Engineering for Humans: STPA Analysis of an Automated Parking System

John Thomas and Megan France

Systems Engineering Research Lab

Partnership for a Systems Approach to Safety

Massachusetts Institute of Technology

Cambridge, MA

June 1, 2016

Prepared for General Motors

Table of Contents

Table of Contents 2
List of Acronyms and Abbreviations 3
1: Introduction 4
1.1: Purpose and Motivation 4
1.2: STAMP and STPA 4
1.3: Human Factors 5
1.4: Objectives and Scope 9
2: Automated Parking Assist 10
2.1 Types of Automated Driving Features 10
2.2: Automated Parking Assist 11
2.3: Detailed System Descriptions 11
2.4: Summary and Comparison of APA Systems 15
3: Systems-Theoretic Process Analysis (STPA) 17
3.1: STPA Method Overview 17
3.2: Application to Automated Park Assist 20
4: STPA Extension - Engineering for Humans 27
4.1: Engineering for Humans Method Overview 27
4.2: Application to Automated Park Assist 30
4.3 Summary of New Human Controller Model Findings 34
5: New Approach to Engineering Solutions for Humans 35
5.1: Matrix for Engineering Solutions for Humans (MESH) Method 35
5.2: Application to Automated Park Assist 36
6: Conclusions 40
References 41
Appendices 42
Appendix A: Safety Control Structures 43
Appendix B: Unsafe Control Actions 47
Appendix C: Traditional STPA Causal Scenarios 66
Appendix D: Scenarios Using New STPA Extension 71

List of Acronyms and Abbreviations

GM	General Motors
MIT	Massachusetts Institute of Technology
MMB	Mental Model of Process Behavior
MME	Mental Model of the Environment
MMS	Mental Model of Process State
MMU	Mental Model Updates
PM	Process Model
PSAS	Partnership for a Systems Approach to Safety
S	Control Action Selection
SAE	Society of Automotive Engineers
SERL	Systems Engineering Research Lab
STAMP	Systems Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
UCA	Unsafe Control Action

1: Introduction

1.1: Purpose and Motivation

Modern automobiles are incorporating more and more advanced features such as automated parking, lane keeping assist, adaptive cruise control, and a growing number of automated or semi-automated systems. Increasingly complex behaviors are now being incorporated into safety-critical software and there are very few physical constraints that limit the complexity of the automotive features. While this has allowed many innovative features that were not possible in the past, the additional complexity has the potential to introduce new problems such as driver mode confusion and new types of human error. These issues are frequently being discovered late in development, testing, and even during production when the problems are the most expensive to fix and when the range of practical solutions is the most limited. For example, in December 2011 the National Highway Traffic Safety Administration said that keyless ignition vehicles presented a "clear safety problem" related to driver interactions with the system, and they proposed changes to the way these systems are allowed to operate (Weisbaum, 2016). As more complex features are being introduced, there is a growing need for effective and efficient engineering methods to understand and anticipate driver interactions with these systems.

STPA (System Theoretic Process Analysis) is a hazard analysis method that was developed to handle the increased complexity of modern systems, including interactions between many different types of components. In this report, an extension to STPA is proposed to anticipate potentially unsafe driver interactions, identify potential causes of these interactions, and help the engineering team develop solutions that address these interactions.

1.2: STAMP and STPA

STAMP: Systems-Theoretic Accident Model and Processes

System-Theoretic Accident Model and Processes (STAMP) was developed to capture more types of accident causal factors including social and organizational structures, design and requirements flaws, and dysfunctional interactions among non-failed components (Leveson, 2012). Rather than treating safety as a failure problem or simplifying accidents to a linear chain of events, STAMP treats safety as a control problem in which accidents arise from complex dynamic processes that may operate concurrently and interact to create unsafe situations. Accidents can then be prevented by identifying and enforcing constraints on component interactions. This model captures accidents due to component failure, but also explains increasingly common *component interaction accidents* that occur in complex systems without any component failures. For example, software can create unsafe situations by behaving exactly as instructed or operators and automated controllers can individually perform as intended but together they may create unexpected or dangerous conditions.

STPA: Systems-Theoretic Process Analysis

STPA is a hazard analysis method based on STAMP. It differs from traditional hazard analysis techniques (including Fault Tree Analysis, Event Tree Analysis, and HAZOP) by including a broader range of factors like systemic influences and social, organizational, and management factors that are not captured by other methods.

In STPA, the analyst must determine what kinds of accidents must be prevented and define what constitutes a "hazardous state." This determines the scope of the analysis. The analyst can then state the

high-level constraints necessary to prevent these hazardous states. The rest of the analysis then systematically identifies causes and scenarios that violate the high-level constraints.

There are two steps to an STPA analysis. Step 1 identifies "unsafe control actions," or actions which could lead to a hazardous state. Unsafe control actions may be performed by any controller, whether human or software. Step 2 considers the ways in which each unsafe control action may occur, as well as the ways in which safe control actions may not be followed or executed. These "causal scenarios" describe the context in which unsafe behaviors can occur and may include factors throughout the system that contribute to those behaviors. When human controllers are involved, human engineering principles can be used to understand the reasoning behind unsafe actions.

1.3: Human Factors

The field of human factors examines the relationships between humans and technology. It is concerned with interactions, both physical and cognitive, between the human and their tasks, as well as the quality of performance on those tasks - this performance is often examined in terms of speed, accuracy, and attentional demands. (Wickens, Hollands, Banbury & Parasuraman, 2013)

A number of human models have been developed to examine relationships between humans and technology. One popular model known as the human information processing model is shown in Figure 1 below (Wickens, Hollands, Parasuraman, & Banbury, 2013). This model summarizes the process through which environmental input passes from the sensory system through stages of perception, working memory (or cognition), and the final selection and execution of a decision, which in turn influences the environment.

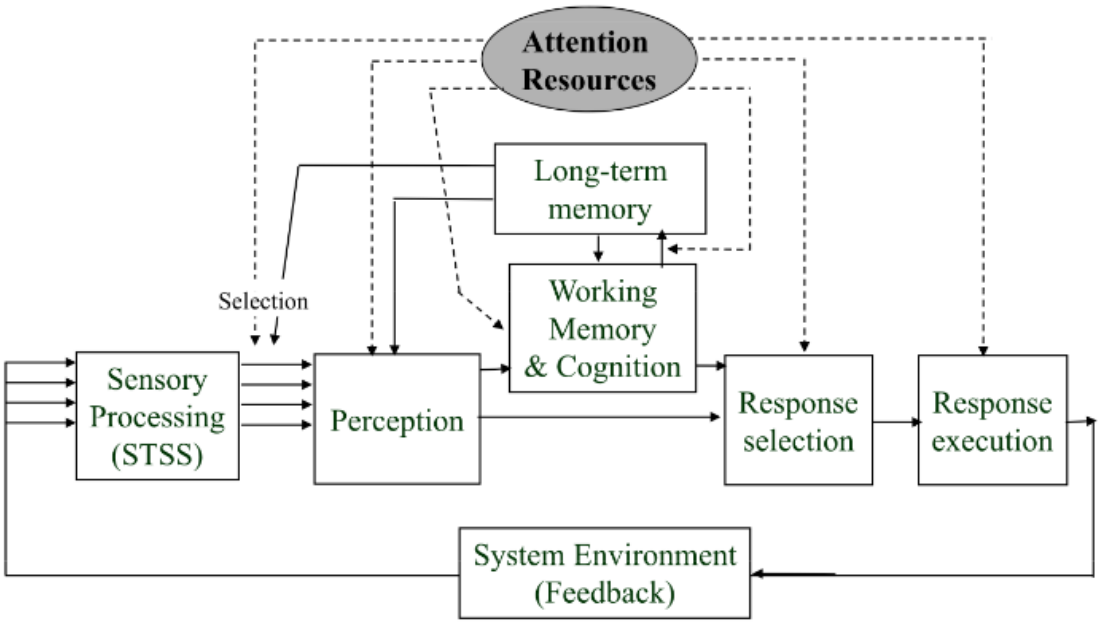


Figure 1: Human information-processing model. (Wickens, Hollands, Banbury & Parasuraman, 2013)

Another version of this model divides information processing into "Perceptual" "Cognitive" and "Action" stages, as shown in Figure 2 (Wickens, Hollands, Parasuraman, & Banbury, 2013).

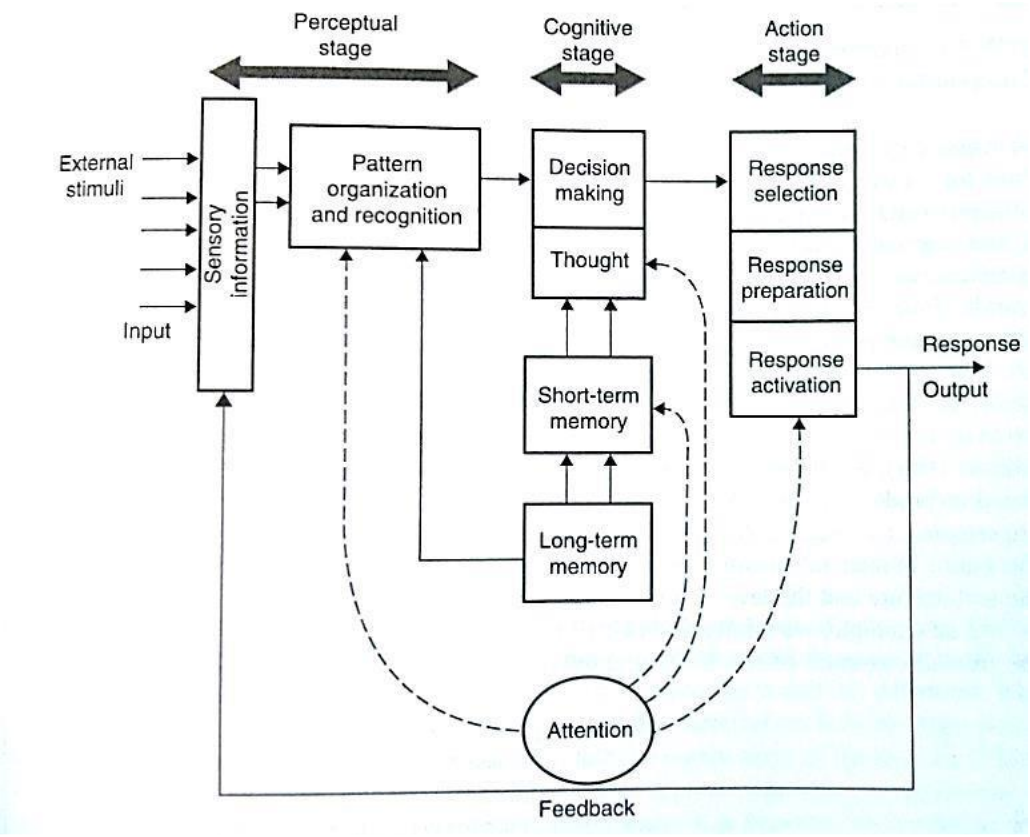


Figure 2: Human information-processing model with perceptual, cognitive, and action phases (Wickens, Hollands, Parasuraman, & Banbury, 2013).

Other models, such as Rasmussen's 1982 taxonomy of human errors (Figure 3) provide a different way of visualizing this process. In this case, information processing is broken into "skill-based," "rule-based" and "knowledge-based" levels.

- At the skill-based level, an action is selected almost automatically as soon as the features of a situation are recognized. This is related to concepts of muscle memory. For example, when a driver wants to stop her car, she presses the brake with an appropriate level of force. She does not need to think about it carefully; the action is almost automatic.

- At the rule-based level, the situation must be recognized and classified as a familiar type of situation, at which point the operator may rely upon his or her mental rules for that type of situation. For example, when a driver hears a police siren or ambulance, she relies on rules for how to act: in this case, the proper action is to pull over. Once the sound is recognized and categorized as a siren, the driver knows the right action to take.

- At the knowledge-based level, the operator does not have stored rules for the situation and must attempt to predict and evaluate possible outcomes of his or her action based on their knowledge of the system. A decision is then based on the results of this mental simulation. For example, when a driver is passing through an unfamiliar intersection, she will have to make a more complex decision than the previous examples. She may evaluate signage to determine which lanes will lead which directions, and consider any maps that she has seen of the area. She will then pick a lane and direction to take based on her belief about the outcome of that action.

At each of these three levels, different types of error or unsafe action may arise.

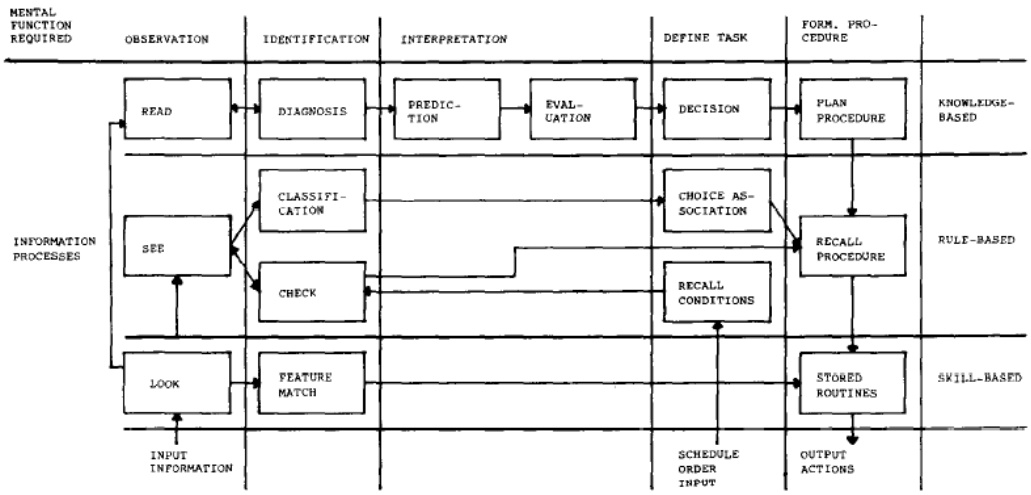


Figure 3: "The diagram illustrates how the same required mental function can be served by different information processes, each with particular error mechanisms" (Rasmussen, 1982).

Some models have attempted to directly show the interactions between humans and technology. Sheridan is well known for defining and modeling levels of automation, as shown in Figure 4 (Sheridan, 1992). These ideas have had a significant influence on human factors work today, including the classification of levels of automotive automation defined by the Society of Automotive Engineers (SAE J3016, 2014).

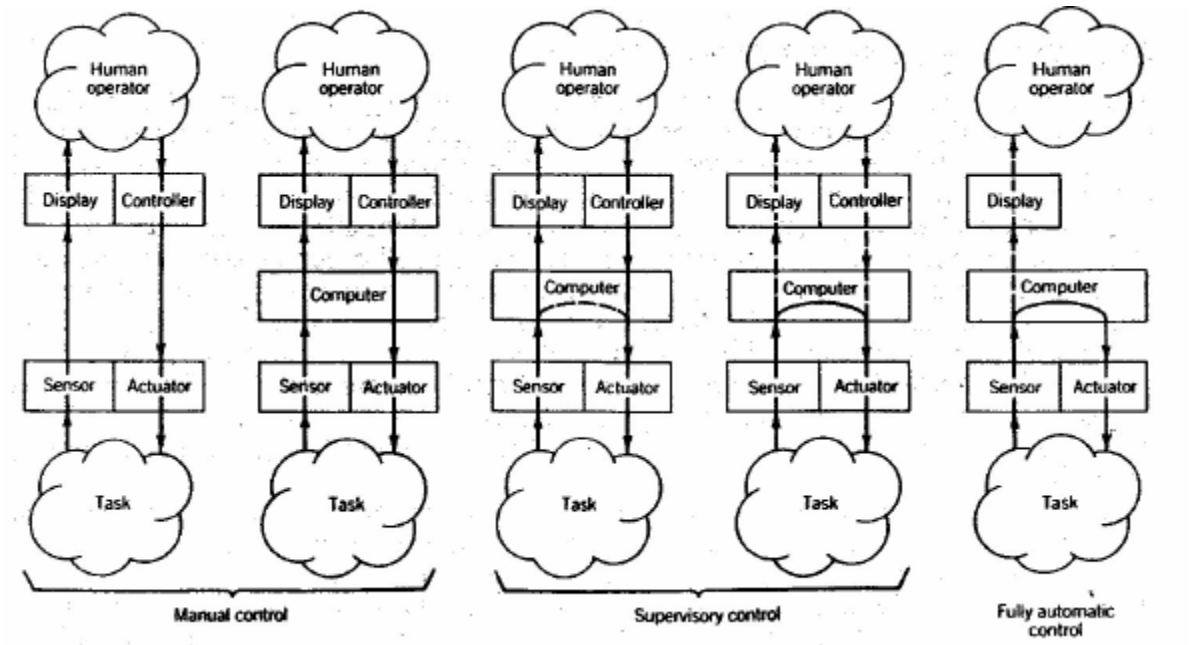


Figure 4: The spectrum of control modes. Broken line indicates minor control loops are closed through computer, major loops through human. Solid line indicates major loops are closed through computer, minor loops through human (Sheridan, 1992).

Models such as these can be very useful tools for understanding human cognitive processes. However, there are a number of limitations which reduce their usefulness.

First, these models are rooted in psychology. Their intended use is to help understand the precise phenomena involved in human information processing. The level of detail in these models may be useful for such applications, but may be disadvantageous when seeking a method which may be used with limited time and training. A simpler model would be sufficient for the majority of engineering applications, where the focus is on human interactions within a system rather than on the inner workings of the human mind.

Second, these are models, not methods. No guidance is provided to apply these models to the analysis of a system. While measures do exist for various constructs within these models, such as measures of human perception or attentional demands, these do not fulfil the purpose of a single coherent method of system analysis.

Third, these models do not apply directly to safety. Though they provide a way to model and explain human behavior and interactions with automation, they do not provide guidance to identify specific unsafe scenarios and they do not provide any specific safety-driven tools for engineering those systems. In order to incorporate human factors concepts into the STPA process, there is need for a better way to map human cognitive processes to sources of unsafe actions.

Finally, one of the greatest limitations of human factors is that it is often examined only at the end of engineering projects, if at all. At late stages of development, there is little that can be done besides simple interface fixes. This undervalues the potential of incorporating an understanding of human needs and capabilities early in the design process – at the time where conducting STPA is also most beneficial.

To address these limitations, this work aimed to develop a new method, inspired by the body of human factors research, but which can be easily used by engineers of all backgrounds. This new method will be integrated into the existing STPA hazard analysis process. This will provide a straightforward, safety-focused method which can be used at early stages of design.

1.4: Objectives and Scope

The primary objective of this project was to develop engineering methods and tools to analyze the role of humans in complex, automated, safety-critical automotive systems. This approach is based on systems-theoretic techniques, and provides an engineering extension to the STPA method that assists the user in understanding human process models and capturing additional causal scenarios. To demonstrate this engineering extension, it will be applied to an automotive automated parking assistance feature. An additional extension will then be proposed for the development of engineering solutions.

2: Automated Parking Assist

2.1 Types of Automated Driving Features

Today's automated driving features provide a wide variety of capabilities, from relatively simple emergency braking systems to more complex autopilot systems. To make it easier to classify and understand these systems, the SAE defines five levels of automation as shown in Figure 5. The interactions between driver and automation can be studied at each of these levels.

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	**High Automation**	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Copyright © 2014 SAE International. The summary table may be freely copied and distributed provided SAE International and J3016 are acknowledged as the source and must be reproduced AS-IS.

Figure 5: Society of Automotive Engineers levels of automation (SAE J3016, 2014).

Most of the systems on the market today can be classified as "driver assistance" or "partial automation," with a growing number of proposed "conditional automation" features. In these types of system, the driver is partially responsible for the operation of the vehicle – whether they perform most tasks at all times, or only some tasks at some times. As drivers start to use these technologies, their role changes from manual to increasingly supervisory to monitory.

2.2: Automated Parking Assist

Automated Parking Assist (APA) is one of many automated driving technologies currently available. It provides an interesting test case for the new methods proposed in this report because parking requires many different types of control: steering, braking, shifting, and accelerating are all involved at some point in the task. APA technologies can also be implemented at high or low levels of automation.

At low levels of automation, the automated parking assist system may merely aid in steering and provide instructions to the driver. At higher levels, the system may provide steering, braking, shifting, and acceleration commands while the driver performs a supervisory role (level 2) or the driver may only be necessary as a fallback if the system is unable to operate under the current conditions (level 3).

This research examined four unique implementations of an automated park assist system, summarized in Table 1. All of these systems are hypothetical, but designed to reflect the range of features available in current vehicles on the market.

Table 1: Summary of automation capabilities for four different APA implementations. Numbering is consistent with SAE automation level; letters indicate multiple implementations within the same classification level.

