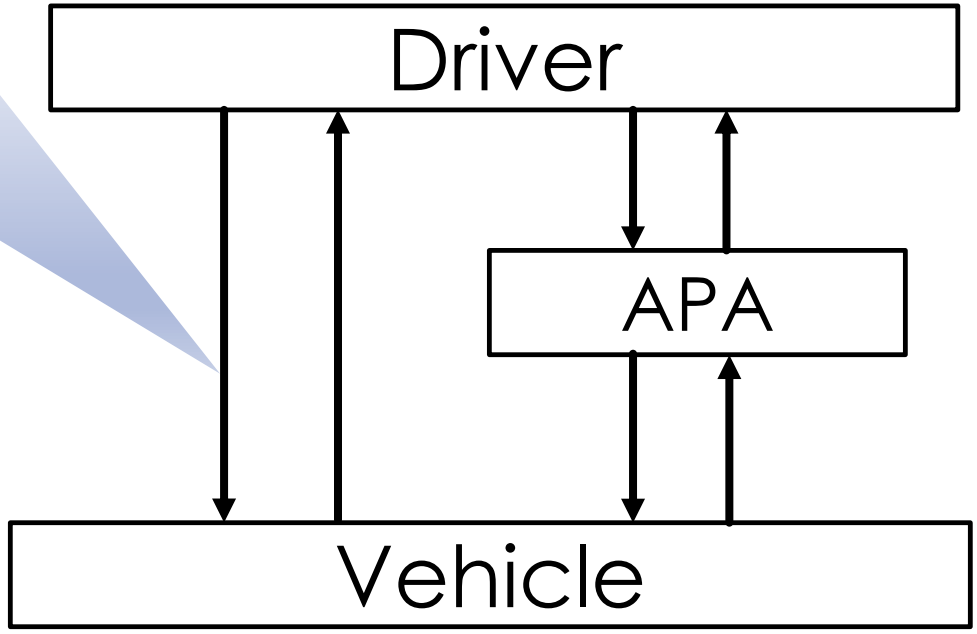


NEW PROCESS

- 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 PROCESS

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

- Identify Process Model variables
  -
  -
  -
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe Control Action Selections

NEW PROCESS

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

- Identify Process Model variables
  -
  -
  -
- Identify Process Model Flaws
- Identify flaws in Process Model Updates
- Identify unsafe Control Action Selections

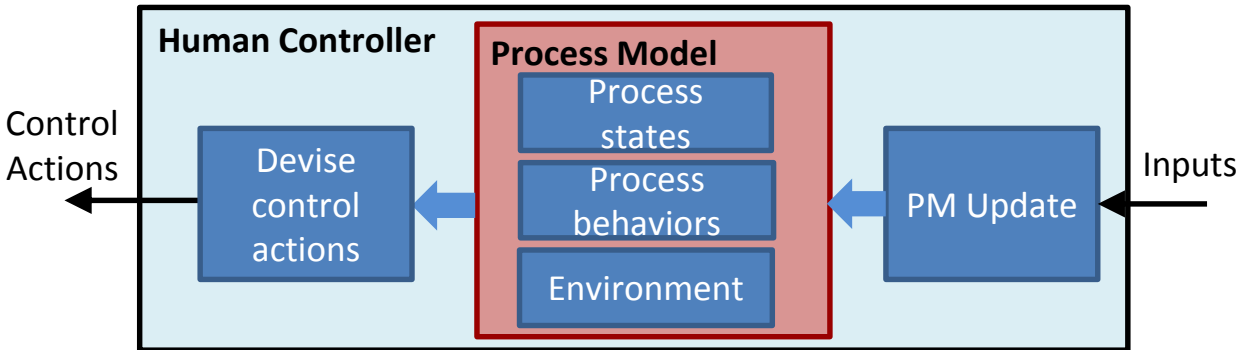
NEW PROCESS

- 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

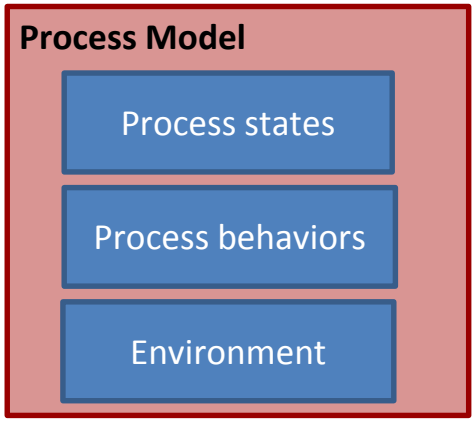
NEW PROCESS

- 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 PROCESS

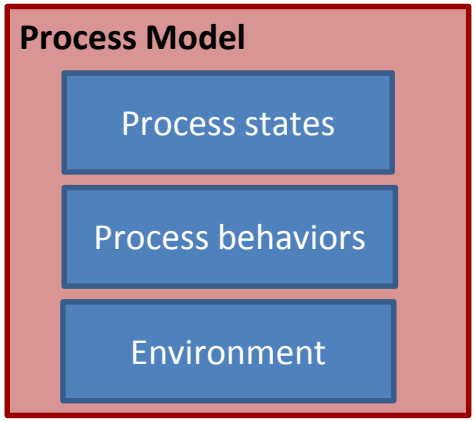
- Identify UCAs
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify unsafe decisions (Control Action Selections)
- Identify inadequate Process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



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

NEW PROCESS

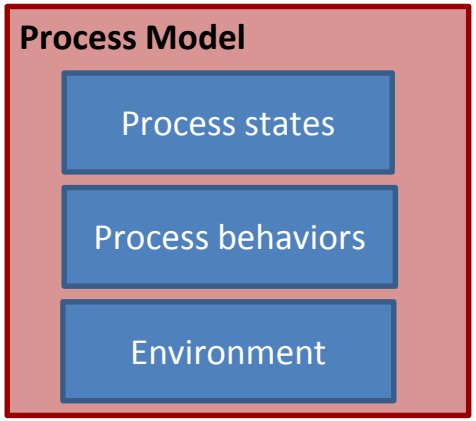
- Identify UCAs
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify unsafe decisions (Control Action Selections)
- Identify inadequate Process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



