Application of Hierarchy to STPA:
A Human Factors Study on Vehicle Automation

By
Rachel Cabosky

B.S. Engineering (2018)
Miami University

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

At the
Massachusetts Institute of Technology

September 2020

Signature of Author _____
System Design and Management Program
August 14, 2020

Certified by _____
John P. Thomas, Ph.D.
Thesis Supervisor
Department of Aeronautics and Astronautics

Accepted by _____
Joan Rubin
Executive Director, System Design & Management Program

Application of Hierarchy to STPA:
A Human Factors Study on Vehicle Automation

By

Rachel Cabosky

Submitted to the Department of System Design and Management on Aug 14, 2020
in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Engineering and Management

Abstract

In a world where vehicle automation designed to remove "human error" is increasingly present on our roadways, are we actually safer? As we replace human tasks and decision making, the machines and the software used to substitute these actions become more complex.

This increased complexity drives the need to thoroughly understand changes to the associated risk as well as the impacts to, and changing relationships with, the human driver. System-Theoretic Process Analysis (STPA) has been proven as an effective tool to evaluate risk by analyzing the system as a whole rather than at the component level. Notably, STPA includes, and evaluates, the operator as a part of the system. Additionally, STPA methodology provides the means to simply depict and communicate intricate system controls. Though it is clear that STPA can be performed with a range of system specificity, it has yet to be documented what types of recommendations can be provided as more complexity and detail is included in the system description.

This thesis is used to demonstrate that STPA can be performed iteratively, and that significant insights to the system design can be obtained at each iteration or level. This method of evaluation includes the human factors extension and basic scenario generation to supplement the refinement process. To perform this analysis, an SAE Level 2 feature intended for highway traffic assist, proposed by Zenuity, is evaluated at three levels of detail—focusing on the driver-feature interface. Iteration and refinement are possible at all steps of STPA, but special attention is given here to the control structures, unsafe control actions, and scenarios. This work benefits risk management and hazard analysis by offering a methodology for managing complexity through hierarchical iteration, such that insights can be derived early and be refined throughout the analysis process.

Thesis Supervisor: John P. Thomas

Title: Research Engineer, Director of Engineering Systems Lab, Aeronautics and Astronautics

Acknowledgements

I would like to thank my advisor, Dr. John Thomas, for his ongoing support and ever-present excitement in helping me contribute to the body of STPA research. I am incredibly grateful for this opportunity to have learned and contributed to this method in the span of only a few short months.

I would also like to thank the members of the Zenuity team for their assistance in building the control structures for the analysis. In particular, I would like to thank Shabin Mahadevan, Amardeep Sidhu, and Rachel Alexander for all the extra time they volunteered to help build my understanding of their system. I would also like to recognize and thank Charles "Chuck" Green for his help in understanding Cadillac's Super Cruise.

Special thanks to the PALACE Acquire program and USAF, without whom I would have never applied to MIT or even thought to pursue my Master's Degree.

I would like to thank Timothy Dormady for his unwavering support and encouragement. His understanding throughout this process, and in our time together, has been appreciated more than he knows.

Lastly, I wouldn't be where I am today without the love and support of my family. I am incredibly grateful to them for always encouraging me to pursue my dreams. Over the years they have proof read many a paper, but this one is by far the longest.

Table of Contents

Table of Figures

Table of Tables

Chapter 1: Introduction

1.1 Research Purpose

The increasing presence yet relatively recent entry of vehicle automation in the market makes it an excellent candidate for risk analysis. Compared to other vehicle subsystems, self-driving automation demonstrates rapidly increasing complexity, and regulation of safety and standardization is not universal. Though automated features are intended to increase safety, these factors may actually transfer and create risks in new areas. The increased number of parts and interfaces drive the need to analyze and understand how those systems, and their interaction with the human driver, affect the risk and safe operation of this new class of vehicles.

System Theoretic Process Analysis, or STPA, is a hazard analysis method that goes beyond traditional methods that focus on component-level failures. STPA does this by evaluating system-level weaknesses caused by, or resulting from, interactions or interfaces between components. One of the fundamental building blocks of STPA is the control structure which allows systems to be easily communicated and analyzed by emphasizing control relationships in the system. Current STPA guidance indicates that the method can be iterated to perform a comprehensive analysis, where one could refine work from a system level down to the component level. However, more work is needed to demonstrate and evaluate the process through multiple iterations, compare the insights that are produced at each level, and determine how detailed iterations should be to produce the most useful recommendations for improving the system.

This thesis demonstrates each step of the full process including the control structure, the unsafe control actions, and the scenario generation across three levels of iteration. In addition to exploring the iterative nature of STPA, this thesis will evaluate a scenario generation process to better manage complexity and an integrated human factors refinement approach.

1.2 Objectives

The primary objective of this study is to demonstrate and evaluate the iterative nature of STPA including several types of refinement that might be used in each step.

STPA will be applied at three distinct levels of detail to a “Hands Off Eyes On” vehicle automation feature. The system analyzed in this thesis is based on real systems in development and in production, using information collected through extensive interviews with major automotive organizations. The STPA analysis is performed iteratively using a process of structured hierarchical refinement as proposed by J. Thomas 2020 [33]. The results are then evaluated to determine how effective the process is, including the scalability of the approach as complexity increases and its ability to identify system weaknesses and recommendations.

Human operator interactions are critical to the success of supervised automation features, and special attention will be given to human behaviors. Relatively new techniques are demonstrated and evaluated to help tackle this problem within an STPA analysis, including a technique for efficient scenario building [29, 33] and a technique to develop human-related scenarios [28, 30, 31].

A question that was raised during interview discussions involved the sensitivity of the analysis to changes or mistakes in the control structure model that is used. Therefore, a secondary objective of this work was to answer that question by comparing the analysis results with those obtained using an alternative interpretation of the system (a different control structure). Though it has been hypothesized that it is possible to arrive to similar scenarios when mistakes are made (like switching the feedback and control actions), it has yet to be formally evaluated and documented in STPA literature.

1.3 Thesis Structure

Chapter 1 introduces the purpose and objectives of this study.

Chapter 2 will provide background information for the reader to become familiar with some issues pertaining to current automated vehicles, existing guidance for the derivation of automation requirements, an overview of human factors concepts, limitations of risk analysis methods, and an overview of the STPA method—including detail on the human factors extension.

Chapter 3 will provide a detailed overview of the STPA analysis performed on the Zenuity-derived case study. This will be a sample of a full analysis, to include Losses and Hazards, control structures, a sample of UCAs, and a sample of scenarios. (Full tables of UCAs can be found in the Appendices). This content will be available for Level 1, Level 2, and Level 3 analyses to demonstrate hierarchical differences to the results of different steps of STPA.

Chapter 4 will evaluate the results of the analysis. This content will cover unique insights derived from this study, including a discussion on switching human controls for automated feedback as the highest authority, and a demonstration of the evolution of a horizontal input/output into tangible controls. Furthermore, an analysis of the refinement applied to each step of STPA will be provided. Lastly, this section will describe the insights and recommendations derived from the hierarchical evaluation.

Chapter 5 will conclude with a summary of the key insights and conclusions from this analysis and suggestions for future expansions of this work.

Chapter 2: Literature Review

Automation in road vehicles is an increasingly growing presence in today's market. With every new "self-driving" system introduced to the road, we learn more about their capability to operate in real world environments. While automation is often introduced to reduce human error, issues persist with the human-machine interface (HMI) and many accidents with automated vehicles continue to be labeled as human error. To understand how hazards manifest themselves within the automation, it is necessary to look at the whole system and understand how emergent properties like safety and trust are affected by key choices made during development.

This chapter discusses critical knowledge that underlies a holistic analysis of automated vehicles with emphasis on human factors, including current issues and standards as well as human factors and analysis methodologies. This chapter will also overview the process for Systems Theoretic Process Analysis (STPA) and the extension for examining human behavior. These sections will offer terms and frameworks that will be referenced in later chapters of this thesis.

2.1 Vehicle Automation Today

Automation in vehicles ranges from features like antilock brakes engaging in icy conditions, to a fully autonomous self-driving car. The popular Society of Automotive Engineers (SAE) definition of autonomy states that an autonomous vehicle must have sustained automation which is capable of reacting to its environment [26].

Today, most automated vehicles on the market have low levels of automation compared to a fully self-driving car, but that is changing as higher levels of automation are actively being researched for market use. Particularly with these lower levels of automation, these vehicles internally rely on substantial human supervision and interaction. Furthermore, as these systems integrate onto roadways, they must reconcile with the fact that they must externally interface with the unpredictability of other human drivers. This section highlights challenges of integration in today's physical roadways and existing legal guidance.

2.1.1 Case Studies

The following case studies are surmised from crash and incident reports involving the use of automated driving settings.

2.1.1.1 Tesla

According to Highway Accident Brief 1907 [16], a Tesla 2014 Model S P85 car was operating using the advanced driver assistance system, "Autopilot," in traffic in the HOV lane, and the vehicle crashed into a stopped firetruck in the driver's lane—resulting in damage to both vehicles. The driver was cited as eating/drinking, listening to the radio, and may have been looking down at a phone before the crash. The driver's vehicle was following another car and traveling under 25 mph when the lead vehicle changed lanes to avoid the stopped truck ahead. The Tesla proceeded to speed up and crash into the stopped vehicle. The driver was minimally using hand contact on the wheel to prevent escalation of alerts but had hands off at the time of the crash.

This is one of at least 3 near identical crashes in the course of one year [27] that included a Tesla and stopped firetruck, let alone other accident occurrences. In these specific incidents, the system was unable to detect a stopped vehicle and react after following a lead vehicle. Though the driver's manual explicitly states this as a limitation of the system, it is evident that users have higher trust in the system than appropriate for its capabilities. Some argue that the driver did not pay enough attention to the environment to be able to take over in dangerous scenarios, but this may be partly or largely due to the design of the automation and the escalation strategy for the warning system. The algorithm varies according to vehicle speed, but ultimately the number of driver interactions required by the system combined with the ability to easily game the system means that drivers do not have to afford much

attention to keep the system operational. This is evidence that the design is insufficient to encourage the driver attention necessary for this type of driving system.

2.1.1.2 Google

In 2015, Google reports that "In the six years of our project, we've been involved in 16 minor accidents during more than 2 million miles of autonomous and manual driving combined. Not once was the self-driving car the cause of the accident" [34]. Though Google claims that human error and decision making are at fault, there is at least some traceability to the system design which indicates that the human may not be entirely at fault.

In 2009 a test car froze at a four way stop because its decision algorithm would not allow it to move if all other vehicles were not completely stopped, and in 2015 a Google vehicle was coming to a stop for a pedestrian but the driver was worried about the response time and braked more aggressively—leading to the following vehicle rear-ending the driver's car [34]. The first instance where Google assumed partial responsibility was in a 2016 accident in which the Google vehicle pulled out in front of a bus to avoid an obstacle in its lane [37]. Though in each of these cases human behavior may lead to a fault, it is possible to imagine design decisions that could have been made to prevent or mitigate the effects of the unsafe controls. A common issue throughout these scenarios is a misalignment in the human's mental model for driving versus the autonomy's mental model. With the knowledge that autonomous vehicles will increasingly need to share the road with human drivers in the coming years, it is important to make sure that other humans in the system understand the behavior and decision making of the autonomous systems in their vehicle and that autonomous systems are designed to be understandable when they are supervised by humans.

2.1.1.3 Uber

In what is considered the first death caused by a self-driving vehicle, Uber's robot car struck and killed a pedestrian walking her bike across the street at night. The pedestrian was wearing dark clothes and did not cross at a crosswalk; consequently the vehicle did not correctly classify her and thus did not predict her path, notifying the driver that emergency braking was necessary only 1.3 seconds before the collision [17]. NBC's McCausland reported that:

> "Uber had disabled the emergency braking system, relying on the driver to stop in this situation, but the system wasn't designed to alert the operator, who "intervened less than a second before impact by engaging the steering wheel," [14].

The driver had not been attentive and was actively streaming a show. In the SAE classification of levels of vehicle automation, Level 3 describes automation for which the driver needs to be ready to intervene as necessary. Level 3 vehicles offer unique challenges for the HMI due to its precarious distribution of automated versus driver control and responsibility. This particular scenario demonstrates challenges at both the vehicle's processing level and the design of the human controls.

2.1.2 Existing Standards and Guidance

This section summarizes automation level guidance, Operational Design Domain terminology, and two ISO standards (ISO 26262 and 21448) pertaining to electrical and electronic (E/E) vehicle components. This list is by no means comprehensive; further reading may include but is not limited to ISO 20077 and ISO 21434.

2.1.2.1 SAE J3061 Surface Vehicle Recommended Practice

The Society of Automotive Engineers (SAE) have created a means of categorizing a vehicle's level of automation* [26]. This document describes capabilities for each level of automation, but there are no explicit measures of compliance or safety. It offers guidance surrounding the expected roles of the user for successful vehicle operation, according to the level of automation implemented. Lastly, level designations are never fractional due to the role specifications between the user and the driving automation system (DAS). However, a single DAS may have features that operate at different levels of automation.

The six defined levels of automation are:

- (Level 0) No driving automation
- (Level 1) Driver Assistance
- (Level 2) Partial Driving Automation
- (Level 3) Conditional Driving Automation
- (Level 4) High Driving Automation
- (Level 5) Full Driving Automation

Driving automation systems are categorized into levels based on capability of lateral and longitudinal motion, capability for object and event detection and response, ability to perform dynamic driving task (DDT) fallback, and operational design domain (ODD) limitations. For the automation to be considered higher than Level 0, it must be able to "support sustained operation" and be able to "dynamically react to its environment" [26]. For example, cruise control is sustained but not able to respond to the environment, and active safety systems (e.g. automated emergency braking) are able to react to the environment, but are not sustained. [26].

Today, most "automated" vehicles require supervision. At levels 1 and 2, the user takes the role of driver, and is responsible for monitoring the vehicle and the environment, including the automation system. Automated features at these levels, "support, but do not replace," [26] a *driver* in performing DDTs; this means that the "support" offered instead replaces a *driving task* with a partial or supervisory task on the part of the driver. The expectation is that the driver will maintain a readiness to respond as needed; this may include monitoring feature performance and responding to inappropriate actions taken by the feature, among other dynamic tasks. [26].

Level 3 is a special case. The automation has been determined to not fall within the category of designed for operation exclusively by automation, though this is still subject to debate. At Level 3, the user takes the role of DDT fallback-ready user, and is expected to achieve minimal risk conditions according to their own judgement or requests to intervene, and may perform DDTs independently. The SOTIF standard (section 2.1.2.4) also specifically calls out this role and maintains that the user "must be able to operate and intervene in the case of DDT performance failure" [26]. This level of driver readiness is not assumed at levels 4 and 5. [26].

At higher levels of driving automation (levels 3-5), the ADS monitors its own performance. Level 3-5 systems qualify as "Automated Driving Systems (ADS)." Truly driverless vehicles are only Level 4 and 5, where, when the automation is engaged, the user takes the role of passenger. Unlike Level 4, Level 5

* J3061 offers guidance to use caution with the words "autonomous" and "control." These words have distinct meanings to different groups (legal, engineering, common language). As such, their use can give false meaning to features. It suggests "driving automation" in place of "autonomous" and "DDT performance" or "operate" to replace "control." [26]. Though this thesis may use the words interchangeably, any ambiguous meaning should be assigned to these J3061 definitions.

does not have ODD limitations. (Limitations may include environment, geography, time of day, traffic/road conditions, weather, lighting, etc.) [26].

Because the use case discussed in this paper will involve SAE Level 2 automation, the expectations of the driver and the DAS in Level 2 will be explicitly described. Level 2 DAS includes (sustained and ODD-specific) execution of both lateral and longitudinal vehicle motion in response to the DDT, while at all times the driver must: complete all DDT not fulfilled by the automation (up to and including immediate response), supervise and intervene on behalf of the automation to maintain safe operation, and determine the appropriate engagement/disengagement of the system. This driver/system interaction is necessary due to the limitations of the system's recognition and response capabilities. As a result, absence of supervision may result in the vehicle being brought to a controlled stop as a mitigation strategy. [26].

The SAE levels acknowledge the importance of the user for the success of the system. Level 0-1 features are not considered to have enough automation to facilitate significant automation misuse, and Level 4-5 features are effectively "driverless" and thus negate much of the need for human system interaction. As such, Levels 2 and 3 place the highest demand on the human/system interaction. At these levels, user monitoring is the main countermeasure employed against automation misbehavior and capability gaps. Driver monitoring and receptivity allude to the trust in automation and attention versus arousal curves, respectively. [26]

2.1.2.2 Operational Design Domain for Automated Driving Systems – Taxonomy of Basic Terms

The WISE Lab offers the Operational Design Domain (ODD) for Automated Driving Systems (ADS) document [1] to explain basic terms and explain ADS behavior for SAE automation levels. It is intended for use in Levels 4 and 5 because it does not consider the user/system interaction. Broadly speaking, the ODD specifies limits to the operating environment according to the road conditions, vehicle behavior, and vehicle state. Road environment conditions are the most commonly limited elements within an ODD [1]; for example, limiting a feature's use to highways. The document also offers different models of operational domains, such as degraded system capability and a resulting restriction of feature capability.