	Driver Assistance	**Partial Automation**		**Conditional Automation**
	System 1	**System 2a**	**System 2b**	**System 3**
Steering	✓	✓	✓	✓
Braking	-	✓	✓	✓
Shifting and Acceleration	-	-	✓	✓
Active Event Monitoring	-	-	-	✓

2.3: Detailed System Descriptions

System 1: Driver Assistance

Procedures for Normal Operation

To begin the parking maneuver in System 1, the driver presses the APA button to engage automated parking assist. The driver then uses the directional signal to indicate the direction on which to look for parking spaces; if this step is skipped, the system will default to searching on the right side.
The driver drives forward normally while the system searches for a spot. Once a spot has been identified, the system instructs the driver to remove his or her hands from the wheel and prepare to follow instructions while the system aids in the parking maneuver.

In System 1, the APA system instructs the driver when to shift, brake, and accelerate while the APA system automatically steers as necessary to complete the parking maneuver. The driver is responsible for monitoring and avoidance of obstacles by braking or overriding steering and shutting off APA if necessary. This meets the SAE definition for a Level 1 (Driver Assistance) system:

> *"the driving mode-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task"*
>
> *(SAE J3016, 2014)*

When the parking maneuver is complete, the driver is instructed to shift into park. The driver then presses the APA button to conclude autoparking. The driver is responsible for shutting off the engine and locking the vehicle after exiting.

Overriding the Automation

There are no temporary overrides in System 1; the driver is already responsible for shifting, braking, and accelerating, and any attempt by the driver to steer will shut off the system.

Canceling the Automation

The parking maneuver will be aborted and the driver will be expected to resume manual control if the driver at any time:

- grabs the steering wheel
- accelerates past a certain speed
- presses the APA button

The system will not automatically revert to manual mode for changes in external driving conditions.

System 2a: Partial Automation

Procedures for Normal Operation

To begin the parking maneuver in System 2a, the driver presses the APA button to engage automated parking assist. The driver then uses the directional signal to indicate the direction on which to look for parking spaces; if this step is skipped, the system will default to searching on the right side.
The driver drives forward normally while the system searches for a spot. Once a spot has been identified, the system instructs the driver to remove his or her hands from the wheel and foot from the brake and prepare to follow instructions while the system aids in the parking maneuver.

In System 2a, the APA system instructs the driver when to shift and accelerate while the APA system steers and brakes as necessary to complete the parking maneuver. The driver is responsible for monitoring and avoidance of obstacles by overriding braking or overriding steering and shutting off APA if necessary. This meets the SAE definition for a Level 2 (Partial Automation) system:

> *"the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task"*
>
> *(SAE J3016, 2014)*

When the parking maneuver is complete, the driver is instructed to shift into park. The driver then presses the APA button to conclude autoparking. The driver is responsible for shutting off the engine and locking the vehicle after exiting.

Overriding the Automation

In System 2a, the driver may temporarily override the actions of the automation through *contributory braking*. This means that when the driver presses the brake pedal for a short time, the system responds to driver input and then resumes automatic control.

Canceling the Automation

The parking maneuver will be aborted and the driver will be expected to resume manual control if the driver at any time:

- grabs the steering wheel
- accelerates past a certain speed
- presses the APA button
- brakes for >2 seconds

The system will not automatically revert to manual mode for changes in external driving conditions.

System 2b: Partial Automation

Procedures for Normal Operation

To begin the parking maneuver in System 2b, the driver presses the APA button to engage automated parking assist. The driver then uses the directional signal to indicate the direction on which to look for parking spaces; if this step is skipped, the system will default to searching on the right side. The system instructs the driver to remove his or her hands from the wheel and feet from the pedals, but to remain vigilant and prepared to resume control. The system then drives the car forward while it searches for a spot, and notifies the driver when a space has been found.

In System 2b, the APA system performs all control actions necessary to complete the parking maneuver, including steering, braking, shifting, and accelerating. The driver is responsible for monitoring and avoidance of obstacles by overriding braking or acceleration or overriding steering or shifting and shutting off APA if necessary. While including more features than System 2a, System 2b also meets the SAE definition for a Level 2 (Partial Automation) system:

> *"the driving mode-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task"*
>
> *(SAE J3016, 2014)*

When the parking maneuver is complete, the system shifts into park and automatically turns off automated park assist. The driver is then notified that parking is complete. The driver is responsible for shutting off the engine and locking the vehicle after exiting.

Overriding the Automation

In System 2b, the driver may temporarily override the actions of the automation through *contributory braking*. This means that when the driver presses the brake pedal for a short time, the system responds to

driver input and then resumes automatic control. The driver may also temporarily override acceleration in the same fashion.

Canceling the Automation

The parking maneuver will be aborted and the driver will be expected to resume manual control if the driver at any time:

- grabs the steering wheel
- attempts to shift
- accelerates past a certain speed
- presses the APA button
- brakes for >2 seconds

The system will not automatically revert to manual mode for changes in external driving conditions.

System 3: Conditional Automation

Procedures for Normal Operation

To begin the parking maneuver in System 3, the driver presses the APA button to engage automated parking assist. The driver then uses the directional signal to indicate the direction on which to look for parking spaces; if this step is skipped, the system will default to searching on the right side. The system instructs the driver to remove his or her hands from the wheel and feet from the pedals, and notifies the driver that he or she will be alerted if it is necessary to resume manual control. The system then drives the car forward while it searches for a spot, and notifies the driver when a space has been found.

In System 3 the APA system performs all control actions necessary to complete the parking maneuver, including steering, braking, shifting, and accelerating. The system is also responsible for monitoring and avoidance of obstacles; if conditions are identified which are beyond the capabilities of the system to respond, the system will alert the driver to resume manual control. System 3 meets the SAE definition for a Level 3 (Conditional Automation) system:

> *"the driving mode-specific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene"*
>
> *(SAE J3016, 2014)*

When the parking maneuver is complete, the system shifts into park and automatically turns off automated park assist. The driver is then notified that parking is complete. The driver is responsible for shutting off the engine and locking the vehicle after exiting.

Overriding the Automation

In System 3, the driver may temporarily override the actions of the automation through *contributory braking*. This means that when the driver presses the brake pedal for a short time, the system responds to driver input and then resumes automatic control. The driver may also temporarily override acceleration in the same fashion.

Canceling the Automation

The parking maneuver will be aborted and the driver will be expected to resume manual control if the driver at any time:

- grabs the steering wheel
- attempts to shift
- accelerates past a certain speed
- presses the APA button
- brakes for >2 seconds

If the system detects the need to revert to manual mode, it will alert the driver and await the driver's response. If the driver does not respond, the system will attempt to pull over and shut off the engine.

2.4: Summary and Comparison of APA Systems

The descriptions in the previous section are summarized in Table 2.

Table 2: Summary and comparison of system functionalities.

	System 1	**System 2a**	**System 2b**	**System 3**
Initiating APA	-Driver presses APA button, then uses directional signal -Driver drives forward while the system searches for a space -APA computer identifies a spot, notifies driver	-Driver presses APA button, then uses directional signal -Driver drives forward while the system searches for a space -APA computer identifies a spot, notifies driver	-Driver presses APA button, then uses directional signal -APA computer drives forward while it searches for a space -APA computer identifies a spot, notifies driver	-Driver presses APA button, then uses directional signal -APA computer drives forward while it searches for a space -APA computer identifies a spot, notifies driver
Parking maneuver	-Driver relinquishes control of steering only -Driver performs braking, shifting and acceleration as instructed	-Driver relinquishes control of steering and braking -Driver performs shifting and acceleration as instructed	-Driver relinquishes control, but monitors the APA computer closely -Driver responds to unexpected events and obstacles	-Driver relinquishes control unless alerted -System alerts driver in the event of an unexpected obstacle or unsuitable conditions for APA
Temporary overrides	N/A	-Driver may brake for short periods of time and the system will take the driver input into account	-Driver may brake for short periods of time or accelerate and the system will take the driver input into account	-Driver may brake for short periods of time or accelerate and the system will take the driver input into account
Canceling automation	-Driver grabs wheel -Driver accelerates beyond a specified speed -Driver presses APA button	-Driver grabs wheel -Driver accelerates beyond a specified speed -Driver presses brake for >2 seconds -Driver presses APA button	-Driver grabs wheel -Driver accelerates beyond a specified speed -Driver presses brake for >2 seconds -Driver presses APA button	-Driver grabs wheel -Driver accelerates beyond a specified speed -Driver presses brake for >2 seconds -Driver presses APA button
Concluding APA	-Driver is told to shift into park -Driver presses APA button to conclude	-Driver is told to shift into park -Driver presses APA button to conclude	-APA computer shifts into park -APA computer shuts off and notifies driver	-APA computer shifts into park -APA computer shuts off and notifies driver

3: Systems-Theoretic Process Analysis (STPA)

3.1: STPA Method Overview

Foundations

System Level Accidents

Before any safety analysis can be performed, it is essential to understand the types of accident that the analysis is concerned with. In Leveson's STAMP framework, an accident is defined as "an undesired and unplanned event that results in a loss, including loss of human life or injury, property damage, environmental pollution, mission loss, etc." (Leveson, 2012)

System Level Hazards

Second, when using STAMP, the system hazards must be identified. A hazard is defined as "a system state or set of conditions that, together with a particular set of worst-case environment conditions, will lead to an accident (loss)." (Leveson, 2012) Beginning the analysis with a small number of high-level hazards allows the safety practitioner to effectively analyze and control for these hazards, rather than attempting to control for many more low-level hazards and potentially overlooking important information.

Safety Control Structure

In order to understand how hazards may occur, we must build a model of the safety control structure. This is a hierarchical structure that shows the relationships between the controllers and the controlled processes in the system, including human and software controllers. Each controller can provide controls to lower-level entities in the control structure and may receive feedback to help inform future decisions. For example, Figure 6 shows a system in which a driver may provide commands directly to a vehicle or to the automation, which in turn may control the vehicle.

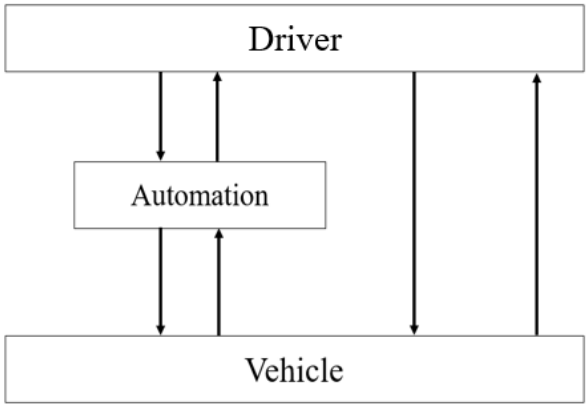


Figure 6: A simple safety control structure example.

Step 1: Unsafe Control Actions

For each control action in the safety control structure, four types of unsafe control actions can be identified:

- A control action required for safety is not provided
- An unsafe control action is provided that leads to a hazard
- A potentially safe control action provided too late, too early, or out of sequence
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action)

These "UCAs" are organized in a table as shown in Figure 7.

Control Action	Not providing causes hazard	Providing causes hazard	Too early/too late, wrong order causes hazard	Stopping too soon/applying too long causes hazard

Figure 7: Identifying Unsafe Control Actions as described in (Leveson, 2012)

Each unsafe control action has four parts:

- *Source Controller*: the controller that can provide the control action
- *Type:* one of the four types described above (provided, not provided, etc.)
- *Control Action:* the command that was provided or missing
- *Context:* the conditions for the hazard to occur

Once the unsafe control actions are identified, the following step in STPA identifies scenarios that explain why each unsafe control action might be taken.

Step 2: Causal Scenarios

For each unsafe control action, we can develop causal scenarios that explain how that control action came about. Because controllers chose actions which seem reasonable at the time, the goal is to understand how the unsafe actions might appear reasonable.

Figure 8 illustrates a number of control flaws that might occur. This is not meant to be used as a checklist – it merely provides guidance from which to begin brainstorming and developing causal scenarios. The process of generating causal scenarios relies on creativity and familiarity with the system, as well as on principles from control theory such as examining feedback loops.

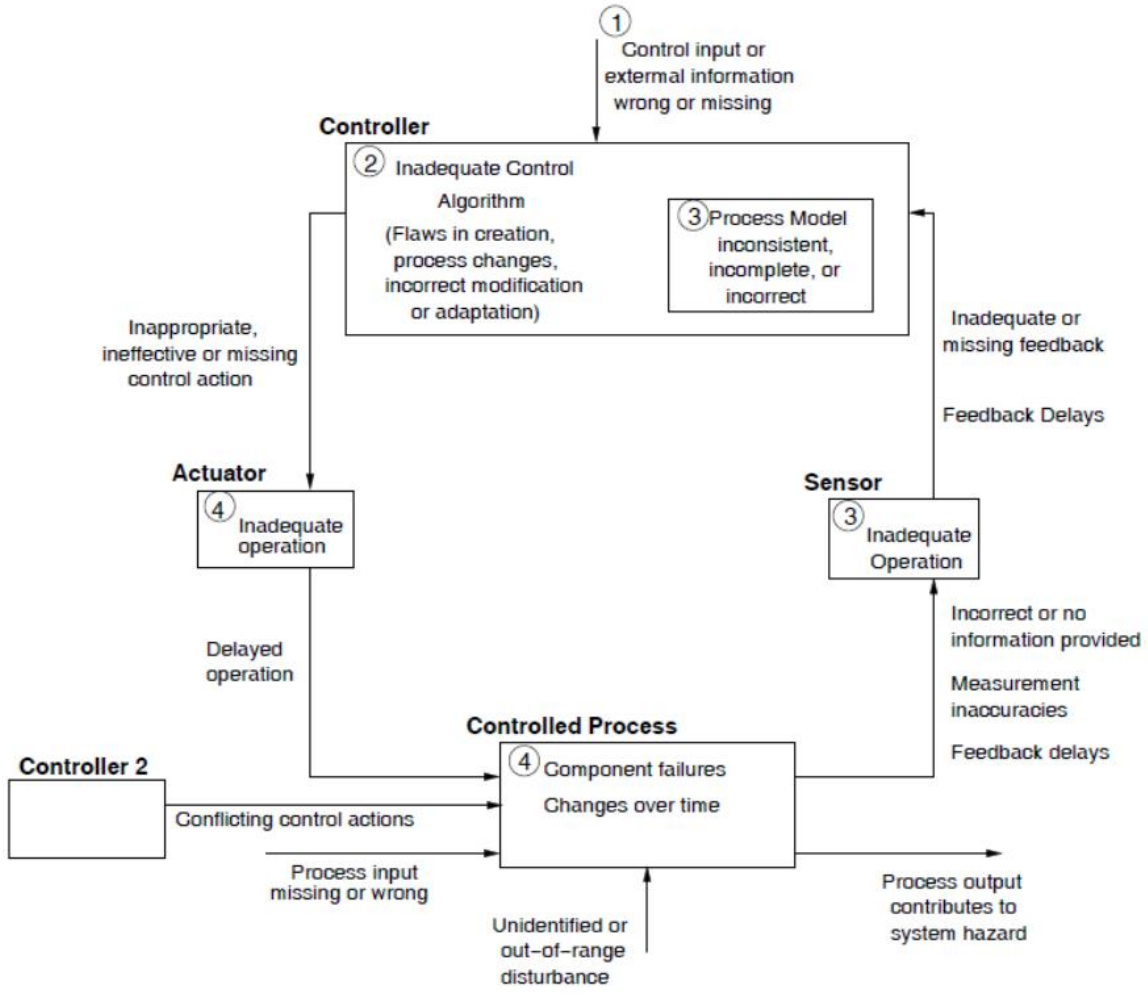


Figure 8: A classification of control flaws that can lead to hazards (Leveson, 2012)

3.2: Application to Automated Park Assist

Foundations

For any level of automation, the system-level accidents and hazards for an automated parking system are the same. Therefore, the accidents and hazards can be used in the analysis of all four systems described in this report.

System Level Accidents

The first step of this analysis was defining the system level accidents of interest.

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.

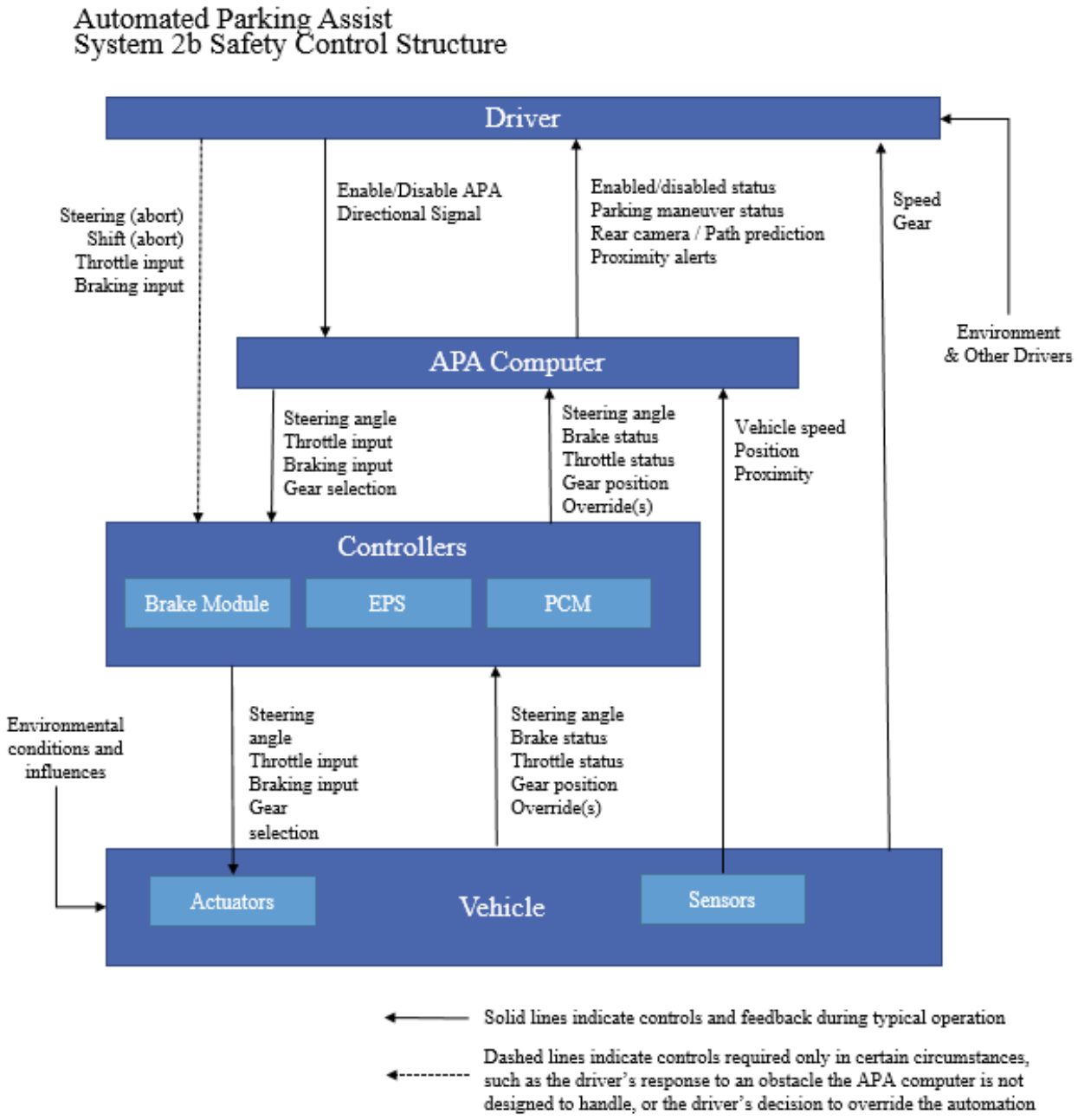
System Level Hazards

Next, we defined three system level hazards.

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]

Safety Control Structures

Below is a sample safety control structure for System 2b. Control structures for the remaining systems analyzed can be found in Appendix A: Safety Control Structures.



Step 1: Unsafe Control Actions

Table 3 and Table 4 show samples of the UCAs identified in this analysis for both software and human controllers. The full list of UCAs identified in this analysis can be found in Appendix B: Unsafe Control Actions.

Table 3: Sample software UCAs for System 2b.

Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Incorrect Timing/ Order**	**Stopped Too Soon / Applied Too Long**
Brake (APA Computer)	**UCA 2b-25:** APA computer does not brake when braking is necessary to prevent collision. [H-1]	**UCA 2b-26:** APA computer brakes when APA is disabled. [H-1] **UCA 2b-27:** APA computer brakes when doing so creates an obstruction. [H,1] **UCA 2b-28:** APA computer brakes when doing so exposes the occupants and cargo to sudden high forces. [H-2]	**UCA 2b-29:** APA computer brakes too soon to complete the maneuver. [H-3] **UCA 2b-30:** APA computer waits too long to brake to avoid collision. [H-1]	**UCA 2b-31:** APA computer continues braking for too long and stops short of completing the maneuver. [H-3] **UCA 2b-32:** APA computer does not brake for long enough to avoid collision or stop within desired bounds. [H-1]

Each of these UCAs consists of the four parts described in the previous section. For example, "APA Computer brakes when APA is off" can be decomposed as: APA Computer (*source controller*) brakes (*type = provides, control action = braking*) when APA is off (*context*).

