Virtual Button and Graphical Interface System Safety Evaluation Using STPA

Jesse Johnston
System Safety Engineer – Non-Motion Controls

Mark A. Vernacchia
GM Technical Fellow, Principal System Safety Engineer – Propulsion Systems

Global Safety, Systems, & Integration
General Motors Company

MIT STAMP Workshop
August 3, 2020

Introduction

- Examine how STPA can be used to explore safety concerns associated with interactions between human operators and virtual controls
- Inclusion of humans as control structure elements enables representation as a “human controller”
- Discuss how to organize STPA generated system safety requirements, and how these requirements can be documented and used by system engineers

Overview of Topics

- What Are “Virtual Controls?” Why Popular?
- Mechanical/Electrical vs. Virtual Control Interface Differences
- STPA Related Activities:
  - Early use of STPA in Concept Stage is important
  - Deciding if a virtual control is safety critical
  - Use of “human controller” aspects Mental Models
    - Process State
    - Process Behavior
    - Environment

Overview of Topics

- Virtual Control Example Evaluation Using STPA
  - Operating Conditions
  - Control Structure and Unsafe Control Actions (UCAs)
  - Causal Scenarios and Requirements Leveraging Mental Models
- Lessons to Share

What Are “Virtual Controls?” Why Are They Becoming Popular?

- “Virtual controls” are controls that do not require physical actuation of a moving part
  - Touch (*focus for this presentation*)
  - Voice
  - Gestures
- Switches, buttons, dials, etc. can be “virtualized”
  - Cost savings
  - Greater design freedom
  - Modern approach desired by customers

Virtual Control Examples

- Cell phones – smart phones replaced most physical buttons with virtual controls, with fewer buttons as design evolves
- Home automation – “smart homes” replace lighting, temperature and other controls with virtual controls
- Automotive examples
  - Audio controls
  - Climate controls
  - Lighting controls
  - …with even more on the horizon

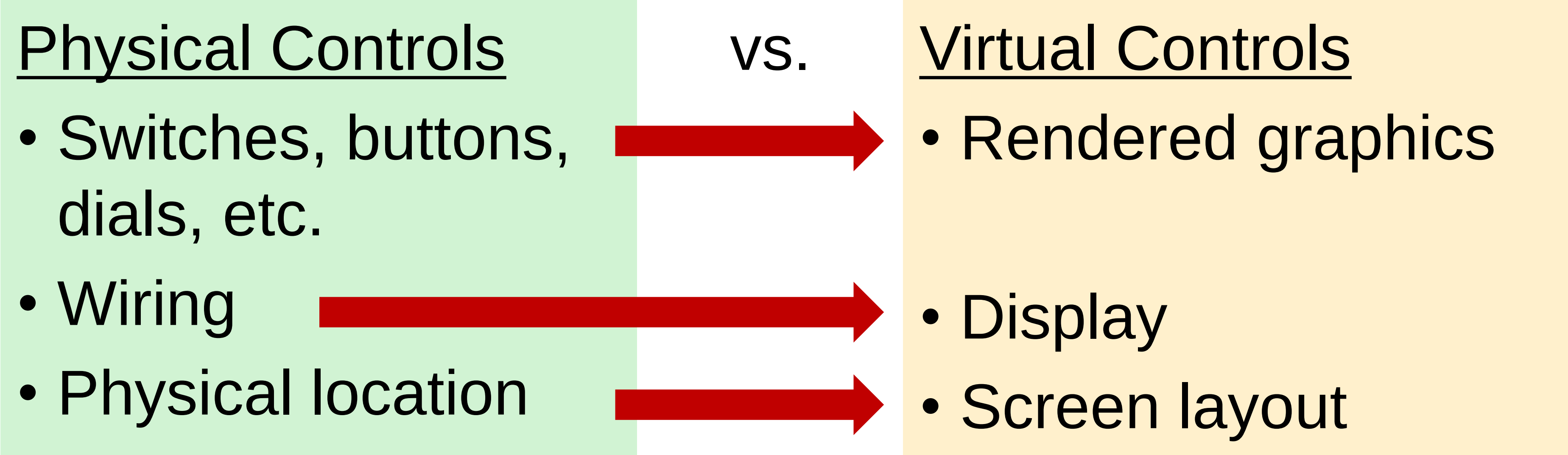
Safety Considerations: Benefits of Replacing Physical With Virtual

- Mechanical key ignition switches and electrical start-stop switches have various fault mechanisms
  - Vehicle vibration and frictional forces influence operation
  - Cable connections and wire harness faults occur

- Elimination of key ignition mechanical and electrical components can eliminate these types of problems

- Hardware verification testing reduction opportunity

Differences in Safety Considerations



Physical Controls

- Switches, buttons, dials, etc.
- Wiring
- Physical location

vs.