ODDs are classified according to analysis of situations and scenarios that are statistically characterized according to their likelihood of occurrence and existence in the operational environment, in addition to their risk category (normal driving, near crash, crash, or fallback). Crash scenarios are analyzed according to their severity and loss type. ISO 26262 loss scenarios are focused on personal injury in accordance with classification of hazards and associated probability of occurrence, though according to ODD specifications, loss may also include property damage. Crash data is used to inform scenarios, and near-crash data is used to supplement the analysis. [1].

ODD classifies situations from low to extreme demand. Demand is increased by higher speeds, poor weather, poor visibility, high traffic volumes, construction, complex urban environments, and other factors [1]. Environmental conditions affect the performance demand felt by both the driver and the ADS to maintain safe driving conditions.

The document also references Fuller's argument on task difficulty homeostasis theory, "that human drivers target a specific level of task difficulty that they are comfortable with and that this choice determines their driving behavior," and that "the statistical risk of collisions increases sharply when the situation demand surpasses the road user capability" [1]. This aligns with the Yerkes-Dodson model of arousal and performance; when arousal (demand) exceeds a certain threshold, the individual's performance begins to degrade.

Another useful introduction from ODD is the inclusion of an ontology of the "Operational World Model." This model breaks down the environment into five categories, (1) the road structure, (2) the road users, (3) animals, (4) other obstacles that might be found on the roadway, and (5) environmental conditions. This tool helps describe the settings and limitations of an ADS. [1].

2.1.2.3 ISO 26262 Road Vehicles – Functional Safety

ISO standards offer guidance for production and management of systems across industries. However, with the emergence of "self-driving" vehicles being a relatively new capability, there is limited guidance specifically for autonomous vehicles. For this reason, we see a wide range in levels of and techniques for implementation. Current guidance is primarily derived from ISO FDIS 26262 [9], "Road Vehicles – Functional Safety," which specifically refers to E/E systems within the vehicle. In this version there are zero references specifically to "autonomy." Terms like "driver assistance" must cover a wide array of functions from ABS to self-driving vehicles. To assume that these functions have the same safety guidance is at determent to the safety analysis. Though the standard alludes to needs pertaining to driver behavior, it does not offer a minimum acceptable thresholds or ways to quantify success for the human-system interaction—in short, there is no standard for driver engagement. It is evident that existing standards and requirements are not intended for this purpose, but as the presence of autonomous functions and vehicles on the road continues to increase the need for standardized guidance will be more pronounced.

One important thing to note from this standard is that a baseline is defined regarding the expectations for human performance and training. ISO 26262-3 states:

> "It is assumed that the driver is in an appropriate condition to drive (e.g. they are not tired), has the appropriate driver training (they have a driver's license) and is complying with the applicable legal regulations, including due care requirements to avoid risks to other traffic participants." [9]

This statement inherently implies that the human (driver) will behave predictably and safely. The danger of such blanket statements is that they act to justify that the design and performance guidance focus on the behavior of the car rather than performance limitations of the driver. Furthermore, when we look at driver education and training, it is standardized to non-automated vehicles. The learning of additional features such as cruise control, automatic parking, and hands-off driving is largely the responsibility of the driver.

For example, in defining *safety mechanism*, additional notes specify it should either be able to facilitate a safe state transition itself, or be "able to alert the driver such that the driver is expected to control the effect of the failure as defined in the functional safety concept," yet nowhere is ability to alert the driver quantified. The *warning and degradation strategy* is defined as a "specification of how to alert the driver of potentially reduced functionality and of how to provide this reduced functionality to reach a safe state" [9]. Again, the danger is that the base action of providing notification shifts the responsibility to the driver without guidance on what alert strategies are sufficient to gather attention and other considerations like response and processing time. Notably, the standard includes the requirement that notification of mode transitions must be featured (which should encourage "appropriate involvement and controllability"). Ultimately the document provides insight for what *should* exist, but not *how* it should be included—leaving it up to the manufacturers' discretion.

Expectations for human-machine interaction are defined as what is acceptable for the vehicle with inadequate regard to what is acceptable for the driver.

> "The assumptions regarding human behavior, including controllability and human response, in the hazard analysis and risk assessment, the functional safety concept and the technical safety concept, as well as the technical assumptions relevant for the ASIL classification are validated (see ISO 26262-3:2018 Clause 6, ISO 26262-3:2018 Clause 7, and ISO 26262-4:2018 Clause 8)" [9].

These clauses specifically refer to (in order), Hazard Analysis and Risk Assessment (including controllability), Functional Safety Concept, and Safety Validation.

Controllability is ranked from C0 to C3, C0 being "controllable in general" and C3 being "difficult to control or uncontrollable" and is used to define a hazardous event. The difference between levels is the degree of probability for gaining control to sufficiently avoid and/or mitigate the effects of a hazardous event. Controllability is one factor which contributes to the hazard analysis in combination with exposure and severity, and is the only factor that has quantifiable human testing indicated for the assignment of a specific ranking. These factors combined create Automotive Safety Integrity Levels (ASILs) ranked from "A" (least stringent) to "D" (most stringent), which help define the safety goals and requirements. [9].

Functional safety requirements are behaviors or methods that must be specified, including strategies for driver warnings to reduce risk exposure time and increase controllability (section 7.4.2.3). Human factors such as driver task overload and mode confusion are acknowledged as "helpful" and the resulting warning degradation strategy are "potential inputs" for the user's manual. [9].

Lastly, safety validation is incorporated into technical assumptions and includes testing for controllability, effectiveness, and assumptions that influence ASIL. The eventual controllability through human intervention is influenced by the design of the item and is therefore evaluated during the safety validation (see ISO 26262-4:2018, Clause 8). Validation of controllability includes testing for intended use and "foreseeable" misuse. [9].

Though the standard recognizes that higher complexity is correlated to increased system level risks, the guidance specifically pertaining to the HMI is limited at best.

2.1.2.4 ISO/PAS 21448 Road vehicles— Safety of the Intended Functionality

ISO 21448 Safety of the intended functionality (SOTIF) and ISO 26262 Functional safety both apply to E/E systems. SOTIF is intended for use in the design, verification, and validation phases of development, and is defined as "absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons" [10]. The document offers steps to achieve compliance and means to assess remaining residual risk from both the system and driver capability. Compliance is achieved by documentation of achieved objectives through the associated work products. [10].

SOTIF recognizes a shortcoming in the 26262 standard such that there is further potential for error that can arise from limitations in sensing and understanding the environment—an acknowledgement that there are key issues that are unique to autonomous vehicles. Characterization of limitations includes descriptions of policy algorithms, dynamic driving tasks (DDT), DDT fallback (response by system or driver), erroneous patterns, performance limitations, and triggering conditions. Other system limitations may be caused by "incorrect classification, incorrect measurements, incorrect tracking, misdetection, ghosts, incorrect target selection, incorrect kinematic estimation, occluded areas, etc." [10]. Another significant difference in SOTIF over 26262 is the acknowledgement of limitations of human behavior (both of the driver and other road users), and thus the importance of the design of the human/machine interface. Such behavior includes: foreseeable misuse (not including abuse), overconfidence, reaction time, authority capability, human misuse process (recognition, judgement, action), and mental models (as system understanding and expectations). Lastly, SOTIF does not utilize ASIL for characterizing hazards but does use similar factors for validation purposes. [10].

Scenario generation for SOTIF analysis falls under one of four categories: known and hazardous, known and not hazardous, unknown and hazardous, unknown and not hazardous. The goals are to generally reduce hazard and increase known scenarios. Use cases include both correct use and foreseeable misuse-direct and indirect, and functionality issues including performance of sensors, decision algorithms, and actuators are analyzed at the vehicle, system, and component levels. Analysis of limitations helps produce a list of triggering conditions to evaluate their acceptability. If deemed unacceptable, they may be avoided, reduced, or mitigated by redundancy, diversity, and functional restrictions, among other solutions. For example, "reduction or mitigation of reasonably foreseeable misuse effects [may include]:

Improving the information provided to the driver about the intended functionality (User manual), Improving the Human-Machine Interface; Implementation of a monitoring and warning system." [10]

Validation targets may be wholly or partially derived from government and industry regulations in conjunction with other means to ensure safety [SOTIF]. This effort relies on some means to quantify avoidance of unreasonable risk. Targets may be derived from applicable traffic data and pre-existing targets from similar vehicles or functions. With the knowledge that autonomous behavior is a relatively new entrant and "good practice" is actively being defined, the ALARP ("as low as reasonably practicable") principle is recommended in the SOTIF risk management framework. In this approach, risk versus cost of reduction are weighed such that risk is reduced to a "reasonably practicable" level. Like 26262, the validation targets are not explicitly stated in the SOTIF. However, this document offers a framework of guidance for analysis and means to statistically suggest hazard has been sufficiently avoided. [10].

Lastly for this study, the degradation strategy is of particular importance. The SOTIF states that the degradation concept must include warning strategies, maneuvering for control transitions, and driver monitoring. Take over and fall back conditions must provide sufficient warning for the driver to intervene, as well as the functionality and status of the mode. [10].

2.2 Human Factors Overview

A commonly cited cause of accidents is that of human error. Human error is "often invoked as a contributing factor to a disaster… meaning that something that the operator or user did or did not do played a role in the mishap" [22]. However, it is important to remember that the operator is a critical part of the total system, so their behavior can and should be optimized. According to Peters & Peters [21], human errors are often "attributable to the design of the human-machine interface and/or the training provided to the operator." This means that some of the issues that cause human error are actually due to design error, and are consequently *preventable*.

The idea that man and machine should work together rather than replace each other is not exclusive to engineering practice. This relationship is particularly important in the lower levels of automation because the automation is not there to replace the human entirely, but rather to augment and enhance their capabilities. The AI Paradox, as described by Guszcza & Schwartz [7] states,

> "… tasks which humans find difficult – such as memorizing facts and recalling information, accurately and consistently weighing risk factors, rapidly performing repetitive tasks, proving theorems, performing statistical procedures… are often comparatively easy to automate. The seeming paradox is that the inverse also holds true: things that come naturally to most people – using common sense, understanding context, navigating unfamiliar landscapes, manipulating objects in uncontrolled environments … are often the hardest to implement in machines."
>
> Furthermore, "… unlike humans, algorithms possess neither the common sense nor conceptual understanding needed to handle unfamiliar environments, edge cases, ethical considerations, or changing situations."

If done correctly, automation and human operation are natural compliments and *should* improve system capability. As seen in the use case examples, there are flaws in the current implementation—specifically how and when a human needs to intervene and be alerted to intervene. The following sections highlight different human factors which require specific attention when designing vehicle automation, including misuse, trust, training, decision making, attention, and control design. These factors are of particular importance when there is a critical human interaction, evident in SAE Levels 1-3.

2.2.1 Intent and Use Classification

Knowing that errors do occur, it is helpful to be able to classify them. Broadly speaking, we can classify human intention error into one of four categories [22] (Proctor & Van Zandt, p 63):

- *Slips* are failures in execution or attention
- *Lapses* are memory failures where some intended action was not performed
- *Mistakes* are errors that arise from errors in planning of action—that is, the planned or intended action was incorrect
- *Violations* are a disregard for, or failure to follow established rules and procedures

Each of these intention errors are applicable to driving scenarios—whether it is a problem of omission such as not realizing you have a headlight out (slip) to "gaming" your car's automation by feigning attention (violation). Specifically, within the bounds of the human-machine interface, there are many ways for these actors to interact. Parasuraman & Riley [20] offer the following categories for human use of automation technology:

- *Use* occurs where a human operator is able to engage/disengage the automation
- *Misuse* is an overreliance upon automation
- *Disuse* is mistrust and underutilization of automation
- *Abuse* is the automation of functions without regard for the consequences for human performance

These guidelines offer a framework that indicates two key parameters, the level of use and the level of trust. The goal of any automated system should be to properly align the user's knowledge and trust of the system to its actual capability (Figure 1). In the case studies presented earlier in this chapter, the common issue is that of improperly calibrated trust. The Tesla drivers exhibited overtrust, in that their assumptions or mental model of the vehicle's operation was misaligned to its actual ability. When they should have been vigilant monitors, they grew overconfident in the system's ability to respond to the environment. Meanwhile, for the Google case at the crosswalk, the driver distrusted the system's ability to stop for the pedestrian at the crosswalk and overrode the system— braking suddenly enough to cause the following vehicle to rear end them.

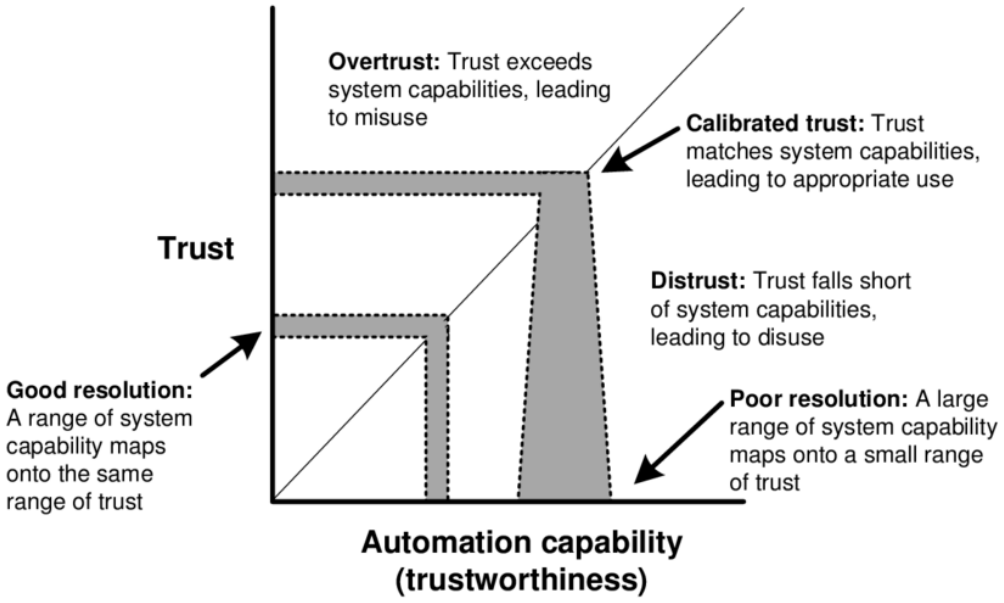

Figure 1: Automation, Trust versus Capability diagram [11]

While any system is capable of fault, the operator should be fully aware of the capabilities and limitations before use. Though guidance from standards details that we can expect drivers to be capable and licensed

(see ISO 26262), the current "training" is based off of the understanding and operation of non-automated vehicles. This means that there will likely be gaps in the user's understanding, which will need to be compensated for by either further instruction or intuitive operation.

2.2.2 Learning and Training

For a system to be understandable, the user's mental model of how it works should align with its actual operation. A mental model is "a dynamic representation or simulation of a problem held in working memory" [22]. When the two become misaligned, there is greater room for operational error. For this reason, it is necessary that designers make appropriate instruction available. This design may be influenced in part by the expected amount of knowledge the user will have and the anticipated familiarity of the operational environment. As it pertains to automated vehicles, drivers may be ill-prepared to operate due to an incomplete understanding of the automation, and thus, an incomplete or incorrect mental model of its operation. Driver education via owner's manual or interactive tutorials may assist in helping users achieve a better understanding of the automation [4]. The models described in this section provide some insight into the basis for design, but are not a comprehensive collection of methods to analyze learning or training.

Rasmussen's model of human performance is useful for modeling learning in familiar and unfamiliar conditions (see Figure 2). This model can inform human interface design to help the operator form the correct mental model, according to the needs associated with the anticipated use cases. At the skill-based level, the human can take in signals and respond with action that requires no conscious thought, like riding a bike. Rule-based operates under a "feedforward effect" where the person can operate based on previously learned rules, such as using learned methods for cooking new recipes. Lastly, the knowledge-based level operates by trial and error—the person has no knowledge or rules to guide their behavior and operates by setting a goal and experimenting to achieve this goal. At this level, there is a greater variability in the mental models that operators may form and consequently there is more room for interpretation and error. [23].