Unsafe control actions for the human operator vary between systems as the allocation of functions to the human and the automation shifts. The UCAs reflect the driver's role as either the sole controller of a function, a supervisory controller, or a backup controller, and whether that role was performed safely.

Table 4: Sample human operator UCAs for System 2b.

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]

Note that labeling a control action as unsafe does not mean the operator is to blame for the accident. Often the actions taken appear completely reasonable within the actual context, and another operator in the same situation would have made similar choices.

Unsafe control actions were identified for all four versions of APA described in Chapter 2: Automated Parking Assist. Table 1 summarizes the UCAs identified for both the driver and the automation in each of the four versions of APA.[1]

Table 5: Summary of UCAs identified for each version of APA

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

[1] Although considering the number of UCAs may provide some insights, it should be noted that the number of UCAs do not indicate a level of safety. UCAs merely represent opportunities for unsafe behavior.

In general, as the level of automation increases from left to right, the number of unsafe control actions that can potentially be issued by the APA Computer increases. This also corresponds to an increased number of safety requirements needed to prevent unsafe behavior and an increased number of design controls or mitigations to enforce those requirements.

One might expect that the number of driver UCAs would decrease from left to right, representing fewer opportunities for unsafe driver behavior as the level of automation increases. However, Table 5 shows that this is not the case. In fact, the system with the highest level of automation (System 3) produced the highest number of driver UCAs. Although a few driver UCAs were eliminated or reduced with increased automation, many new types of driver tasks and responsibilities were introduced by increasing the automation. For example, System 3 is capable of detecting suitable environments and abnormal situations and can instruct the driver to take over control of the vehicle. This introduces several new UCAs in which the driver may not immediately resume control when instructed or they may resume control when instructed but experience delays in understanding the situation and are unable to provide appropriate controls right away.

The UCAs for each system were not all unique, in fact all of the systems included several UCAs that were shared with other systems. Table 6 summarizes the shared UCAs for each system. Figure 9 shows the number of new and unique driver UCAs that needed to be identified for each system. Because the majority of driver UCAs were found to be shared across systems, very little effort is needed to adapt the STPA results from one version of automated parking to another. Once the driver UCAs for System 1 were identified, about 80% of the identified UCAs were found to be applicable to the other systems.

Table 6: UCAs that each system has in common

	System 1	System 2a	System 2b	System 3
Driver UCAs	42	41	38	44
	35 in common		**32 in common**	
		30 in common		
APA Computer UCAs	5	13	28	28
	5 in common		**28 in common**	
		13 in common		
Total	47	54	66	72
	40 in common		**60 in common**	
		43 in common		

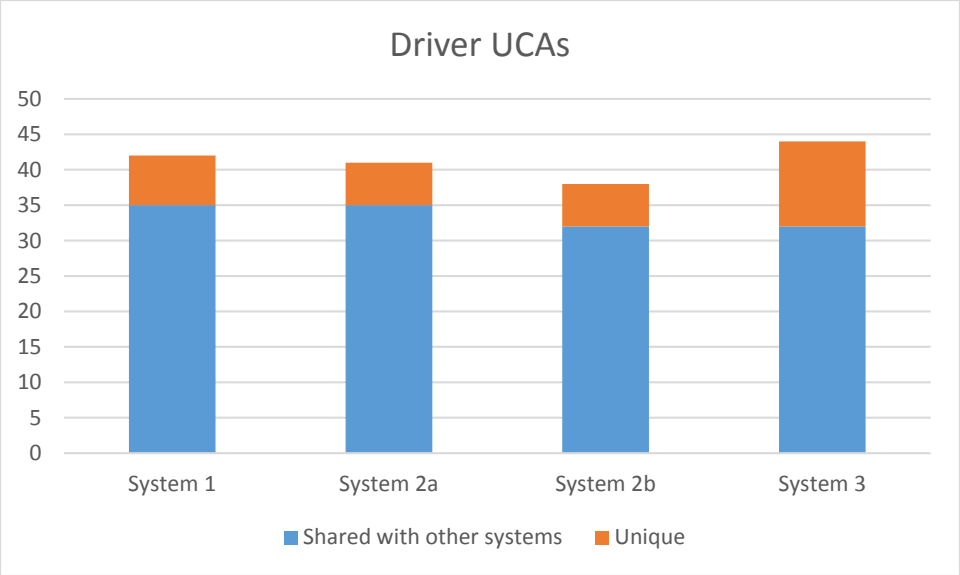


Figure 9: Driver UCAs that are shared vs. unique for each system

As shown in Figure 10, the APA Computer UCAs exhibited even more overlap. As the level of automation increased, new UCAs were introduced that did not exist previously. However the reverse is not true: increasing the level of automation simply introduced more opportunities for unsafe computer behavior, it did not eliminate any of the UCAs that were identified for lower levels of automation. In terms of requirements, additional requirements were needed as the level of automation increased while none of the requirements needed for lower levels of automation were found to be inapplicable with higher levels of automation.

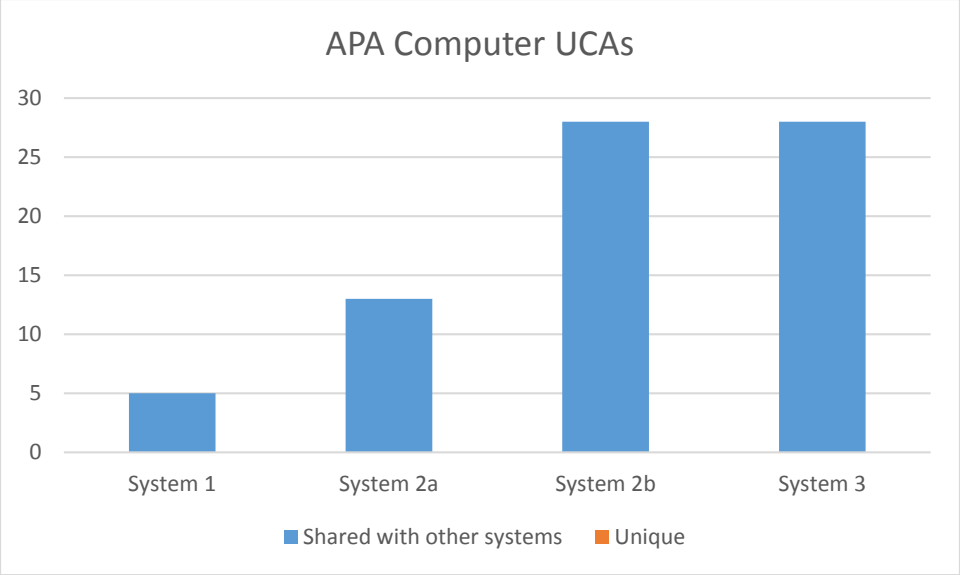


Figure 10: APA Computer UCAs that are shared vs. unique for each system

Although identifying UCAs is a necessary step in STPA, the purpose of the analysis is not just to determine what actions are "wrong" but rather to see why they may appear to be right. The next section explains STPA Step 2, which explores why UCAs might appear to be safe and correct at the time.

Step 2: Causal Scenarios

Several possible causal scenarios were identified for each UCA we analyzed. These scenarios explain how each control action came about. For example, several scenarios are shown for the UCA below.

UCA 2b-34: Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle.
[H-1]

- **Scenario 21:** While auto-parking, an obstacle appears in the vehicle's path. The driver believes the APA Computer will brake for the obstacle, therefore the driver does not brake for the obstacle (UCA 2b-34)
- **Scenario 22:** While auto-parking, an obstacle appears in the vehicle's path. The driver doesn't see the obstacle and still believes there is no obstacle. Therefore the driver does not brake for the obstacle. (UCA 2b-34)

Both of these scenarios provide plausible explanations for why the driver might not brake in that situation. Causal scenarios for the remaining UCAs analyzed can be found in Appendix C: Traditional STPA Causal Scenarios.

4: STPA Extension - Engineering for Humans

4.1: Engineering for Humans Method Overview

Since this extension is designed to support the identification of a richer set of causal scenarios, the analysis begins just as in traditional STPA. The steps for identifying accidents, hazards, the safety control structure, and unsafe control actions will not be repeated here.

The difference between this extension and a traditional STPA application lies in the generation of causal scenarios for human controllers. For any software controllers, in the system, use the approach described in the previous section. The controller section of the model is reproduced in

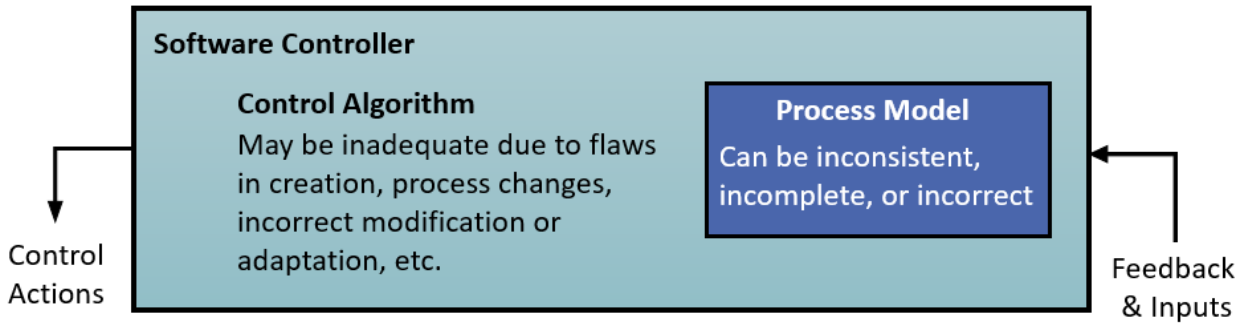


Figure 11 for easy comparison.

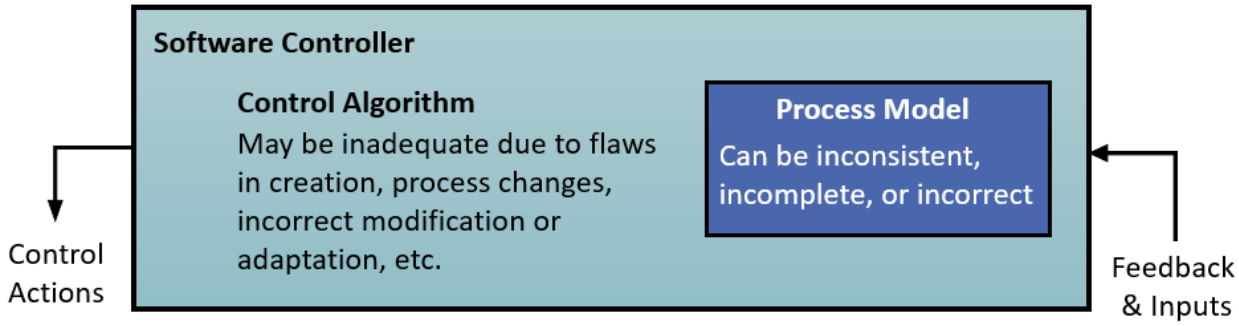


Figure 11: Basic controller model, adapted from Leveson (2012) and Leveson (2004).

For human controllers, a new model and method are proposed to support the creation of robust causal scenarios. The new model is shown in Figure 12.[2]

[2] The right-to-left flow in the new model was chosen to match the convention used in Leveson (2012) and Leveson (2004)

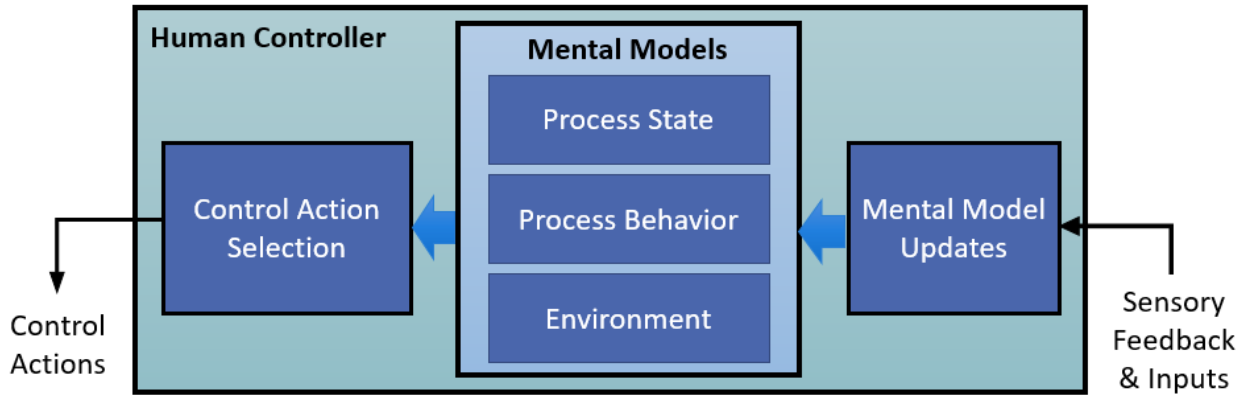


Figure 12: New human controller model.

This model draws upon a number of established human engineering models, yet maintains as much simplicity as possible to ensure that it can be learned and applied by those without extensive training and background in this area. It is meant to be used as a starting point to guide practitioners in the process of scenario generation.

In the following sections additional guidance is provided for the use of this model. For each box, a number of suggested areas to consider are presented in order to help ensure coverage.

Control Action Selection

The Control Action Selection phase corresponds to the Control Algorithm in the software controller model, and aims to explain why a particular control action is chosen.

Some factors which should be considered in this area are:

- *Goals:* Humans may have priorities besides successful completion of the parking maneuver, such as arriving on time to a destination, that affect the actions chosen. Consider the influence of these goals on the ultimate control action selection.
- *Alternatives:* The driver may not always be aware of all possible alternative actions. Consider how the mental models influence the driver's awareness of these alternatives and the prioritization of one or more alternatives over the others.
- *Automatic (skill-based) selection:* Some simple actions are performed through muscle memory. These behaviors occur in familiar situations, and entail the least amount of delay. However, as a result they also involve no careful thought or deliberate planning on behalf of the operator. Consider how these reactions may help explain the potentially unsafe behaviors identified.
- *Rule-based selection:* Slightly more complex decisions may be made based on simple rules formed through experience. Consider what rules might be developed over time to help explain the current scenario.
- *Complex (knowledge-based) selection:* In unfamiliar or complex situations, human operators will need to rely on their past experience and mental models to try to predict the outcome of their control actions. These behaviors require deliberate planning and careful thought, and as a result they can exhibit significant delays. Consider how these delays and previous experience can help explain the current scenario.

The last three points are based on Rasmussen's "Skills-Rules-Knowledge" model (1983). Although there is a significant body of literature on human decision making, the basic principles described above should serve as sufficient starting points to help understand why a control action may be selected.

Mental Models

"Mental models" in this context can be understood as cognitive representations of the world. Though more specific definitions of the term have been used by researchers across many disciplines, the broader concept of mental models has existed for decades. Kenneth Craik first proposed the idea that decision making relies on "'small-scale model[s]' of external reality" which are used to test alternatives and predict future outcomes (Craik, 1943, Ch. 5. p. 61 as cited in Johnson-Laird, 2005). This idea has been studied, described, and accepted widely in psychology and human factors communities.

Johnson-Laird (2005) emphasizes that mental models are always partial representations – even if a representation includes all *necessary* information for a particular situation, some unnecessary information must also be excluded because it is impossible to simultaneously comprehend all elements of the real world. This is an important factor in the new method; in order to understand sources of unsafe action, it is useful to examine where necessary information is absent from a model, or unnecessary or incorrect information is wrongly included.

In this representation of a human controller, mental models include the driver's understanding of the controlled process – both its state and behaviors – and the driver's understanding of the environment. The following bullet points indicate topics to consider when analyzing each of these areas.

Mental Model of Process State

- Modes: The human operator may be unaware of the current software mode, particularly if mode changes occur automatically or without feedback to the operator.
- Phase of operation: Does the operator know the current phase of operation, for processes with multiple steps or phases?

Mental Model of Process Behavior

- Mode-related behavior: If the driver has incorrect beliefs about process states or modes, their expectations about how the system will operate in that mode may differ from the actual operation in the actual mode.
- Ambiguous functions: If a single hardware control performs multiple functions, the human operator may have incorrect beliefs about how the system will behave if that control is actuated (such as being unaware of one of the functions, or being uncertain which will occur).

Mental Model of Environment

The human operator may have incorrect beliefs about the environment which can influence the selection of control actions. Issues may arise from:

- Changes: The operator may be unaware of changes that have occurred in the environment and make decisions based on outdated beliefs.
- Unfamiliar environments: The operator may have difficulty making optimum decisions in an unfamiliar environment.

- Other controllers: Consider what the operator knows (or doesn't know) about other controllers and how they will behave.

Mental Model Updates

To better understand how mental model flaws arise, it is important to examine the process of developing and updating these mental models. Factors to consider include:

- *Initial development.* When first encountering a novel situation, the operator must develop a new set of mental models based on the factors below. Later updates (once a situation becomes familiar) are necessary to maintain accurate mental models. It can be useful to distinguish between the creation of an incorrect model and the failure to update a prior model.
- *Availability of information.* While all information may technically be available, real world limitations like time pressure mean that not all of it can actually be accessed.
- *Saliency:* Which elements of the environment, process states, process behaviors, and available actions are salient? Consider how the interface design and limitations of human sensory systems may influence this.
- *Expectations:* Consider the operator's expectations based on current mental models, and how these may lead the operator to prioritize certain inputs and overlook others.
- *Effort:* Consider the effort required to access information, including process states. Information which requires greater effort, such as layers of menu interaction, is more likely to be overlooked.
- *Value:* Consider the information the operator will believe is most important. This information is likely to be prioritized in generating mental models.
- *Non-feedback inputs:* Consider new information from processes the driver does not directly control, such as instructions in the user manual or the behavior of other drivers.

The factors above draw on Wickens' SEEV Model (Wickens, & McCarley, 2007), but additional concepts of sensation, perception, and attention may be valuable to understanding this area.

Analysts can also consider the effect of self-awareness or metacognition, which affects the information the operator will seek out – or not seek out.

- Does the operator know that they are missing information, i.e. that there is a "known unknown?"
- Is the operator unaware that they are missing information, i.e., there is an "unknown unknown?"

4.2: Application to Automated Park Assist

Since the extension is part of STPA Step 2, the same accidents, hazards, and UCAs can be used as in Section 3.2: Application to Automated Park Assist. Therefore, the focus of this section will be on causal scenario generation. The following examples demonstrate how causal scenarios can be developed using the new method.

Causal Scenario Example 1

Unsafe Control Action

As usual for STPA, scenario creation begins with an unsafe control action.

> **UCA 2b-34**: Driver does not brake for an obstacle when APA is enabled and the APA computer does not react appropriately to an obstacle. . [H-1]

Scenario

The following scenario was identified using the new method:

> **Scenario 2b-34-1**: The driver does not brake for the obstacle (UCA 2b-34) because the driver incorrectly believes that the APA 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.

The relationship between the model and the elements of this scenario is shown graphically in the Figure 13.

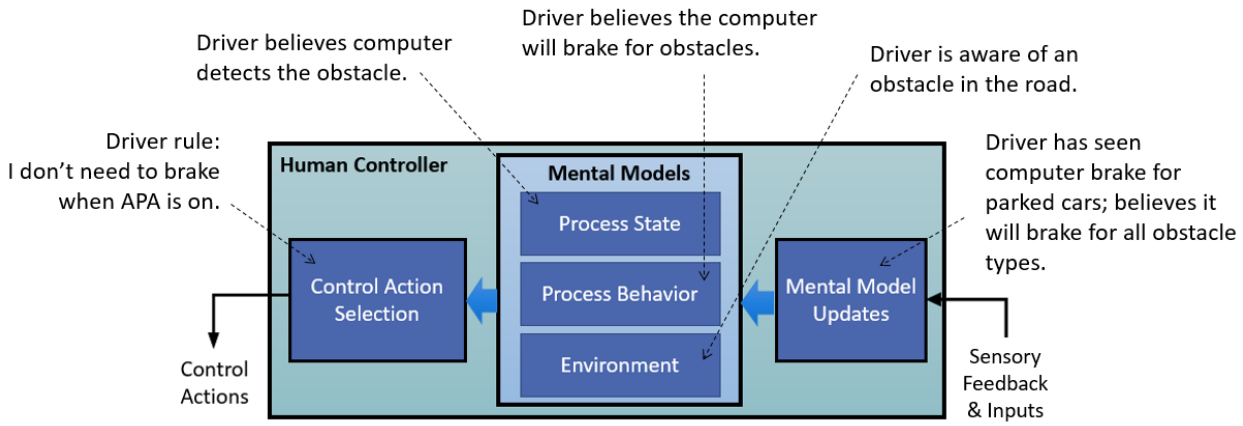


Figure 13: Causal factors relevant to Scenario Example 1.

