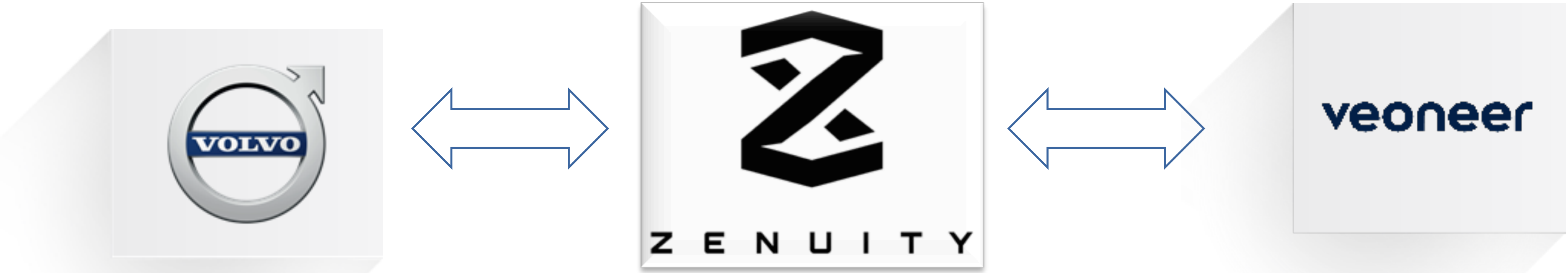
STPA Analysis of Safety Measures for Zenuity's Auto Valet Parking Demo

Amardeep Sidhu

Shabin Mahadevan

Zenuity - set up



Safety Agility Flexibility

Volvo Cars will directly source the AD, ADAS software

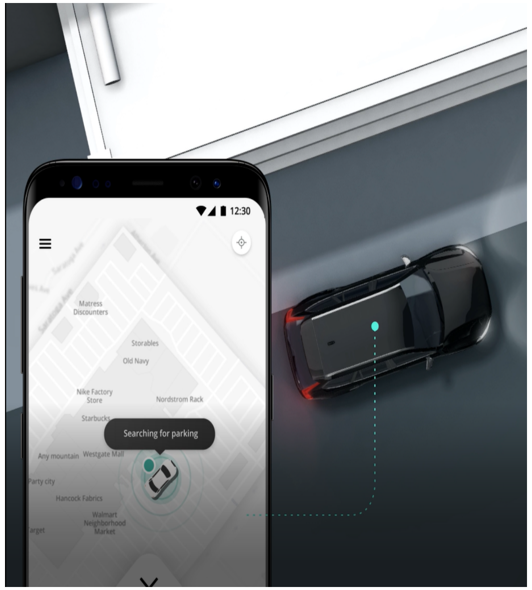
Zenuity develops AD, and ADAS software reference platform (hardware agnostic)

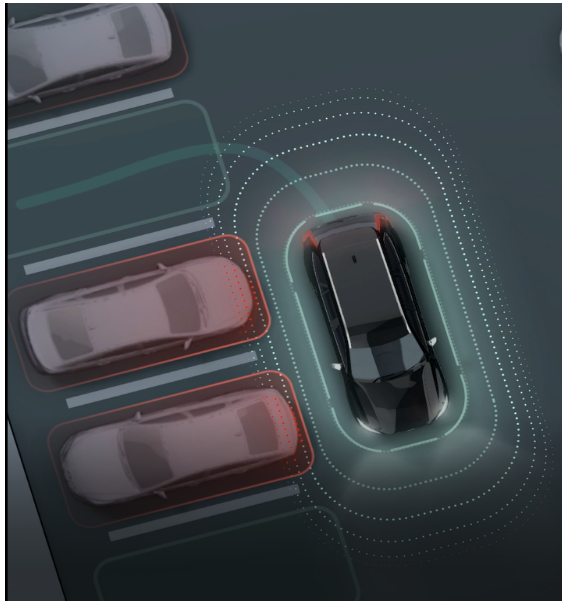
Veoneer markets, licenses, & adapts to customer needs