Virtual Controls

- Rendered graphics
- Display
- Screen layout

Common Considerations

- Software control logic
- Accidental or erroneous activation

STPA Related Activities: Early Use of STPA in Concept Stage is Important

- Very beneficial in the early stages of the design as it provides a way to do exploratory analysis when all potential causes / effects of misbehaviors not known
- Enables review of the anticipated operating scenarios for these virtual control devices and facilitates a discussion about better use scenarios
- Facilitates discussion between system safety engineers and system design engineers as to which requirements are safety related versus performance and/or functional related

STPA Related Activities: Deciding if a Virtual Control is Safety Critical

- ISO-26262 (Automotive Safety Standard)
  - Provides guidance to determine requirements that prevent or manage potential hazards so that the system is “free from unreasonable risk”
  - Focuses on harm to humans (a.k.a. STPA “losses”)

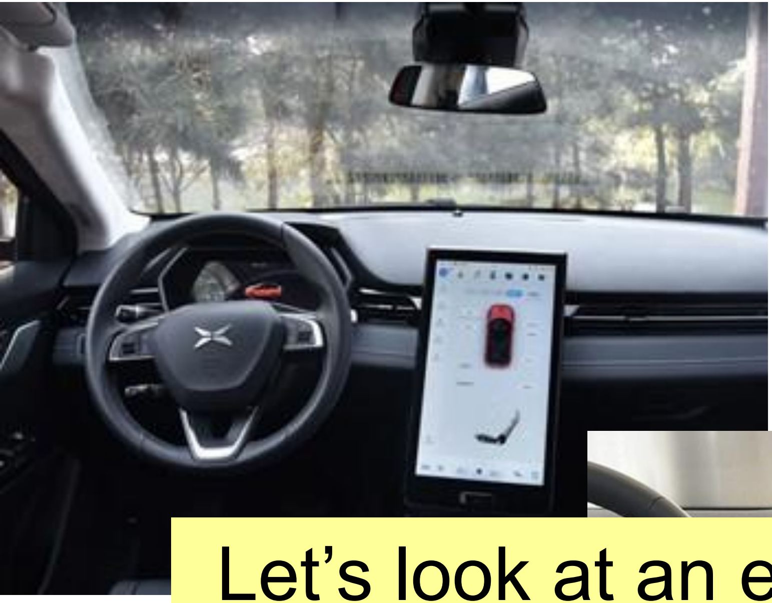
- Preliminary Hazard Analysis
  - HAZOP (Hazard and Operability) – performed to identify potential hazards that might lead to accidents (harm)
  - HARA (Hazard Analysis and Risk Assessment) – analyzes severity, exposure and controllability of hazards, allowing assignment of Automotive Safety Integrity Levels (ASIL)

STPA Related Activities: “Human Controller” Aspects in STPA Evaluation

- Referencing work by Megan France and John Thomas to write scenarios for actions performed by the human operator, using “Human Controller Model” construct

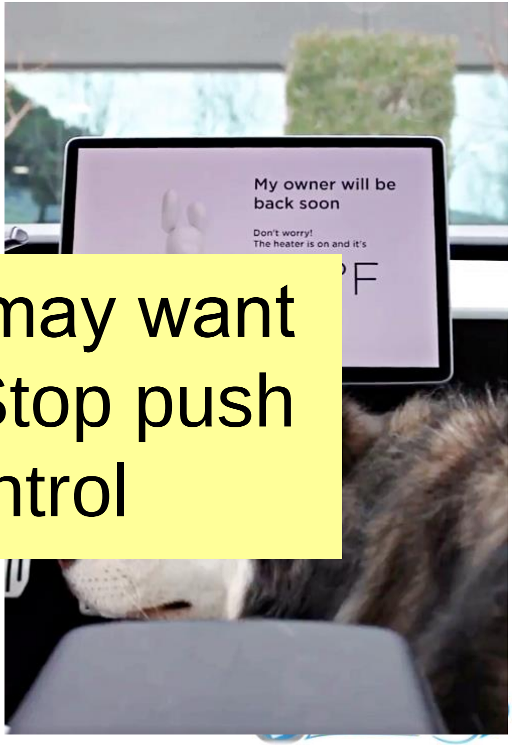
- Human Controller Model focuses on three aspects:
  - The controller’s (driver or occupant) goals & how they make decisions based on what they expect
  - The flaws in how a human controller thinks about system and its environment
  - The influence of human experiences and the expectations related to processing sensory feedback/input

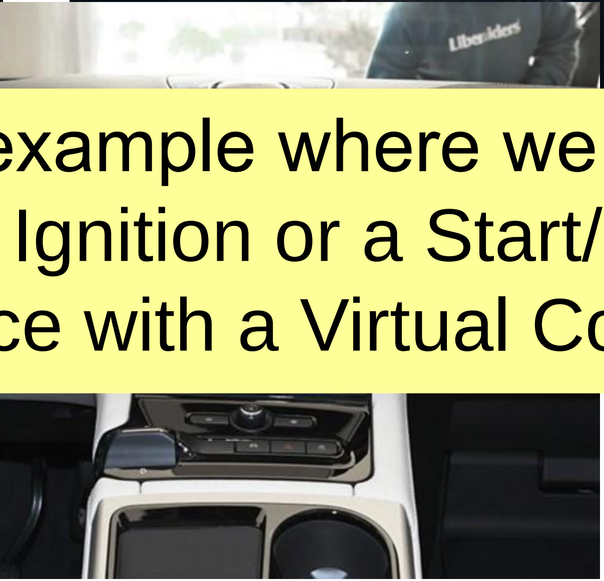
Xiaopeng - Xpeng



Weltmeister - EX5

Tesla “Dog Mode”





Let’s look at an example where we may want to replace a Key Ignition or a Start/Stop push button device with a Virtual Control

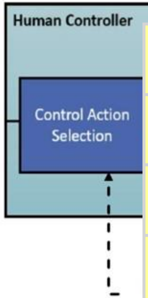
STPA Related Activities: Key or Start/Stop Button Virtualization Example

- Is it safety critical?
  - Yes, it controls the propulsion state of the vehicle (confirm by HAZOP and HARA)

- Operating Contexts:
  - How does driver turn on ignition?
  - How does driver turn off ignition?
  - Impact on living things left in vehicle if driver leaves the vehicle unattended?
  - Entering vehicle, driving vehicle, exiting vehicle, post crash

STPA Human Controller

CONTROL ACTION SELECTION



Control Action Selection

What were operator's goals?