None of these elements alone provides sufficient explanation for the driver's behavior, yet when combined they create a coherent scenario in which the behavior makes sense. Creating a graphical representation is not necessary for the use of this method, but can be a useful way to illustrate the sequence of thoughts and behaviors that occur. In Appendix D: Scenarios Using New STPA Extension a simple coding system is used as an alternate method of showing linkages between the model and scenarios.

Causal Scenario Example 2

Unsafe Control Action

This example uses the same UCA as Example 1.

> **UCA 2b-34**: Driver does not brake for an obstacle when APA is enabled and the APA computer does not react appropriately to an obstacle.

Scenario

For each UCA, multiple causal scenarios can be identified. The scenario below shares some elements with the previous, but represents a different set of thoughts and behaviors that could lead to the same unsafe action.

> **Scenario 2b-34-2**: The driver does not brake for an obstacle when APA is enabled and the APA computer does not react appropriately to an obstacle (UCA 2b-34) because the driver incorrectly believes that the APA Computer detects the obstacle ahead. She knows that braking can cancel the automation and is concerned that if she brakes unnecessarily, she will cancel the automation and need to restart the parking maneuver. She wants to avoid canceling the automation. She does not receive any feedback that the computer is unaware of the obstacle.

As before, the relationship between the model and the elements of this scenario is shown graphically in Figure 14.

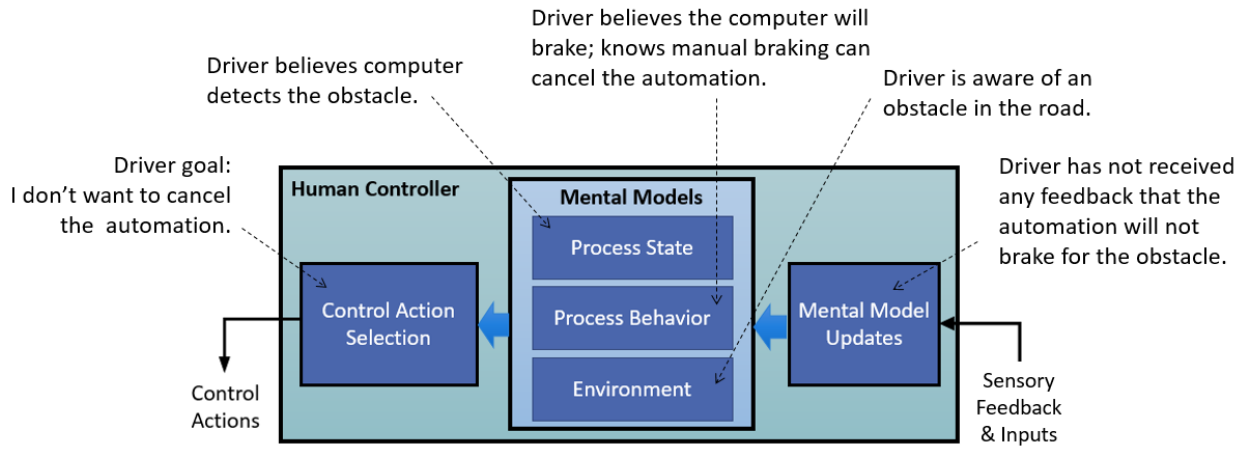


Figure 14: Causal factors relevant to Scenario Example 2.

Causal Scenario Example 3

Unsafe Control Action

> **UCA 3-19**: Driver does not resume steering when instructed to resume manual control.

Scenario

> **Scenario 3-19-1**: Driver does not take over steering when instructed (UCA 3-19) because the driver is following a mental rule that it is safe to perform secondary tasks while the automation is active, since no action is required unless a takeover alert is issued. The driver incorrectly believes there are no obstacles or hazards in the surrounding environment, and that no takeover alert has been issued. The driver overlooked both the change to the environment and the alert to takeover because he was engrossed in a secondary task.

This scenario is represented by Figure 15.

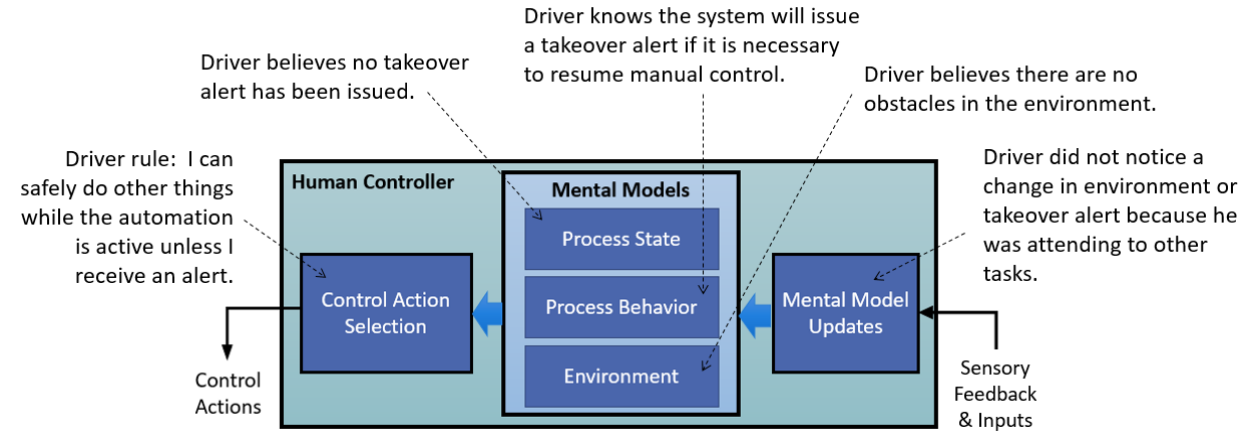


Figure 15: Causal factors relevant to Scenario Example 3.

Causal Scenario Example 4

Unsafe Control Action

This example uses the same UCA as Example 3.

> **UCA 3-19**: Driver does not resume steering when instructed to resume manual control.

Scenario

> **Scenario 3-19-2**: Driver does not resume steering when instructed (UCA 3-19) because the driver is following a mental rule to only take over driving when instructed and incorrectly believes there hasn't been a request to take over. The driver incorrectly believes the takeover alert will be a verbal instruction rather than a tone. Because the driver was not expecting a tone, the driver does not understand the meaning of the takeover alert.

This scenario is represented by Figure 16.

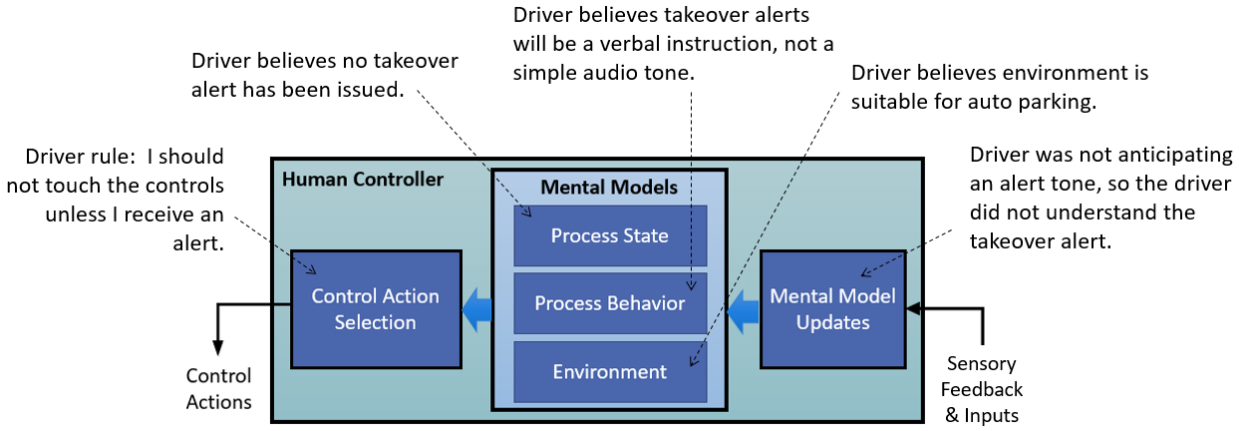


Figure 16: Causal factors relevant to Scenario Example 4.

Causal Scenario Example 5

Unsafe Control Action

> **UCA 2b-20**: Driver does not steer when APA is disabled.[3]

Scenario

> **Scenario 2b-20-1**: The driver stops providing steering commands when APA is disabled (UCA 2b-20). The driver acts on the assumption that he does not need to steer when APA is enabled, and he incorrectly believes that APA is still enabled because he did not intentionally disable it. He had grabbed the steering wheel to swerve around a small obstacle, such as a squirrel or pothole, and incorrectly assumed

[3] This UCA also exists in System 3 as UCA 3-18

this would result in a temporary override because he knows that braking can cause temporary overrides and assumes steering can do the same.

This scenario is represented by Figure 17.

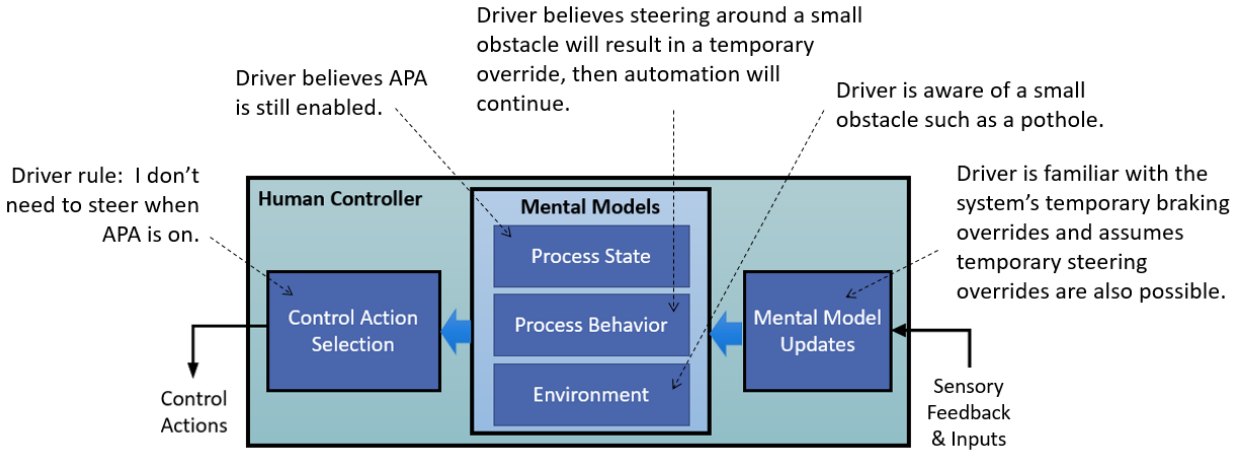


Figure 17: Causal factors relevant to Scenario Example 5.

4.3 Summary of New Human Controller Model Findings

As demonstrated by the scenarios above, each box in the model highlights a unique aspect of the human controller's thoughts and behaviors. Using this model promotes a more thorough understanding of how unsafe control actions may arise, as summarized in Figure 18.

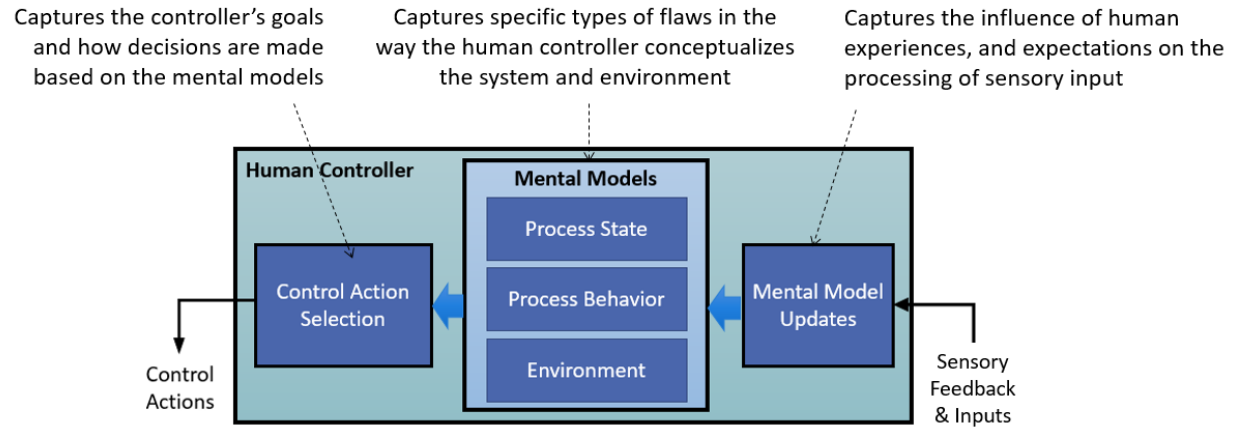


Figure 18: Summary of the new human controller model.

5: New Approach to Engineering Solutions for Humans

Too often, human engineering is considered late in the design process, when the available solutions are relatively limited. One of the greatest strengths of STPA is that it can be used in the early stages of design, when engineers have the most flexibility to solve any problems identified.

Engineers may use the causal scenarios produced in an STPA analysis to help develop powerful solutions. However, STPA does not currently provide guidance for identifying or prioritizing these solutions; this is left to engineering judgment. Therefore, a new tool is proposed to help engineers identify and prioritize solutions in order to aid these judgments.

5.1: Matrix for Engineering Solutions for Humans (MESH) Method

In order to produce solutions based on the needs of human operators, a new method of identifying and prioritizing solutions is proposed: the Matrix for Engineering Solutions for Humans, or "MESH" method. The MESH is shown in Figure 15.

Rasmussen's SRK model of decision making

Hierarchy of Controls (most effective → least effective)

	Knowledge-Based Promotes planning, formation of strong mental models, and ability to react to novel situations	**Rule-Based** Promotes pattern recognition and response and formation of reliable decision strategies	**Skill-Based** Promotes safety at the physical level
Hazard Elimination Completely remove opportunity for unsafe action altogether.	Design systems to match existing mental models and expectations. Remove extraneous operator responsibilities and design for an appropriate cognitive workload.	Avoid environments which would result in exposure to external hazards. Design out any inconsistencies or ambiguities which would create hazards within the system.	Remove potential for physical error through interlocks or full automation.
Hazard Reduction Reduce opportunity for hazards to arise and promote safe actions.	Allocate an appropriate level of human responsibility for the task. Promote accurate mental models through training, documentation, experience, etc.	Make the options available to the operator as clear and unambiguous as possible. Consider use of decision aids. Make the responsibilities of each operator (and the responsibilities and limitations of automation) clear and unambiguous.	Limit human responsibilities to tasks or conditions for which they are suited, with consideration for factors like reaction time, physical strength, etc. Provide interlocks or increase number of steps for actions which are potentially hazardous.
Hazard Control Provide means to recover from hazardous states and reverse unsafe actions.	Provide information necessary to understand how the system has diverged from the desired state and how it can be remedied.	Make emergency recovery procedures as simple and automatic as possible.	In cases where human action cannot be taken in time, use automation for fallback performance of such tasks or enter a failsafe state.
Damage Reduction Limit the severity of an accident.	N/A	N/A	Establish limitations on operation such as maximum speeds. Use protective equipment such as airbags and seatbelts.

Figure 19: Matrix for Engineering Solutions for Humans (MESH) diagram. Provides guidance for categorizing solutions based on level of processing (skills-rules-knowledge) and control hierarchy for effectiveness.

The matrix in Figure 19 is influenced by Rasmussen's "SRK" model (Rasmussen, 1983), and also on the "hierarchy of controls" (Leveson, 1995). The text in each cell describes generic examples for the types of solutions which could be considered in that category; however, these examples are not meant to be a comprehensive list. This matrix can be used as a way to help identify different types of solutions and to ensure that the identified scenarios are addressed in the design.

The hierarchy of controls, along the left column, can be used to identify which solutions will have the best impact. Solutions which fall higher on this hierarchy will be more impactful, but may not always be feasible: though it isn't possible to remove all other vehicles from the road, there are steps that can be taken to reduce the risk of colliding with them.

Controls such as creating additional rules for the driver using the automation and adding feedbacks fall low on this hierarchy. Selecting the level of automation which eliminates or minimizes the most significant hazards is a far more powerful strategy.

The three headings across the top row describe the level of decision making of the human operator. In order to provide the most effective support to human operators, it is important to consider solutions across all three of these levels. Note that in some cases, classification can be difficult; for example, a system may promote safety at the physical or "skill" level by removing the necessity for human skills. Though this seems counterintuitive, the descriptive text beneath each heading and the example solutions should serve as a guide to simplify the classification process. Furthermore, while classification is useful to understand the effectiveness of a potential solution, precise classification is not necessary to use the model to generate valuable ideas.

To apply this solutions extension, analysts should follow a three step method:

(1) Identifying Potential Solutions
First, analysts may examine individual elements of scenarios and consider potential solutions to address those elements. For example, one potential solution may address a flaw in the mental model of process behavior, while another may address a flawed control action selection strategy. These solutions may initially be very basic.

(2) Creating a Preliminary MESH
The second step is to map each of the potential solutions from step 1 into the MESH, using Figure 19 as a guide. This will provide a starting point for identifying additional solutions.

(3) Filling in the MESH
Finally, the analyst should consider possible solutions for the remaining cells in the MESH. This may be done using Figure 19 as a guide and comparing new solutions against those from steps 1 and 2. For example, the analyst may try to come up with a knowledge-level solution for hazard control, which promotes greater understanding of the system than a rule-level hazard control solution created in steps 1 and 2. Note that not all cells must be filled for each case, and multiple solutions may occupy each cell!

5.2: Application to Automated Park Assist

First, each element of the scenario is considered and solutions that correspond to those elements are brainstormed. This will create a wide range of solutions to consider that can then be prioritized as indicated in the matrix.

This application begins with an Unsafe Control Action and scenario.

UCA-2b-34: Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle. [H-1]

Scenario 2b-34-1: The driver does not brake for the obstacle (UCA 2b-34) because the driver incorrectly believes that the APA 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.

Identifying Potential Solutions

This phase of the analysis begins by breaking each scenario down into details and identifying solutions which would address each detail. This is a creative exercise; not all created solutions will be implemented, and some may not be possible. As in most effective brainstorming processes, this should be done in two steps: A) list all potential solutions without careful consideration of feasibility or practicality (to encourage creativity); B) Compare and evaluate the solutions to select the most appropriate solutions, including the potential for hybrid solutions that combine elements of multiple items on the list. For example, consider the scenario elements and potential solutions for scenario 2b-34-1 from the previous section.

Scenario Details

- Driver rule: I don't need to brake when APA is on.
- Driver believes APA computer detects the obstacle.
- Driver believes the APA computer will brake for obstacles.
- Driver has seen APA Computer brake for parked cars; believes it will brake for all obstacle types.

Potential Solutions

- Provide documentation in the manual about when the driver is responsible for braking.
- Provide feedback in the form of status displays showing what the APA computer detects and what it will do next.
- Do not automate braking if the system is not capable of braking in all scenarios.
- Develop a more highly automated system which will brake for all obstacles.

Preliminary Solutions Matrix

The potential solutions listed above can be used to populate a solutions matrix, Figure 20.

	Knowledge-Based Promotes planning, formation of strong mental models, and ability to react to novel situations	**Rule-Based** Promotes pattern recognition and response and formation of reliable decision strategies	**Skill-Based** Promotes safety at the physical level
Hazard Elimination Completely remove opportunity for unsafe action altogether.		Do not automate braking if the system is not capable of braking in all scenarios.	Develop a more highly automated system which will brake for all obstacles.
Hazard Reduction Reduce opportunity for hazards to arise and promote safe actions.		Provide documentation in the manual about when the driver is responsible for braking. Provide feedback in the form of status displays showing what the computer detects and what it will do next.	
Hazard Control Provide means to recover from hazardous states and reverse unsafe actions.			
Damage Reduction Limit the severity of an accident.			

Figure 20: Preliminary solutions matrix containing potential solutions.

The reasoning for the classification of each solution within the matrix is provided in Table 7: Justification for classification of preliminary solutions.

Table 7: Justification for classification of preliminary solutions.

Solution	**Classification**	**Justification**
Provide documentation in the manual about when the driver is responsible for braking.	Hazard reduction Rule-based	Allows the driver to form rules about when to brake and when to let the system brake, thus reducing risk. However, it does not eliminate the risk or improve the driver's overall understanding of the system's function at the knowledge level.
Provide feedback in the form of status displays showing what the APA Computer detects and what it will do next.	Hazard reduction Rule-based	Allows the driver to form rules about how to behave depending on the system status; effectively, this constitutes a decision aid.
Do not automate braking if the system is not capable of braking in all scenarios.	Hazard elimination Rule-based	Eliminates the hazard through use of consistency, allowing driver to form safe rules for behavior.
Develop a more highly automated system which will brake for all obstacles.	Hazard elimination Skill-based	Eliminates the need for the driver to brake, removing risk at the physical level.

Filling the Solutions Matrix

Next, analysts can use the partially-filled matrix to brainstorm additional solutions, resulting in a filled matrix (Figure 21). Using the guidance provided in Section 5.1: , as well as the descriptive text in the title rows and columns, analysts should consider whether any possible solution could fit in each cell.