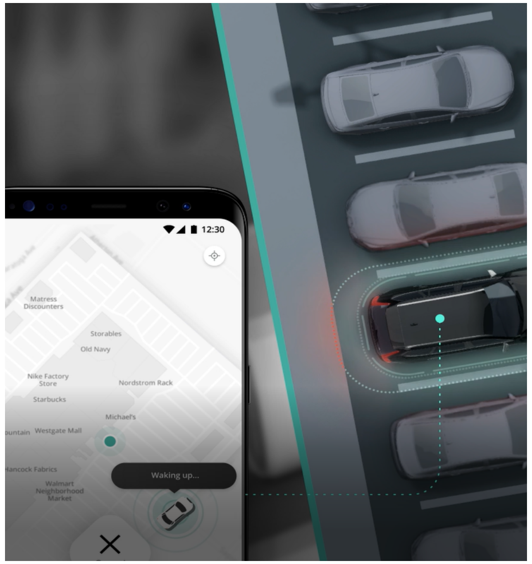
Background

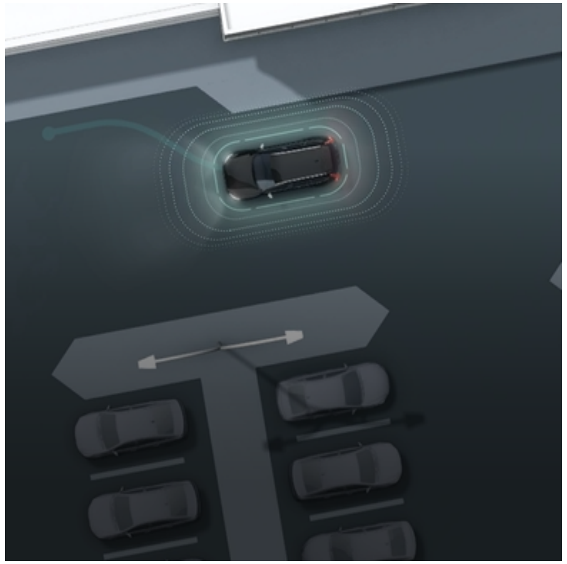
- Autonomous Valet Parking (AVP) feature

- AVP demo at Consumer Electronics Show (CES) Jan 2019









Objectives & Rationale

- Evaluate safety measures for autonomous valet parking and summon during Zenuity's AVP demo

- Informed decision on manned (safety driver) vs. driverless demo

- STPA was chosen to evaluate the safety due to:
  - Multi-agent nature of the demo
  - Complex interactions

System under study: ConOps

Demo Phases

1 Autonomous parking maneuver start

2 Autonomous parking maneuver end

3 Autonomous summon maneuver start

4 Autonomous summon maneuver end

4 demo vehicles running loop
+ 1 stationary safety vehicle

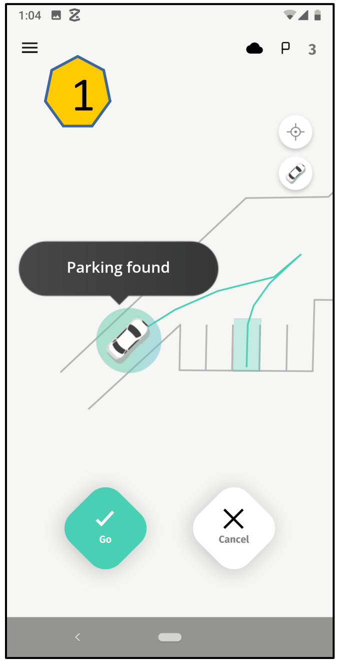
Human Actors

>Demo manager (DM)

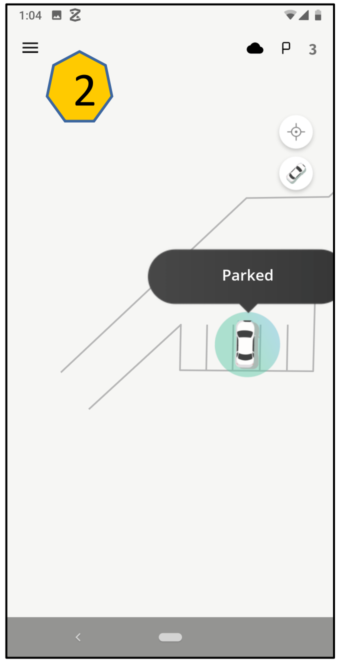
>E-stop operator (ESO)

>Vehicle Signal Monitor (VSM)