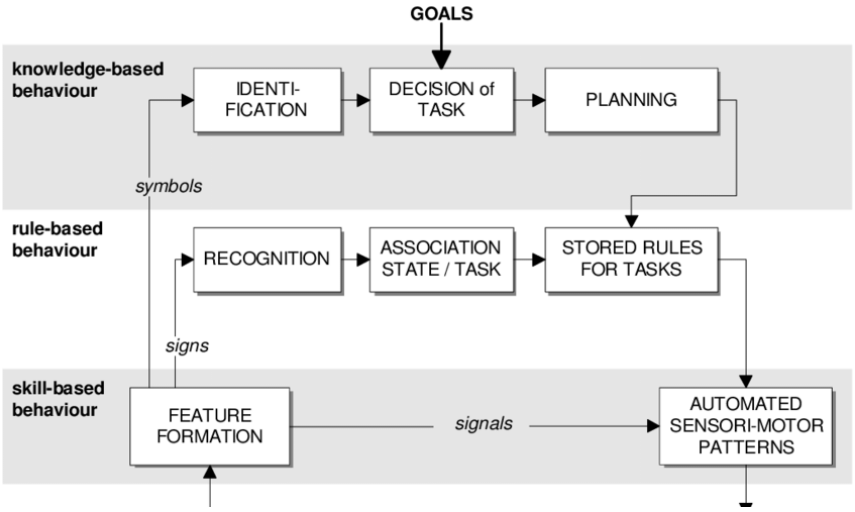

Figure 2: Rasmussen's Behavior Model- Framework for Learning [36]

Fitts' phases of skill acquisition also factor into our learning models as it essentially characterizes the process by which we form habits and gain skills. The cognitive stage involves gaining an understanding and gathering information. The associative stage involves putting tasks together, meaning that one can associate their learned knowledge with improving their performance. The autonomous stage, after significant practice to gain experience, occurs when the action becomes second nature and requires no conscious thought. [8].

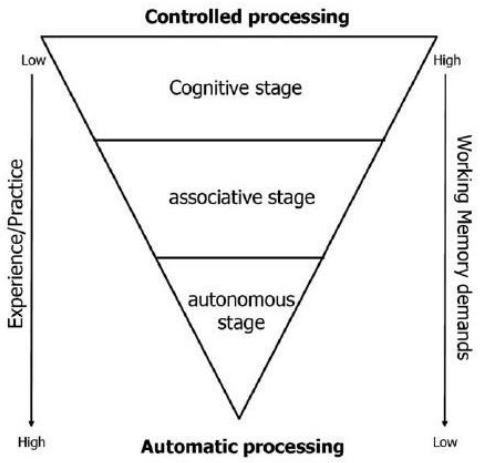

Figure 3: Fitts' Phases of Skill Acquisition [6]

The model (**Error! Reference source not found.**) indicates that the more time one spends performing an action, the less they need to consciously think about performing said action. This does not exclusively pertain to improving performance. Negative behaviors engrained at the autonomous level are essentially bad habits that must be "unlearned." This is seen in practice with some vehicle automation; by combining lane centering technology with turn signal usage, switching lanes requires turn signal use or the vehicle will provide negative feedback. A person who regularly uses turn signals will easily make this transition, where a person who does not regularly use them may have to unlearn their habit.

2.2.3 Decision making and Reaction time

Driving decisions are almost always complex because there are multiple response options for the driver. This means that their reaction time falls under the "*choice* reaction time" category—indicating that the driver will require time to detect the stimulus, identify the stimulus, select a response, and execute that response [22] (Proctor & Van Zandt, pp. 98). In a driving scenario where the vehicle is operating autonomously, the time to execute the response is increased because the driver is not likely in a "ready" position with hands on the wheel or feet on the pedals. The human information processing model below mirrors the three stages of reaction time tasks (where for reaction time the three stages would be stimulus identification, response selection, and response execution, yielding a movement instead of a response). This model illustrates how environmental stimuli are processed by combining memory, attention, and behavior subsystems and their interactions. Broadly speaking, sensory information is recognized and used to inform decision making which is backed by and stored in memory. From this point a response can be made. This output acts on the environment, and the human is able to sense and process the results in this circular cycle. Though for computer information processing the subsystems operate differently, it follows a similar structure where sensors perceive the environment and decision-making algorithms process the information to recommend or produce action.

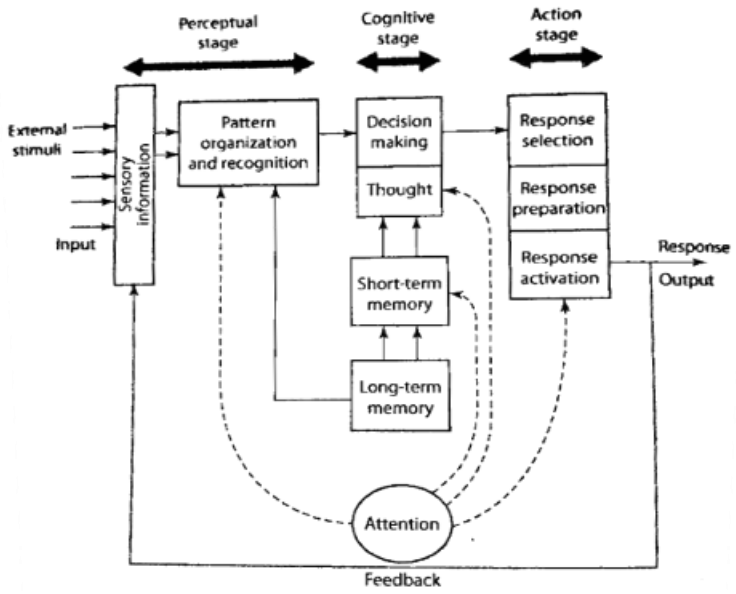

Figure 4: Human Information Processing model [21]

In continuation, the model of situational awareness can build upon the perception stage. It emphasizes "the perception of elements in the environment…, the comprehension of their meaning, and the projection of their status in the near future" [3]. In Figure 5, situational awareness leads to a decision and performance of actions, similar to Figure 4, but notably includes goals and preconceptions. For example, a human is able to perceive a yellow traffic light, comprehend that this means "slow", and project whether or not they'll make the light or not. The inclusion of "goals" may affect the outcome of this event- if the goal is to not get a ticket because a police officer is nearby, the driver may opt to slow down. Conversely, if they are running late to an event, they may opt to speed up to try to make the light.

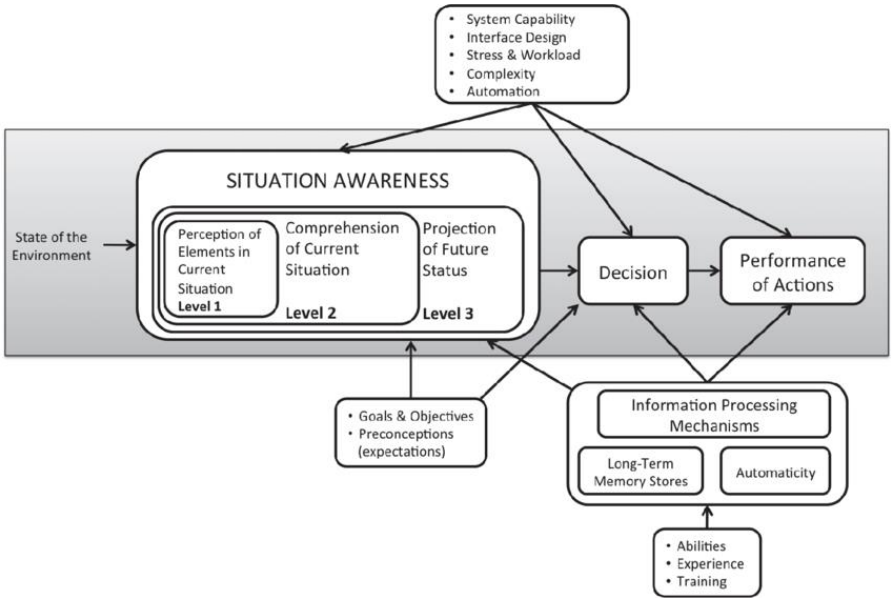

Figure 5: Endsley's Model of Situational Awareness [19]

Automation, as evidenced by the Uber case, can struggle in the comprehension and projection stages, which is why human supervision is necessary. Methods of evaluation include an analysis of the subject's

ability to recall (and predict) a scene from a paused environment, or a dynamic measurement of reaction time and accuracy [22].

2.2.4 Attention

According to Proctor and Van Zandt (pp. 228-233) there are two primary models of attention-- bottleneck and resource models. Bottleneck models operate under the assumption that the amount of information we can process is limited, while resource models view attention as a resource which can be distributed to tasks. Once the information limit is reached, or as the resources are depleted, performance decreases. [22].

Bottleneck models can be further divided into early selection and late selection theories. Early selection concludes that one's mind can focus on only a subset of information at a time and that once the subject of focus is determined, the rest of the information will remain largely unprocessed. Late selection suggests that all inputs may be identified but recallability will exist for only a limited subset. Load theory combines these models by incorporating input complexity—if the inputs are simple enough the processing can occur later, or conversely if the inputs are complex the mind will have to select early on which input they will focus on. [22].

Resource models are divided according to single source processing and multiple source processing. Single source states that different tasks require different allocations of attention. An important insight from studies in this area of research indicate that learned tasks have less attentional demand than new tasks. Multiple resource models expand on this concept by theorizing that visual and auditory cognitive subsystems act to process verbal and spatial information- and if the tasks being processed are distinct under these categories, they can be processed in parallel more effectively. [22].

The insights these models reveal offer guidance for human machine interface (HMI) design. The research suggests that humans have limited processing capabilities, but also that it is possible to strategically prioritize the most "attention grabbing" alerts. For example, if a user is inundated with tonal alerts, they may respond to the loudest or most unique tone first. Alternatively, if most of the information is visually processed, the user may be able to comprehend reading a dashboard and responding to an auditory alert. Furthermore, attentional allocation may vary over the course of a drivers' operation of the vehicle as the features become learned. [22].

2.2.5 Automation and Controls

Driver feedback can be visual, auditory, or tactual (haptic)—each method being best used under certain scenarios and conditions. For example, if the message is complex or you are in a noisy area, a visual signal will work best. Alternatively, if a message is short or calls for immediate action an auditory signal may be preferred. Tactile displays tend to be the most disruptive. [22] (Proctor & Van Zandt, pp. 191 & 221). In the systems analyzed for this thesis, all three methods of feedback are options for the automation escalation strategy. Visual feedback is used for initial alerts and is largely limited to the wheel and dash displays in the form of lighting and informative notifications. Auditory or tactual feedback are options for the secondary and tertiary alerts (used in conjunction with visual cues) in the form of warning chimes or seat vibration.

Human factors design emphasizes making the system useful and usable. These designs take into account perceptual factors including visual, auditory, and tactual information, and optimize them in control design such that the user is able to quickly understand their purpose and is able to employ them successfully. This characteristic is broadly referred to as affordance and indicates the intuitiveness of the design.

Design considerations including consistency, effective mapping between a control and its effects, conformational feedback, and system constraints [18] are particularly important in automated systems that are mode dependent. When transitioning between modes, such as manual to automated, it is possible to become uncertain of the state the vehicle is in. This occurrence is known as mode confusion, and it can

arise from design flaws including, "interface interpretation errors, inconsistent behavior, indirect mode changes, operator authority limits, unintended side effects, and lack of appropriate feedback" [12]. These design efforts help align the users' mental model with the actual operational model of the system, and help prevent mode confusion in addition to improper trust calibration.

When designing the interface and alert system, it is also important to remember that too many features and alerts can actually decrease understanding of the system. When the driver has too much information to process and recall, their performance may decrease as a result. Conversely, with too few alerts (e.g. the Tesla case, with notices to pay attention occurring in the span of minutes rather than seconds) means the drivers overall performance will suffer. This principle of performance and arousal is known as the Yerkes-Dodson Law (Figure 6), and relies upon an allocation of attention.

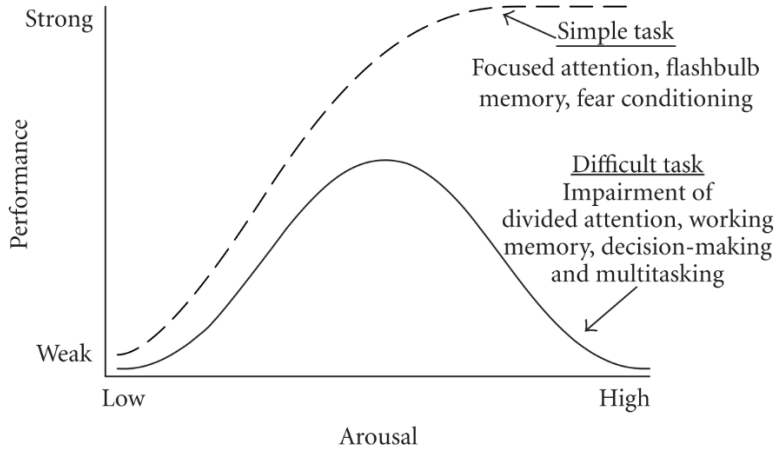

Figure 6: Yerkes-Dodson Law, Performance and Arousal Curve [2]

This principle also is true for the overall driver engagement. To maintain peak performance while retaining an active human in the loop, the driver must have sufficient tasking to remain engaged. Ideally, human limitations, such as monitoring and sensing over long stretches of time, would be the tasks performed by the machine, and machine limitations, such as edge case judgement, would be performed by the driver.

2.3 Risk analysis techniques/shortcomings

2.3.1 Traditional Methodologies

Fault Tree Analysis (FTA) is a deductive top-bottom approach using Boolean logic and symbology to represent sequences of dependencies which may result in a failure [35]. This means that it begins with the problem, and traces the possible sequences which may result in that failure. This method is challenging to apply at the system level, and is not typically used for complex human causality analysis.

Failure Modes and Effects Analysis (FMEA) is an inductive bottom up approach used to "identify a system or product's potential failure modes [and] their effects on performance" [35]. This method often employs quantification of probability and severity of the determined risks. Because this analysis begins at the component level, it provides a good vertical traceability, but weak horizontal analysis of failures occurring across elements.

2.3.2 Human Factors techniques

Cognitive task analysis (CTA), and applied cognitive task analysis (ACTA) are used for "describing and representing the cognitive elements that underlie goal generation, decision making, judgements" to understand the strategies needed for task completion. This method was supported under the argument that

cognitive demands on workers have continued to increase, even with the inclusion of machine work supplementing and/or replacing certain tasks. Applied CTA (ACTA) is a more streamlined version of the analysis which is less resource and time intensive. [15].

ACTA includes a task diagram interview, knowledge audit, simulation interview, and cognitive demands table, which are produced between a researcher and a subject matter expert (SME) [15]. These individual assessments guide the interviewee through the task to be evaluated at both a high and low level, honing in on cognitively loaded elements with contextual examples. The cognitive demands table is output for consolidation purposes which can aid in the production of instructional materials which are intended to lower the cognitive demands felt by the individual. SME knowledge is incredibly useful but can be difficult to harvest due to both the quantity of knowledge they have and the assumptions they make about what might be commonly known. This method is effective for accumulating a holistic picture of the knowledge needed for analysis to help create better training for operators and to better design systems to support human decision making. This operational method is less comprehensive than traditional CTA, and focuses on improvements based on and for existing systems.

Another concept commonly used to examine human factors in an analysis is the swiss cheese model. This looks at the system level "holes" or hazards which lead to losses. The basic concept here is that no individual unsafe act leads to an accident. Instead, there are usually a number of imperfect barriers or safeguards in place that help prevent loss, so a total failure is caused when all these conditions align and allow these failures to propagate. [24]. The holes arise from both latent failures and active failures. Active failures can usually be traced back to operator error (see *Intent classification*) and directly impact the system. Latent errors on the other hand are difficult to identify. They may be caused by designer or management error and lay dormant until conditions align to cause issues.

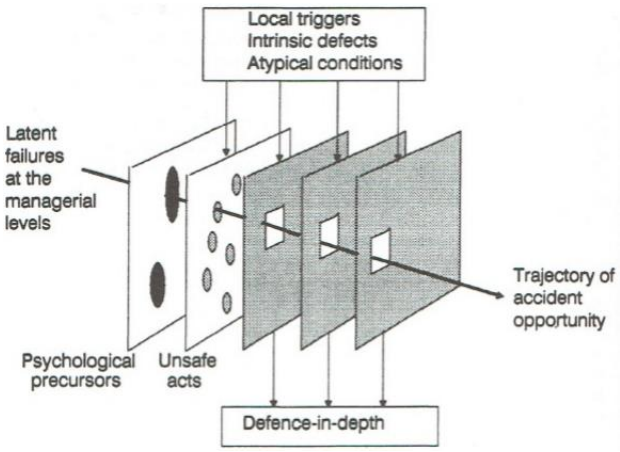

Figure 7: "Swiss Cheese" Model [25]

One issue with this model is that it is often used retroactively to identify the cumulative causes of accidents and is prone to hindsight bias. The model emphasizes human unsafe acts rather than the design of automation and other engineering choices. This model has led to expanded methods such as Human Factors Analysis and Classification System (HFACS), but are similarly limited in that they rely on pattern detection from catalogued accidents linked to human performance.

2.4 System-Theoretic Process Analysis (STPA)

The processes in this section are from the STPA Handbook (Leveson & Thomas [13]) unless otherwise noted.

2.4.1 STPA Overview

One of the key distinguishing features of System-Theoretic Process Analysis (STPA) over other hazard analysis methods is that it looks beyond component failure and considers system level weaknesses and non-failure causes of accidents. This is particularly important with the increasing complexity of systems and interdependence of parts and software. Furthermore, STPA does not require a finished system for analysis; it can and should be used early in the design process to help identify potential risks and generate improvements.

The process for completing the analysis can be broken down into four main steps, (1) Define the purpose of the analysis, (2) Model the control structure, (3) Identify unsafe control actions, and (4) Identify loss scenarios. Products of each step are listed after each section, including their typical designation characters.