- To drive the vehicle
- To have propulsion become active without physical button

How automatic or novel was the behavior?

- Very automatic to enable propulsion - no driver action
- Very novel to turn vehicle <OFF>
- Very novel to allow vehicle to continue to run <Let Run>

How might operator's mental models affect decisions?

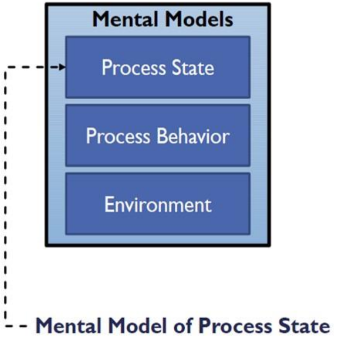
- Mental model of how to start car may impact driver interaction
- MM of how to turn vehicle <OFF> may influence driver interaction
- MM of how to get to <ACC> may influence driver interaction
- MM of how to turn vehicle <OFF> at speed may influence driver interaction

ction

External factors that might affect decision?

- Vehicle automatically goes into propulsion with specific driver action
- Vehicle automatically shuts <OFF> only after driver exits

STPA Human Controller



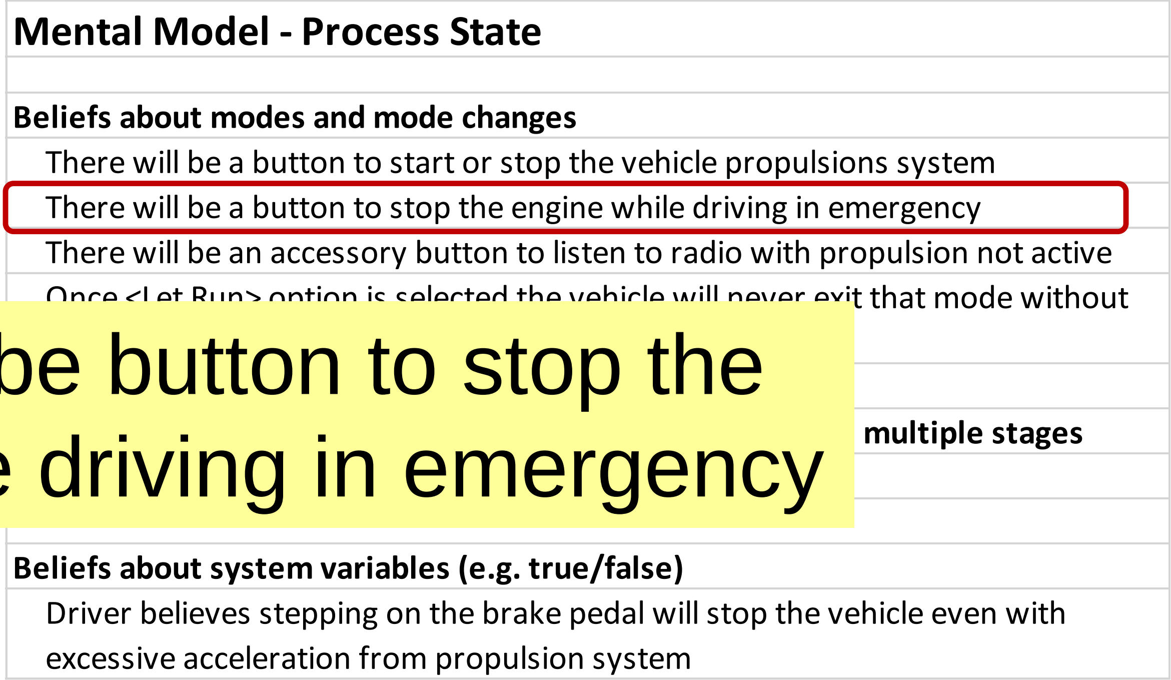
Mental Model of Process State

- 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 are ***partial representations.***

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

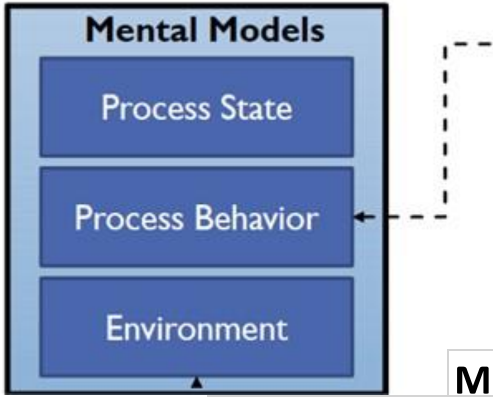
What does the operator believe about the system?