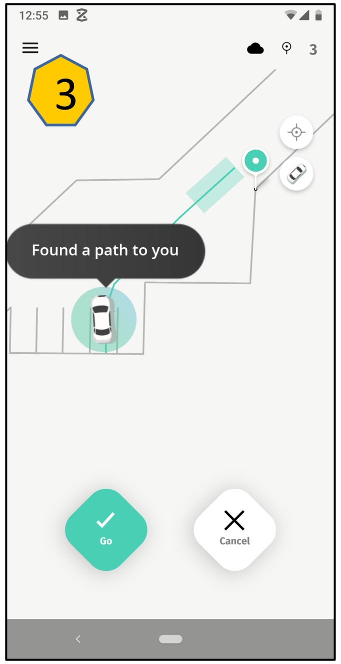
>Maintenance team



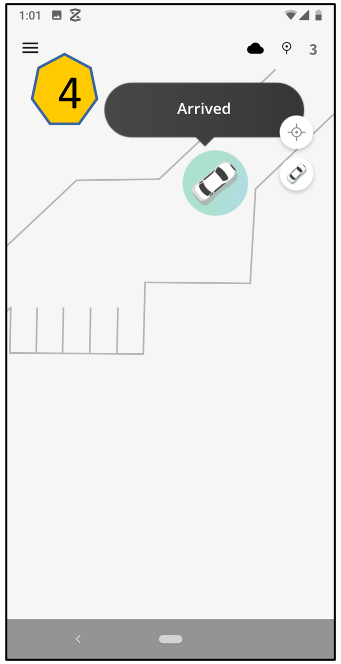
Parking found



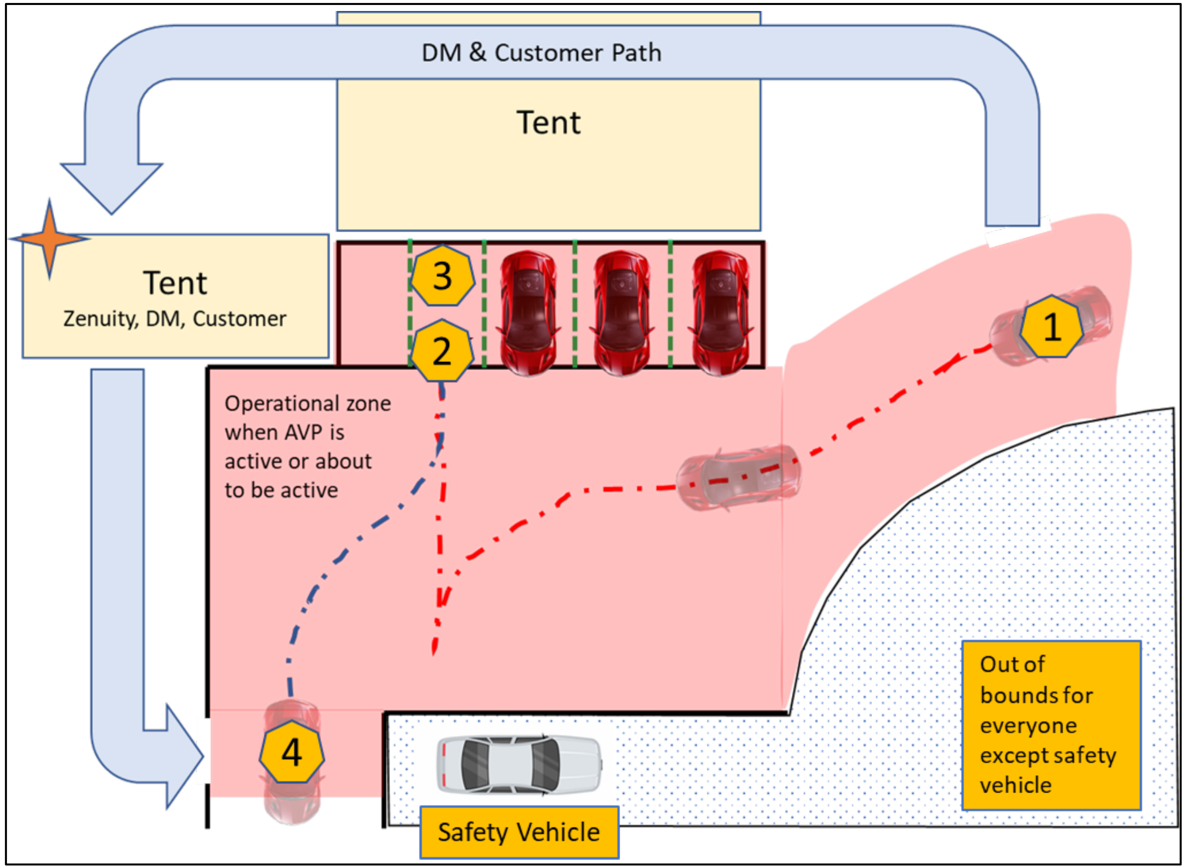
Parked



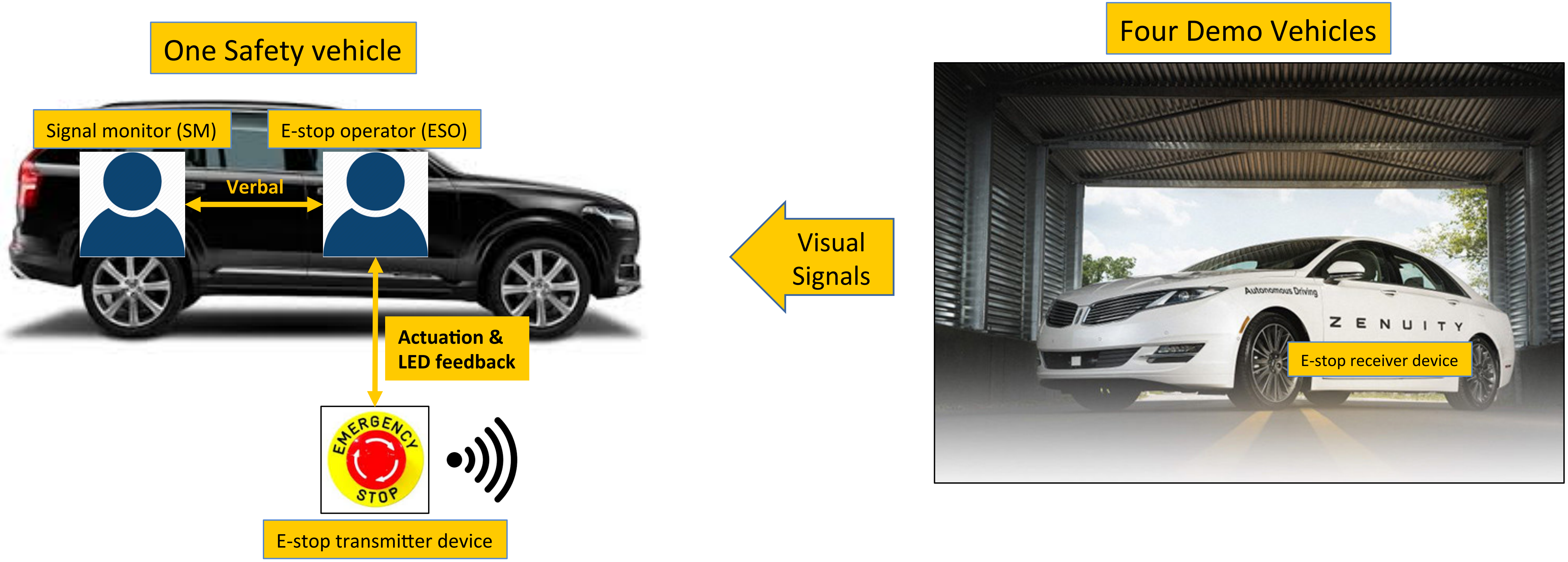
Found a path to you



Arrived


DM & Customer Path
Tent
Tent
Zenuity, DM, Customer
3
2
1
4
Operational zone when AVP is active or about to be active
Out of bounds for everyone except safety vehicle
Safety Vehicle

Zooming into the E-stop system



One Safety vehicle

Signal monitor (SM)

E-stop operator (ESO)

Verbal

Actuation & LED feedback

E-stop transmitter device

Visual Signals

Four Demo Vehicles

E-stop receiver device

- Safety vehicle has two pairs of SM and ESO
- Each SM and ESO pair is assigned to two demo vehicles

STPA Step 1: defining purpose of the analysis

Losses

- L-1 = AV collision with vulnerable road user (VRU)
- L-2 = AV gets damaged
- L-3 = Loss of reputation