Type of PM flaw	Examples
Incorrect beliefs about process state (including modes)	Driver thinks APA is enabled when APA is really disabled (PM-1)
Incorrect beliefs about process behaviors	
Incorrect beliefs about environment	

NEW PROCESS

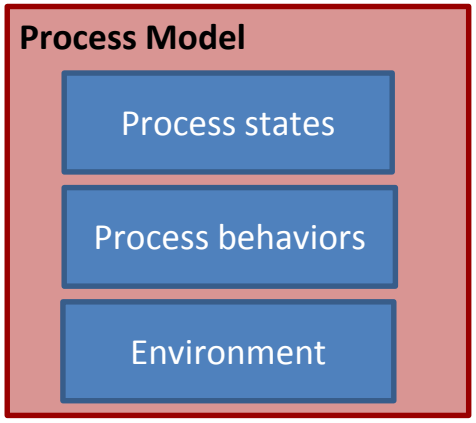
- Identify UCAs
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify unsafe decisions (Control Action Selections)
- Identify inadequate Process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

NEW PROCESS

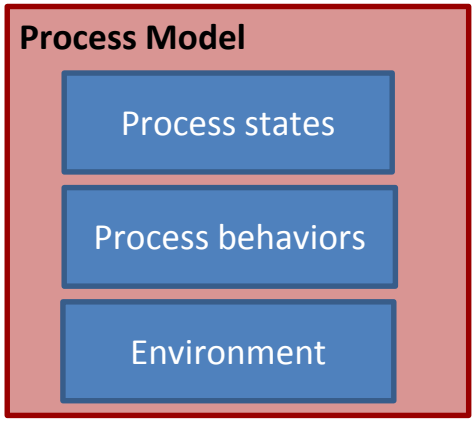
- Identify UCAs
- Identify Process Model variables
  - PM-1: APA is enabled/disabled
  - PM-2: APA computer reacting appropriately/inappropriately
  - PM-3: Obstacle on collision path
- Identify Process Model Flaws
- Identify unsafe decisions (Control Action Selections)
- Identify inadequate Process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

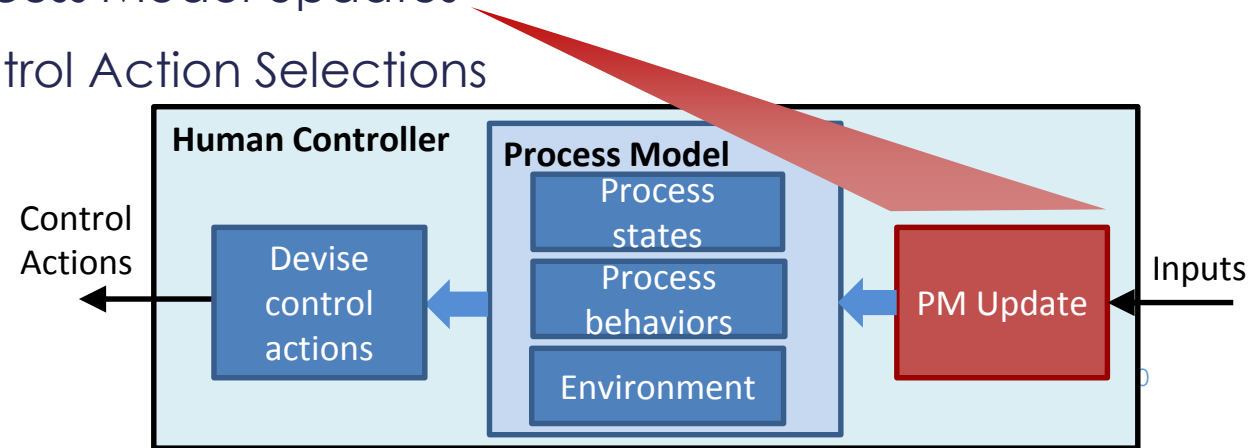
- Identifying Process Model Flaws
  - Incorrect beliefs about process state
    - Automatic mode changes
    - Previous commands ignored
    - Phases of operation
  - Incorrect beliefs about Process behaviors
    - Consider perceived effect of control actions, behavior in other modes, past experiences, 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 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