Mental Model - Process State
Beliefs about modes and mode changes
There will be a button to start or stop the vehicle propulsions system
There will be a button to stop the engine while driving in emergency
There will be an accessory button to listen to radio with propulsion not active
Once <Let Run> option is selected the vehicle will never exit that mode without
multiple stages
Beliefs about system variables (e.g. true/false)
Driver believes stepping on the brake pedal will stop the vehicle even with excessive acceleration from propulsion system

There will be button to stop the engine while driving in emergency

STPA Human Controller

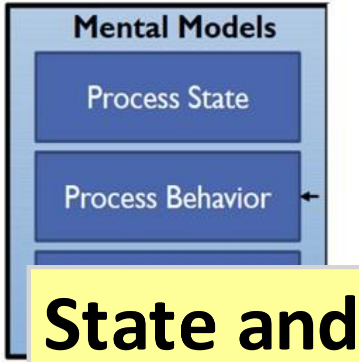


Mental Model of Process Behavior

- 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 - Process Behavior
Beliefs about what the system can do
Start automatically
Turn <OFF> automatically
Vehicle will not rollaway on an incline if driver exits without turning <OFF>
Vehicle will activate a <Let Run> mode automatically because it has one
Beliefs about if-then relationships between operator input and system output
If the driver performs a specific action the vehicle will turn propulsion <ON>
Performing that specific action after propulsion is <ON> will not do anything

STPA Human Controller



- State and behavior of other controllers
- Social and organizational relationships

Mental Model - Environment
Changes in environmental conditions
Driver entering the vehicle
Driver exiting the vehicle
Shift by Wire system is operational and available
A brake override feature is operational and available
Social and organizational relationships
Passenger expectation of vehicle operation

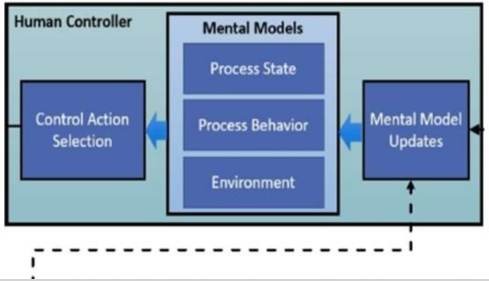
State and behavior of other controllers

Shift by Wire system is operational and available

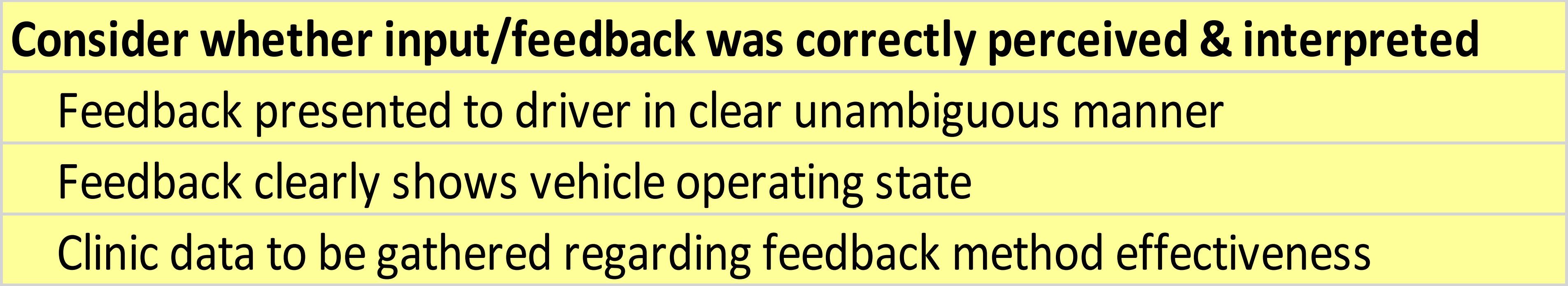
A brake override feature is operational and available

STPA Human Controller

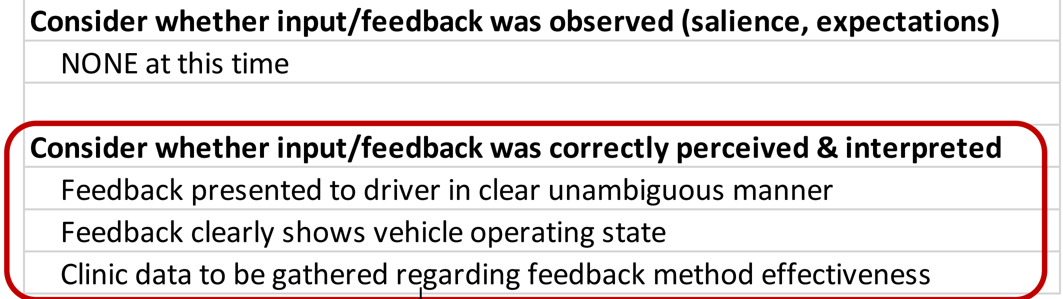
MENTAL MODEL UPDATES



How did the operator come to have their current beliefs?