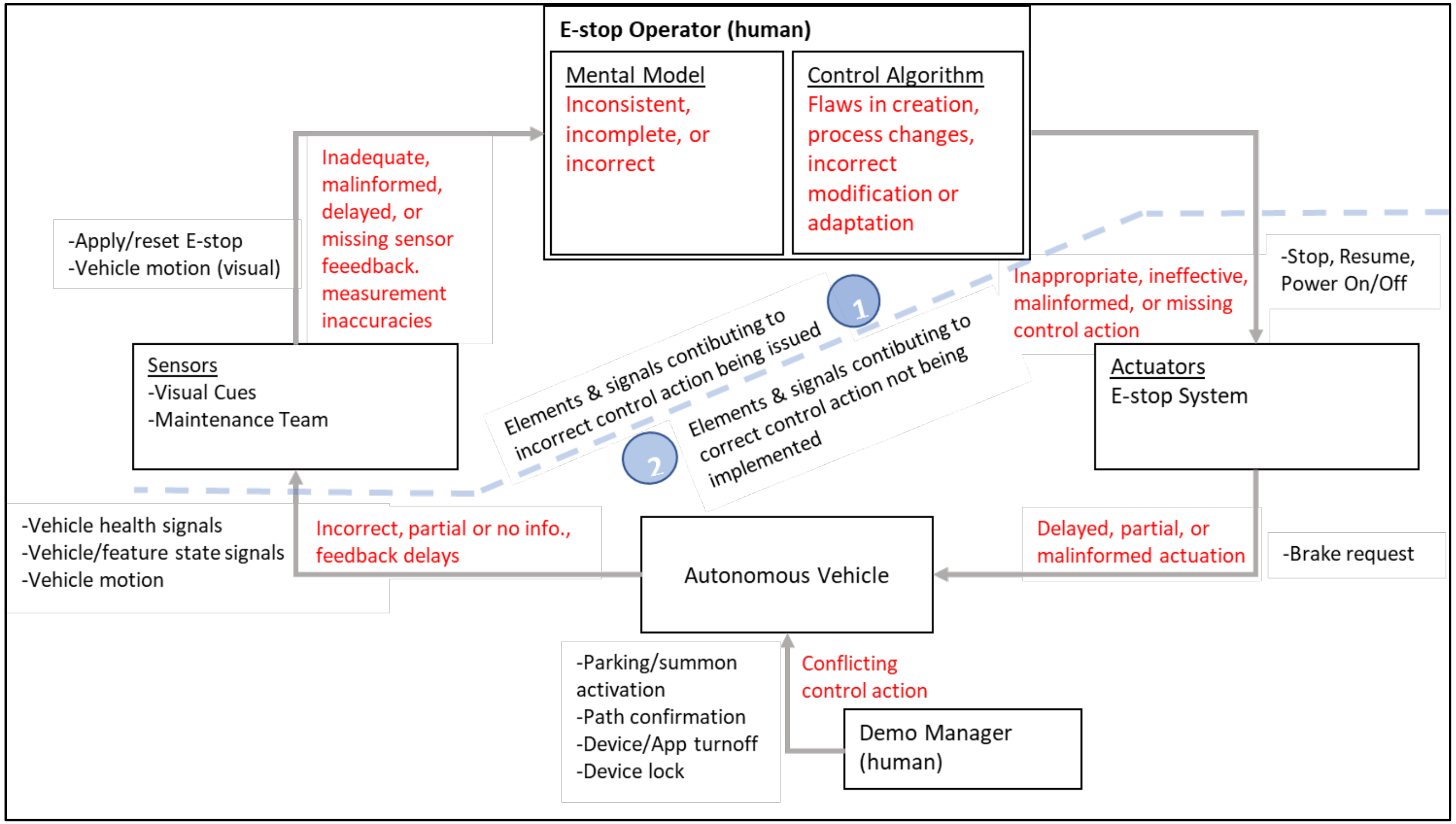
Hazards

- H-1 = AV does not maintain safe distance to VRU [L-1,L-3]
- H-2 = AV leaves the designated demo zone [L-1,L-2,L-3]
- H-3 = AV does not maintain safe distance to another AV [L-2,L-3]
- H-4 = AV does not maintain safe distance to structure [L-2,L-3]
- H-5 = AV activates without request during autonomous maneuver [L-3]
- H-6 = AV activates due to incorrect request during autonomous maneuver [L-3]
- H-7 = AV does not respond to requests during autonomous maneuver [L-1, L-2, L-3]

Process model variables

- Emergency situation: Yes, No
- Vehicle: Stationary, Moving

STPA Step 2: modeling the control structure



E-stop Operator (human)

Mental Model
Inconsistent, incomplete, or incorrect

Control Algorithm
Flaws in creation, process changes, incorrect modification or adaptation

-Apply/reset E-stop
-Vehicle motion (visual)

Inadequate, malinformed, delayed, or missing sensor feeedback. measurement inaccuracies