1- *Define the purpose:* This step bounds the system for analysis and considers the values of stakeholders that will need to be protected. These values are imparted as a list of losses to prevent (such as loss of life, loss of or damage to vehicle, loss of mission, etc.). From this list, we can produce a list of high-level hazards or conditions which *will* lead to loss in certain environments. System constraints are a reframing of the hazard statements to specify conditions that must be upheld to prevent hazard, acting as a high-level requirement.

   Products: Losses (L-#), System-Level Hazards (H-#), System Level Constrains (SC-#)

2- *Model the control structure:* This is a block and arrow diagram which is hierarchically organized according to the level of control authority (from top to bottom). Boxes represent functional elements of the system and arrows represent control actions and feedbacks.

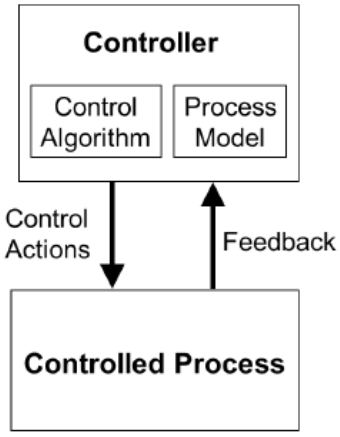

Figure 8: Generic control loop [13]

A basic three box control structure could depict a human controller at the highest level, the automation in the center, and the controlled process at the lowest level. As seen in Figure 8, Control Actions are always directed downward, and feedback is provided up to the controller. From here, increasing levels of detail can be built in to examine internal and external processes and subsystems. Responsibilities can be used to inform the process of adding additional details to the control structure or to formally write out control actions and feedbacks between components, but they are not a required output of this step.
Products: Control Structure Diagram, Responsibilities (R-#)

3- *Identify unsafe control actions*: Unsafe control actions are the control actions from the control structure, framed in such a way that they lead to a hazard. Unsafe control actions fall under one of the following four categories:

- Not providing causes hazard
- Providing causes hazard
- Providing too early, too late, or out of order
- Stopped too soon, applied too long

Each category may have multiple UCAs, and each UCA should be traced to one or more of the identified hazards. In this method, humans are identified as a part of the system and can consequently be analyzed as along with the other controllers. Lastly, similar to system constraints, controller constraints can be identified by mirroring each UCA using language that identifies prevention behavior rather than the unsafe behavior.

Products: Unsafe Control Actions (UCA-#), Controller Constraints (C-#)

4- Identify loss scenarios: These scenarios are generated to "describe the causal factors that can lead to unsafe control actions and hazards" [13] and are identified by considering *why* unsafe control actions may be executed or why safe control actions may be executed improperly. Flaws are identified and may involve the controller, control algorithm, control input, and process model, and other factors as specified in the STPA Handbook. Each scenario is formatted in a sentence structure and describes the state, information received, and the possible explanation for the state. Each scenario should be linked to a UCA.

Products: Scenarios (Scenario #)

Constraints and responsibilities are additional products which are derived from the generation of the primary products—Losses, Hazards, Control Structure, UCAs, and Scenarios.

2.4.2 Human Factors Extension

According to the traditional STPA process, humans are included within the control structure model and are identified as a part of the system; consequently they can be analyzed in the same manner as the other controllers. However, this approach has been expanded for human controllers to provide more insight and develop additional scenarios based on human factors insights. This extension to STPA is based on the work done by J. Thomas, 2013 [31], 2015 [28], and 2019 [30] and by M. France, 2017 [5].

The human factors extension combines a number of human factors models into a simple, easy to use diagram. Unlike other human factors models, this method is biased towards accidents. This makes it a more efficient method to sort through human interactions within the system as it pertains to hazard analysis. Where in STPA the generic controller model would include a generic control algorithm and process model (making it applicable to both human and machine), the extended *Human* Controller model identifies additional human-specific components that input the control action selection and feedback interpretation (see Figure 9).

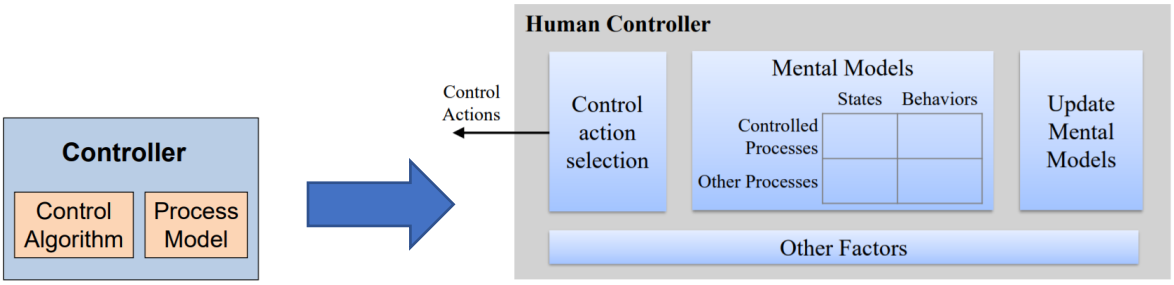

Figure 9: STPA Human Model, adapted controller box [30]

The new human controller model does not affect the creation of UCAs—making it an easy insertion into the existing STPA process. The most impacted step is scenario generation, where the human controller model is used to build more detailed scenarios for humans in the system. The major elements of the human control model are:

- **Control action selection**: addresses how the operator chose the control action to perform.
- **Mental models:** delve into the operator's beliefs about the system
- **Update mental models**: identifies how the operator came to have their beliefs about the system.
- **Other factors**: includes other relevant factors such as workload and human reaction times

To account for these considerations, the new scenario generation methodology uses each box to identify flaws in the decision making and beliefs the operator may have had for a specific UCA.

Starting with the set of human UCAs, the model above is used to build a scenario. First, mental models (MM-#) are identified to explain why the human controller might provide the UCA. These are derived in part from states and conditions in the UCA and UCA context. For example, the UCA may say that an automated feature is on, but the human's mental model may "believe" that it is on or off. Such beliefs are a common cause of human confusion and human error in previous accidents. Additional states and conditions may be included even if they are not explicitly stated in the UCA, like environmental conditions. Next, mental model flaws are identified. These include incorrect beliefs about the variables and states. In the example above, a flawed mental model would occur if the automated feature is actually on but the human's mental model "believes" that it is off. Another type mental model involves a belief about the *behavior* of a process, including its capabilities and future states. These can often be framed as "if X then Y" statements. For example, "If I turn this automation off, then the steering wheel will slowly return to center". Four broad categories of mental models are analyzed: controlled process states, controlled process behaviors, other process states, or other process behaviors.

Mental model updates (or lack thereof) are next identified to explain the mental models. Factors to consider include but are not limited to mode changes, prior commands, and phase of operation; these factors help identify flaws in the human controller's understanding.

Lastly, we must consider the unsafe actions chosen by the human controller. This includes operator awareness of controls, control options, and operator goals. These considerations help explain why the operator made the decision they did.

These elements together help to paint a clearer understanding of the operator's understanding of the system leading to the UCA. This knowledge can be used to create recommendations to help inform and improve the system design for human use.

Chapter 3: Application of STPA to Highway Traffic Automation Feature

This chapter steps through three levels of analysis for a SAE Level 2 highway/traffic driver assist feature. Each increasing level achieves a higher level of detail. It should be noted that this chapter is used to demonstrate the advantages of performing STPA, and is not a full analysis. Samples of each analysis can be found in the following sections, and full-page diagrams for control structures and full UCA tables can be found in the appendices.

3.1 Automation Candidacy and Description

Complex vehicle automation is an excellent candidate for STPA. A feature that is not yet fully developed is preferable so that STPA can be used to inform decisions early.

For the purposes of this thesis, a representative vehicle automation feature was defined. Although the feature is not identical to any one specific manufacturer's implementation, it is based entirely on real decisions and real systems currently in development or in production. The data for defining this feature was collected via a series of interviews with major automotive organizations and engineers that were directly involved in their development.

This automation feature will be labeled as HTAF (Highway Traffic Assist Feature), a fictional name assigned to the feature by the author. The feature is SAE level 2, or "SAE Level 2+", so the operator must maintain full functional vigilance. The HTAF feature is presented from the perspective of a feature that is still under development and does not exist on the market today. At this point, the design team has control over the software design, but the HMI will be determined by the company who implements the software into their vehicle.

The following description of the HTAF subsystem is intended to provide a central description for the feature, which will be referenced for the creation of the Level 1, 2, and 3 analyses.

3.1.1 HTAF Automation Description

Typical Operation: *The driver is driving on the highway. Traffic is fairly congested, so the driver enables HTAF by pressing the corresponding button on their steering wheel. The system turns on and the vehicle maintains the appropriate speed for operation in response to the vehicle ahead. The vehicle also monitors the road markings to stay centered in lane. With this automated control, the driver can remove their hands from the wheel and their foot from the brake/gas pedals. While this is occurring, the driver's attention is being actively monitored by a camera behind the wheel; if the driver looks away from the road ahead for too long, they are provided with an alert to bring their focus back to center. The longer the driver looks away, the more severe the escalation consequence will be. As traffic begins to clear, the driver resumes control of the vehicle, and turns off HTAF.*

HTAF is designed for use in passenger cars. The feature is only operable on highways, and is specifically designed to operate during traffic conditions. The design has evolved over time to include cruise control capability without traffic, but is still primarily centered on satisfying requirements derived from use in the traffic context.

HTAF has the capacity to steer to stay in the center of the lane, and to accelerate and brake (range 0-50 mph, or 0-80 kph) according to lead vehicle position. Knowledge of highway location and position is derived from GPS and preloaded maps updated quarterly. The HTAF concept requires the driver to remain vigilant, and will be subject to the escalation strategy if they do not provide sufficient attention.

Limitations/Assumptions

Note: Limitations and assumptions in this section are listed as indicated by developers in reference to the system's capabilities. This is to say that these gaps in performance are known and considered outside of

the boundary of intended capability and coverage for the software use. STPA does not assume these are true or best practice, but they may be used to inform UCA and scenario creation.

HTAF is not intended for non-highway use. HTAF is capable of performing braking in reaction to lead vehicle speeds but should not be depended on to prevent collision or to replace driver supervision. HTAF is not intended to have full cruise control capability, as the maximum operating speed when feature is enabled is 50 mph (80kph). It will only detect and respond to lane markings and obstacles detectable from the forward sensors and cameras. HTAF does not "watch" for vehicles entering driver's lane, and will not take direct action to accommodate vehicles trying to enter/exit beyond the forward react abilities. Lastly, HTAF will not be operable without the presence of a lead vehicle.

Lastly, in reference to the driver capability assumptions described in ISO 26262, no design decisions have been made to accommodate prevention of unlicensed drivers, or individuals whose driving ability may be compromised from using the system. (E.g. it is assumed that the driver is legally capable of performing the driving task).

Turning on HTAF

Typical operation: *When the driver is on an approved highway, a lead vehicle is present, and the vehicle is operating within the approved HTAF speed range (0-50 mph, 0-80 kph), the HTAF light will indicate that the feature can be enabled. The driver should check the speed they are operating at, as it will become the max speed their vehicle will operate when the feature is enabled. Next the driver presses the enable button, and they can remove their hands from the wheel and foot from the gas/brake*.

The vehicle must be on highway for the HTAF system to become engageable (example HMI: HTAF icon may appear or light up when vehicle is on approved road). HTAF will notify the driver if and why it is unable to turn on. Additionally, the internal HTAF speed limit setting is set at the time HTAF is turned on. To turn on the system:

- The driver must be looking ahead (hands on steering is not a requirement for activation)
- The vehicle should be going the intended speed
- A lead vehicle must be present

HTAF will not engage if the system:

- Is not in good health (capable of diagnosing and detecting faults)
- Is otherwise incapable of monitoring position, location, or environment (e.g. approved highways, lead vehicle, lane markings, and more)

Influence of environmental factors on vehicle function

HTAF was designed to operate in traffic and takes its cues for appropriate speeds from the car in front of it up to an internal HTAF speed limit setting. The internal HTAF speed limit setting is either:

- 50 mph, if HTAF was first enabled when the vehicle was operating <10 mph, or
- The speed the vehicle was going when HTAF was first enabled (10-50 mph)

The design decision to default to 50 mph is due to the fact that the feature is intended to be used in traffic when the vehicle may be moving much slower than the speed limit. It was decided that the automation should be able to increase speed when traffic later improves, hence the default of 50 mph speed limit setting whenever HTAF is first enabled during slow speeds.

Road/lane markings are sensed and processed by the vehicle for the purposes of lane centering. Performance may be degraded at night or in inclement weather due to limitations of the sensors and cameras. If performance degradation is detected, the operator will be instructed to take control of the vehicle via the systems escalation system.

Escalation strategy

Typical operation: *HTAF is on and the driver is letting the vehicle self-operate. They look ahead to monitor the environment and determine if action is necessary to take over the system. The driver looks away for a few seconds, and they receive a first alert from the system to bring their attention to the front. If they respond to the alert by providing the correct attention cues, no further action is required. If they continue to look away, the system escalates to a second level alert, which will include a request to place their hands on the wheel and press the "resume" button. If they continue to look away, the system will assume something is wrong with the driver, and stop in lane.*

Escalation indicators (feedback alert options) along with other elements of the HMI have not yet been decided for the candidate system, so STPA can be used to inform the design decisions. These alerts are provided to the driver to indicate that either they are not fulfilling their role as supervisor by providing appropriate attention to the road ahead, or that the vehicle is in some condition that requires operator control (such as the sudden disappearance of or change to lane markings). These are intended to assist the driver in their role of supervisor while the automation is engaged, and are intended to be intuitive enough that the driver does not have to have read the owner's manual to understand them. Alerts will include some form of visual, audial, or haptic feedback.

The following warning levels are described according to severity. It is not assumed that they have read the driver's manual. A driver may experience a series of level 1 warnings without escalation to level 2, unless the appropriate response is not provided.

- 1st level warning- eyes on road
- 2nd level warning- hands on wheel and driver must press a "resume" button
- 3rd level warning- vehicle requests driver control, if not provided vehicle comes to stop in lane with hazards and brake lights on (requires restart to operate HTAF again)

Duration of/between warnings is on the scale of seconds, and is not a fixed time but rather a time deemed by the system as appropriate (based on average time looking ahead and classifying driver awareness level over period of time). The driver can take over control at any point in the escalation strategy, however if it reaches the 3rd warning the driver will be penalized, and not be able to reengage HTAF again until the next ignition cycle.

If the vehicle encounters an unplanned obstacle and requires the driver to take immediate control, it will jump to the second warning while asking the driver to take control. Some upcoming obstacles may be known in advance (e.g. mapped construction areas) and may be timed to alert the driver earlier. These requests for manual control will be accompanied by a brief explanation to help the driver understand the vehicle's behavior.

Turn off HTAF

Normal Operation: *The driver notices that traffic is speeding up, or decides they want to resume manual control of the vehicle. The driver turns of HTAF and resumes control.*

Another Example: *The driver may wish to only temporarily take control, e.g. to let a vehicle merge into their lane. To do this they might brake briefly (< 3s), and once the merge is over they can allow HTAF to resume control. However, it is possible that the driver may need to intervene to prevent collision, e.g. if a vehicle is approaching from the side. The driver may in that instance opt to perform hands on braking or steering to deactivate HTAF and resume manual control.*

The driver can deactivate or disable HTAF by:

- Using the on/off HMI (requisite hand/eye position required)

- Manually deactivate the system by pressing and holding the gas/brake pedals (>TBD duration, approx. 3s)
- Braking with hands on the wheel
- Turning the wheel beyond a certain radius
- Braking or acceleration <TBD duration (approx. 3s) to temporarily override (after which HTAF will resume vehicle controls)
- Not providing attention cues for extended periods
- Not responding to requests to take control

Environmental conditions may also lead to requests for control, which left unattended will result in feature deactivation by stopping in lane. For example, if the driver monitoring system or vehicle sensors are detected to be blocked, the driver will be asked to take control. Furthermore, certain ODDs may result in sensor degradation, at which point the driver would also be asked to take control. The driver will need to take over when construction is present and when there is a lack of lane markings. Getting off the highway will lead to deactivation alerts and requests.

3.1.1.1 HTAF Modes

There are four major HTAF modes that govern HTAF operation:

HTAF On: Vehicle steering and speed are controlled by HTAF. This mode can be triggered by pressing a button, and requires a lead vehicle to be in range.

HTAF Deactivated: Vehicle steering and speed is under manual control. Deactivation is possible via manual controls (steering, braking, accelerating) or by pressing a button to turn off HTAF. Note: "deactivated" mode is the same as manual vehicle operation.

HTAF Overridden: Vehicle is under HTAF control, but driver temporarily takes over acceleration/braking. When this occurs, HTAF maintains control over steering to keep vehicle in lane. Note: deactivate, not override, occurs when driver operates steering.

Degraded: If the driver does not provide required supervision over system when prompted (measured according to forward eye direction and ability to respond to escalated alert prompts such as place hands on steering wheel), HTAF will degrade the system performance by beginning a stopping sequence. This sequence stops the vehicle in lane and provides hazard/braking lights.