Consider whether input/feedback was correctly perceived & interpreted
Feedback presented to driver in clear unambiguous manner
Feedback clearly shows vehicle operating state
Clinic data to be gathered regarding feedback method effectiveness

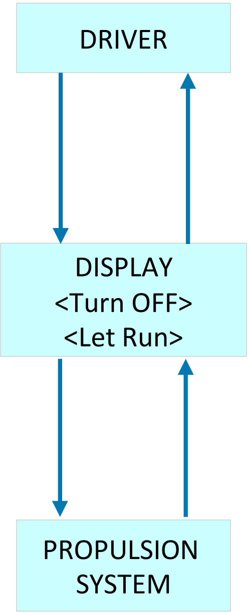


Consider whether input/feedback was observed (salience, expectations)
NONE at this time
Consider whether input/feedback was correctly perceived & interpreted
Feedback presented to driver in clear unambiguous manner
Feedback clearly shows vehicle operating state
Clinic data to be gathered regarding feedback method effectiveness

STPA Human Controller – Accidents, Hazards, and Operating Contexts

EXAMPLE ACCIDENTS		
People injured when car collides with obstacle	A1	
People injured when car collides with another car	A2	
People injured when car collides with pedestrian	A3	
People injured when car interior overheats or gets too cold	A4	
EXAMPLE POTENTIAL HAZARDS		
Car rolls away as driver exits	H1	A1, A2, A3
Propulsion cannot be deactivated when experiencing unintended acceleration	H2	A1, A2, A3
Car overheats with occupants inside	H3	A4
Car gets too cold with occupants inside	H4	A4
EXAMPLE OPERATING CONTEXTS / SCENARIOS		
While Entering Vehicle		
While Seated in Driver Seat		
While Exiting Vehicle		
While in Gear and Stationary		
While in Gear and Moving		