Sensors
-Visual Cues
-Maintenance Team

Elements & signals contibuting to incorrect control action being issued

1

Elements & signals contibuting to correct control action not being implemented

2

Inappropriate, ineffective, malinformed, or missing control action

-Stop, Resume, Power On/Off

Actuators
E-stop System

-Vehicle health signals
-Vehicle/feature state signals
-Vehicle motion

Incorrect, partial or no info., feedback delays

Autonomous Vehicle

Delayed, partial, or malinformed actuation

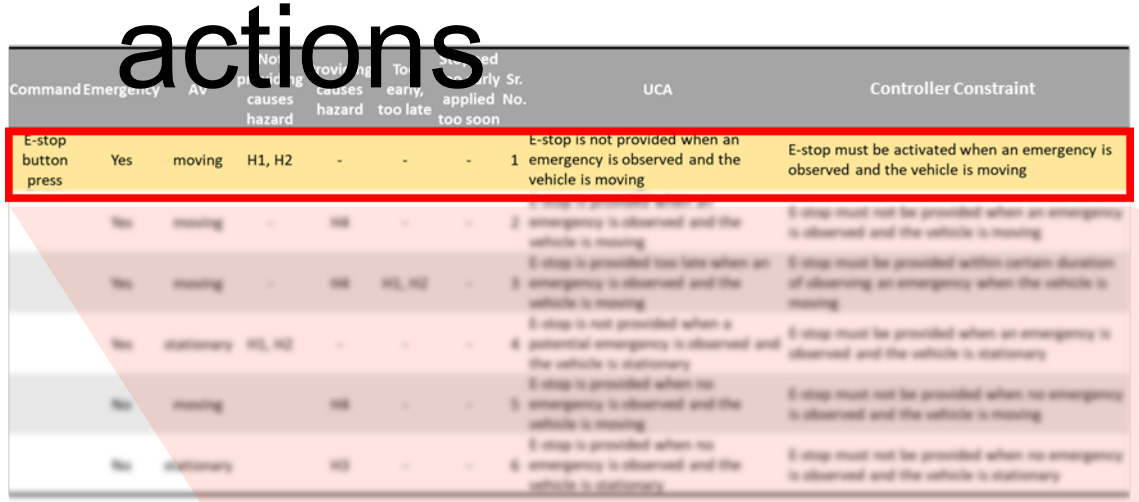
-Brake request

-Parking/summon activation
-Path confirmation
-Device/App turnoff
-Device lock

Conflicting control action

Demo Manager (human)