3.2 Losses and Hazards

For this analysis, losses for this analysis were chosen first according to safety of the persons in or external to the car, and secondly around the usability of the system. In particular, L-4 is a unique add to the list of losses, as it pertains to loss of perceived value rather than tangible (physical) value. It is intended to capture human understanding of automated features, and will ultimately reflect the usability of the system. For example, if the vehicle behaves counter to the user's intent, they may not trust the feature they were using—diminishing its value to the owner/user.

Losses

L-1 Loss of life or injury to people

L-2 Loss of or damage to vehicle

L-3 Loss of life or damage to objects outside of vehicle

L-4 Loss or degradation of customer trust

System Level Hazards

H-1 Vehicle does not maintain safe distance from other vehicles <L-1, L-2, L-3, L-4>

H-2 Vehicle does not maintain safe distance from terrain and other obstacles †<L-1, L-2, L-3, L-4>

H-3 Vehicle does not comply with traffic laws <L-1, L-2, L-3, L-4>

H-4 Vehicle behavior confuses driver or other drivers <L-1, L-2, L-3, L-4>

Though not utilized in this analysis, it is possible to iteratively refine hazards. These may be used to identify more specific constraints. For example, to prevent H-1 and H-2, acceleration, braking, and steering would need to be controlled. Sample refined hazards might include:

H-1.1 Braking is insufficient to slow or stop vehicle

H-1.2 Acceleration is insufficient to maintain safe distance from other vehicles

H-1.3 Steering maneuvers vehicle off of road

H-1.4 Steering maneuvers vehicle into path of other vehicles

3.4 Iteration 1

The purpose of a level one analysis is to identify the overall, high level elements of the system and to determine the high-level control actions taking place. This is typically depicted as a 3-box control structure where the top box is the human controller, the middle box is the automation, and the lowest box is the controlled processes. In Figure 10, automation is broken into two boxes for the sake of simplicity- as we are specifically looking at HTAF and its relationship with the controller and other driver assistance features. (Other features may be automated cruise control, lane assistance, etc. For this analysis, only longitudinal controls are considered). Consequently, we see a unique input/output emerge (yellow arrow) where each of these parts of the automation have some level of control over each other. At level one, we do not have enough information to categorize these as control actions that act on specific elements of the system.

3.4.1 Control Structure

For enlarged copy of image see **Appendix B.1**.

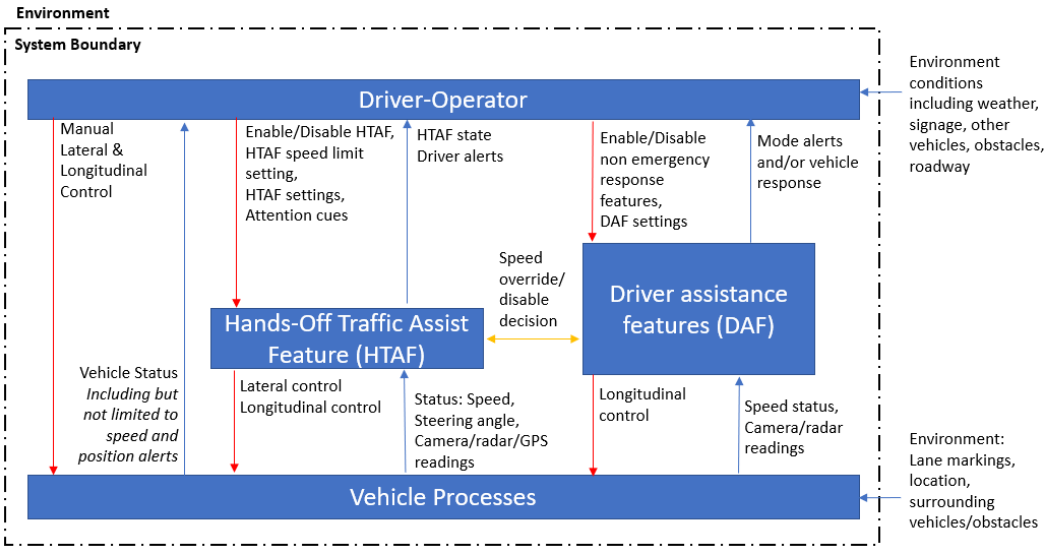

Figure 10: Level 1 Control Structure

† Obstacles includes both stationary and moving objects and includes living and non-living objects like pedestrians, animals, cones, etc.

Symbology: (Consistent through all levels)

- Boxes: Controllers/Controlled processes
- Downward (red) arrows: Control actions
- Upward (blue) arrows: Feedback
- Horizontal (blue) arrows: Information inputs/outputs that cross the system boundary
- Horizontal (yellow) arrow: Other inputs to and outputs from components
- Dashed line (black): Border between the system and the environment; elements inside the box are included in the analysis

3.4.2 Defined Control Actions

The control actions determined above are defined below, including what controller is acting on which controlled process. As the analysis progresses to more defined control structures, these control actions may be redefined with new levels of detail or nomenclature.

The following section is organized by controller. Under each controller is a series of control actions depicted in the control structure. The format of each bulleted control action is as follows:

- **Control Action**
  - ***(Controller →(acts on) Controlled Process)***
  - Definition

Driver Controls

- **Manual Longitudinal Control**
  - ***(Driver → Vehicle Processes)***
  - Acceleration/Braking action performed by the driver via application of force to the gas/brake pedal to affect the longitudinal (forward) movement of the vehicle. Use applies to manual driving mode.
- **Manual Longitudinal Control**
  - ***(Driver → Vehicle Processes)***
  - Steering includes action performed by the driver via the application of toque to the steering wheel to change the lateral (left/right) direction of the vehicle. Use applies to manual driving mode.
- **Enable HTAF**
  - ***(Driver → HTAF)***
  - Enable HTAF refers to the "turning on" of the HTAF system.
- **Disable HTAF**
  - ***(Driver → HTAF)***
  - Disable HTAF refers to the "turning off" of the HTAF system from the enabled mode. This includes both momentary and total disengagement.
- **HTAF Settings**
  - ***(Driver → HTAF)***
  - Following the Super Cruise model, for this structure we will assume the driver has some control over the type of feedback they will receive. For example, they may opt to have haptic feedback over audio feedback.
- **HTAF Speed Limit Setting**
  - ***(Driver → HTAF)***

    - Setting HTAF speed is possible over a minimum threshold. The driver simply drives at their intended max speed for the duration of HTAF use and then enables the system (similar to cruise control). Setting speed requires presence of lead vehicle, and requires it to be "in range" (not too close to driver's vehicle, but not out of range)
- **Provide Attention Cues**
    - ***(Driver → HTAF)***
    - The driver may provide attention cues to maintain "hands off eyes on" control of the vehicle. If the driver looks away for too long they will be alerted by an escalation sequence, which will require them to resume eyes on the road, place hands on steering wheel and resume, or take control of the vehicle.
- **Enable [non-emergency response] DAF**
    - ***(Driver → DAF)***
    - "Turn on" non-emergency response driver assistance features (DAF) such as cruise control.
- **Disable [non-emergency response] DAF**
    - ***(Driver → DAF)***
    - "Turn off" of the DAF from enabled mode; temporary override may be available depending on the feature and its provider.
- **Set DAF Speed**
    - **(Driver → DAF)**
    - Driver reaches their intended speed for the duration of DAF use and then enables the feature.

HTAF Controls

- **Longitudinal Control**
    - ***(HTAF → Vehicle Processes)***
    - Steering performed as calculated by HTAF when engaged in response to environment.
- **Longitudinal Control**
    - ***(HTAF → Vehicle Processes)***
    - Acceleration/Braking performed as calculated by HTAF when engaged. May result from environment sensing or lack of driver engagement.

DAF Controls

- **Longitudinal Control**
    - ***(DAF → Vehicle Processes)***
    - Acceleration/Braking performed as calculated by DAF when engaged. May result from environment or preset driver speeds. Does not require driver permissions to be enabled if it is an emergency response feature.

3.4.3 Unsafe Control Actions

The UCAs below are exclusively linked to use in the highway environment (though attempted use in an incorrect environment does emerge in UCAs). The sample of UCAs below result from the refinement of the "Disable HTAF" control action, seen in Table 1. For additional Level 1 UCAs, see **Appendix B.2: Level 1 UCAs**.

Some terms and phrases are used in the creation of UCAs to help provide context for the action. For the reader's understanding, these terms are here defined:

- **Collision is imminent:** Driver's vehicle will not be able to stop or slow to prevent collision without radical intervention. Collision without action is "unavoidable".
- **Collision path:** Driver's current trajectory and speed, if continued, will cause them to collide with the object/vehicle
- **Traffic guidance:** Includes speed limits, signs, temporary signs/blockages, line markings on road, temporary barriers, traffic speed, weather recommended speed, etc. All rules or regulations pertaining to vehicle operation while on a highway. Most commonly used in reference to speed.
- **Attention cues:** Driver actions that are monitored by HTAF to infer a driver attention level including: eyes ahead, hands to wheel, and take control of vehicle

Table 1: Sample Level 1 UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Disable HTAF	(UCA-26) Driver does not provide disable HTAF command when transitioning to manual driving [H-1, H-2, H-3, H-4] (UCA-27) Driver does not provide disable HTAF command to take control when HTAF is on and not responding to obstacle(s) in path [H-1, H-2, H-3, H-4] […]	(UCA-28) Driver provides disable HTAF command when driver is unable to mitigate an imminent collision but HTAF is [H-1, H-2, H-4] (UCA-29) Driver provides disable HTAF command when driver preparedness to take control is low [H-1, H-2, H-3, H-4] (UCA-30) Driver performs insufficient action to disable HTAF when transitioning to manual driving [H-1, H-2, H-3, H-4] […]	(UCA-31) Driver provides disable HTAF command too early before they are ready to take manual control [H-1, H-2, H-3, H-4] (UCA-32) Driver provides disable HTAF command too late after vehicle is on collision path [H-1, H-2, H-3, H-4] […]	(UCA-33) Driver stops providing disable HTAF command too soon before mode change is applied [H-1, H-2, H-3, H-4] […]

UCA-28 might mean that customer trust is lost or degraded because the driver is providing control actions when the HTAF system is actually better equipped to respond to the environment and may not be not actively on a collision course until the driver adjusts the vehicle behavior. Another example, UCA-33, might mean that the driver did not complete the action required to transition from automated driving to either override or turn off HTAF.

The next step is to generate scenarios based on these UCAs.

3.4.4 Sample Basic Scenario Generation

Scenario generation can provide insights into system weaknesses and vulnerabilities, but it can also raise new challenges. Challenges include managing a large number of scenarios, demonstrating coverage and detecting the possible omission of scenarios, managing large amounts of repetition (inefficiency), and managing the amount of time spent on scenario generation.

A new approach to scenario generation was developed to address these challenges and provide a more time-efficient and organized approach. "Basic Scenario Generation and Refinement" [29, 32] is top-down approach which generates high level scenarios that can be refined as needed. The process generates four types of scenarios based on a controller's interactions with a controlled process. These basic scenario types are (1) Unsafe controller behavior, (2) Unsafe feedback path, (3) Unsafe controlled path,

and (4) Unsafe controlled process behavior. The first two scenarios pertain to how the controller takes in information and makes a decision, while the latter two refer to issues with how the control action is transmitted and enforced internally. Basic scenarios can be refined and combined to build more complex scenarios.

This methodology pairs well with hierarchy management, as it provides traceable generation while limiting the amount of information the analyst must process at once. Basic scenarios can provide full coverage over the control structure, but allow room for expansion and refinement as necessary. The following table can be used as a template to populate basic scenarios for each type of UCA.

Table 2: Generic Basic Scenario Generation

(UCA-#)s (For reference)				
…				
	UCA type 1: not providing causes hazard (UCA-#)	**UCA type 2: providing causes hazard (UCA-#)**	**UCA type 3: too early, too late, out of order causes hazard (UCA-#)**	**UCA type 4: stopped too soon, applied too long causes hazard (UCA-#)**
Scenario Type 1: Unsafe Controller Behavior	- controller doesn't provide <cmd> - controller received feedback (or other inputs) that indicated <context>	- controller provides <cmd> '- controller received feedback (or other inputs) that indicated <context>	- controller provides <cmd> too late/early/out of order '- controller received feedback (or other inputs) that indicated <context> on time / in order	- controller stops providing <cmd> too soon '- controller received feedback (or other inputs) that indicated <context> on time
Scenario Type 2: Unsafe Feedback Path	- feedback received by controller does not indicate <context> - <context> is reflected in information from controlled process	- feedback received by controller does not indicate <context> - <context> is reflected in information from controlled process	- feedback received by controller does not indicate <context> on time / in order - <context> is reflected in information from controlled process on time / in order	- feedback received by controller does not indicate <context> - <context> is reflected in information from controlled process
Scenario Type 3: Unsafe Control Path	- controller does provide <cmd> - <cmd> is not received by controlled process	- controller does not provide <cmd> - <cmd> is received by controlled process	- controller provides <cmd> on time / in order- <cmd> is received by controlled process too late/early/out of order	- controller provides <cmd> with appropriate duration- <cmd> is received by controlled process with in appropriate duration
Scenario Type 4: Unsafe Controlled Process Behavior	- <cmd> is received by controlled process '- controlled process does not respond by <…>	- <cmd> is not received by controlled process '- controlled process does not respond by <…>	- <cmd> is received by controlled process on time / in order '- controlled process does not respond by <…>	- <cmd> is received by controlled process with appropriate duration'- controlled process does not respond by <…>

A sample of UCAs are shown below to demonstrate the full range of scenario types for each UCA type. In the following table, the chosen UCAs are listed on the top of the chart for reference, and the corresponding number is listed in the appropriate column. Each UCA has four basic scenarios in its respective column. All UCAs chosen for this scenario generation pertain to human control actions on the HTAF automation.

Table 3: Level 1 Basic Scenario Generation

(UCA-34) Driver does not provide HTAF speed limit setting to regulate longitudinal control when the hands-off feature speed limit is not suitable for the region (e.g. legal limits) [H-3, H-4]				
(UCA-22) Driver provides enable HTAF command when in an environment that exceeds HTAF capabilities (e.g. weather, construction, emergency vehicles, etc.) [H-3, H-4]				
(UCA-24) Driver provides enable HTAF command too early before lead vehicle is in appropriate range [H-1, H-2, H-3, H-4]				
(UCA-33) Driver stops providing disable HTAF command too soon before mode change is applied [H-1, H-2, H-3, H-4]				
	UCA type 1: not providing causes hazard (UCA-34)	**UCA type 2: providing causes hazard (UCA-22)**	**UCA type 3: too early, too late, out of order causes hazard (UCA-24)**	**UCA type 4: stopped too soon, applied too long causes hazard (UCA-33)**
Scenario Type 1: Unsafe Controller Behavior	(BS-34.1) Driver does not provide new HTAF speed limit setting; driver receives correct indication of HTAF speed limit setting and suitable speed for region (e.g. legal limits)	(BS-22.1) Driver provides enable HTAF command; driver receives correct indication of environment that exceeds HTAF capabilities	(BS-24.1) Driver provides enable HTAF too soon; driver receives correct indication of HTAF status and relative vehicle position on time	(BS-33.1) Driver stops providing disable HTAF command too soon (HTAF remains enabled); driver receives correct indication HTAF is still enabled
Scenario Type 2: Unsafe Feedback Path	(BS-34.2) Feedback received by driver does not indicate suitable regional speed limit and/or HTAF speed limit setting; vehicle speed is not suitable for region	(BS-22.2) Feedback received by driver does not clearly indicate the environment exceeds HTAF capabilities; current environment exceeds HTAF capabilities	(BS-24.2) Feedback received by driver does not indicate vehicle is in range or HTAF status; vehicle position is not suitable for HTAF engagement	(BS-33.2) Feedback received by driver does not indicate HTAF is still enabled; HTAF is still controlling the vehicle
Scenario Type 3: Unsafe Control Path	(BS-34.3) Driver does provide HTAF speed limit setting; speed limit setting is not received by HTAF	(BS-22.3) Driver does not provide enable HTAF command; enable HTAF command is received by HTAF	(BS-24.3) Driver does not provide enable command; enable command is received by HTAF (especially when lead vehicle is not in range)	(BS-33.3) Driver continued providing disable HTAF for appropriate duration; disable HTAF command not received for sufficient duration by HTAF
Scenario Type 4: Unsafe Controlled Process Behavior	(BS-34.4) Speed limit setting is received by HTAF; HTAF does not respond by enforcing this limit for longitudinal control	(BS-22.4) Enable HTAF command is not received by HTAF; HTAF does enable	(BS-24.4) Driver enable command is not received by HTAF; HTAF becomes enabled (especially when lead vehicle is not in range)	(BS-33.4) Disable HTAF command is received by HTAF; HTAF does not become disabled

3.4.5 Sample Human Factors Refinement

To demonstrate the possible refinement process, the human factors approach to STPA will be applied (as proposed by Thomas 2015 [28], evaluated by France 2017 [5], and refined by Thomas 2019 [30]). Chapter 2 explains this process in more detail. Though this is not typically applied to Level 1 UCAs, it is performed here to explore how feasible the method is with limited detail for the control actions and feedback. The following model is used to generate mental model flaws (MM-#), read from right to left.