For example, for the "Hazard Reduction, Knowledge-Based" cell, one can consider how the user could develop a stronger mental model of the system which would reduce, but not completely eliminate risks. One way to do this is to provide clear documentation regarding the system's capabilities and limitations. While documentation may not seem like a novel solution, the key detail is that the documentation must *explain the capabilities of the system*: in other words, not just "what to do" but "how it works." This type of information will be useful across a wider range of situations than the more limited, rule-based "what to do" guidance. The form this solution takes may vary. It could be simply included in the manual, or it could be something more unique, like an online video or a training session upon purchase of the vehicle.

For each other cell, solutions can be imagined in the same manner to support driver decisions at the skill-based, rule-based, or knowledge-based levels and address hazards with varying degrees of control.

	Knowledge-Based Promotes planning, formation of strong mental models, and ability to react to novel situations	**Rule-Based** Promotes pattern recognition and response and formation of reliable decision strategies	**Skill-Based** Promotes safety at the physical level
Hazard Elimination Completely remove opportunity for unsafe action altogether.	Ensure that the system will not require a driver takeover without sufficient time for the driver to assess the situation and react.	Do not automate braking if the system is not capable of braking in all scenarios.	Develop a more highly automated system which will brake for all obstacles.
Hazard Reduction Reduce opportunity for hazards to arise and promote safe actions.	Provide documentation and training regarding the capabilities and limitations of the system when it is purchased	Provide documentation in the manual about when the driver is responsible for braking. Provide feedback in the form of status displays showing what the computer detects and what it will do next.	Limit use of in-car entertainment systems while autopark is active to reduce opportunities for distraction which could reduce reaction time.
Hazard Control Provide means to recover from hazardous states and reverse unsafe actions.	N/A – the system is not aware that the environment is no longer safe so it cannot provide that information.	Simple status displays will help the driver notice that APA is not reacting.	Ensure that it is easy for the driver to brake or shut off APA quickly if they realize APA is not reacting.
Damage Reduction Limit the severity of an accident.			Maximum operating speed. When the driver initiates braking, prepare the seatbelts and airbags in case of impact.

Figure 21: Filled solutions matrix.

Once the matrix is complete, engineers may decide on a set of final solutions. Note that though "damage reduction" solutions are classified as least effective, this is not to say they are not valuable. The purpose of classifying these solutions is to implement the most effective solutions feasible, and to cross-cut the levels of decision making to ensure that the needs of the driver are well-covered. It is possible to implement solutions on multiple levels, and often favorable to do so if the constraints of the project allow. For example, providing documentation and designing a simple, intuitive status display may greatly reduce the risk that the driver will not brake; however, this does not mean there is no value in adding seatbelts! As always, this tool should be used to supplement (not replace) engineering judgement.

6: Conclusions

In this work, a new engineering tool was successfully developed to analyze the role of humans in complex, automated, safety-critical automotive systems. An engineering extension to the STPA method was created to assists in understanding human process models and capturing additional causal scenarios, as well as an extension for the development of engineering solutions. By applying these extensions to an Automated Park Assist system, it was found that they were feasible to apply to an automated driving context.

Each module of the extension was found to be useful in the analysis, and the scenarios that were identified covered a wide range of issues specific to different aspects of human cognition. In comparison to more complex human factors models and the generic controller model used in traditional STPA, this model provides an intermediate level of guidance which was successfully applied as a method to a case study. Compared to the traditional STPA approach, it was used identify scenarios with much more detail and led to additional potential solutions being identified.

The benefit of using the proposed extension compared to traditional STPA was that it provided additional guidance for creating causal scenarios. The scenarios were easier to identify using the human controller model as a starting point for creative thinking, and more interesting causal influences were identified when prompted by the method to consider specific aspects and stages of human cognition.

In addition to providing additional guidance for scenarios, an extension was provided which added a process for developing solutions. This extension was found to be valuable in both creating more solutions than brainstorming alone, and in allowing engineers to prioritize solutions based on their potential effectiveness for reducing human unsafe control actions and minimizing or eliminating hazards.

These extensions add functionality to the STPA method, while retaining all the benefits of traditional STPA such as applicability to early development efforts. As a systems-based approach, the STPA extension captured more than just physical failures; it also captured unsafe actions that occur as a result of human behavior and interactions between system elements. It facilitated understanding of a range of causal factors rather than a single root cause, and perhaps most importantly, it can be used early in the development process as a tool to guide design – allowing more effective safety measures to be implemented from the start, rather than necessitating solutions with limited effectiveness or requiring costly rework. The use of STPA with this new extension could prove valuable for any complex system involving humans.

Future work building on this extension could include: (1) having engineers test it on a real-world system to examine how much training and time is required to use it, (2) applying the extension to other automated systems to test generalizability of the findings in this report, or (3) examining issues that have arisen in automated systems and examining recall data to determine whether applying this method would have been cost-effective if used to prevent those issues. Exploration of several of these ideas for future work is currently planned to further validate this method.

References

Leveson, N. G. (2012). *Engineering a safer world: Systems thinking applied to safety.* Cambridge, MA: The MIT Press.

Leveson, N. G. (2004). *A New Accident Model for Engineering Safer Systems.* Safety science, 42(4), 237-270.

Leveson, N. G. (1995). *Safeware: System Safety and Computers.* Cambridge, MA: The MIT Press.

Johnson-Laird, P. N. (2005). *The history of mental models.* Princeton, NJ: Princeton University.

Rasmussen, J. (1982). Human errors. A taxonomy for describing human malfunction in industrial installations, *Journal of Occupational Accidents, 4,* 311-333.

SAE J 3016: Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. (2014). SAE International.

Sheridan, T. B. (1992). *Telerobotics, Automation, and Human Supervisory Control.* Cambridge, MA: The MIT Press.

Weisbaum, H. (2016, January 5). Keyless automobile ignition systems are fatally flawed, critics say. Retrieved from http://www.nbcnews.com/business/autos/keyless-automobile-ignition-systems-are-fatally-flawed-critics-say-n490111

Wickens, C. D., Hollands, J. G., Parasuraman, R., & Banbury, S. (2012). *Engineering Psychology and Human Performance*, 4th ed. Pearson.

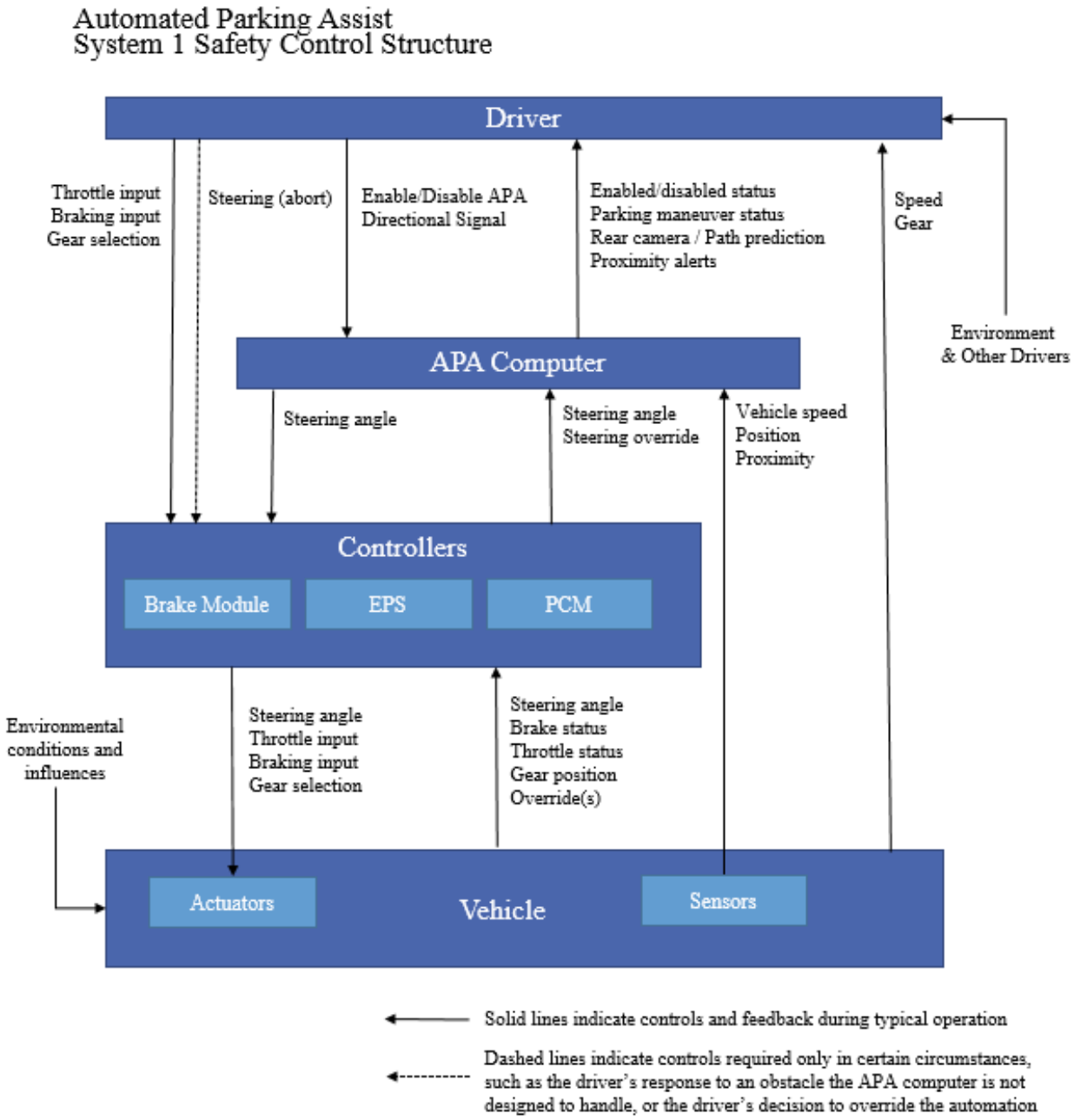
Wickens, C. D., & McCarley, J. S. (2007). *Applied Attention Theory.* Boca Raton, FL: CRC Press.

Appendices

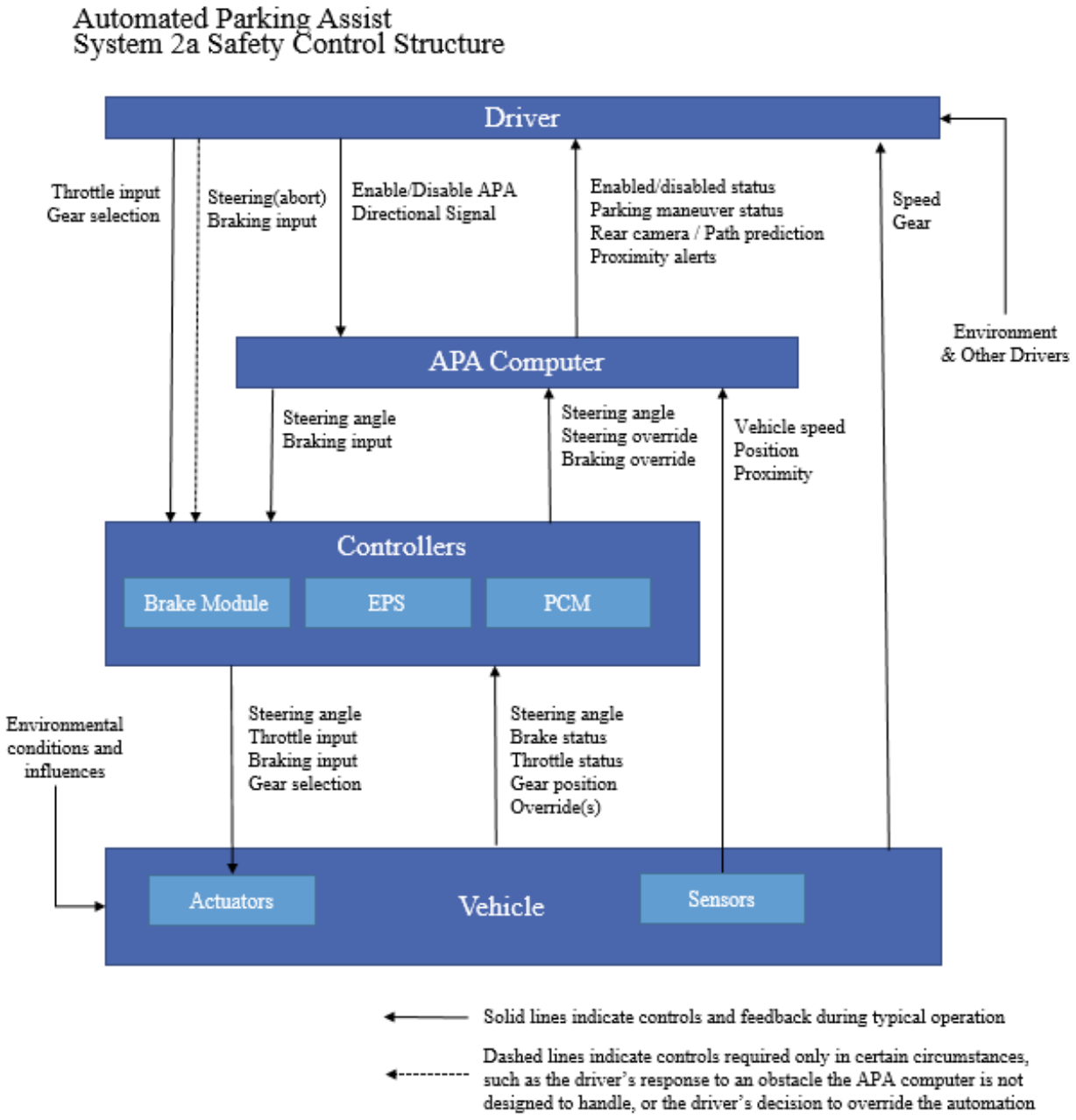
Appendix A: Safety Control Structures 43
Appendix B: Unsafe Control Actions 47
Appendix C: Traditional STPA Causal Scenarios 66
Appendix D: Scenarios Using New STPA Extension 71

Appendix A: Safety Control Structures

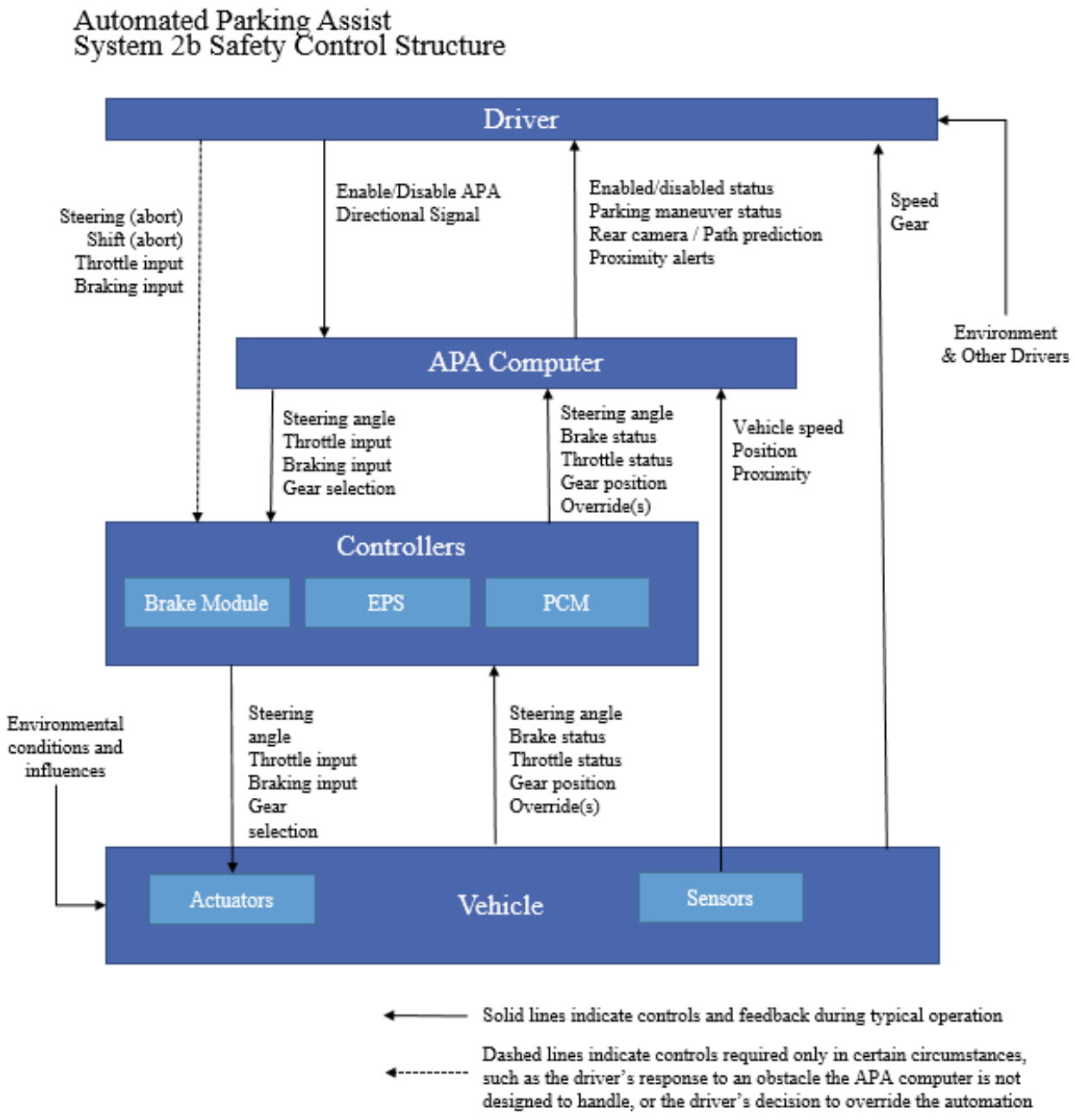
System 1: "Driver Assistance"



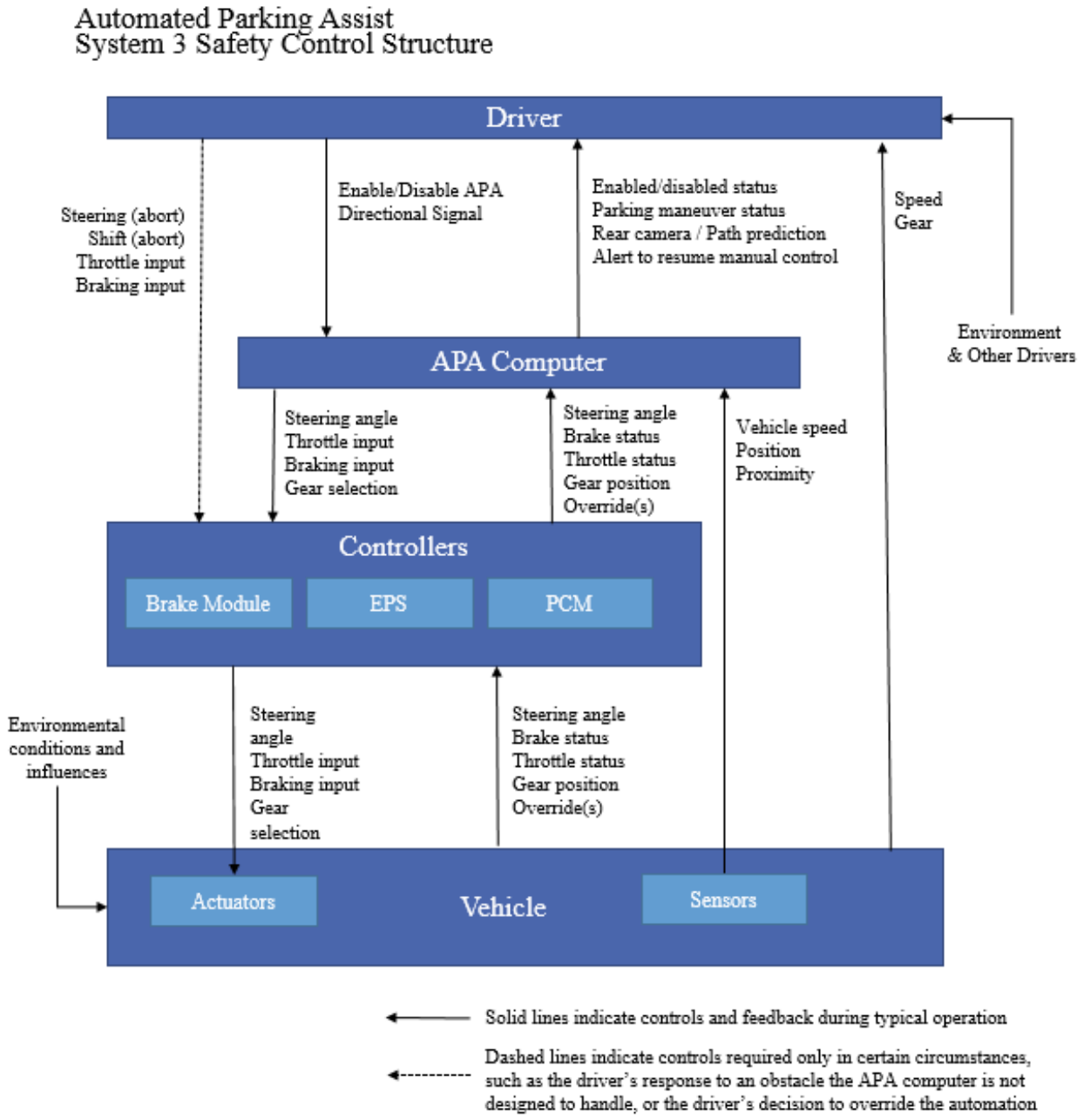
System 2a: "Partial Automation"