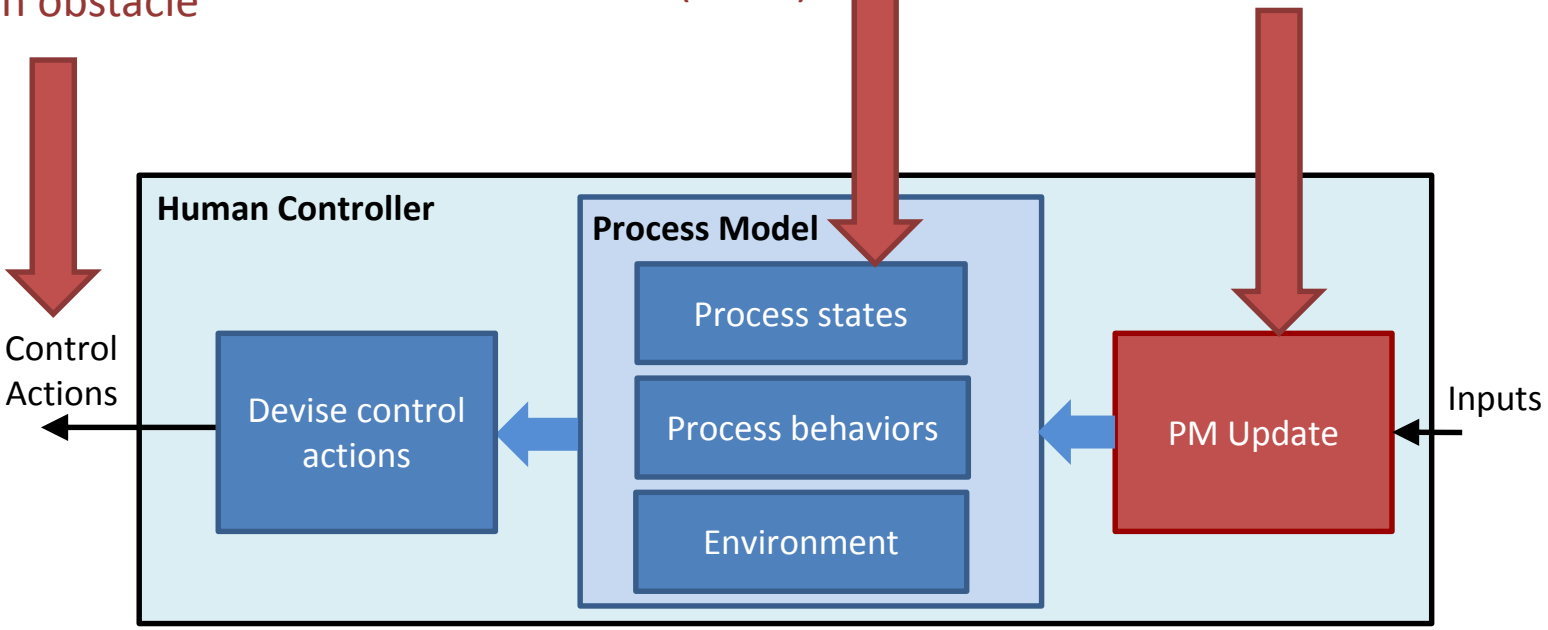


NEW PROCESS

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)

Consider:
1. Automatic mode changes
2. Previous cmds ignored
3. Phases of operation
4. Etc.