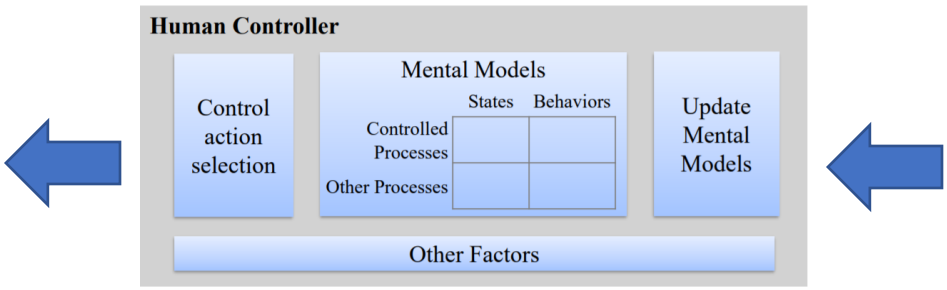

Figure 11: Generic Human Controller Model [30]

Based on this template and the UCAs above, we can identify potential "Mental Models" that explain how flawed beliefs about states and behaviors can lead to a UCA.

Table 4: Human Factors Refinement: Mental Models

(UCA-34) Driver does not provide HTAF speed limit setting to regulate longitudinal control when the hands-off feature speed limit is not suitable for the region (e.g. legal limits) [H-3, H-4]		
(BS-34.1) Driver does not provide new HTAF speed limit setting; driver receives correct indication of HTAF speed limit setting and suitable speed for region (e.g. legal limits) [UCA-34]		
	States	**Behaviors**
Controlled Processes	(MM-1) Driver believes HTAF is using driver-provided speed limit setting (but it is not)	(MM-2) Driver believes that turning on HTAF will set the HTAF speed limit (if I turn on HTAF, then the vehicle will not go any faster than it is now)
Other Processes	(MM-3) Driver believes that the region speed limit is different than it is	(MM-4) Driver believes their vehicle will automatically adjust to changes in lead vehicles and regional speed limits

These mental models describe a potential flaw in the driver's understanding of the system. The next step is to identify why these beliefs might be wrong and why they might occur anyway.

For example, consider MM-1: driver believes that HTAF is using a driver-provided speed limit setting. That belief would be valid in many cases. For example, if the driver is driving at 12 mph (20 kph) when they engage HTAF, then the fastest the vehicle will be allowed to travel is 12 mph (20 kph)—the driver-provided speed limit setting in this case. *Are there cases when this driver belief (MM-1) could be incorrect?* The belief would be incorrect any time HTAF is engaged while in standstill traffic < 10 mph (16 kph), because the vehicle would then instead automatically use a default speed limit setting of 50 mph (80 kph). If that speed is not suitable for the region, UCA-34 has occurred.

The true state of the vehicle may be that it is operating using a default speed setting, but the driver may think the vehicle is using a driver-provided a speed setting.

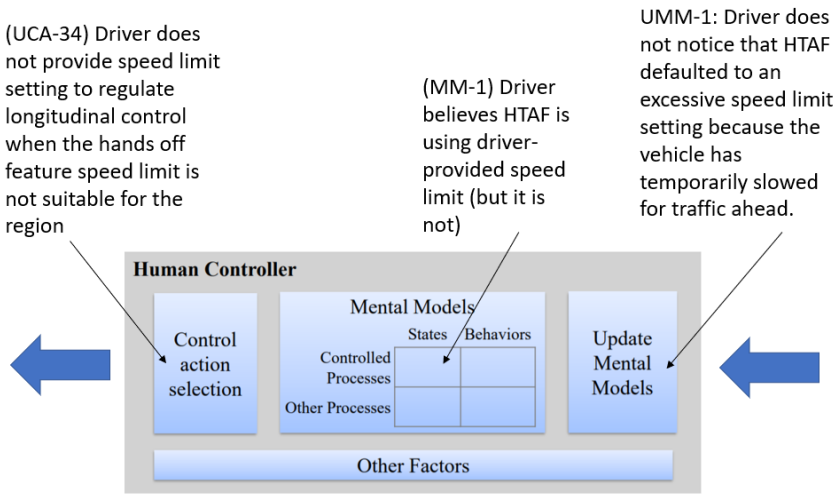

Figure 12: Refining Mental Models for Scenarios, Graphic Form

Figure 12 in paragraph form might read as follows:

Refined Scenario 1 (RF-34.1.1): *Vehicle operates at a speed that is unsuitable for the region. The reason is because the driver did not provide a new speed limit setting when the current speed limit setting was not suitable for the region [UCA-34]. The driver believed that HTAF was using a lower speed limit than it actually was [MM-1]. Although the actual speed limit setting was correctly indicated [BS-34.1], the driver learned from previous experience that turning on HTAF is one way to set the speed limit (the vehicle would not go any faster than the current speed when HTAF was turned on) [MM-2]. Although that is accurate in some cases, the driver did not know that HTAF only behaves that way when the vehicle speed is over TBD mph (10 mph or 16 kph for this analysis) when HTAF is turned on. Otherwise, HTAF will use a default speed limit of 50 mph. The discrepancy may not be obvious because the vehicle would behave no differently as long as the vehicle remains in slow traffic [UMM-1]. If the traffic disappears or picks up speed, the vehicle will unexpectedly accelerate to a speed that may be unsafe (e.g. if is raining or roads are icy, a lower speed will be safer).*

The refined scenario RF-34.1.1 explains why basic scenario BS-34.1 might occur—why the driver might not provide a new HTAF speed limit setting. The next step is to develop requirements and recommendations to address these scenarios. This is explored in Chapter 4.

3.5 Rules for Hierarchical Differences between Levels of UCAs

As proposed by Thomas 2020 [33], three types of refinement can help to manage multiple levels of iterations of STPA. These refinements can be applied to the creation of UCAs, detailing subsystems within the control structure, detailing the context conditions, and refining control actions into specific behaviors/acts to perform the control. It should be noted that these types of refinement are not necessarily exhaustive, and multiple methods can be applied to bring a UCA or scenario to the next level. Each hierarchical level should promote the creation of new insights and information that can help determine what conditions exist for an unsafe control action or scenario. Creating and organizing UCAs and scenarios according to hierarchy is a helpful tool for managing complexity as it decreases the analyst's mental load by "chunking" the content. Each level is a manageable increase that is based on the level prior. Starting at a very high level helps minimize the risk of overlooking UCAs and scenarios.

Method 1 *Subsystem Detailing:* Provide more detail for a box in the control structure by including the subsystems within it, as well at the resulting internal control actions and feedbacks.

Method 2 *Context Conditions:* Take the context (typically from a UCA) and provide more detail into the conditions under which it is true. This may result in additional insight that leads to a change to the original UCA or the identification of additional UCAs. More detail should be provided than in the prior iteration.

Method 3 *Control Action Detailing:* Take one control action and determine if that action can be performed in multiple ways. If it can, each of these actions can be modeled as separate control actions at the next level of iteration.

These methods will be applied to derive a Level 2 and Level 3 analysis, and detailed samples from the analysis will be discussed further in Chapter 4.

3.6 Iteration 2

The first iteration produces high-level results that can be used to guide concept development, early design decisions, and architecture development. The first iteration also provides a basis which can be refined to produce a more detailed second iteration of analysis that can lead to new insights. This section will demonstrate a second iteration, or "Level 2" analysis, by demonstrating refinement to the steps of STPA including building the control structure, creation of UCAs, and scenario generation. These steps will include the following refined products:

- Control Structure
- Control Actions
- Feedback and Other Information
- Unsafe Control Actions
- Scenarios

3.6.1 Control Structure

The Level 2 control structure, shown in Figure 13, demonstrates a refinement of the control structure analyzed in Level 1. More detail about the automation is included to explain how the driver actions affect the different subsystems within the vehicle. Additionally, both the HTAF and DAF automation boxes are refined to identify high-level subsystems such as Driver Monitoring. These additions help define the control actions that are internal to the automation, and also promote a greater understanding of the interfaces between the automation and the driver. Though the human factors approach was demonstrated in the prior section, this is the level at which the STPA human factors model is actually brought into the diagram. This is because Level 2 typically provides a sufficient level of detail to inform the driver's control action selection.

Based on the refinement methods defined in Section 3.5, the transformation below to a Level 2 control structure demonstrates Method 1 and Method 3. The first method is evident via the inclusion of subsystems in the HTAF automation box, and the DAF automation box. The third method is evident where lateral/longitudinal controls refine into acceleration, braking, and steering, where attention cues refines into engage/disengage HTAF, where DAF longitudinal control refines into speed keeping and emergency braking, and where disable HTAF refines into override, deactivate, and "turn off." At this stage, the yellow arrow from Figure 10: Level 1 Control Structure indicating "other inputs to and outputs from components" disappears and is replaced by two separate control actions (now shown as blue arrows in Figure 13) due to the increased knowledge of the internal subsystems. This means that the automations' authority over each other can now be explicitly modeled.

For an enlarged version of the of image below, see **Appendix C.1: Enlarged Level 2 Control Structure.**

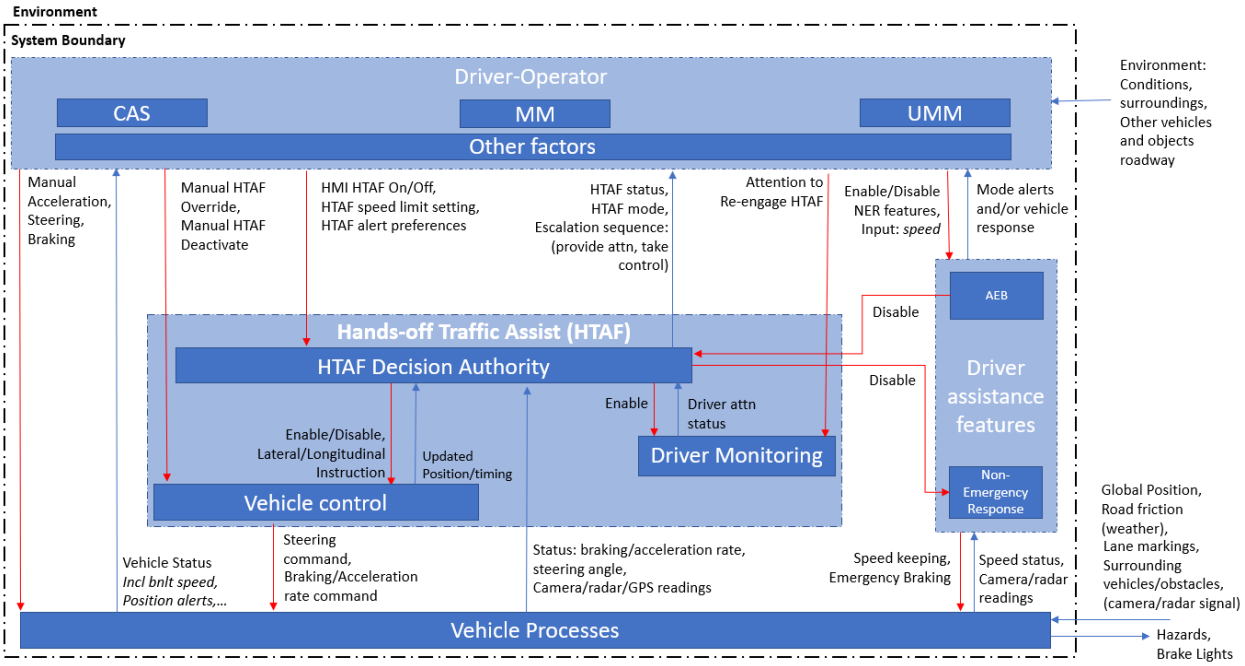

Figure 13: Level 2 Control Structure[‡]

The newly emerged controllers within HTAF include the HTAF decision authority, vehicle control, and driver monitoring. The decision authority is responsible for making the decisions which lead to steering, braking, and acceleration controls to maintain speed and react to the environment. These decisions are informed by environmental inputs, vehicle status, and driver attention cues. Driver monitoring is responsible for gauging that the driver is supplying sufficient attention cues. Vehicle control takes the direction imparted by the decision authority and provides the command to the vehicle processes. Within DAF, the newly emerged controllers include automatic emergency braking (AEB) and non-emergency response [driver assistance] features. Non-emergency response features include all functions that have longitudinal control over the vehicle, but are not intended for accident prevention (e.g. cruise control).

3.6.2 New and Amended Control Actions

Driver Controls

- **Manual Acceleration**
  - ***(Driver → Vehicle Processes)***
  - Acceleration action performed by the driver via application of force to the gas pedal to affect the longitudinal (forward) movement of the vehicle.
- **Manual Braking/Deceleration**
  - ***(Driver → Vehicle Processes)***
  - Braking action performed by the driver via application of force to the brake pedal to affect the longitudinal (forward) movement of the vehicle.
- **Manual Steering**
  - ***(Driver → Vehicle Processes)***
  - No change to control definition.

[‡] New Symbology: Dashed lines around light blue colored HTAF and Driver Assistance Features (DAF) boxes are left to indicate that the dark blue control boxes are elements belonging to those subsystems.

- **Manual HTAF Override**
  - ***(Driver → Vehicle Control)***
  - Temporary disengagement of HTAF caused by manual action on vehicle controls.
- **Manual HTAF Deactivate**
  - ***(Driver → Vehicle Control)***
  - Full disengagement of HTAF caused by manual action on vehicle controls
- **Turn HTAF Off**
  - ***(Driver → Mode Manager)***
  - HTAF is turned off via a pushbutton interface. Does not require hands on wheel or foot on pedal(s).
- **Turn HTAF On**
  - ***(Driver → Mode Manager)***
  - Control was previously named "enable HTAF", but definition is carried over
- **Set HTAF Alert Preferences**
  - ***(Driver → Mode Manager)***
  - Following the Super Cruise model, for this structure we will assume the driver has some control over the type of feedback they will receive. For example, they may opt to have haptic feedback over audio feedback.
- **Set HTAF Speed**
  - ***(Driver → Mode Manager)***
  - The driver reaches their intended speed for the duration of HTAF before enabling the HTAF (similar to cruise control) up to 50 mph.
- **Attention Cues to Re-engage HTAF**
  - ***(Driver → Driver Monitoring)***
  - Provide attention cues has been refined according to the level or amount of attention cues provided. If above a certain threshold, the driver can continue operating the vehicle with HTAF use (or sufficient to "engage" HTAF)—even if attention alerts are provided. Providing attention cues below a certain threshold, and not responding to vehicle alerts or commands (3rd level warning) will yield a "disengage" where the vehicle stops in lane in response to the attention cues provided. HTAF may not be reengaged until the next ignition cycle.
- **Enable [non-emergency response]**
  - **DAF *(Driver → DAF)***
  - No change to control definition.
- **Disable [non-emergency response] DAF**
  - ***(Driver → DAF)***
  - No change to control definition.
- **Set DAF Speed**
  - **(Driver → DAF)**
  - No change to control definition.

Decision Authority Controls

- **Enable Driver monitoring**
  - ***(Decision Authority → Driver Monitoring)***
  - Enable eye tracking and alert system when HTAF is engaged
- **Enable Automated Vehicle Control**
  - ***(Decision Authority → Vehicle Control)***

- Convey "on" to vehicle controls (acceleration, braking, steering)

- **Disable Automated Vehicle Control**
  - ***(Decision Authority → Vehicle Control)***
  - Convey "off" to vehicle controls (acceleration, braking, steering)
- **Set Steering Angle**
  - ***(Decision Authority → Vehicle Processes)***
  - Determine/calculate appropriate steering angle/duration of steering to keep vehicle in lane based on sensor readings of environmental inputs
- **Set Acceleration Rate**
  - ***(Decision Authority → Vehicle Processes)***
  - Determine/calculate appropriate acceleration rate to allow vehicle to maintain set speed and safe following distance based on sensor readings of environmental inputs
- **Set Braking/Deceleration Rate**
  - ***(Decision Authority → Vehicle Processes)***
  - Determine/calculate appropriate braking rate/duration to allow vehicle to maintain set speed and safe following distance based on sensor readings of environmental inputs
- **Disable**
  - ***(Decision Authority → Non-Emergency Response (NER) DAF)***
  - Disable NER driver assistance features such as cruise control when HTAF is enabled

Vehicle Control (VC) Controls

- **Enforce Steering Angle**
  - ***(VC → Vehicle Processes)***
  - Enforce steering command to keep vehicle in lane
- **Enforce Acceleration Rate**
  - ***(VC → Vehicle Processes)***
  - Enforce acceleration command to allow vehicle to maintain set speed and safe following distance
- **Enforce Braking/Deceleration Rate**
  - ***(VC → Vehicle Processes)***
  - Enforce acceleration rate to allow vehicle to maintain set speed and safe following distance

Driver Assistance Features (DAF)

- **Speed Keeping**
  - ***(DAF → Vehicle Processes)***
  - Provide longitudinal control to maintain set speed (may or may not enforce safe following distance)
- **Emergency Braking**
  - **(DAF Authority → Vehicle Processes)**
  - Provide braking to slow/stop vehicle when it violates minimum forward distance to prevent/lessen intensity of collision
- **Disable**
  - ***(AEB → Decision Authority)***
  - Provide disable to vehicle automation (HTAF) controls when engaged

Recall the control action "Disable HTAF" from Level 1. At Level 2, this control action is "absent" from the control structure because it has been refined to three new control actions; Manual HTAF Deactivate, Manual HTAF Override, and Turn HTAF Off.