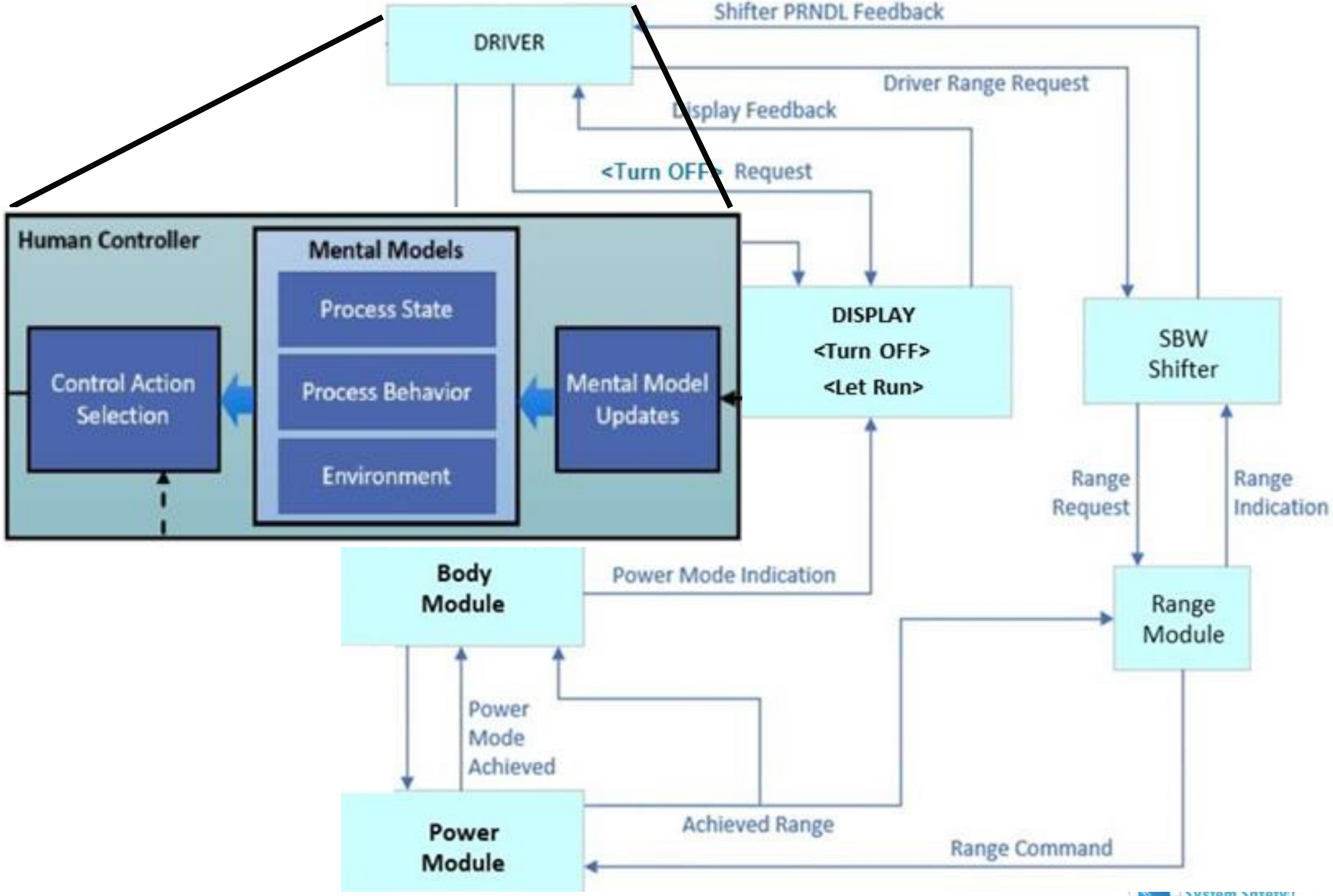
STPA Control Structure Example



DRIVER

DISPLAY
<Turn OFF>
<Let Run>

PROPULSION SYSTEM



DRIVER

Shifter PRNDL Feedback

Driver Range Request

Display Feedback

<Turn OFF> Request

Human Controller

Mental Models

Process State

Process Behavior

Environment

Control Action Selection

Mental Model Updates

DISPLAY
<Turn OFF>
<Let Run>

SBW Shifter

Range Request

Range Indication

Body Module

Power Mode Indication

Range Module

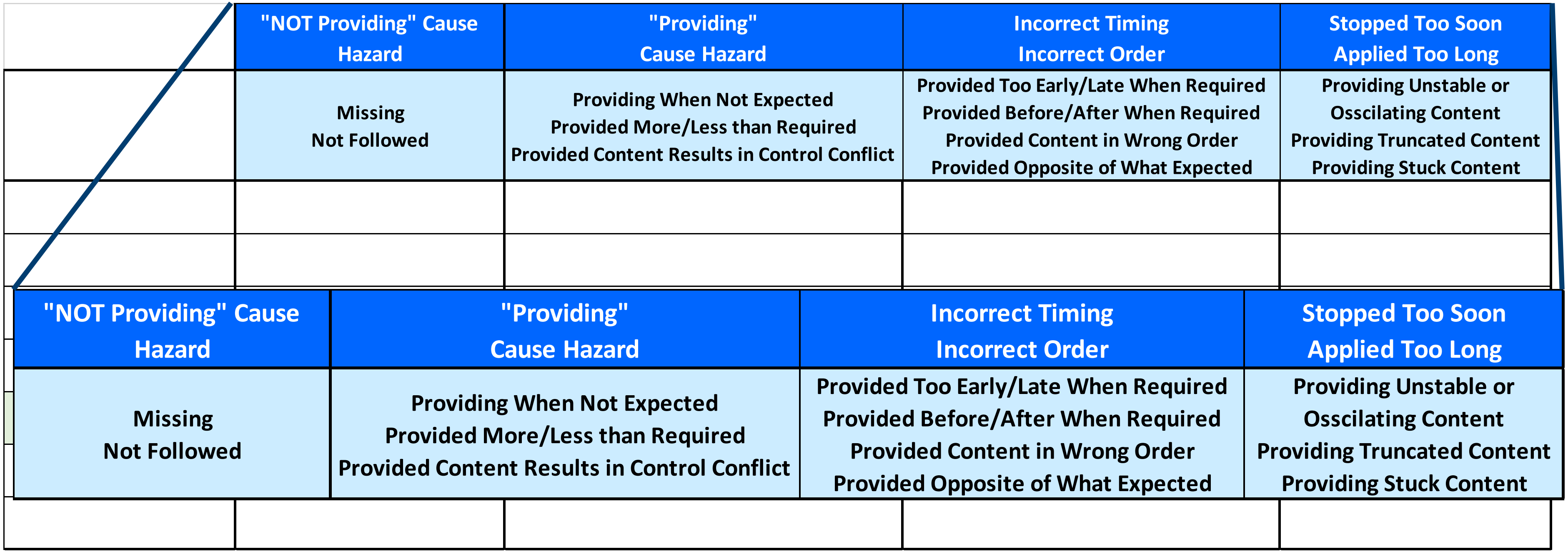
Power Mode Achieved

Power Module

Achieved Range

Range Command

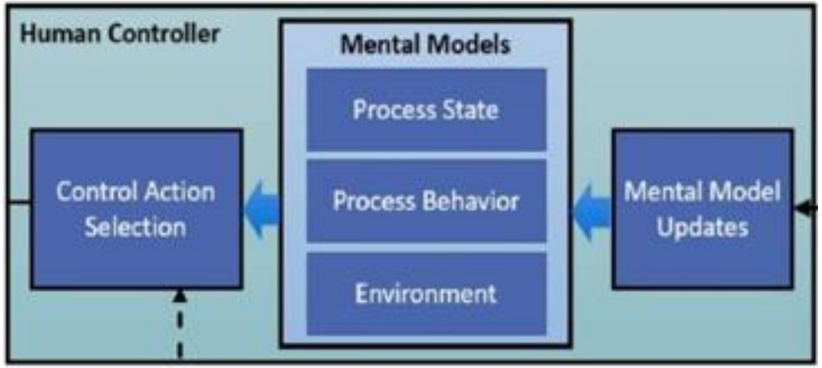
STPA UCA Approach



	"NOT Providing" Cause Hazard	"Providing" Cause Hazard	Incorrect Timing Incorrect Order	Stopped Too Soon Applied Too Long
	Missing Not Followed	Providing When Not Expected Provided More/Less than Required Provided Content Results in Control Conflict	Provided Too Early/Late When Required Provided Before/After When Required Provided Content in Wrong Order Provided Opposite of What Expected	Providing Unstable or Osscilating Content Providing Truncated Content Providing Stuck Content

"NOT Providing" Cause Hazard	"Providing" Cause Hazard	Incorrect Timing Incorrect Order	Stopped Too Soon Applied Too Long
Missing Not Followed	Providing When Not Expected Provided More/Less than Required Provided Content Results in Control Conflict	Provided Too Early/Late When Required Provided Before/After When Required Provided Content in Wrong Order Provided Opposite of What Expected	Providing Unstable or Osscilating Content Providing Truncated Content Providing Stuck Content

STPA Causal Scenario Development Utilizing Mental Model Framework



Control Action Selection

- Replacement of mechanical devices is very novel idea
- Anticipate need for instruction and guidance cues