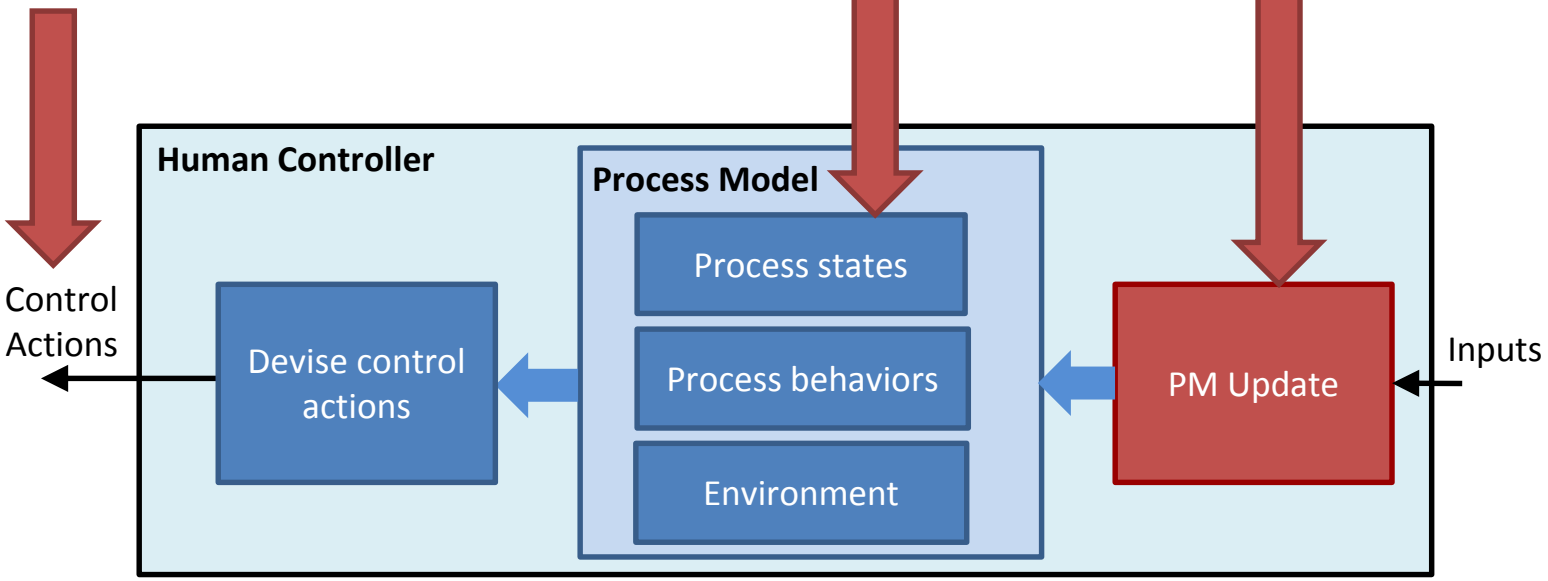


NEW PROCESS

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

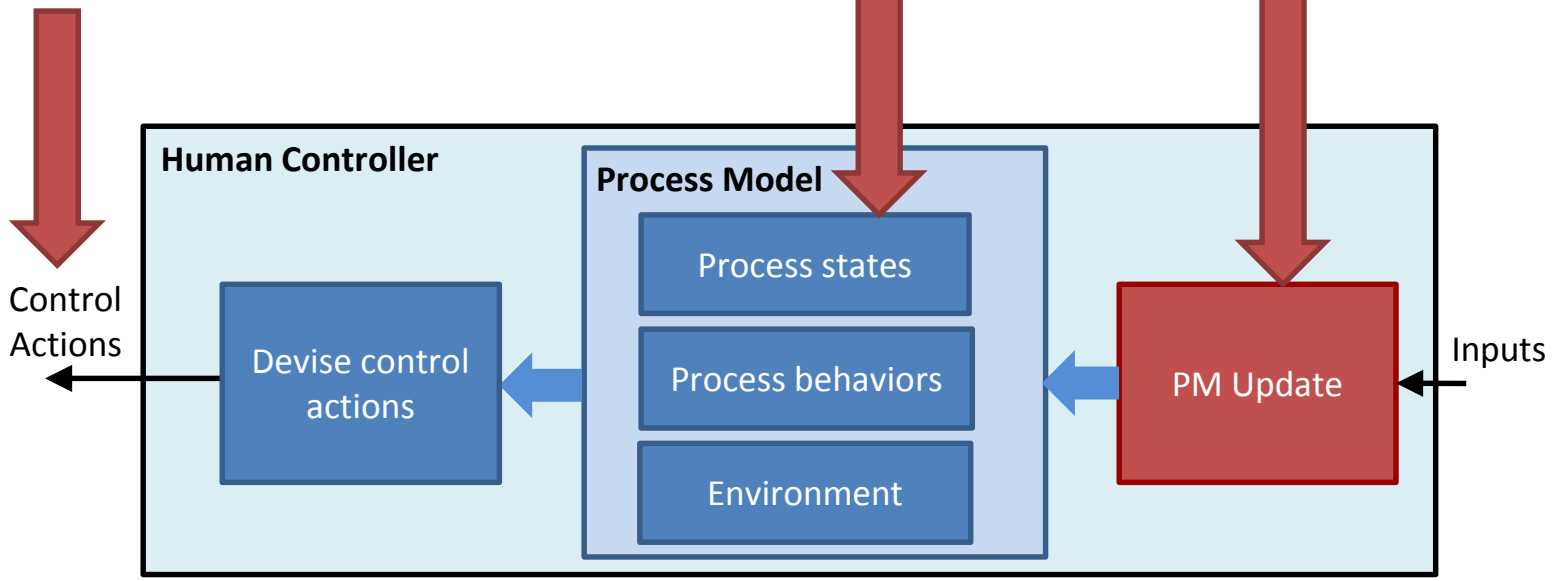


NEW PROCESS

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

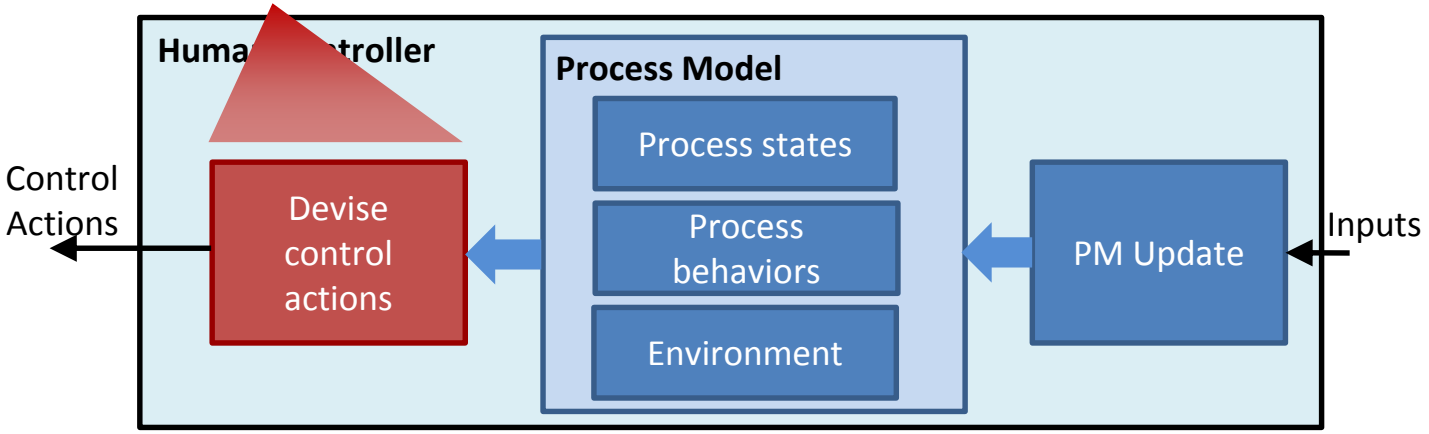
Driver thinks APA is enabled when APA is really disabled (PM-1)