System 2b: "Partial Automation"



System 3: "Conditional Automation"



Appendix B: Unsafe Control Actions

System 1: "Driver Assistance"

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
Directional Signal (Driver)	**UCA 1-1:** Driver does not provide a directional signal before attempting to autopark on the non-default side. [H-1, H-3]	**UCA 1-2:** Driver provides the wrong directional signal for the direction of the desired parking space. [H-1, H-3]	**UCA 1-3:** Driver provides directional before enabling APA when attempting to autopark on the non-default side. [H-1, H-3]	**UCA 1-4:** Driver turns off directional signal before reaching a parking space when attempting to autopark on the non-default side. [H-1, H-3]
Turning on APA (Driver)	**UCA 1-5:** Driver does not provide "APA on" command when attempting to autopark [H-1].	**UCA 1-6:** Driver provides "APA on" command when not attempting to autopark [H-1]. **UCA 1-7:** Driver provides "APA on" command when conditions are not suitable for APA. [H-1, H-3]	**UCA 1-8:** Driver releases control before providing "APA on" command when doing so puts the vehicle on a collision path. [H-1]	N/A
Turning off APA (Driver)	**UCA 1-9:** Driver does not provide "APA off" command when environment is no longer suitable for APA. [H-1, H-3] **UCA 1-10:** Driver does not provide "APA off" command when APA computer is improperly parking the vehicle. [H-3]	**UCA 1-13:** Driver provides "APA off" command without resuming control when the vehicle is on a collision path. [H-1]	**UCA 1-14:** Driver provides "APA off" command too late when environment is no longer suitable.[H-1, H-3] **UCA 1-15:** Driver provides "APA off" command too late when APA computer is improperly parking the vehicle or parking in an invalid space.[H-3]	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	UCA 1-11: Driver does not provide "APA off" command when APA Computer is parking in an invalid space. [H-3] **UCA 1-12:** Driver does not provide "APA off" command when maneuver is complete. [H-1]			
Steering (APA computer)	**UCA 1-16:** APA computer does not provide steering commands when they are necessary to complete the maneuver or avoid collision. [H-1, H-3]	**UCA 1-17:** APA computer provides steering commands while APA is disabled[4]. [H-1] **UCA 1-18:** APA computer provides steering command that puts vehicle on a collision course. [H-1]	**UCA 1-19:** APA computer steers too late to complete the maneuver or avoid collision. [H-1, H-3] **UCA 1-20:** APA computer steers too early to complete the maneuver or avoid collision. [H-1, H-3]	N/A
Steering (Driver)	**UCA 1-21:** Driver does not steer when APA is disabled. [H-1] **UCA 1-22:** Driver does not steer when APA is enabled and the APA computer does not react	**UCA 1-23:** Driver attempts to steer when wheel is turning quickly. [H-2] **UCA 1-24:** Driver provides steering override that directs the vehicle toward an object. [H-1]	**UCA 1-25:** Driver takes control of the wheel too late after disabling APA. [H-1]	

[4] "Disabled" may include: (1) APA was never enabled or (2) APA was cancelled, deliberately or accidentally.

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	appropriately to an obstacle. [H-1]			
Brake (Driver)	**UCA 1-26:** Driver does not brake when APA is disabled and the vehicle is on a collision path. [H-1] **UCA 1-27:** Driver does not brake when APA is enabled and an obstacle is about to collide with the vehicle. [H-1]	**UCA 1-28:** Driver brakes when doing so puts the vehicle on a collision path. [H-1] **UCA 1-29:** Driver brakes when doing so exposes the occupants and cargo to sudden high forces. [H-2] **UCA 1-30:** Driver provides insufficient braking to avoid an obstacle. [H-1]	**UCA 1-31:** Driver brakes too early before braking is needed, putting the vehicle on a collision path. [H-1] **UCA 1-32:** Driver waits too long to brake putting the vehicle on a collision path. [H-1]	**UCA 1-33:** Driver continues braking for too long and stops short, putting the vehicle on a collision path. [H-1, H-3] **UCA 1-34:** Driver does not brake for long enough to avoid collision or stop within desired bounds. [H-1. H-3]
Shift (Driver)	**UCA 1-35:** Driver does not shift when APA is disabled and shifting is necessary to prevent a collision. [H-1] **UCA 1-36:** Driver does not shift when APA is enabled and shifting is necessary to prevent a collision. [H-1] **UCA 1-37:** Driver does not shift into park when	**UCA 1-38:** Driver shifts into a range that puts the vehicle on a collision path. [H-1]	**UCA 1-39:** Driver shifts too early when doing so puts the vehicle on a collision path. [H-1] **UCA 1-40:** Driver waits too long to shift when doing so puts the vehicle on a collision path. [H-1]	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	autoparking is complete. [H-1]			
Accelerate (Driver)	**UCA 1-41:** Driver does not accelerate when APA is disabled and acceleration is necessary to avoid creating an obstruction. [H-1] **UCA 1-42:** Driver does not accelerate when APA is enabled and acceleration is necessary to avoid creating an obstruction. [H-1]	**UCA 1-43:** Driver accelerates when doing so puts the car on a collision path. [H-1]	**UCA 1-44:** Driver accelerates before it is appropriate, putting the car on a collision path. [H-1] **UCA 1-45:** Driver waits too long to accelerate, creating an obstruction. [H-1]	**UCA 1-46:** Driver continues accelerating too long while on a collision path. [H-1] **UCA 1-47:** Driver does not accelerate for long enough to reach the desired position or to clear a collision path. [H-1, H-3]

System 2a: "Partial Automation"

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
Directional Signal (Driver)	**UCA 2a-1:** Driver does not provide a directional signal before attempting to autopark on the non-default side. [H-1, H-3]	**UCA 2a-2:** Driver provides the wrong directional signal for the direction of the desired parking space. [H-1,H-3]	**UCA 2a-3:** Driver provides directional before enabling APA when attempting to autopark on the non-default side. [H-1,H-3]	**UCA 2a-4:** Driver turns off directional signal before reaching a parking space when attempting to autopark on the non-default side. [H-1,H-3]
Turning on APA (Driver)	**UCA 2a-5:** Driver does not provide "APA on" command when attempting to autopark. [H-1]	**UCA 2a-6:** Driver provides "APA on" command when not attempting to autopark. [H-1] **UCA 2a-7:** Driver provides "APA on" command when conditions are not suitable for APA. [H-1, H-3]	**UCA 2a-8:** Driver releases control before providing "APA on" command when doing so puts the vehicle on a collision path. [H-1]	N/A
Turning off APA (Driver)	**UCA 2a-9:** Driver does not provide "APA off" command when environment is no longer suitable for APA. [H-1, H-3] **UCA 2a-10:** Driver does not provide "APA off" command when APA computer is improperly parking the vehicle. [H-3] **UCA 2a-11:** Driver does not provide "APA off" command when APA Computer is	**UCA 2a-13:** Driver provides "APA off" command without resuming control when the vehicle is on a collision path. [H-1]	**UCA 2a-14:** Driver provides "APA off" command too late when environment is no longer suitable. [H-1, H-3] **UCA 2a-15:** Driver provides "APA off" command too late when APA computer is improperly parking the vehicle or parking in an invalid space. [H-3]	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	parking in an invalid space. [H-3] **UCA 2a-12:** Driver does not provide "APA off" command when maneuver is complete. [H-1]			
Steering (APA computer)	**UCA 2a-16:** APA computer does not provide steering commands when they are necessary to complete the maneuver or avoid collision. [H-1]	**UCA 2a-17:** APA computer provides steering commands while APA is disabled. [H-1] **UCA 2a-18:** APA computer provides steering command that puts vehicle on a collision course. [H-1]	**UCA 2a-19:** APA computer steers too late to complete the maneuver or avoid collision. [H-1, H-3] **UCA 2a-20:** APA computer steers too early to complete the maneuver or avoid collision. [H-1, H-3]	N/A
Steering (Driver)	**UCA 2a-21:** Driver does not steer when APA is disabled. [H-1] **UCA 2a-22:** Driver does not steer when APA is enabled and the APA computer does not react appropriately to an obstacle. [H-1]	**UCA 2a-23:** Driver attempts to steer when wheel is turning quickly. [H-2] **UCA 2a-24:** Driver provides steering override that puts vehicle on a collision course. [H-1]	**UCA 2a-25:** Driver takes control of the wheel too late after disabling APA. [H-1]	

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
Brake (APA computer)	**UCA 2a-26:** APA computer does not brake when braking is necessary to prevent collision. [H-1]	**UCA 2a-27:** APA computer brakes when APA is disabled. [H-1] **UCA 2a-28:** APA computer brakes when doing so creates an obstruction. [H-1. H-3] **UCA 2a-29:** APA computer brakes when doing so exposes the occupants and cargo to sudden high forces. [H-2]	**UCA 2a-30:** APA computer brakes too soon to complete the maneuver. [H-3] **UCA 2a-31:** APA computer waits too long to brake to avoid collision. [H-1]	**UCA 2a-32:** APA computer continues braking for too long and stops short of completing the maneuver. [H-1, H-3] **UCA 2a-33:** APA computer does not brake for long enough to avoid collision or stop within desired bounds. [H-1, H-3]
Brake (Driver)	**UCA 2a-34:** Driver does not brake when APA is disabled and the vehicle is on a collision path. [H-1] **UCA 2a-35:** Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle. [H-1]	**UCA 2a-36:** Driver provides insufficient brake command when APA computer does not react appropriately to an obstacle. [H-1] **UCA 2a-37:** Driver provides too much brake when doing so puts other traffic on collision course or causes passenger injury. [H-1, H-2]	**UCA 2a-38:** Driver waits too long to brake after the automation does not react appropriately to an obstacle. [H-1] **UCA 2a-39:** Driver brakes too early before braking is needed, putting the vehicle on a collision path. [H-1]	**UCA 2a-40:** Driver continues override braking for too long and disables automation when doing so puts the vehicle on a collision path. [H-1] **UCA 2a-41:** Driver does not brake for long enough to avoid collision when automation is not reacting appropriately to an obstacle. [H-1]
Shift (Driver)	**UCA 2a-42:** Driver does not shift when APA is disabled and shifting is necessary to	**UCA 2a-45:** Driver shifts into a range that puts the vehicle on a collision path.	**UCA 2a-46:** Driver shifts too soon to complete maneuver or avoid collision. [H-1, H-3]	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	prevent the vehicle from being on a collision path. [H-1] **UCA 2a-43:** Driver does not shift when APA is enabled and shifting is necessary to prevent the vehicle from being on a collision path. [H-1] **UCA 2a-44:** Driver does not shift into park when autoparking is complete. [H-1]	[H-1]	**UCA 2a-47:** Driver waits too long to shift to complete the maneuver or avoid collision. [H-1, H-3]	
Accelerate (Driver)	**UCA 2a-48:** Driver does not accelerate when APA is disabled and acceleration is necessary to avoid creating an obstruction. [H-1] **UCA 2a-49:** Driver does not accelerate when APA is enabled and acceleration is necessary to avoid creating an obstruction. [H-1]	**UCA 2a-50:** Driver accelerates when doing so puts the car on a collision path. [H-1]	**UCA 2a-51:** Driver accelerates before it is appropriate, putting the car on a collision path. [H-1] **UCA 2a-52:** Driver waits too long to accelerate, creating an obstruction. [H-1]	**UCA 2a-53:** Driver continues accelerating too long while on a collision path. [H-1] **UCA 2a-54:** Driver does not accelerate for long enough to reach the desired position or clear a collision path. [H-1, H-3]

System 2b: "Partial Automation"

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
Directional Signal (Driver)	**UCA 2b-1:** Driver does not provide a directional signal before attempting to autopark on the non-default side. [H-1, H-3]	**UCA 2b-2:** Driver provides the wrong directional signal for the direction of the desired parking space. [H-1, H-3]	**UCA 2b-3:** Driver provides directional before enabling APA when attempting to autopark on the non-default side. [H-1, H-3]	**UCA 2b-4:** Driver turns off directional signal before reaching a parking space when attempting to autopark on the non-default side. [H-1, H-3]
Turning on APA (Driver)	**UCA 2b-5:** Driver does not provide "APA on" command when attempting to autopark. [H-1]	**UCA 2b-6:** Driver provides "APA on" command when not attempting to autopark. [H-1] **UCA 2b-7:** Driver provides "APA on" command when conditions are not suitable for APA. [H-1, H-3]	**UCA 2b-8:** Driver releases control before providing "APA on" command when doing so puts the vehicle on a collision path. [H-1]	N/A
Turning off APA (Driver)	**UCA 2b-9:** Driver does not provide "APA off" command when environment is no longer suitable for APA. [H-1, H-3] **UCA 2b-10:** Driver does not provide "APA off" command when APA computer is improperly parking the vehicle. [H-3] **UCA 2b-11:** Driver does not provide "APA off"	**UCA 2b-12:** Driver provides "APA off" command without resuming control when the vehicle is on a collision path. [H-1]	**UCA 2b-13:** Driver provides "APA off" command too late when environment is no longer suitable. [H-1, H-3] **UCA 2b-14:** Driver provides "APA off" command too late when APA computer is improperly parking the vehicle or parking in an invalid space. [H-1, H-3]	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	command when APA Computer is parking in an invalid space. [H-3]			
Steering (APA computer)	**UCA 2b-15:** APA computer does not provide steering commands when they are necessary to complete the maneuver or avoid collision. [H-1, H-3]	**UCA 2b-16:** APA computer provides steering commands while APA is disabled. [H-1] **UCA 2b-17:** APA computer provides steering command that puts vehicle on a collision course. [H-1]	**UCA 2b-18:** APA computer steers too late to complete the maneuver or avoid collision. [H-1, H-3] **UCA 2b-19:** APA computer steers too early to complete the maneuver or avoid collision. [H-1, H-3]	N/A
Steering (Driver)	**UCA 2b-20:** Driver does not steer when APA is disabled. [H-1] **UCA 2b-21:** Driver does not steer when APA is enabled and the APA computer does not react appropriately to an obstacle. [H-1]	**UCA 2b-22:** Driver attempts to steer when wheel is turning quickly. [H-2] **UCA 2b-23:** Driver provides steering override that puts vehicle on a collision course. [H-1]	**UCA 2b-24:** Driver takes control of the wheel too late after disabling APA. [H-1]	
Brake (APA computer)	**UCA 2b-25:** APA computer does not brake when braking is necessary to prevent collision. [H-1]	**UCA 2b-26:** APA computer brakes when APA is disabled. [H-1] **UCA 2b-27:** APA computer brakes	**UCA 2b-29:** APA computer brakes too soon to complete the maneuver. [H-3] **UCA 2b-30:** APA computer waits	**UCA 2b-31:** APA computer continues braking for too long and stops short of completing the maneuver. [H-3]

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
		when doing so creates an obstruction. [H,1] **UCA 2b-: 28**APA computer brakes when doing so exposes the occupants and cargo to sudden high forces. [H-2]	too long to brake to avoid collision. [H-1]	**UCA 2b-32:** APA computer does not brake for long enough to avoid collision or stop within desired bounds. [H-1]
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]
Shift (APA Computer)	**UCA 2b-41:** APA computer does not shift into park when the maneuver is complete. [H-1] **UCA 2b-42:** APA computer does not shift when required to avoid hitting an obstacle or creating an	**UCA 2b-43:** APA computer shifts when APA is disabled. [H-1] **UCA 2b-44:** APA computer shifts into park when vehicle is not in a valid parking spot. [H-3] **UCA 2b-45:** APA computer shifts when	**UCA 2b-46:** APA computer shifts too soon to complete the maneuver or avoid collision. [H-1, H-3] **UCA 2b-47:** APA computer waits too long to shift to complete the	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	obstruction. [H-1]	doing so would put vehicle an inappropriate distance from objects. [H-1]	maneuver or avoid collision. [H-1, H-3]	
Shift (Driver)	**UCA 2b-48:** Driver does not shift when APA is disabled and shifting is necessary to prevent the vehicle from being on a collision path. [H-1] **UCA 2b-49:** Driver does not shift when APA is enabled and the APA computer is not reacting appropriately to prevent the vehicle from being on a collision path. [H-1]	**UCA 2b-50:** Driver attempts to shift when doing so will put the vehicle on a collision path.[5] [H-1]	**UCA 2a-51:** Driver shifts too soon before shifting is needed to complete maneuver or avoid collision. [H-1, H-3] **UCA 2a-52:** Driver waits too long to shift to complete the maneuver or avoid collision when APA is enabled and the APA computer is not reacting appropriately. [H-1, H-3]	N/A
Accelerate (APA computer)	**UCA 2b-53:** APA computer does not accelerate when required to avoid creating an obstruction. [H-1]	**UCA 2b-54:** APA computer provides accelerate command when APA is disabled. [H-1] **UCA 2b-55:** APA computer provides accelerate command when doing so will put the vehicle on a collision path.	**UCA 2b-57:** APA computer accelerates before shifting into the proper gear, putting the vehicle on a collision path. [H-1] **UCA 2b-58:** APA computer waits too long to accelerate,	**UCA 2b-59:** APA computer continues accelerating too long, putting the vehicle is on a collision path. [H-1] **UCA 2b-60:** APA computer does not accelerate long enough to clear an obstacle safely. [H-1]

[5] Note that attempting to shift in System 2b or System 3 will automatically cancel the automation.

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
		[H-1] **UCA 2b-56:** APA computer accelerates too quickly when doing so exposes occupants or cargo to sudden high forces. [H-2]	creating an obstruction. [H-1]	
Accelerate (Driver)	**UCA 2b-61:** Driver does not accelerate when APA is disabled and acceleration is necessary to avoid being in the path of an approaching vehicle. [H-1] **UCA 2b-62:** Driver does not accelerate when APA is enabled the APA computer is not reacting to an approaching vehicle. [H-1]	**UCA 2b-63:** Driver provides accelerate command to override automation when doing so puts the vehicle on a collision path. [H-1]	**UCA 2b-64:** Driver provides accelerate command to override automation too late to avoid obstacles. [H-1]	**UCA 2b-65:** Driver continues accelerating too long when overriding automation, putting the vehicle on a collision path. [H-1] **UCA 2b-66:** Driver does not accelerate for long enough when overriding automation to clear an obstacle. [H-1]

System 3: "Conditional Automation"

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
Directional Signal (Driver)	**UCA 3-1:** Driver does not provide a directional signal before attempting to autopark on the non-default side. [H-1, H-3]	**UCA 3-2:** Driver provides the wrong directional signal for the direction of the desired parking space. [H-1, H-3]	**UCA 3-3:** Driver provides directional before enabling APA when attempting to autopark on the non-default side. [H-1, H-3]	**UCA 3-4:** Driver turns off directional signal before reaching a parking space when attempting to autopark on the non-default side. [H-1, H-3]
Turning on APA (Driver)	**UCA 3-5:** Driver does not provide "APA on" command when attempting to autopark. [H-1]	**UCA 3-6:** Driver provides "APA on" command when not attempting to autopark. [H-1] **UCA 3-7:** Driver provides "APA on" command when conditions are not suitable for APA. [H-1, H-3]	**UCA 3-8:** Driver releases control before providing "APA on" command when doing so puts the vehicle on a collision path. [H-1]	N/A
Turning off APA (Driver)	**UCA 3-9:** Driver does not provide "APA off" command when APA computer is improperly parking the vehicle. [H-3] **UCA 3-10:** Driver does not provide "APA off" command when APA Computer is parking in an invalid space. [H-3]	**UCA 3-11:** Driver provides "APA off" command without resuming control when the vehicle is on a collision path. [H-1]	**UCA 3-12:** Driver provides "APA off" command too late when APA computer is improperly parking the vehicle or parking in an invalid space. [H-3]	N/A
Steering (APA computer)	**UCA 3-13:** APA computer does not provide steering commands when they are necessary	**UCA 3-14:** APA computer provides steering commands while APA is disabled. [H-1]	**UCA 3-16:** APA computer steers too late to complete the	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	to complete the maneuver or avoid collision. [H-1, H-3]	**UCA 3-15:** APA computer provides steering command that puts vehicle on a collision course. [H-1]	maneuver or avoid collision. [H-1, H-3] **UCA 3-17:** APA computer steers too early to complete the maneuver or avoid collision. [H-1, H-3]	
Steering (Driver)	**UCA 3-18:** Driver does not steer when APA is disabled. [H-1] **UCA 3-19:** Driver does not take over steering when instructed to resume manual control. [H-1] **UCA 3-20:** Driver does not take over steering if the APA system malfunctions. [H-1]	**UCA 3-21:** Driver attempts to steer when wheel is turning quickly. [H-2] **UCA 3-22:** Driver provides an override steering command which directs the vehicle toward an obstacle. [H-1]	**UCA 3-23:** Driver waits too long to steer to avoid collision after being instructed to take over. [H-1] **UCA 3-24:** Driver takes control of the wheel too late after APA is disabled. [H-1]	
Brake (APA computer)	**UCA 3-25:** APA computer does not brake when braking is necessary to prevent collision. [H-1]	**UCA 3-26:** APA computer brakes when APA is disabled. [H-1] **UCA 3-27:** APA computer brakes when doing so creates an obstruction. [H-1] **UCA 3-28:** APA computer brakes when doing so exposes the	**UCA 3-29:** APA computer brakes too soon to complete the maneuver. [H-3] **UCA 3-30:** APA computer waits too long to brake to avoid collision. [H-1]	**UCA 3-31:** APA computer continues braking for too long and stops short of completing the maneuver. [H-3] **UCA 3-32:** APA computer does not brake for long enough to avoid collision or stop within desired bounds.