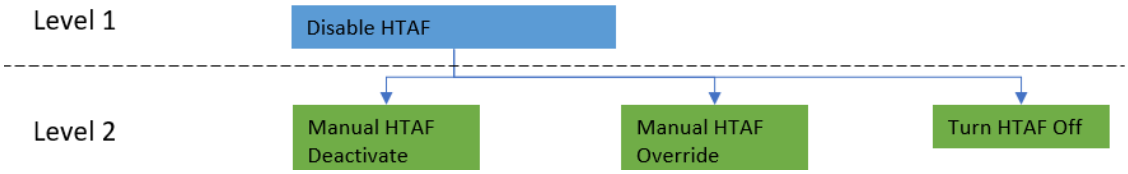

Figure 14: Level 1 to Level 2 Control Action Refinement

This is an example of the third refinement method. Each of these new control actions, and all other control actions from the control structure, are the new basis for UCA generation. These UCAs will expand on those created in Level 1.

3.6.3 Unsafe Control Actions

At this step, refinement to context (Method 2) can be applied.

For example:

Level 1 (UCA-27) "Driver does not provide disable HTAF command to take control when HTAF is on and not responding to obstacle(s) in path," is refined to Level 2 (UCA-31) "Driver does not provide manual override when HTAF is not responding to prevent a collision."

The change to the control action "disable" (Method 3 refinement) is evident in the control structure, and propagated in the new UCA as "manual override". Method 2 is indicated by changing "not responding to obstacles in path" to "not responding to prevent collision".

In this section, a sample of UCAs is provided to demonstrate the Level 1 "Disable HTAF" refinement into 3 control actions the driver can perform to temporarily or fully disable HTAF. Manual override includes actions which allow the driver to temporarily take over vehicle control, after which HTAF resumes automated control. The driver may wish to override to allow a vehicle to merge in front of them, for example. Manual deactivate fully disables HTAF upon driver intervention. Both deactivate and override are performed by braking, accelerating, or steering, with slight changes between the two disable options. "Turn Off HTAF" exclusively refers to the driver pressing a button on the steering wheel which will turn off HTAF.

For additional Level 2 UCAs, see **Appendix C.2: Level 2 UCAs**.

Table 5: Sample Level 2 UCAs, expanded from Disable HTAF

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Manual Override HTAF	(UCA-31) Driver does not provide manual override when HTAF is not responding to prevent a collision [H-1, H-2, H-3, H-4] […]	(UCA-32) Driver provides manual override to change vehicle speed while hands are on the wheel (resulting in unintended deactivation and confusion) [H-4] (UCA-33) Driver provides manual override to change vehicle speed while applying torque to	(UCA-34) Driver performs override too late after vehicle is on collision path [H-1, H-2, H-3, H-4] (UCA-35) Driver performs override too early before they are ready to take temporary manual	(UCA-36) Driver continues providing manual override too long (3s) until system deactivates when driver is temporarily overriding [H-1, H-2, H-3, H-4] (UCA-37) Driver provides manual override too long

		the steering wheel (resulting in unintended deactivation and confusion) [H-4] […]	control [H-1, H-2, H-3, H-4] […]	until vehicle enters collision path [H-1, H-2, H-3] UCA-38) Driver stops providing manual override too soon before collision is averted [H-1, H-2, H-3] […]
Manual Deactivate HTAF	(UCA-38) Driver does not provide manual deactivate to change vehicle speed/direction when vehicle is on collision path [H-1, H-2, H-3, H-4] (UCA-40) Driver does not provide manual deactivate to change vehicle speed/direction when HTAF is unable to supervise the vehicle effectively [H-1, H-2, H-3, H-4] […]	(UCA-41) Driver provides manual deactivate when vehicle is on collision path and driver is unable to mitigate [H-1, H-2, H-3, H-4] (UCA-42) Driver provides manual deactivate to take manual control of speed/direction when their hands are off the wheel or their foot is off the gas/brake [H-1, H-2, H-3, H-4] […]	(UCA-43) Driver performs manual deactivate too late after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-44) Driver performs manual deactivate too early before they have full manual control [H-1, H-2, H-3, H-4] […]	(UCA-45) Driver stops performing manual deactivate too soon before HTAF is fully deactivated [H-1, H-2, H-3, H-4] […]
Turn Off HTAF (via control panel)	(UCA-46) Driver does not turn off HTAF to take over control when vehicle does not respond to obstacle(s) in path [H-1, H-2, H-3, H-4] (UCA-47) Driver does not turn off HTAF when road/environmental conditions are too degraded for continued HTAF use [H-1, H-2, H-3, H-4] […]	(UCA-48) Driver turns off HTAF, putting vehicle on a collision path when no collision was imminent [H-1, H-2, H-3, H-4] (UCA-49) Driver turns off HTAF when driver is not attending manual controls [H-1, H-2, H-3, H-4] (UCA-50) Driver turns off HTAF when driver is not monitoring road conditions [H-1, H-2, H-3, H-4] […]	(UCA-51) Driver turns off HTAF too late after already deactivating via manual controls [H-1, H-2, H-3, H-4] (UCA-52) Driver turns off HTAF too late after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-53) Driver turns off HTAF too early before they are prepared to take manual control [H-1, H-2, H-3, H-4] […]	[…]

For the manual deactivation UCAs, one that may cause some confusion is UCA-41. This might refer to the automation being better suited to perform in those conditions to prevent collision, OR the driver's deactivation causing vehicle behavior that was unpredictable to other drivers—leading to collision. A potential design flaw also emerges based on UCA-44, "Driver performs manual deactivate too early before they have full manual control." That the driver is allowed to fully deactivate the automation

without demonstrating full manual control demonstrates a need for there to be some level of control over the transition to manual driving.

"Turn off HTAF" UCAs are unique in that the driver is making a conscious decision to turn off HTAF (unless somehow accidentally performed), whereas the manual control-based actions are likely to include more reactionary derived controls. That said, even a conscious action is not always the safest control. UCA-48 lists turning off HTAF as unsafe when no collision was imminent. This is possible where the vehicle is better equipped to handle driving in that instant. For example, if the driver turns off HTAF midway through a curve in a road, and they are not prepared to take immediate control, then they may have been better off when automation had control.

The next step in the STPA process is to build scenarios to explore why the driver might perform UCAs such as these.

3.6.4 Sample Basic Scenario Generation

Level 2 scenarios are based on level 2 UCAs, so they are already more refined than the Level 1 scenarios. At this level they have more specific inputs/outputs for the control action or feedback, or more specific action consequences on the system. These scenarios are still considered "basic" until they are refined with factors like mental model beliefs that help us understand the causes of the scenarios.

Table 6: Level 2 Basic Scenario Generation

(UCA-47) Driver does not turn off HTAF when road/environmental conditions are too degraded for continued HTAF use [H-1, H-2, H-3, H-4]				
(UCA-49) (UCA-61) Driver turns off HTAF when driver is not attending manual controls [H-1, H-2, H-3, H-4]				
(UCA-44) Driver performs manual deactivate too early before they have full manual control [H-1, H-2, H-3, H-4]				
(UCA-45) Driver stops performing manual deactivate too soon before collision is averted [H-1, H-2, H-3, H-4]				
	UCA type 1: not providing causes hazard (UCA-47)	**UCA type 2: providing causes hazard (UCA-49)**	**UCA type 3: too early, too late, out of order causes hazard (UCA-44)**	**UCA type 4: stopped too soon, applied too long causes hazard (UCA-45)**
Scenario Type 1: Unsafe Controller Behavior	(BS-47.1) Driver does not provide turn off HTAF command; driver has correct indication of road/environment conditions and HTAF status	(BS-49.1) Driver provides turn off HTAF command; driver receives correct indication of their control of vehicle and HTAF status	(BS-44.1) Driver provides deactivate HTAF too early; driver has correct indication that full manual control has not occurred	(BS-45.1) Driver stops providing manual deactivation too soon; feedback correctly indicated collision was not yet averted
Scenario Type 2: Unsafe Feedback Path	(BS-47.2) Feedback received by driver does not adequately indicate or road/environment conditions; road/environment conditions are not suitable for automated driving	(BS-49.2) Feedback received by driver does not indicate vehicle is not under manual control; driver does not have full manual control	(BS-44.2) Feedback received by driver does not adequately indicate full manual control has not occurred; driver does not have full manual control	(BS-45.2) Feedback received by driver did not indicate collision was not yet averted; the collision was still imminent

Scenario Type 3: Unsafe Control Path	(BS-47.3) Driver does provide turn off HTAF command; command is not received by HTAF decision authority	(BS-49.3) Driver does not provide turn off HTAF command; turn off HTAF command is received by decision authority	(BS-44.3) Driver does not perform deactivate command; deactivate command is received by HTAF decision authority (especially before driver has manual control)	(BS-45.3) Driver continued providing manual deactivate for adequate duration; manual deactivate received for insufficient duration by vehicle controls
Scenario Type 4: Unsafe Controlled Process Behavior	(BS-47.4) Turn off HTAF command is received by decision authority; vehicle control does not transition to manual control	(BS-49.4) Turn off HTAF command not received by decision authority; vehicle transitions to manual control	(BS-44.4) Deactivate command is not received by decision authority; HTAF automation is fully deactivated (especially before driver has manual control)	(BS-45.4) Deactivate command is received with adequate duration by vehicle control; vehicle control does not (fully) disengage HTAF

The next step will demonstrate how to perform a human factors refinement on basic scenarios, and explain why a human would make these decisions. The first row involves unsafe controller (driver) behavior, so these are good candidates for the human factors refinement.

3.6.5 Sample Human Factors Refinement

To demonstrate the human factors refinement at Level 2, UCA-44 is analyzed below— "Driver performs manual deactivate too early before they have taken full manual control" (partial manual control being unsafe as the driver only has control over steering or speed). Type 1 Basic Scenarios are structured perfectly to align with the further refinement via the human factors extension method, as demonstrated in the table below.

Table 7: Human Factors Refinement: Mental Models

(UCA-44) Driver performs manual deactivate too early before they have taken full manual control [H-1, H-2, H-3, H-4]		
BS-44.1: Driver provides deactivate HTAF too early; driver has correct indication that full manual control has not occurred		
	States	**Behaviors**
Controlled Processes	(MM-1) Driver believes HTAF has been overridden (not deactivated) when HTAF is deactivated (MM-2) Driver believes HTAF is still on but it isn't	(MM-3) Driver believes the vehicle path will not change significantly before they have taken full manual control (MM-4) Driver believes HTAF is capable of distinguishing full manual control from brief inadvertent manual actuation
Other Processes	(MM-5) Driver believes other vehicles are not on collision path before driver has taken full manual control	(MM-6) Driver believes AEB will prevent collision in interval before they have full manual control

3.6.5 **Sample Human Factors Refinement**
To demonstrate the human factors refinement at Level 2, UCA-44 is analyzed below— "Driver performs manual deactivate too early before they have taken full manual control" (partial manual control being unsafe as the driver only has control over steering or speed). Type 1 Basic Scenarios are structured perfectly to align with the further refinement via the human factors extension method, as demonstrated in the table below.

Table 7 demonstrates that it is possible to have more than one mental model belief per quadrant. For example, controlled process states and behaviors each have two flawed beliefs.

Once the mental models have been identified, the next step is to explain why they might occur. The update mental model process is explored to identify why mental models might not have been updated when needed and why they might have been updated incorrectly. For example, MM-2 (driver believes HTAF is still on but it isn't) might occur if HTAF automatically disengages and the driver does not immediately notice. Figure 15 graphically depicts this scenario by integrating a Driver UCA, Driver Mental Models, and Mental Model updates (or lack thereof).

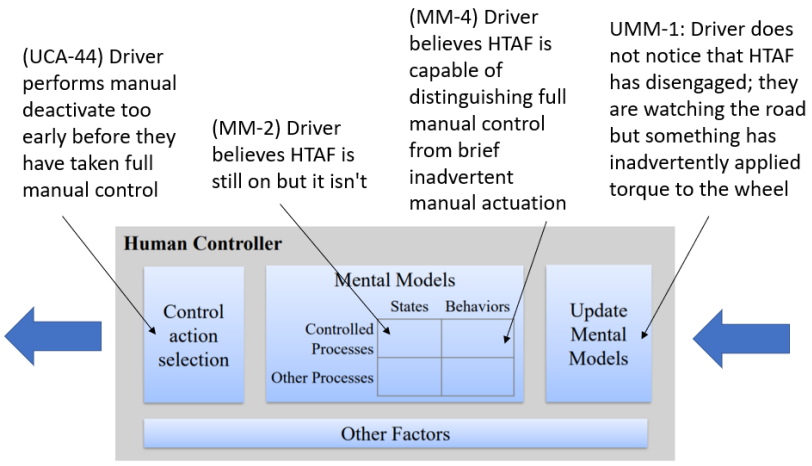

Figure 15: Refining Mental Models for Scenarios II, Graphic Form

Based on Figure 15, (which includes MM-2, and MM-4) the following scenario might be generated:

Refined Scenario 1 (RF-44.1.1): *Driver performs manual deactivate too early before they have taken full manual control, resulting in uncontrolled vehicle steering and speed [UCA-44]. The driver believed that HTAF was still on but it actually wasn't [MM-2], even though the driver has correct indication that full manual control has not occurred [BS-44.1]. The driver learned from previous experience that HTAF is capable of distinguishing between hand placement on the wheel to allow HTAF to remain on (e.g. a response to an attention alert) versus hand placement to deactivate HTAF (e.g. when the driver changes lanes). The driver therefore believes HTAF is capable of distinguishing full manual control from brief inadvertent manual interaction [MM-4]. Although both of those examples are valid, the driver does not realize that torque application is what is critical to deactivate HTAF. The discrepancy may not be obvious, as there is a small range of torque that can be applied that will not deactivate HTAF- this is to prevent accidental nudges from deactivating the system. If the driver's body or clothing was touching the wheel for an extended period of time, they might not immediately notice the deactivation (UMM-1). If this occurs on a curved road, and the vehicle is temporarily without steering or speed control, it will be unable to follow the curvature of the road and may exit its lane and collide with an adjacent vehicle.*

The graphic form above does not need to be used to generate scenarios, but it can be helpful to summarize the factors involved. A common mistake is to list individual factors but not scenarios that demonstrate how factors affect each other. Therefore, scenarios in paragraph form should include all relevant factors that explain the hazardous behavior.

A scenario based on MM-1 may read as follows:

Refined Scenario 2 (RF-44.1.2): *Driver performs manual deactivate too early before they have taken full manual control, resulting in uncontrolled vehicle steering and speed [UCA-44]. They are aware they don't have full manual control of the vehicle (steering and speed) [BS-44.1], because they believed that HTAF had only been overridden when HTAF was actually deactivated [MM-1] They believed HTAF would resume once they completed their action. The driver came to have this belief because they have limited experience operating HTAF, so they were unaware that extended control action duration could*

lead to feature deactivation. The driver did not realize they had exceeded the allotted time for an override by accelerating or braking for >TBD seconds (e.g. 3 seconds) in order to allow a vehicle to merge into their lane. After the merge finished, they released control of acceleration/braking. As a result, HTAF is deactivated, the vehicle does not resume its task to maintain speed, and steering control is lost.

For MM-3:

Refined Scenario 3 (RF-44.1.3): *Driver performs manual deactivate too early before they have taken full manual control, resulting in uncontrolled vehicle steering and speed [UCA-44]. The driver believed that the vehicle path would not change significantly before they have taken full manual control [MM-3] even though they have correct indication that full manual control has not occurred [BS-44.1]. The driver came to have this belief because though they have correctly used HTAF before, until this instance they always have taken immediate manual control of steering and speed when they deactivate HTAF. Any other deactivation performed may have occurred on a straight road, so their experience demonstrated that the vehicle would be able to continue the current trajectory in the brief interval where the transition to manual control occurs. When they hit the brakes without taking the steering wheel, the steering disengages and the vehicle exits the lane. On a curved road, this is particularly dangerous as the steering wheel may return to center or freeze in its current direction, causing the vehicle to exit its lane and collide with an adjacent vehicle.*

Notice that Scenario 1 incorporates multiple mental model flaws: MM-2 and MM-4. Scenarios 2 and 3 are only involve one flawed belief each (MM-1 and MM-3, respectively). A scenario does not need to have two mental model flaws, but the additional insight may help strengthen the understanding of the operator's decision making. Requirements and recommendations can be developed using either scenario build. This next step will be explored in further detail in Chapter 4.