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



NEW 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

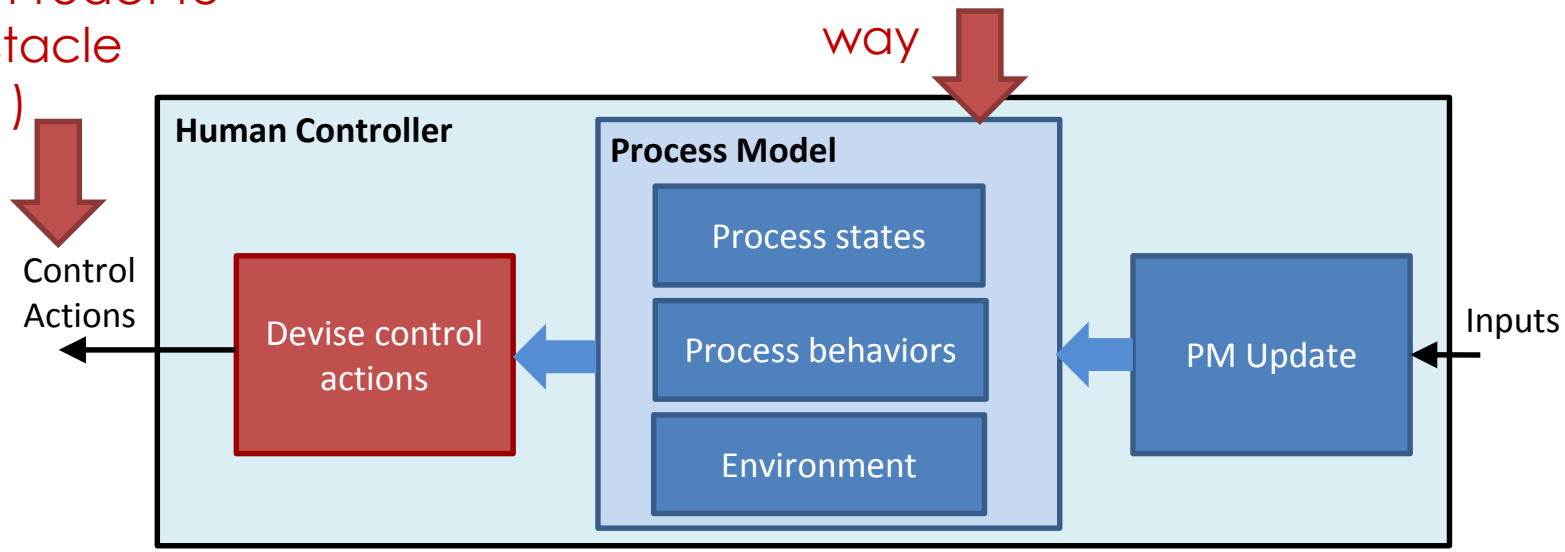


NEW PROCESS

- Identify unsafe Control Action Selections

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

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



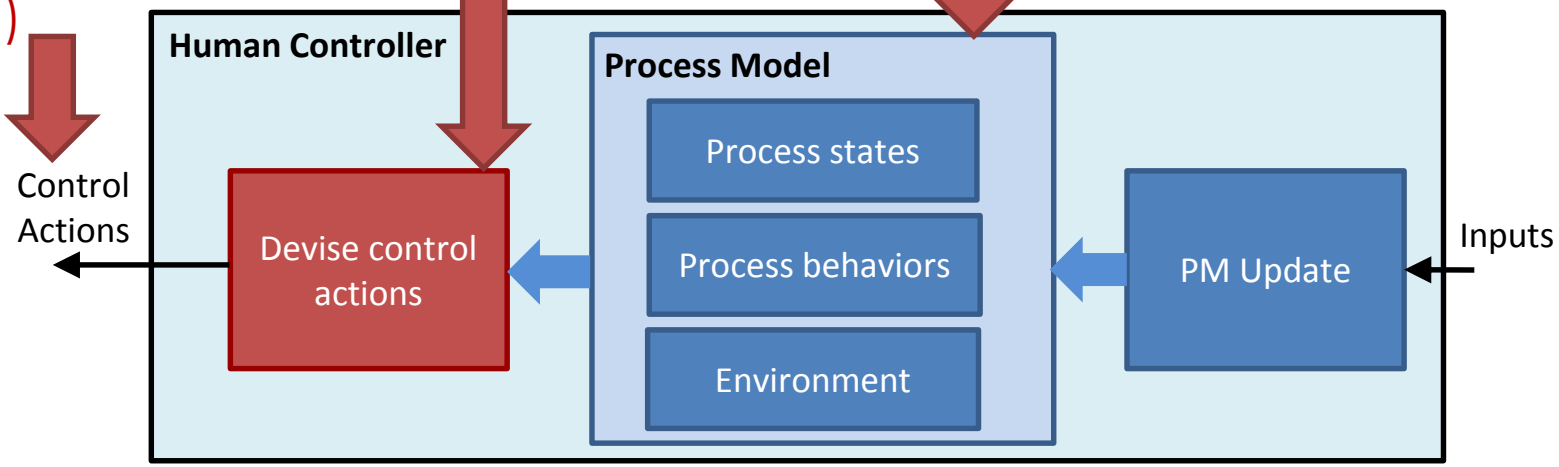
NEW PROCESS

- Identify unsafe Control Action Selections

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



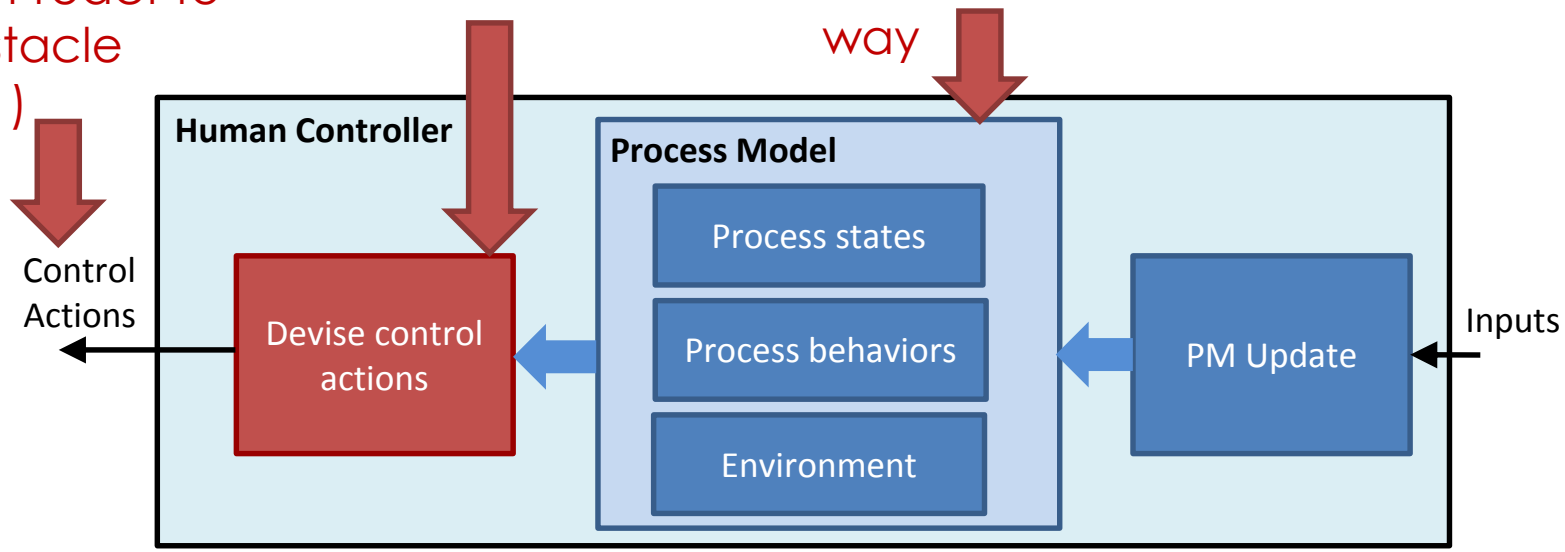
NEW PROCESS

- Identify unsafe Control Action Selections

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

Maybe driver decides to disable APA instead

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



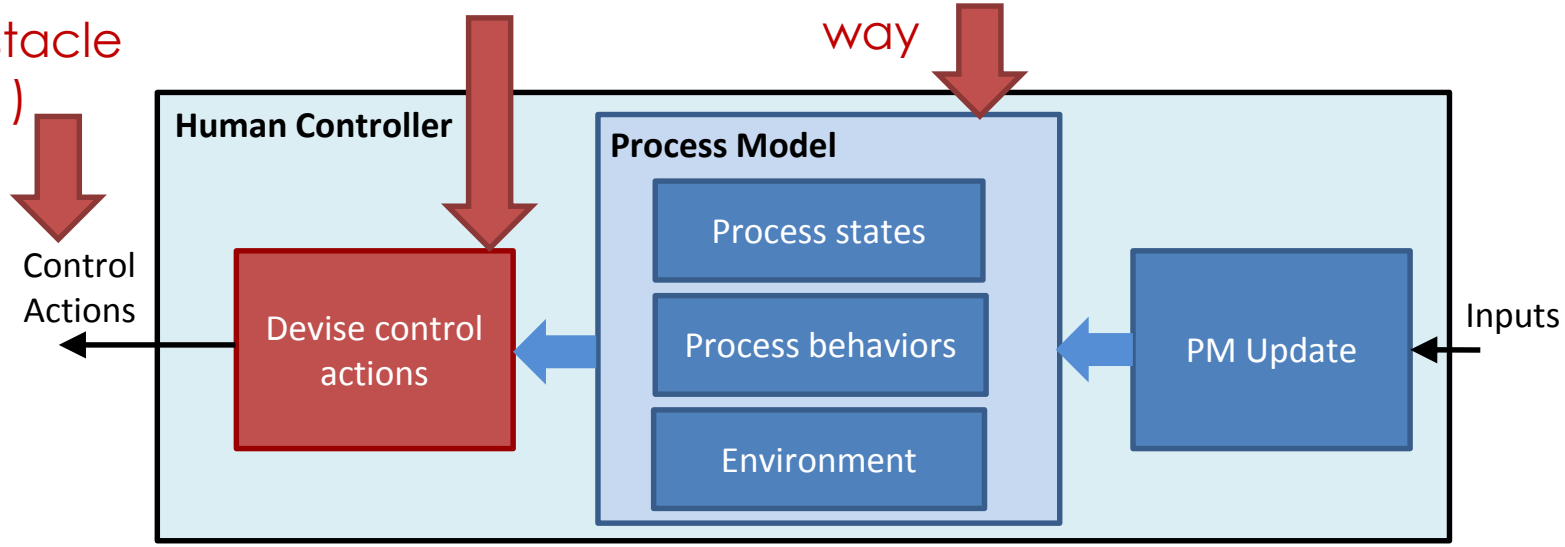
NEW PROCESS

- Identify unsafe Control Action Selections