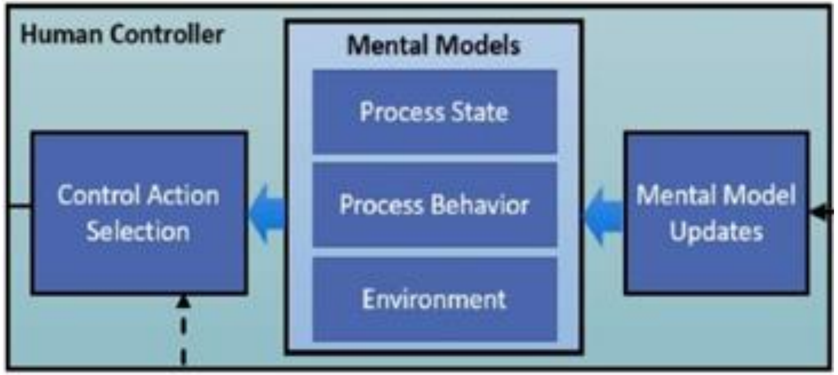
Process State

- There will be mechanical means to start / stop
- There is a way to turn propulsion off in emergency

Process Behavior

- The system will start and turn off automatically

STPA Causal Scenario Development Utilizing Mental Model Framework



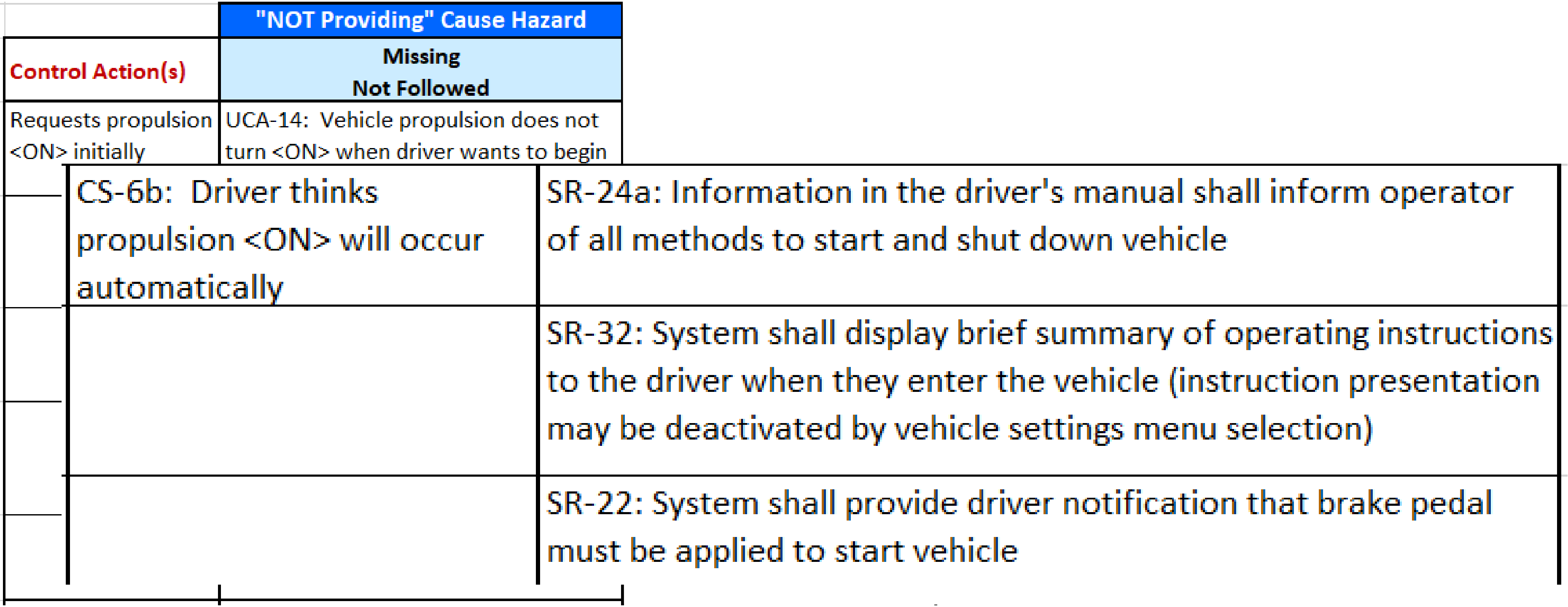
Environment

- How system will behave when driver enters or exits vehicle
- Other vehicle systems (e.g., shift by wire, braking, etc.) operation will not be affected/changed

Metal Model Updates

- Feedback of propulsion state needs to be clear
- Feedback mechanisms evaluated for effectiveness