STPA Step 3: identifying unsafe control actions

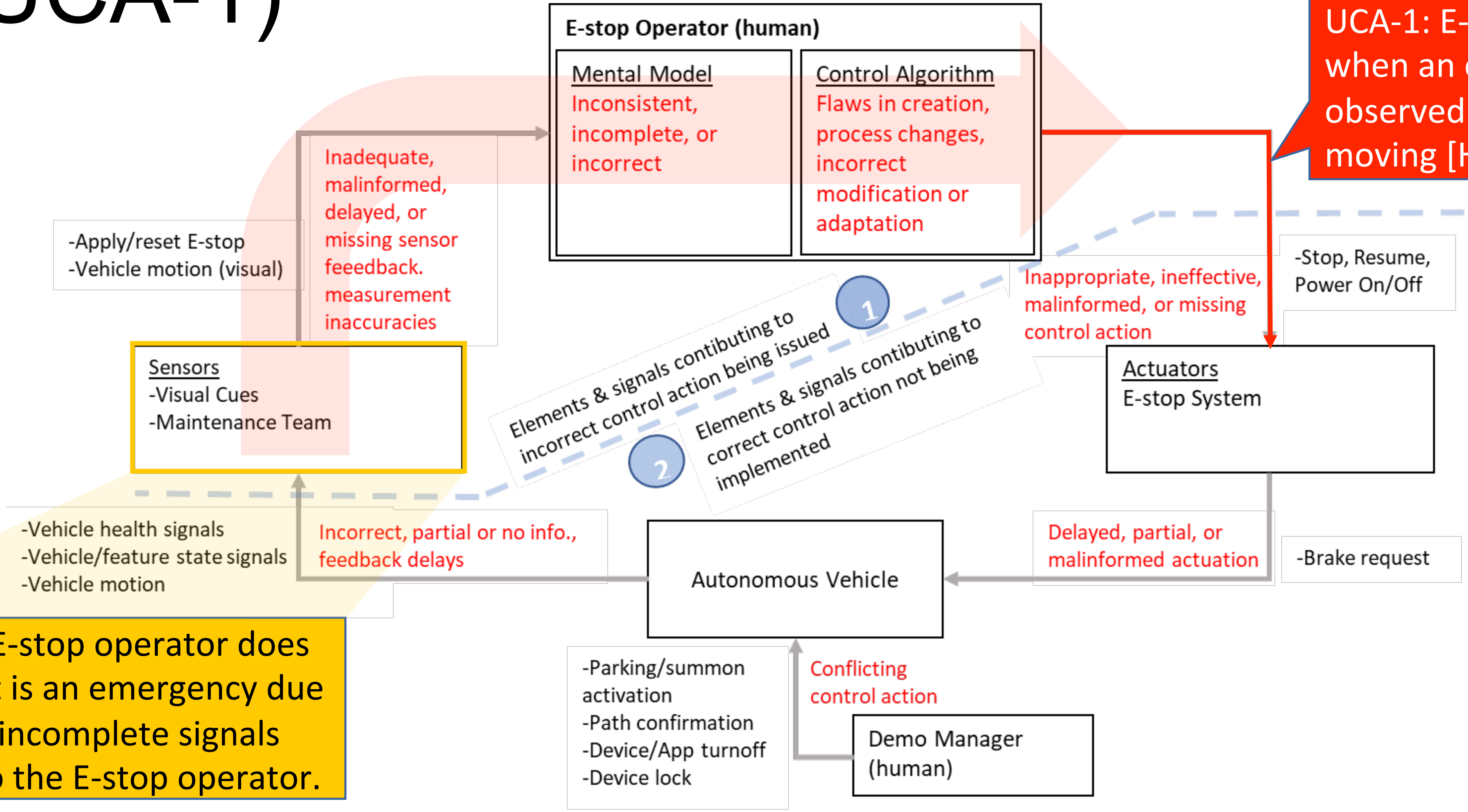


Command	Emergency	AV	Not providing causes hazard	Providing causes hazard	Too early, too late	Stopped too early applied too soon	Sr. No.	UCA	Controller Constraint
E-stop button press	Yes	moving	H1, H2	-	-	-	1	E-stop is not provided when an emergency is observed and the vehicle is moving	E-stop must be activated when an emergency is observed and the vehicle is moving
	Yes	moving	-	H4	-	-	2	E-stop is provided when an emergency is observed and the vehicle is moving	E-stop must not be provided when an emergency is observed and the vehicle is moving
	Yes	moving	-	H4	H1, H2	-	3	E-stop is provided too late when an emergency is observed and the vehicle is moving	E-stop must be provided within certain duration of observing an emergency when the vehicle is moving
	Yes	stationary	H1, H2	-	-	-	4	E-stop is not provided when a potential emergency is observed and the vehicle is stationary	E-stop must be provided when an emergency is observed and the vehicle is stationary
	No	moving		H4	-	-	5	E-stop is provided when no emergency is observed and the vehicle is moving	E-stop must not be provided when no emergency is observed and the vehicle is moving
	No	stationary		H3	-	-	6	E-stop is provided when no emergency is observed and the vehicle is stationary	E-stop must not be provided when no emergency is observed and the vehicle is stationary

Command	Emergency	AV	Not providing causes hazard	Providing causes hazard	Too early, too late	Stopped too early applied too soon	Sr. No.	UCA	Controller Constraint
E-stop button press	Yes	moving	H-1, H-2, H-3, H-4	-	-	-	1	E-stop is not provided when an emergency is observed and the vehicle is moving	E-stop must be realized when an emergency is observed and the vehicle is moving

STPA Step 4: identify loss scenarios (UCA-1)

UCA-1: E-stop is not provided when an emergency is observed and the vehicle is moving [H-1, H-2]



E-stop Operator (human)

Mental Model
Inconsistent, incomplete, or incorrect

Control Algorithm
Flaws in creation, process changes, incorrect modification or adaptation

Inadequate, malinformed, delayed, or missing sensor feeedback. measurement inaccuracies

-Apply/reset E-stop
-Vehicle motion (visual)