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
		occupants and cargo to sudden high forces. [H-2]		[H-1]
Brake (Driver)	**UCA 3-33:** Driver does not brake when APA is disabled and the vehicle is on a collision path. [H-1] **UCA 3-34:** Driver does not brake when instructed to resume manual control and braking is necessary to avoid a collision. [H-1] **UCA 3-35:** Driver does not brake if the APA system malfunctions by not reacting appropriately to an obstacle. [H-1]	**UCA 3-36:** Driver provides insufficient brake command if APA system malfunctions. [H-1] **UCA 3-37:** Driver provides an override braking command which creates an obstruction. [H-1]	**UCA 3-38:** Driver waits too long to resume control of braking after being instructed to take over. [H-1] **UCA 3-39:** Driver waits too long to brake to avoid collision if APA system malfunctions. [H-1] **UCA 3-40:** Driver brakes too early before braking is needed, putting the vehicle on a collision path. [H-1]	**UCA 3-41:** Driver stops braking too soon to avoid collision after resuming control of brakes. [H-1] **UCA 3-42:** Driver continues braking too long after resuming control of brakes and creates an obstruction. [H-1]
Shift (APA computer)	**UCA 3-43:** APA computer does not shift into park when the maneuver is complete. [H-1] **UCA 3-44:** APA computer does not shift when required to avoid hitting an obstacle or creating an	**UCA 3-45:** APA computer shifts when APA is disabled. [H-1] **UCA 3-46:** APA computer shifts into park when vehicle is not in a valid parking spot. [H-3] **UCA 3-475:** APA computer shifts when doing so would put	**UCA 3-48:** APA computer shifts too soon to complete the maneuver or avoid collision. [H-1, H-3] **UCA 3-49:** APA computer waits too long to shift to complete the maneuver or avoid collision.	N/A

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
	obstruction.[H-1]	vehicle an inappropriate distance from objects. [H-1]	[H-1, H-3]	
Shift (Driver)	**UCA 3-50:** Driver does not shift when instructed to resume manual control and shifting is necessary to avoid being on a collision path. [H-1] **UCA 3-51:** Driver does not shift when APA is disabled and shifting is necessary to avoid being on a collision path. [H-1] **UCA 3-52:** Driver does not shift if the APA system malfunctions and shifting is necessary to avoid being on a collision path. [H-1]	**UCA 3-53:** Driver attempts to shift when doing so will put the vehicle on a collision path. [H-1]	**UCA 3-54:** Driver shifts too soon before shifting is needed to complete maneuver or avoid collision. [H-1, H-3] **UCA 3-55:** Driver waits too long to shift to avoid collision after being instructed to take over. [H-1] **UCA 3-56:** Driver waits too long to shift to avoid collision after APA system malfunctions. [H-1]	N/A
Accelerate (APA computer)	**UCA 3-57:** APA computer does not accelerate when required to avoid creating an obstruction. [H-1]	**UCA 3-58:** APA computer provides accelerate command when APA is disabled. [H-1]	**UCA 3-61:** APA computer accelerates before shifting into the proper gear, putting the vehicle on a collision path.	**UCA 3-63:** APA computer continues accelerating too long, putting the vehicle is on a collision path. [H-1]

	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Order	Stopped Too Soon / Applied Too Long
		UCA 3-59: APA computer provides accelerate command when doing so will put the vehicle on a collision path. [H-1] **UCA 3-60:** APA computer accelerates too quickly when doing so exposes occupants or cargo to sudden high forces. [H-2]	**UCA 3-62:** APA computer waits too long to accelerate, creating an obstruction. [H-1]	**UCA 3-64:** APA computer does not accelerate long enough to clear an obstacle safely. [H-1]
Accelerate (Driver)	**UCA 3-65:** Driver does not accelerate when instructed to resume manual control and acceleration is necessary to avoid creating an obstruction. [H-1] **UCA 3-66:** Driver does not accelerate when APA is disabled and acceleration is necessary to avoid creating an obstruction. [H-1] **UCA 3-67:** Driver does not accelerate if the APA system malfunctions and acceleration is necessary to avoid creating an obstruction. [H-1]	**UCA 3-68:** Driver provides an override accelerate command which directs the vehicle toward an obstacle. [H-1]	**UCA 3-69:** Driver waits too long to accelerate to avoid collision after being instructed to take over. [H-1] **UCA 3-70:** Driver waits too long to accelerate to avoid collision after APA system malfunctions. [H-1]	**UCA 3-71:** Driver continues accelerating too long when overriding automation, putting the vehicle on a collision path. [H-1] **UCA 3-72:** Driver does not accelerate for long enough when overriding automation to clear an obstacle. [H-1]

Appendix C: Traditional STPA Causal Scenarios

The scenarios below all relate to human controller UCAs, and are grouped by system or automation level. Some unsafe control actions occur in multiple systems due to the similarities in the automated features of those systems, which also results in similar scenarios.

In order to illustrate the role of the human controller's process model in these scenarios, all statements regarding the driver's process model will be tagged with the letters "PM."

Note that this list is not meant to be exhaustive; it is meant simply to illustrate the breadth of scenarios captured by STPA when it is used to examine the actions of a human controller.

System 1: "Driver Assistance"

UCA 1-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 1:** Driver provides an "APA on" command when conditions are not suitable for APA because the driver incorrectly believed the conditions were suitable (PM). The driver did not realize that the system was not capable of parallel parking on curved roads.

- **Scenario 2:** Driver provides an "APA on" command when conditions are not suitable for APA because the driver incorrectly believed the system would not activate if conditions were not suitable (PM). The driver did not realize that the system sensors would not work in poor weather.

UCA 1-9: Driver does not provide "APA off" command when environment is no longer suitable for APA.

- **Scenario 3:** Driver does not provide an "APA off" command while car is in an inappropriate space – blocking a fire hydrant or in a resident only area – because the driver incorrectly believes the parking space is permissible (PM). The driver did not notice that the spot was inappropriate and the system sensors were not designed to read signs or look for fire hydrants.

UCA 1-12: Driver does not provide "APA off" command when maneuver is complete.

- **Scenario 4:** Driver does not provide an "APA off" command because the driver incorrectly believes the system had completed the parking maneuver (PM). The driver missed or did not understand system feedback.

UCA 1-38: Driver shifts into a range that puts the vehicle on a collision path.

- **Scenario 5:** Driver shifts into a range that puts the vehicle on a collision path because the driver incorrectly believed it was safe to follow the APA computer's instruction (PM). However, the controlled process had changed and an obstacle had appeared behind the car just before shifting into reverse.

- **Scenario 6:** Driver shifts into a range that puts the vehicle on a collision path because the driver incorrectly believed he or she had shifted into a different range (PM). The driver did not notice that they were not in the correct range prior to following instructions to accelerate.

UCA 1-46: Driver continues accelerating too long while on a collision path

- **Scenario 7:** Driver continues accelerating too long while on a collision path because driver incorrectly believes it is safe to continue accelerating (PM). The driver does not notice the distance to the next car diminishing because they are in reverse and relying on instructions rather than looking behind them.

- **Scenario 8:** Driver continues accelerating too long while on a collision path because driver incorrectly believes it is safe to continue accelerating (PM). The driver does not understand the feedback given by the automation directing them to release the gas pedal.

System 2a: "Partial Automation"

UCA 2a-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 9:** Driver provides an "APA on" command when conditions are not suitable for APA because the driver incorrectly believed the conditions were suitable (PM). The driver did not realize that the system was not capable of parallel parking on curved roads.

- **Scenario 10:** Driver provides an "APA on" command when conditions are not suitable for APA because the driver incorrectly believed the system would not activate if conditions were not suitable (PM). The driver did not realize that the system sensors would not work in poor weather.

UCA 2a-9: Driver does not provide "APA off" command when environment is no longer suitable for APA.

- **Scenario 11:** Driver does not provide an "APA off" command while car is in an inappropriate space – blocking a fire hydrant or in a resident only area – because the driver incorrectly believes the parking space is permissible (PM). The driver did not notice that the spot was inappropriate and the system sensors were not designed to read signs or look for fire hydrants.

UCA 2a-12: Driver does not provide "APA off" command when maneuver is complete.

- **Scenario 12:** Driver does not provide an "APA off" command because the driver incorrectly believes the system had completed the parking maneuver (PM). The driver missed or did not understand system feedback.

UCA 2a-45: Driver shifts into a range that puts the vehicle on a collision path.

- **Scenario 13:** Driver shifts into a range which puts the vehicle on a collision path because the driver incorrectly believed it was safe to follow the APA computer's instruction (PM). However, the controlled process had changed and an obstacle had appeared behind the car just before shifting into reverse.

- **Scenario 14:** Driver shifts into a range which puts the vehicle on a collision path because the driver incorrectly believed he or she had shifted into a different range (PM). The driver did not notice that they were not in the correct range prior to following instructions to accelerate.

UCA 2a-53: Driver continues accelerating too long while on a collision path.

- **Scenario 15:** Driver continues accelerating too long while on a collision path because driver incorrectly believes it is safe to continue accelerating (PM). The driver does not notice the distance to the next car diminishing because they are in reverse and relying on instructions rather than looking behind them.

- **Scenario 16:** Driver continues accelerating too long while on a collision path because driver incorrectly believes it is safe to continue accelerating (PM). The driver does not understand the feedback given by the automation directing them to release the gas pedal.

System 2b: "Partial Automation"

UCA- 2b-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 17:** Driver provides an "APA on" command when conditions are not suitable for APA because the driver incorrectly believed the conditions were suitable (PM). The driver did not realize that the system was not capable of parallel parking on curved roads.

- **Scenario 18:** Driver provides an "APA on" command when conditions are not suitable for APA because the driver incorrectly believed the system would not activate if conditions were not suitable (PM). The driver did not realize that the system sensors would not work in poor weather.

UCA 2b-20: Driver does not steer when APA is disabled.

- **Scenario 19:** The driver does not steer when APA is disabled because the driver incorrectly believes that APA is still enabled (PM). The driver did not notice or understand the indicator that APA was disabled when he grabbed the steering wheel to swerve around a small obstacle, such as a squirrel or pothole.

- **Scenario 20:** The driver does not steer when APA is disabled because the driver incorrectly believes that APA is still enabled (PM). He didn't notice or understand the indicator that APA was disabled after accidentally bumping the steering wheel while reaching for something inside the vehicle.

UCA 2b-34: Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle.

- **Scenario 27:** Driver does not brake for an obstacle because the driver incorrectly believes the APA computer will brake for the obstacle (PM). The driver does not receive feedback that the APA computer does not detect the obstacle.

- **Scenario 28:** Driver does not brake for an obstacle because the driver incorrectly believes there is no obstacle (PM). The driver did not see the obstacle.

UCA 2b-50: Driver attempts to shift when doing so will put the vehicle on a collision path.

- **Scenario 23:** Driver attempts to shift when doing so will put the vehicle on a collision path because the driver incorrectly believes the system is in the incorrect gear (PM). The gear stick does not move when shifting is performed automatically, so the driver is receiving misleading feedback about the system state.

- **Scenario 24:** Driver attempts to shift when doing so will put the vehicle on a collision path because the driver incorrectly believes the gear is unchanged (PM). The driver had bumped the gear selector accidentally, and did not notice or understand the indicator that APA was disabled.

UCA 2b-62: Driver does not accelerate when APA is enabled the APA computer is not reacting to an approaching vehicle.

- **Scenario 25:** Driver does not accelerate because the driver incorrectly believes there is no vehicle approaching (PM). The driver did not notice the other vehicle.

  Scenario 26: Driver does not provide accelerate command because the driver incorrectly believes that the APA computer detects the approaching vehicle and will accelerate out of the way (PM).

System 3: "Conditional Automation"

UCA 3-7: Driver provides "APA on" command when conditions are not suitable for APA..

- **Scenario 27:** Driver provides an "APA on" command because the driver incorrectly believed the conditions were suitable (PM). The driver did not realize that the system was not capable of parallel parking on curved roads.

- **Scenario 28:** Driver provides an "APA on" command because the driver incorrectly believed the system would not activate if conditions were not suitable (PM). The driver did not realize that the system sensors would not work in poor weather.

UCA 3-18: Driver does not steer when APA is disabled.

- **Scenario 29:** The driver stops providing steering commands because the driver incorrectly believes that APA is still enabled (PM). The driver did not notice or understand the indicator that APA was disabled when he grabbed the steering wheel to swerve around a small obstacle, such as a squirrel or pothole.

- **Scenario 30:** The driver stops providing steering commands because the driver incorrectly believes that APA is still enabled (PM). He didn't notice or understand the indicator that APA was disabled after accidentally bumping the steering wheel while reaching for something inside the vehicle.

UCA 3-19: Driver does not take over steering when instructed to resume manual control.

- **Scenario 31:** Driver does not take over steering because driver does not believe he or she needs to take over (PM). Driver did not understand instruction to take over due to the way it was presented.

- **Scenario 32:** Driver does not take over steering because driver does not believe he or she needs to take over (PM). Driver did not notice instruction to take over because the driver was involved in another activity.

UCA 3-34: Driver does not brake when instructed to resume manual control and braking is necessary to avoid a collision.

- **Scenario 33:** Driver does not take over braking when instructed to do so because the driver incorrectly believes that he is not responsible to take over (PM). The driver did not notice the alert to take over when road conditions changed.

- **Scenario 34:** Driver does not take over braking when instructed to do so because the driver incorrectly believes that he is not responsible to take over (PM). The driver noticed but did not understand the alert to take over when road conditions changed.

UCA 3-53: Driver attempts to shift when doing so will put the vehicle on a collision path

- **Scenario 35:** Driver attempts to shift because the driver incorrectly believes the system is in the incorrect gear (PM). The shift lever does not move when shifting is performed automatically, so the driver is missing feedback about the system state.

- **Scenario 36:** Driver attempts to shift because the driver incorrectly believes the gear is unchanged (PM). The driver had bumped the gear selector accidentally, and did not notice or understand the indicator that APA was disabled.

Appendix D: Scenarios Using New STPA Extension

This appendix provides scenarios that were derived from the UCAs in Appendix B: Unsafe Control Actions using the new human controller model. Scenarios were developed for the same UCAs used in Appendix C: Traditional STPA Causal Scenarios in order to highlight a variety of different issues and to enable comparisons and conclusions. To show mappings from these scenarios to the human controller model, a coding system will be used as shown in Figure 22.

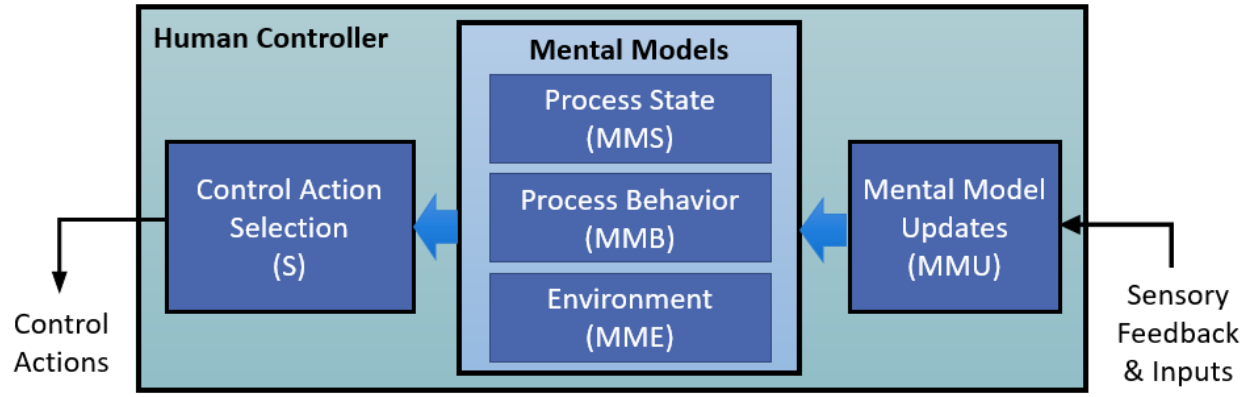


Figure 22: Coding system used for mapping scenarios to the human controller model

System 1: "Driver Assistance"

UCA 1-1: Driver does not provide a directional signal before attempting to autopark on the non-default side.

- **Scenario 1-1-1:** The driver does not provide the left directional signal (UCA 1-1) because the driver previously provided the left directional signal (S) and thinks the directional signal is still on (MMS). Before the desired spot was located, the left directional signal was automatically cancelled and the driver's corresponding mental model was not updated (MMU). The left directional signal would be automatically cancelled if the steering angle meets the corresponding threshold for turn signal cancellation.

- **Scenario 1-1-2:** The driver does not provide the directional signal (UCA 1-1) because the driver previously provided the directional signal (S) but the directional signal was automatically cancelled. The driver knows the directional signal was canceled (MMU) but believes APA will continue looking on the left (non-default) side because the feature was activated with the directional signal on (MMB).

UCA 1-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 1-7-1:** Driver provides an "APA on" command when road conditions are not suitable for APA (UCA 1-7) because the driver incorrectly believed the conditions were suitable (MME). The driver also believed that the system would detect and notify him if conditions were unsuitable (MMB). The driver did not realize that the system was not capable of parallel parking on curved roads because the driver had successfully used APA on curved roads in the past and assumed the system could do the same again (MMU). However, the driver did not realize that the

curvature of the current road was slightly more than the curvature for previous successful applications (MMS) and beyond the capabilities of the system (MMB).

- **Scenario 1-7-2:** Driver provides an "APA on" command when weather conditions are not suitable for APA (UCA 1-7) because the driver incorrectly believed conditions were suitable (MME) and the system would not activate if conditions were not suitable (MMB). The driver did not realize that the system sensors would not work in poor weather because the driver had never attempted to use the system in poor weather before (MMU).

UCA 1-9: Driver does not provide "APA off" command when environment is no longer suitable for APA.

- **Scenario 1-9-1:** Driver does not provide an "APA off" command while car is in an inappropriate space (UCA 1-9), such as blocking a fire hydrant or in a resident only area. The driver was relying on the automation to select a parking space (S) because the driver incorrectly believed the system sensors could detect unsuitable or invalid spots (MMB) and believed that the space selected was therefore appropriate (MME).

UCA 1-12: Driver does not provide "APA off" command when maneuver is complete.

- **Scenario 1-12-1:** Driver does not provide "APA off" command when maneuver is complete (UCA 1-12) because the driver did not know it was necessary to press the APA off button when the system has finished parking (S). She incorrectly believes APA will shut itself off once she shifts into park (MMB), based on past experience with a more highly automated system which did shut off automatically (MME).

UCA 1-14: Driver provides "APA off" command too late when environment is no longer suitable.

- **Scenario 1-14-1:** Driver provides an "APA off" command too late (UCA 1-14) because the driver typically makes decisions by doing as the system instructs (S) and the driver misunderstood the system instructions (MMU). The system instructions that were provided actually meant that something had gone wrong and it was necessary to resume manual parking, but the driver thought it meant that parking was complete and successful (MMU).

UCA 1-38: Driver shifts into a range which puts the vehicle on a collision path.

- **Scenario 1-38-1:** Driver shifts into a gear which puts the vehicle on a collision path (UCA 1-38) because the driver trusts the automation to make safe decisions (S). The driver incorrectly believed the APA computer was aware of any obstacles in the environment (MMS) and that the APA computer would adjust instructions accordingly (MMB). However, the driver had not realized an obstacle had appeared behind the car (MME). The driver did not notice the obstacle because they were relying solely on the automation's cues rather than visual checks (MMU).