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

Driver may still be waiting for APA to act

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

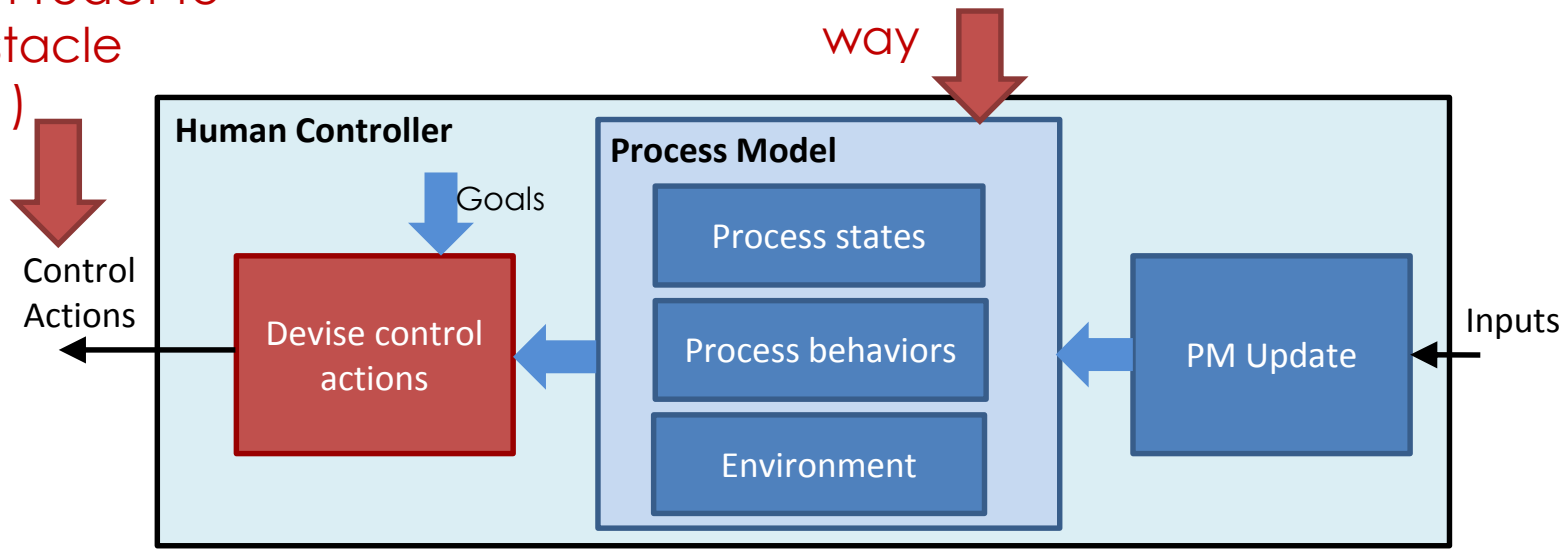


NEW PROCESS

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

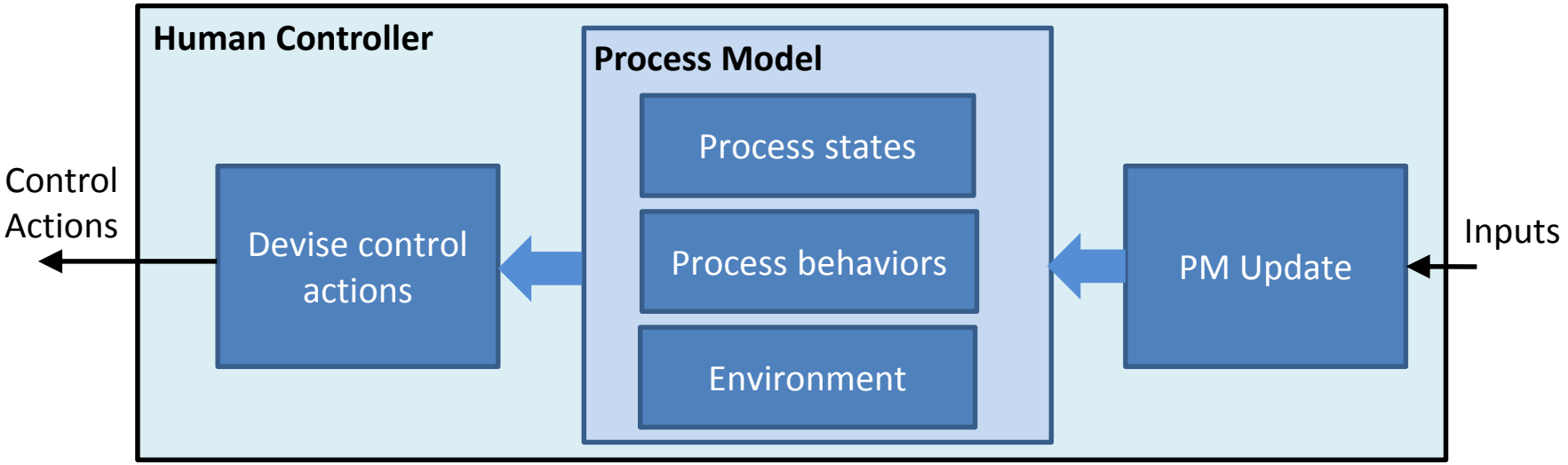
Driver does not brake when auto-parking and computer doesn't react to an obstacle (UCA-1)

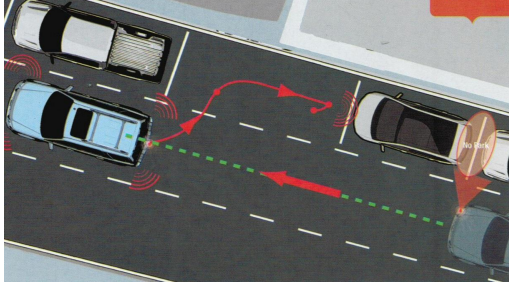
Driver knows APA is on
Driver knows APA hasn't reacted yet
Driver knows there is an obstacle in the way



NEW PROCESS

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





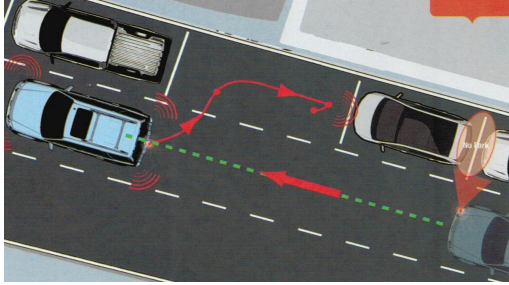
AUTOMATED PARKING

Features of each system considered for this analysis:

	Level 0* No Driving Automation	Level 1 "Driver Assistance"	Level 2a "Partial Automation"	Level 2b "Partial Automation"	Level 3 "Conditional Automation"