Sensors
-Visual Cues
-Maintenance Team

Inappropriate, ineffective, malinformed, or missing control action

-Stop, Resume, Power On/Off

1 Elements & signals contibuting to incorrect control action being issued

2 Elements & signals contibuting to correct control action not being implemented

Actuators
E-stop System

-Vehicle health signals
-Vehicle/feature state signals
-Vehicle motion

Incorrect, partial or no info., feedback delays

Autonomous Vehicle

Delayed, partial, or malinformed actuation

-Brake request

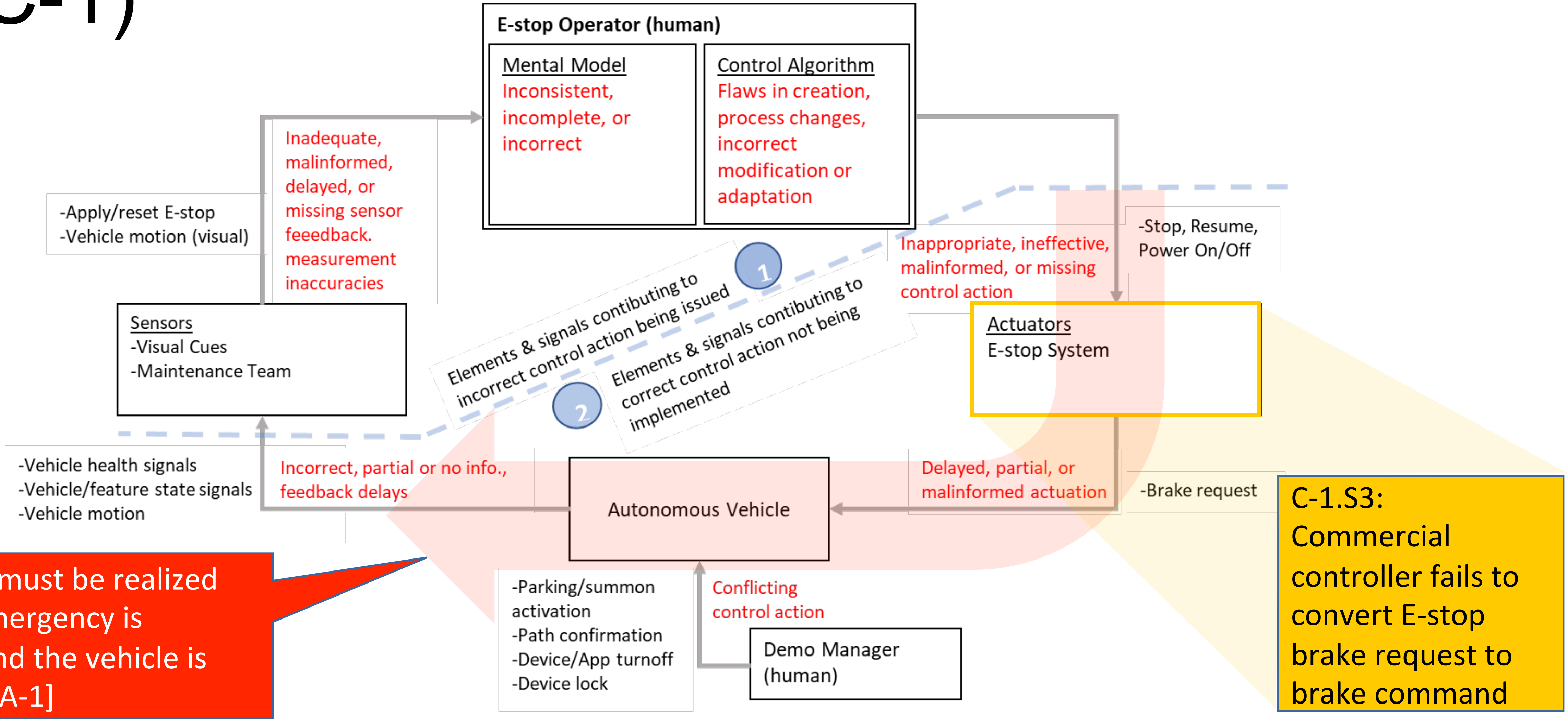
-Parking/summon activation
-Path confirmation
-Device/App turnoff
-Device lock

Conflicting control action

Demo Manager (human)

UCA-1.S1: E-stop operator does not know it is an emergency due to missing/incomplete signals available to the E-stop operator.

STPA Step 4: identify loss scenarios (C-1)


E-stop Operator (human)
Mental Model
Inconsistent, incomplete, or incorrect
Control Algorithm
Flaws in creation, process changes, incorrect modification or adaptation
-Apply/reset E-stop
-Vehicle motion (visual)
Inadequate, malinformed, delayed, or missing sensor feeedback. measurement inaccuracies
Sensors
-Visual Cues
-Maintenance Team
Elements & signals contibuting to incorrect control action being issued
1
Elements & signals contibuting to correct control action not being implemented
2
Inappropriate, ineffective, malinformed, or missing control action
-Stop, Resume, Power On/Off
Actuators
E-stop System
-Vehicle health signals
-Vehicle/feature state signals
-Vehicle motion
Incorrect, partial or no info., feedback delays
Autonomous Vehicle
Delayed, partial, or malinformed actuation
-Brake request
-Parking/summon activation
-Path confirmation
-Device/App turnoff
-Device lock
Conflicting control action
Demo Manager (human)

C-1: E-stop must be realized when an emergency is observed and the vehicle is moving [UCA-1]

C-1.S3: Commercial controller fails to convert E-stop brake request to brake command

Key results

1. Derived non-material solutions (operational requirements)
   - Not having more than one moving AV in the demo zone at any given time
2. Identified the need for a dedicated engineer (signal monitor) to complement ESO
   - Monitoring vehicle signals not visible to the E-stop operator
3. Identified the need for a redundant brake implementation
   - Single point failures of off-the-shelf intermediate controller
4. Recommended protected access to the AVP mobile app
5. Demo checklist with roles and expectations were created for demo training
   - For stakeholders both internal (Zenuity) and external (Veoneer)
6. Systems engineering and STPA artifacts from this analysis were instrumental in driving clarity and a common language across the organization
   - ConOps, functional control structures, control diagrams

[Video from CES Demo](#) (1.5x)

Next Steps

- Extending system boundary to consider additional control loops in the AVP feature
- Integrating STPA into Zenuity's systems engineering process
- Improve human controller analysis using the STPA Engineering for Humans extension

Thank you for your time.
Questions?

Contact Info:
Amardeep Sidhu: Amardeep.Sidhu@Zenuity.com
Shabin Mahadevan: Shabin.Mahadevan@Zenuity.com