- **Scenario 1-38-2:** Driver shifts into a gear which puts the vehicle on a collision path (UCA 1-38) because the driver intended to shift into the instructed gear (S) but made a mistake performing the action. The driver incorrectly believed he or she had shifted into the desired gear (MMS) and did not notice that they were in the wrong gear because they had already begun to perform the next step instructed (MMU).

- **Scenario 1-38-3:** Driver shifts into a range that puts the vehicle on a collision path (UCA 1-38) because the driver incorrectly believed APA feedback meant it was safe to shift (MMS). The driver believed the instructions meant that the APA computer was confirming that it was safe to shift (MMB), when in reality the APA computer was showing the next step of the autopark process, but not the absence of obstacles. An obstacle such as another car in front reversing made it unsafe to shift (MME).

UCA 1-43: Driver accelerates when doing so puts the car on a collision path. [H-1]

- **Scenario 1-43-1:** Driver accelerates when doing so puts the car on a collision path (UCA 1-43) because driver is basing decisions solely on instructions from the automation as a rule (S) and incorrectly believes it is safe to accelerate because she was instructed to accelerate (MMS). The driver believes the system will not give instructions to accelerate if there is an obstacle ahead (MMB) and is unaware of a stopped car (MME). The driver is watching the APA display for instructions (MMU) and therefore could not monitor the environment as closely as during manual parking.

UCA 1-46: Driver continues accelerating too long while on a collision path

- **Scenario 1-46-1:** Driver continues accelerating too long while on a collision path (UCA 1-46) because driver is basing decisions solely on instructions from the automation as a rule (S). The driver incorrectly believes there are no immediate obstacles in the environment (MME). The driver does not notice the distance to the next car diminishing because they are in reverse and relying on instructions rather than looking behind them (MMU).

- **Scenario 1-46-2:** Driver continues accelerating too long while on a collision path (UCA 1-46) because driver is basing decisions solely on instructions from the automation (S). The driver incorrectly believes the automation will explicitly instruct them to cease accelerating (MMB) and does not understand the meaning of the tone intended to notify them (MMU).

System 2a: "Partial Automation"

UCA 2a-1: Driver does not provide a directional signal before attempting to autopark on the non-default side.

- **Scenario 2a-1-1:** The driver does not provide the left directional signal (UCA 2a-1) because the driver previously provided the left directional signal (S) and thinks the directional signal is still on (MMS). Before the desired spot was located, the left directional signal was automatically cancelled and the driver's corresponding mental model was not updated (MMU). The left directional signal would be automatically cancelled if the steering angle meets the corresponding threshold for turn signal cancellation.

- **Scenario 2a-1-2:** The driver does not provide the directional signal (UCA 2a-1) because the driver previously provided the directional signal (S) but the directional signal was automatically cancelled. The driver knows the directional signal was canceled (MMU) but believes APA will continue looking on the left (non-default) side because the feature was activated with the directional signal on (MMB).

UCA 2a-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 2a-7-1:** Driver provides an "APA on" command when road conditions are not suitable for APA (UCA 2a-7) because the driver incorrectly believed the conditions were suitable (MME). The driver also believed that the system would detect and notify him if conditions were unsuitable (MMB). The driver did not realize that the system was not capable of parallel parking on curved roads because the driver had successfully used APA on curved roads in the past and assumed the system could do the same again (MMU). However, the driver did not realize that the curvature of the current road was slightly more than the curvature for previous successful applications (MMS) and beyond the capabilities of the system (MMB).

- **Scenario 2a-7-2:** Driver provides an "APA on" command when weather conditions are not suitable for APA(UCA 2a-7) because the driver incorrectly believed conditions were suitable (MME) and the system would not activate if conditions were not suitable (MMB). The driver did not realize that the system sensors would not work in poor weather because the driver had never attempted to use the system in poor weather before (MMU).

UCA 2a-9: Driver does not provide "APA off" command when environment is no longer suitable for APA.

- **Scenario 2a-9-1:** Driver does not provide an "APA off" command while car is in an inappropriate space (UCA 2a-9), such as blocking a fire hydrant or in a resident only area. The driver was relying on the automation to select a parking space (S) because the driver incorrectly believed the system sensors could detect unsuitable or invalid spots (MMB) and believed that the space selected was therefore appropriate (MME).

UCA 2a-12: Driver does not provide "APA off" command when maneuver is complete.

- **Scenario 2a-12-1:** Driver does not provide "APA off" command when maneuver is complete (UCA 2a-12) because the driver did not know it was necessary to press the APA off button when the system has finished parking (S). She incorrectly believes APA will shut itself off once she shifts into park (MMB), based on past experience with a more highly automated system which did shut off automatically (MME).

UCA 2a-14: Driver provides "APA off" command too late when environment is no longer suitable.

- **Scenario 2a-14-1:** Driver provides an "APA off" command too late (UCA 2a-14) because the driver typically makes decisions by doing as the system instructs (S) and the driver misunderstood the system instructions (MMU). The system instructions that were provided actually meant that something had gone wrong and it was necessary to resume manual parking, but the driver thought it meant that parking was complete and successful (MMU).

UCA 2a-45: Driver shifts into a range which puts the vehicle on a collision path.

- **Scenario 2a-45-1:** Driver shifts into a range which puts the vehicle on a collision path (UCA 2a-45) because the driver trusts the automation to make safe decisions (S). The driver incorrectly believed the APA computer was aware of any obstacles in the environment (MMS) and that the APA computer would adjust instructions accordingly (MMB). However, the driver had not realized an obstacle had appeared behind the car (MME). The driver did not notice the obstacle because they were relying solely on the automation's cues rather than visual checks (MMU).

- **Scenario 2a-45-2:** Driver shifts into a range which puts the vehicle on a collision path (UCA 2a-45) because the driver intended to shift into the instructed gear (S) but made a mistake performing the action. The driver incorrectly believed he or she had shifted into the desired gear (MMS) and did not notice that they were in the wrong gear because they had already begun to perform the next step instructed (MMU).

- **Scenario 2a-45-3:** Driver shifts into a range that puts the vehicle on a collision path (UCA 2a-45) because the driver incorrectly believed APA feedback meant it was safe to shift (MMS). The driver believed the instructions meant that the APA computer was confirming that it was safe to shift (MMB), when in reality the APA computer was showing the next step of the autopark process, but not the absence of obstacles. An obstacle such as another car in front reversing made it unsafe to shift (MME).

UCA 2a-50: Driver accelerates when doing so puts the car on a collision path. [H-1]

- **Scenario 2a-50-1:** Driver accelerates when doing so puts the car on a collision path (UCA 2a-50) because the driver is following the rule "I do what the system instructs" (S) and incorrectly believes it is safe to accelerate as instructed (MMS). The driver believes the system will not give instructions to accelerate if there is an obstacle ahead (MMB) and is unaware of a stopped car (MME). The driver is not monitoring the environment closely because he is watching the APA display for instructions (MMU).

UCA 2a-53: Driver continues accelerating too long while on a collision path

- **Scenario 2a-53-1:** Driver continues accelerating too long while on a collision path (UCA 2a-53) because driver is basing decisions solely on instructions from the automation as a rule (S). The driver incorrectly believes there are no immediate obstacles in the environment (MME). The driver does not notice the distance to the next car diminishing because they are in reverse and relying on instructions rather than looking behind them (MMU).

- **Scenario 2a-53-2:** Driver continues accelerating too long while on a collision path (UCA 2a-53) because driver is basing decisions solely on instructions from the automation (S). The driver incorrectly believes the automation will explicitly instruct them to cease accelerating (MMB) and does not understand the meaning of the tone intended to notify them (MMU).

System 2b: "Partial Automation"

UCA 2b-1: Driver does not provide a directional signal before attempting to autopark on the non-default side.

- **Scenario 2b-1-1:** The driver does not provide the left directional signal (UCA 2b-1) because the driver previously provided the left directional signal (S) and thinks the directional signal is still on (MMS). Before the desired spot was located, the left directional signal was automatically cancelled and the driver's corresponding mental model was not updated (MMU). The left directional signal would be automatically cancelled if the steering angle meets the corresponding threshold for turn signal cancellation.

- **Scenario 2b-1-2:** The driver does not provide the directional signal (UCA 2b-1) because the driver previously provided the directional signal (S) but the directional signal was automatically cancelled. The driver knows the directional signal was canceled (MMU) but believes APA will continue looking on the left (non-default) side because the feature was activated with the directional signal on (MMB).

UCA 2b-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 2b-7-1:** Driver provides an "APA on" command when road conditions are not suitable for APA (UCA 2b-7) because the driver incorrectly believed the conditions were suitable (MME). The driver also believed that the system would detect and notify him if conditions were unsuitable (MMB). The driver did not realize that the system was not capable of parallel parking on curved roads because the driver had successfully used APA on curved roads in the past and assumed the system could do the same again (MMU). However, the driver did not realize that the curvature of the current road was slightly more than the curvature for previous successful applications (MMS) and beyond the capabilities of the system (MMB).

- **Scenario 2b-7-2:** Driver provides an "APA on" command when weather conditions are not suitable for APA (UCA 2b-7) because the driver incorrectly believed conditions were suitable (MME) and the system would not activate if conditions were not suitable (MMB). The driver did not realize that the system sensors would not work in poor weather because the driver had never attempted to use the system in poor weather before (MMU).

UCA 2b-20: Driver does not steer when APA is disabled.

- **Scenario 2b-20-1:** The driver stops providing steering commands when APA is disabled (UCA 2b-20). The driver acts on the assumption that he does not need to steer when APA is enabled (S), and he incorrectly believes that APA is still enabled (MMS) because he did not intentionally disable it. He had grabbed the steering wheel to swerve around a small obstacle, such as a squirrel or pothole, and incorrectly assumed this would result in a temporary override (MMB) because he knows that braking can cause temporary overrides and assumes steering can do the same (MMU).

- **Scenario 2b-20-2:** The driver stops providing steering commands when APA is disabled (UCA 2b-20). The driver acts on the assumption that he does not need to steer when APA is enabled (S), he incorrectly believes that APA is still enabled (MMS), and he did not notice or understand the indicator that APA was disabled (MMU). The driver had bumped the steering wheel accidentally while reaching for something inside the vehicle and exceeded the programmed noise threshold

which automatically disabled APA. The driver knows that he has bumped the steering wheel in the past and APA was not disabled as a result, and believes the system will behave the same way this time (MMB). However the driver does not realize there is a noise threshold or that it was exceeded this time (MMB).

UCA 2b-34: Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle.

- **Scenario 2b-34-1:** Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle (UCA 2b-34) because the driver incorrectly believes that the APA computer detects (MMS) and will brake (MMB) for the obstacle ahead. This belief stems from past experience (MMU) in which she has seen the APA computer apply the brakes to avoid hitting other parked vehicles. She does not receive any feedback that the APA computer is unaware of the obstacle.

- **Scenario 2b-34-2:** Driver does not brake when APA is enabled and the APA computer does not react appropriately to an obstacle (UCA 2b-34) because the driver incorrectly believes that the APA computer detects (MMS) the obstacle ahead. She knows that braking can cancel the automation (MMB) and is concerned that if she brakes unnecessarily, she will cancel the automation and need to restart the parking maneuver (S). She wants to avoid cancelling the automation (S). She does not receive any feedback that the APA computer is unaware of the obstacle (MMU).

UCA 2b-40: Driver does not brake for long enough to avoid collision when automation is not reacting appropriately to an obstacle.

- **Scenario 2b-40-1:** Driver does not brake for long enough when automation is not reacting appropriately to an obstacle (UCA 2b-40) because the driver is making decisions just like she does when in manual mode (S). The driver saw an obstacle and pressed the brake. The driver knows from past experience that pressing the brake can disable the automation (MMB), and incorrectly believes that the automation is now disabled (MMS) and it is safe to release the brake (MMS). In reality, the duration of manual braking did not meet the programmed threshold to disable APA. It is unsafe for the car to roll forward, but because the automation is still not reacting appropriately it resumes accelerating as soon as the brake pedal is released and accelerates into the obstacle.

UCA 2b-49: Driver does not shift when APA is enabled and the APA computer is not reacting appropriately to prevent the vehicle from being on a collision path.

- **Scenario 2b-49-1:** The driver does not shift when APA is enabled and the APA computer is not reacting appropriately to prevent the vehicle from being on a collision path (UCA 2b-49). The driver is operating under the rule that he does not need to shift when APA is active (S). The driver incorrectly believes that APA is still in the middle of the maneuver (MMS) when in fact the APA computer has shifted into park and is about to shut off. The driver is aware that the vehicle is still partially in the road and there are cars approaching (MME). The driver did not notice that APA changed gears because the gear shifter did not physically move (MMU).

- **Scenario 2b-49-2:** The driver does not shift when APA is enabled and the APA computer is not reacting appropriately to prevent the vehicle from being on a collision path (UCA 2b-49). The driver is operating under the rule that he does not need to shift when APA is active (S). The driver believes he has seen APA respond to obstacles before (MMU) and incorrectly believes that APA detects the emergency vehicle approaching (MMS) and the APA computer will shift and move out of the way of the emergency vehicle (MMB). The driver did notice the emergency vehicle (MME) but does not know that the APA system cannot react to emergency vehicles.

UCA 2b-50: Driver attempts to shift when doing so will put the vehicle on a collision path.

- **Scenario 2b-50-1:** Driver attempts to shift when doing so will put the vehicle on a collision path (UCA 2b-50) because the driver believes the system is in the incorrect gear (MMS). The driver believes there is an obstacle in the path of the vehicle (or soon will be), and quickly shifts from R to D (or D to R) while the automation is accelerating.

- **Scenario 2b-50-2:** Driver attempts to shift when doing so will put the vehicle on a collision path (UCA 2b-50) because the driver is nervous granting control to the automation for the first time and is attempting to oversee closely (S). The driver incorrectly believes the system is in the incorrect gear (MMS) because the gear lever does not move when shifting is performed automatically, which the driver perceived as feedback confirming the system state has not changed (MMU).

- **Scenario 2b-50-3:** Driver attempts to shift when doing so will put the vehicle on a collision path (UCA 2b-50) because the driver did not intend to shift (S). The driver incorrectly believes APA is still enabled (MMS). The driver bumped the gear selector accidentally, but the gear selector returned to its original position (null-position shifter). The driver did not notice the message that he had changed the gear and disabled the automation (MMU).

UCA 2b-62: Driver does not accelerate when APA is enabled and the APA computer is not reacting to an approaching vehicle.

- **Scenario 2b-62-1:** Driver does not accelerate when APA is enabled and the APA computer is not reacting to an approaching vehicle (UCA 2b-62) because the driver is operating under the rule that it is not necessary to accelerate while the automation is active, so it is safe to engage in secondary tasks (S). The driver incorrectly believes there is no other vehicle approaching (MME) and does not notice the other vehicle approaching because he is checking his email (MMU).

- **Scenario 2b-62-2:** Driver does not accelerate when APA is enabled and the APA computer is not reacting to an approaching vehicle (UCA 2b-62) such as an emergency vehicle because the driver is operating under the rule that it is not necessary to accelerate while the automation is active, so it is safe to engage in secondary tasks (S). The driver detects a vehicle approaching rapidly (MME) but incorrectly believes the system will accelerate out of the way (MMB) because he has seen the system accelerate in other contexts (MMU).

System 3: "Conditional Automation"

UCA 3-1: Driver does not provide a directional signal before attempting to autopark on the non-default side.

- **Scenario 2b-1-1:** The driver does not provide the left directional signal (UCA 2b-1) because the driver previously provided the left directional signal (S) and thinks the directional signal is still on (MMS). Before the desired spot was located, the left directional signal was automatically cancelled and the driver's corresponding mental model was not updated (MMU). The left directional signal would be automatically cancelled if the steering angle meets the corresponding threshold for turn signal cancellation.

- **Scenario 2b-1-2:** The driver does not provide the directional signal (UCA 2b-1) because the driver previously provided the directional signal (S) but the directional signal was automatically cancelled. The driver knows the directional signal was canceled (MMU) but believes APA will continue looking on the left (non-default) side because the feature was activated with the directional signal on (MMB).

UCA 3-7: Driver provides "APA on" command when conditions are not suitable for APA.

- **Scenario 3-7-1:** Driver provides an "APA on" command when road conditions are not suitable for APA (UCA 3-7) because the driver incorrectly believed the conditions were suitable (MME). The driver also believed that the system would detect and notify him if conditions were unsuitable (MMB). The driver did not realize that the system was not capable of parallel parking on curved roads because the driver had successfully used APA on curved roads in the past and assumed the system could do the same again (MMU). However, the driver did not realize that the curvature of the current road was slightly more than the curvature for previous successful applications (MMS) and beyond the capabilities of the system (MMB).

- **Scenario 3-7-2:** Driver provides an "APA on" command when weather conditions are not suitable for APA (UCA 3-7) because the driver incorrectly believed conditions were suitable (MME) and the system would not activate if conditions were not suitable (MMB). The driver did not realize that the system sensors would not work in poor weather because the driver had never attempted to use the system in poor weather before (MMU).

UCA 3-18: Driver does not steer when APA is disabled.

- **Scenario 3-18-1:** The driver stops providing steering commands when APA is disabled (UCA 3-18). The driver acts on the assumption that he does not need to steer when APA is enabled (S), and he incorrectly believes that APA is still enabled (MMS) because he did not intentionally disable it. He had grabbed the steering wheel to swerve around a small obstacle, such as a squirrel or pothole, and incorrectly assumed this would result in a temporary override (MMB) because he knows that braking can cause temporary overrides and assumes steering can do the same (MMU).

- **Scenario 3-18-2:** The driver stops providing steering commands when APA is disabled (UCA 3-18). The driver acts on the assumption that he does not need to steer when APA is enabled (S), he incorrectly believes that APA is still enabled (MMS), and he did not notice or understand the indicator that APA was disabled (MMU). The driver had bumped the steering wheel accidentally

while reaching for something inside the vehicle and exceeded the programmed noise threshold which automatically disabled APA. The driver knows that he has bumped the steering wheel in the past and APA was not disabled as a result, and believes the system will behave the same way this time (MMB). However the driver does not realize there is a noise threshold or that it was exceeded this time (MMB).

UCA 3-19: Driver does not resume steering when instructed to resume manual control.

- **Scenario 3-19-1:** Driver does not resume steering when instructed to resume manual control (UCA 3-19) because the driver is following a mental rule that it is safe to perform secondary tasks while the automation is active, since no action is required unless a takeover alert is issued (S). The driver incorrectly believes there are no obstacles or hazards in the surrounding environment (MME), and that no takeover alert has been issued (MMS). The driver overlooked both the change to the environment and the alert to takeover because he was engrossed in a secondary task (MMU).

- **Scenario 3-19-2:** Driver does not resume steering when instructed to resume manual control (UCA 3-19) because the driver is following a mental rule to only take over driving when instructed (S) and incorrectly believes there hasn't been a request to take over (MMS). The driver incorrectly believes the takeover alert will be a verbal instruction rather than a tone (MMB). Because the driver was not expecting a tone, the driver does not understand the meaning of the takeover alert (MMU).

UCA 3-34: Driver does not brake when instructed to resume manual control and braking is necessary to avoid a collision.

- **Scenario 3-34-1:** Driver does not brake when instructed to resume manual control and braking is necessary to avoid a collision (UCA 3-34) because the driver is operating under the rule that he does not need to take over unless he receives an alert (S). The driver incorrectly believes that no alert has been issued (MMS) and external conditions are safe for APA (MME) because he did not notice the change to external conditions or alert to take over (MMU).

- **Scenario 3-34-2:** Driver does not brake when instructed to resume manual control and braking is necessary to avoid a collision (UCA 3-34) because the driver is operating under the rule that he does not need to take over unless he receives an alert (S). The driver incorrectly believes that no alert has been issued (MMS) because he expected a verbal instruction, rather than a simple tone (MMB). Because he expected a verbal instruction, the driver did not understand the alert tone (MMU).

UCA 3-53: Driver attempts to shift when doing so will put the vehicle on a collision path.

- **Scenario 3-53-1:** Driver attempts to shift when doing so will put the vehicle on a collision path (UCA 3-53) because the driver believes the system is in the incorrect gear (MMS). The driver believes there is an obstacle in the path of the vehicle (or soon will be), and quickly shifts from R to D (or D to R) while the automation is accelerating.

- **Scenario 3-53-2:** Driver attempts to shift when doing so will put the vehicle on a collision path (UCA 3-53) because the driver is nervous granting control to the automation for the first time and is attempting to oversee closely (S). The driver incorrectly believes the system is in the incorrect

gear (MMS) because the gear lever does not move when shifting is performed automatically, which the driver perceived as feedback confirming the system state has not changed (MMU).

- **Scenario 3-53-3:** Driver attempts to shift when doing so will put the vehicle on a collision path (UCA 3-53) because the driver did not intend to shift (S). The driver incorrectly believes APA is still enabled (MMS). The driver bumped the gear selector accidentally, but the gear selector returned to its original position (null-position shifter). The driver did not notice the message that he had changed the gear and disabled the automation (MMU).