Steering	–	✓	✓	✓	✓
Braking	–	–	✓	✓	✓
Shifting and Acceleration	–	–	–	✓	✓
Object and Event Detection and Response	–	–	–	–	✓

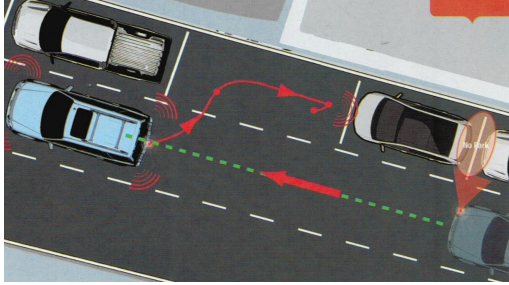
*System numbering is consistent with SAE definitions for levels of automation, while "a" and "b" indicate different implementations which are classified within the same SAE level.

AUTOMATED PARKING

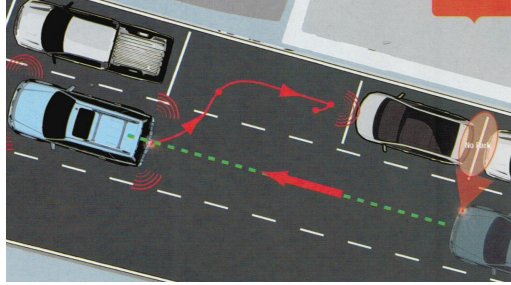


	Level 1 "Driver Assistance"	Level 2a "Partial Automation"	Level 2b "Partial Automation"	Level 3 "Conditional Automation"
Driver UCAs				
APA Computer UCAs	5	13	28	28
Total				

AUTOMATED PARKING



	Level 1 "Driver Assistance"	Level 2a "Partial Automation"	Level 2b "Partial Automation"	Level 3 "Conditional Automation"
Driver UCAs	42	41	38	44
APA Computer UCAs	5	13	28	28
Total				