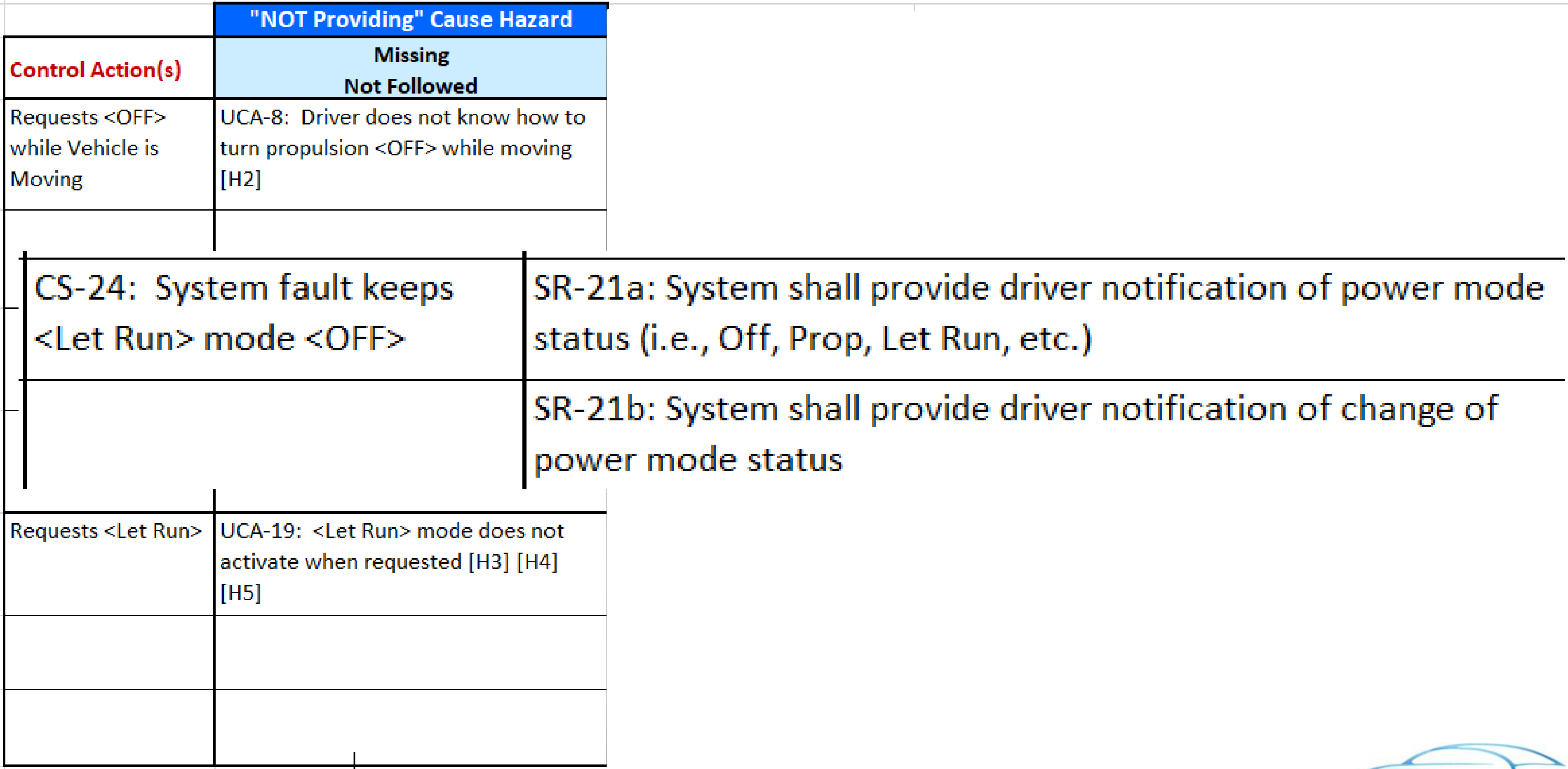
STPA Example Causal Scenarios and Potential Requirements



	"NOT Providing" Cause Hazard
Control Action(s)	Missing Not Followed
Requests propulsion <ON> initially	UCA-14: Vehicle propulsion does not turn <ON> when driver wants to begin

CS-6b: Driver thinks propulsion <ON> will occur automatically	SR-24a: Information in the driver's manual shall inform operator of all methods to start and shut down vehicle
	SR-32: System shall display brief summary of operating instructions to the driver when they enter the vehicle (instruction presentation may be deactivated by vehicle settings menu selection)
	SR-22: System shall provide driver notification that brake pedal must be applied to start vehicle

STPA Example Causal Scenarios and Potential Requirements



	"NOT Providing" Cause Hazard
Control Action(s)	Missing Not Followed
Requests <OFF> while Vehicle is Moving	UCA-8: Driver does not know how to turn propulsion <OFF> while moving [H2]
Requests <Let Run>	UCA-19: <Let Run> mode does not activate when requested [H3] [H4] [H5]

CS-24: System fault keeps <Let Run> mode <OFF>	SR-21a: System shall provide driver notification of power mode status (i.e., Off, Prop, Let Run, etc.)
	SR-21b: System shall provide driver notification of change of power mode status

Lessons to Share From This Example

- STPA evaluation can lead to suggestions to redesign initial propulsion activation strategy
  - Original strategy may have been to wait until the driver makes an initiating action before presenting propulsion activation information
  - How to develop a user interface to guide the driver through “OFF” or “Let Run” options

Lessons to Share From This Example

- Assess, and redesign if necessary, the control structure based on potential shortcomings or trade-off study feedback.
  - Requirements to prevent or manage potential hazardous states for driver and occupants due to an erroneous or inadvertent driver action
  - Requirements for shift-by-wire or brake system to secure vehicle upon driver exit can be defined early

Lessons to Share From This Example

- Joint use of STPA between system safety engineers and system design groups helps to:
  - …think beyond a "failed" component perspective (e.g., FMEA or FTA)
  - …consider a "controls" design perspective and system usage scenarios that could lead to control actions being improperly executed or not executed
  - …evaluate causal scenarios that enable UCAs to occur and prevent or manage these scenarios by defining appropriate requirements

Virtual Button & Graphical Interface System Safety Evaluation Using STPA

Questions??