AUTOMATED PARKING

	Level 1 "Driver Assistance"	Level 2a "Partial Automation"	Level 2b "Partial Automation"	Level 3 "Conditional Automation"
Driver UCAs	42	41	38	44
APA Computer UCAs	5	13	28	28
Total	47	54	66	72

35 in common

32 in common

30 in common

5 in common

28 in common

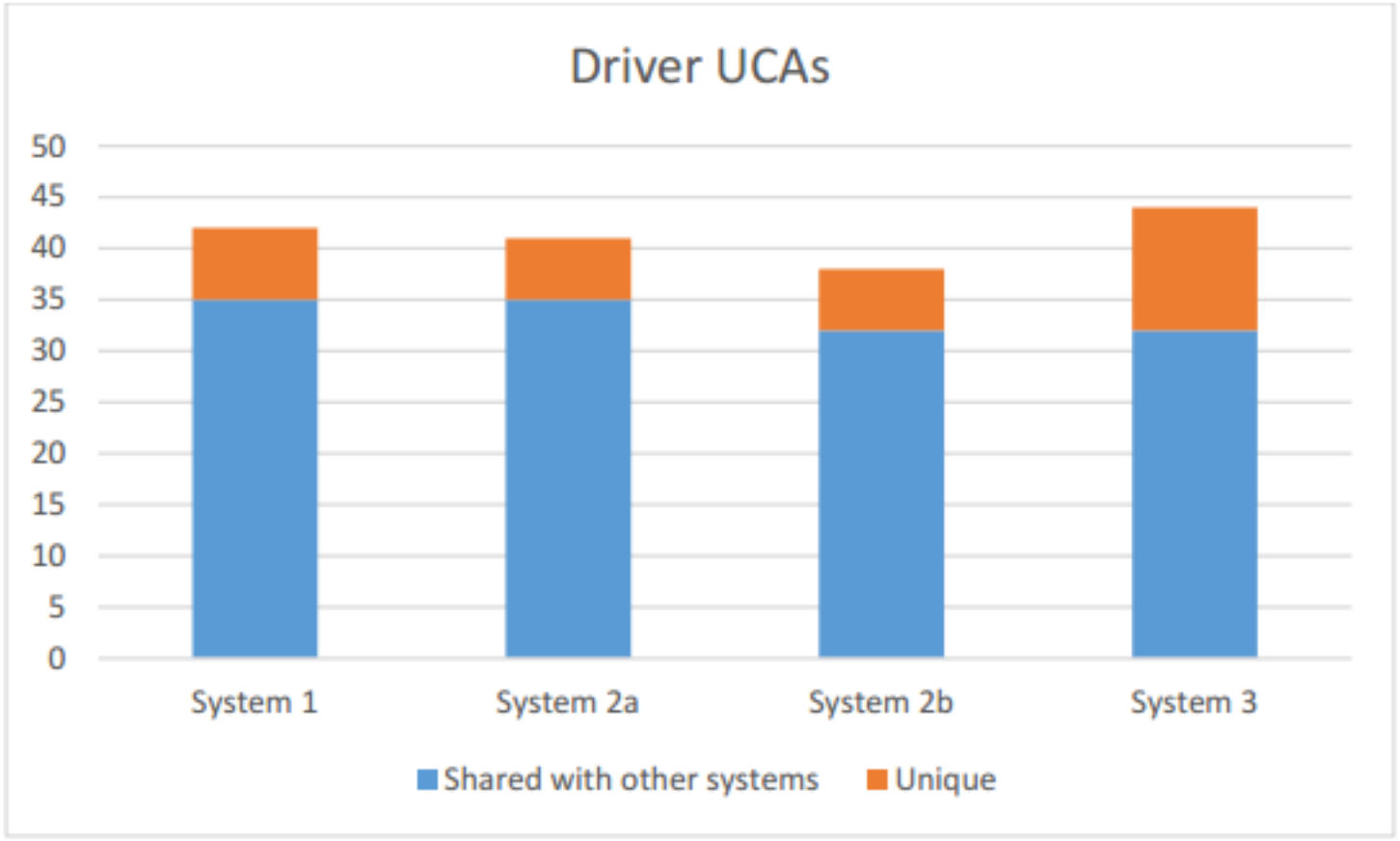
13 in common

40 in common

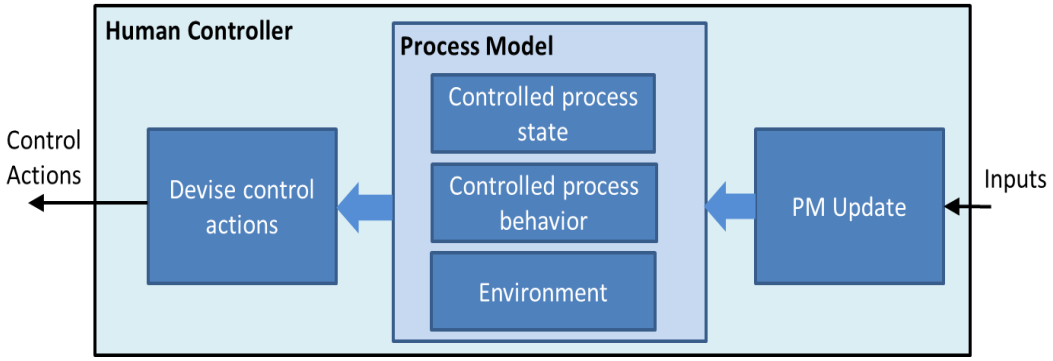
60 in common

43 in common

	Level 1	Level 2a	Level 2b	Level 3
Driver UCAs	42	41	38	44
APA Computer UCAs	5	13	28	28
Total	47	54	66	72



CONCLUSIONS



New human engineering extension strengths:

- Provides additional guidance for engineers to understand and anticipate human interactions
- Can help suggest solutions, not just problems
- Can be used earlier in design process than detailed simulations or prototypes