3.7 Iteration 3

At Level 3, the control structure is further refined. The automation can now be examined in more detail, including exploring the inner workings of the decision authority and the vehicle control subsystems. The control actions are also examined in more detail. For example, the HTAF Override command from the driver can be provided via the brake pedal or accelerator. These types of refinement, combined with providing more contextual detail, help provide the information necessary for Level 3 UCA and scenario creation.

3.7.1 Control Structure

Applying the refinement methods defined in Section 3.5, the Level 3 control structure again demonstrates Method 1 and Method 3. At Level 3, the HTAF subsystem is selected as a focus area to provide more detail for the method 1 refinement; by doing so the decision authority and vehicle control subsystems are depicted with greater clarity with regard to their inner workings. The third method, now applied for the second time, provides great insight into the physical actions the driver can take to have a precise consequence on HTAF. Where disable was broadly refined to include "turn off", override, and deactivate at Level 2, at Level 3, detailed instruction like "hands on braking" is included to show a possible way deactivate can be performed. Even internal to the HTAF subsystem Method 3 refinement is evident, such as how longitudinal instruction refines into HTAF enforced: HTAF speed limit setting, lead vehicle set speed limit, intended path, set acceleration, and set braking. (To see a comprehensive lists of Type 3 refinements (from Level 1 to 3), view in Appendix F, and see additional discussion in Section 4.4).

For enlarged copy of image see **Appendix D.1: Enlarged Level3 Control Structure**.

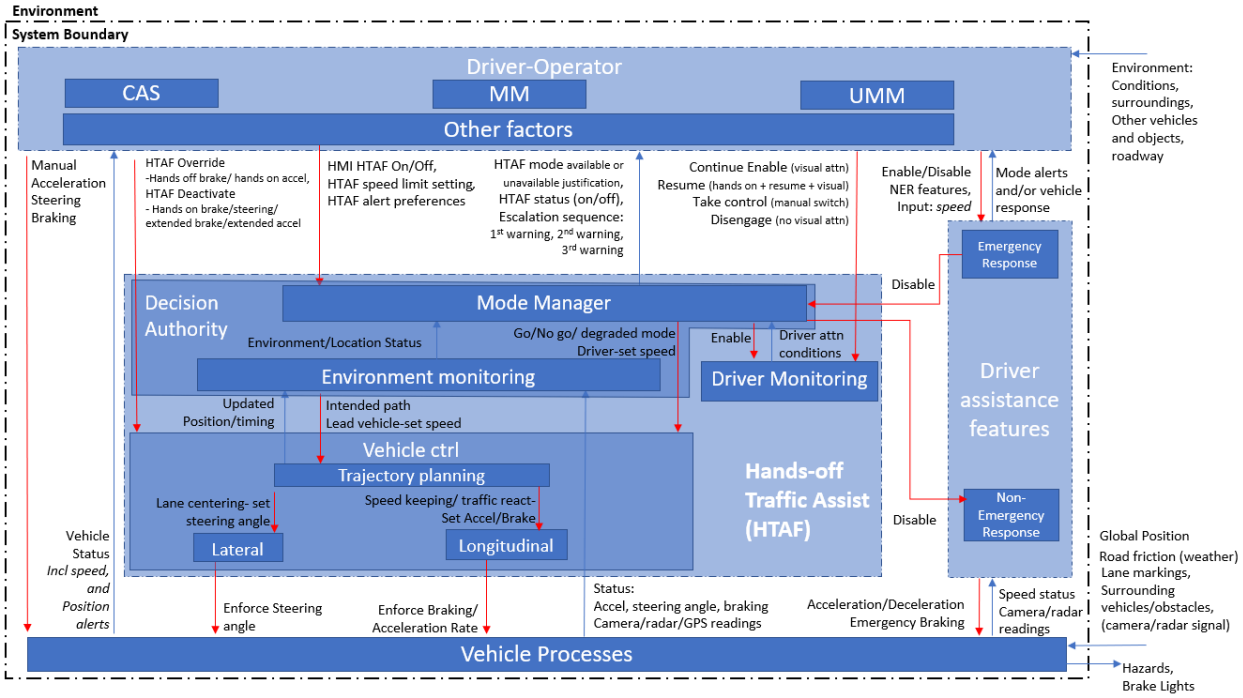

Figure 16: Level 3 Control Structure

3.7.2 New and Amended Control Actions

Driver Controls

- **Manual Steering**
  - ***(Driver → Vehicle Processes)***
  - No change to control definition
- **Manual Acceleration**
  - **(Driver → Vehicle Processes)**
  - No change to control definition
- **Manual Braking/Deceleration**
  - **(Driver → Vehicle Processes)**
  - No change to control definition
- **Hands off Braking - Override**
  - ***(Driver → Vehicle Control)***
  - Temporary disengagement of HTAF caused by application of pressure to brake pedal without hand-to-steering wheel contact (<TBD second duration, e.g. 3s)
- **Hands on Acceleration – Override**
  - ***(Driver → Vehicle Control)***
  - Temporary disengagement of HTAF caused by application of pressure to gas pedal while hands are at wheel (<TBD second duration, e.g. 3s).
- **Hands on Braking – Deactivate**
  - ***(Driver → Vehicle Control)***
  - Full disengagement of HTAF occurs when hands on braking is applied to vehicle controls; transitions to manual control.
- **Extended Braking – Deactivate**
  - ***(Driver → Vehicle Control)***

    - Full disengagement of HTAF occurs when braking is applied to brake pedal (>TBD second duration, e.g. 3s); transitions to manual control.
- **Extended Acceleration**
    - ***(Driver → Vehicle Control)***
    - Full disengagement of HTAF occurs when pressure is applied to gas pedal (>TBD second duration, e.g. 3s); transitions to manual control.
- **Steering – Deactivate**
    - ***(Driver → Vehicle Control)***
    - Full disengagement of HTAF occurs when torque is applied to steering wheel; transitions to manual control.
- **Turn HTAF On**
    - ***(Driver → Mode Manager)***
    - No change to control definition.
- **Turn HTAF Off**
    - ***(Driver → Mode Manager)***
    - No change to control definition.
- **Set HTAF Alert Preferences**
    - ***(Driver → Mode Manager)***
    - No change to control definition.
- **Set HTAF Speed**
    - ***(Driver → Mode Manager)***
    - The driver reaches their intended speed for the duration of HTAF before enabling the HTAF (similar to cruise control), when operating above TBD threshold (e.g. >10kph).
- **Attention to Continue Enable**
    - ***(Driver → Driver Monitoring)***
    - Engage attention has been refined according to action taken- continue enable requires forward attention for a TBD duration of HTAF usage.
- **Attention to Resume**
    - ***(Driver → Driver Monitoring)***
    - Engage attention has been refined according to action taken- resume occurs after the second level warning alert and driver needs to place hands on steering wheel and press a "resume" button (HMI TBD).
- **Attention to Take Control**
    - ***(Driver → Driver Monitoring)***
    - Engage attention has been refined according to action taken- resume occurs after the third level warning alert due to road conditions; driver needs to take full manual control but can reengage HTAF.
- **Provide Attention to Disengage**
    - ***(Driver → Driver Monitoring)***
    - No change to control definition.
- **Enable [non-emergency response] DAF**
    - ***(Driver → DAF)***
    - No change to control definition.
- **Disable [non-emergency response] DAF**
    - ***(Driver → DAF)***
    - No change to control definition.

- **Set DAF Speed**
  - **(Driver → DAF)**
  - No change to control definition.

Mode Manager Controls

- **Enable Driver monitoring**
  - ***(Decision Authority → Driver Monitoring)***
  - No change to control definition.
- **Go (or "Enable")**
  - ***(Mode Manager → Vehicle Controls)***
  - Conditions informed by environment monitoring and driver monitoring indicate HTAF enabled to take/continue control
- **No Go (or "Disable")**
  - ***(Mode Manager → Vehicle Controls)***
  - Conditions informed by environment monitoring and driver monitoring indicate HTAF is not in conditions to be enabled to take control
- **Degraded Mode**
  - ***(Mode Manager → Vehicle Controls)***
  - Conditions informed by environment monitoring and driver monitoring indicate HTAF operation is compromised while in use and should safely stop
- **Disable**
  - ***(Mode Manager → Non-Emergency Response (NER) DAF)***
  - No change to control definition.

Environment Monitoring

- **Path Planning**
  - ***(Environment Monitoring → Trajectory Planning)***
  - Initial processing/planning of environmental inputs and alignment with intended path (forward/within lane)
- **Lead Vehicle-Set Speed**
  - ***(Environment Monitoring → Trajectory Planning)***
  - When operating HTAF below TBD threshold (e.g. <10kph), vehicle uses lead vehicle speed for vehicle speed limit up to 80kph.

Trajectory Planning

- **Set Steering Angle**
  - ***(Decision Authority → Vehicle Processes)***
  - No change to control definition.
- **Set Acceleration Rate**
  - ***(Decision Authority → Vehicle Processes)***
  - No change to control definition.
- **Set Braking Rate**
  - ***(Decision Authority → Vehicle Processes)***
  - No change to control definition.

Lateral [Control]

- **Enforce Steering Angle**
  - ***(Lat Control → Vehicle Processes)***

- No change to control definition.

Longitudinal [Control]

- **Enforce Acceleration Rate**
  - ***(Long Control → Vehicle Processes)***
  - No change to control definition.
- **Enforce Braking/Deceleration Rate**
  - ***(Long Control → Vehicle Processes)***
  - No change to control definition.

Driver Assistance Features (DAF)

- **Acceleration**
  - ***(DAF → Vehicle Processes)***
  - Provide acceleration to maintain set speed (may or may not enforce safe following distance)
- **Deceleration**
  - ***(DAF → Vehicle Processes)***
  - Provide deceleration to maintain set speed (may or may not enforce safe following distance)
- **Emergency Braking**
  - ***(DAF → Vehicle Processes)***
  - No change to control definition.
- **Disable**
  - ***(AEB → Decision Authority)***
  - Provide disable to vehicle automation (HTAF) controls when engaged

3.7.3 Unsafe Control Actions

The Level 1 analysis identified high-level UCAs for the "Disable HTAF" control action. At Level 2, that control action was refined into three distinct types of commands could disable HTAF in different ways, like the difference between an override and deactivation. Level 2 UCAs were identified for each. Now at Level 3, seven specific driver control actions have been identified that provide greater detail into the tangible actions the driver can take. For example, one way the driver can provide the override command is to provide hands-off braking (braking with hands off the steering wheel). These are explicit actions the driver may take to override or deactivate HTAF. The table below examines each of the specific Level 3 control actions to identify Level 3 UCAs. Refinement by context is also applied again at this step, so the UCAs at Level 3 may provide more detailed contexts than the UCAs at Level 2. For additional Level 3 UCAs, see **Appendix D.2.**

Table 8: Sample Level 3 UCAs, expanded from Manual Override, Manual Disable, and Turn HTAF Off

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Hands off braking (Override)	(UCA-51) Driver does not provide hands off braking to override HTAF when sensors are degraded/ malfunctioning [H-1, H-2, H-3, H-4]	(UCA-53) Driver provides hands-off braking to override and moves vehicle onto collision path [H-1, H-2, H-3, H-4] (UCA-54) Driver provides hands-off braking to override and maintain safe	(UCA-56) Driver performs hands-off braking to override too late after forward minimum distance is violated [H-1, H-2, H-3, H-4]	(UCA-58) Driver continues performing hands-off braking to override too long after override sequence duration is exceeded (resulting

	(UCA-52) Driver does not provide hands off braking to override HTAF when obstacle enters from side and other control measures are absent [H-1, H-2, H-4] […]	distance from forward vehicle while torque is applied to the wheel (e.g. clothing, knees, etc.) [H-1, H-2, H-3, H-4] (UCA-55) Driver provides hands-off braking to override while on a curved road [H-1, H-2, H-3, H-4] […]	(UCA-57) Driver provides hands-off braking to override too early before they have monitored environment [H-1, H-2, H-3, H-4] […]	in feature deactivation) [H-1, H-2, H-3, H-4] (UCA-59) Driver stops performing hands-off braking to override too soon before safe minimum distance is achieved between vehicles [H-1, H-2, H-3, H-4] […]
Hands on acceleration (Override)	(UCA-60) Driver does not provide hands on acceleration to override HTAF when following vehicle or side vehicle violates minimum distance between vehicles and other control measures are absent [H-1, H-2, H-4] […]	(UCA-61) Driver provides hands on acceleration to override when there is a forward obstacle travelling at a slower speed and below a minimum distance [H-1, H-2, H-4] (UCA-62) Driver provides hands on acceleration to override while inadvertently applying torque to steering wheel (resulting in unintended behavior and confusion) [H-4] […]	(UCA-63) Driver performs hands on acceleration to override too late after rear/side minimum distance is violated [H-1, H-2, H-3, H-4] (UCA-64) Driver provides hands-on acceleration to override before checking lateral vehicles' position [H-1, H-2, H-3] […]	(UCA-65) Driver continues providing hands on acceleration to override too long after override duration sequence is exceeded [H-1, H-2, H-3, H-4] […]
Hands on braking (Deactivate)	(UCA-66) Driver does not provide hands on braking to deactivate HTAF when vehicle is on forward or lateral collision path and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-67) Driver does not provide hands on braking to deactivate HTAF when HTAF is unable to supervise the vehicle effectively [H-1, H-2, H-3, H-4] […]	(UCA-68) Driver applies hands on braking that moves vehicle onto collision path (e.g. rear/side) [H-1, H-2, H-3, H-4] (UCA-69) Driver applies hands on braking to override while inadvertently applying torque to steering wheel (applies hands on instead of hands-off braking, resulting in unintended deactivation and confusion) [H-4] (UCA-70) Driver performs hands on braking while something other than hands are applying torque to the steering wheel (e.g. knee or other object) [H-1, H-2, H-3, H-4] […]	(UCA-71) Driver performs hands on braking too late after forward/ lateral minimum distance is violated and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-72) Driver performs hands on braking too early before checking rear environment [H-1, H-2, H-3, H-4] (UCA-73) Driver performs hands on braking out of order, braking before placing hands on wheel [H-1, H-2, H-3, H-4] […]	[…]

Extended braking (Deactivate)	(UCA-74) Driver does not provide extended braking to deactivate HTAF when vehicle is on forward or lateral collision path and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-75) Driver does not provide extended braking to deactivate HTAF when HTAF is unable to supervise the vehicle effectively [H-1, H-2, H-3, H-4] […]	(UCA-76) Driver provides extended braking with hands off the wheel to deactivate HTAF while on a curved road [H-1, H-2, H-4] (UCA-77) Driver applies extended braking when steering is better suited to prevent collision [H-1, H-2] […]	(UCA-78) Driver performs extended braking too late after forward/side minimum safe distance is violated and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-79) Driver performs extended braking to deactivate too early before Driver is ready to take lateral control [H-1, H-2, H-3, H-4] […]	(UCA-80) Driver stops providing extended braking too soon (TBD duration) before HTAF fully deactivates when HTAF is not able to avoid a collision or other hazard [H-3, H-4] (UCA-81) Driver applies extended braking too long after it's deactivated when there is a rear-end collision danger [H-1, H-2, H-3] […]
Extended acceleration (Deactivate)	(UCA-82) Driver does not provide extended acceleration to deactivate HTAF when vehicle is not responsive to a rear-approaching or lateral collision path [H-1, H-2, H-3] […]	(UCA-83) Driver provides extended acceleration with hands off the wheel while on a curved road [H-1, H-2, H-3, H-4] (UCA-84) Driver applies extended acceleration to increase speed when there is a forward obstacle travelling at a slower speed and below a minimum distance [H-1, H-2, H-3, H-4] […]	(UCA-85) Driver performs extended acceleration to deactivate too late after rear or lateral obstacle violates minimum distance and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-86) Driver performs extended acceleration to deactivate too early before there is sufficient space to complete command without violating minimum distance [H-1, H-2, H-3, H-4] […]	(UCA-87) Driver stops providing acceleration too early before TBD duration triggers change from override to deactivate [H-3, H-4] […]
Steering (Deactivate)	(UCA-88) Driver does not provide steering to deactivate HTAF when vehicle is on imminent collision path and other control measures are absent [H-1, H-2, H-3] (UCA-89) Driver does not provide steering to deactivate	(UCA-91) Driver applies steering torque that inadvertently causes HTAF to deactivate when there is no obstacle (resulting in unintended behavior and confusion) [H-4] (UCA-92) Driver performs steering to deactivate when Driver is not prepared to take longitudinal control [H-1, H-2, H-3, H-4]	(UCA-95) Driver performs steering too late after obstacle violates minimum distance and other control measures are absent [H-1, H-2, H-4] (UCA-96) Driver performs steering to deactivate and change direction too early	(UCA-97) Driver stops providing steering to deactivate too soon before TBD torque is achieved to transition to manual control when HTAF is unable to navigate the current environment [H-1, H-2, H-3, H-4]

	HTAF when [H-1, H-2] (UCA-90) Driver does not provide steering to deactivate when HTAF does not detect in-lane obstacle and other deactivation cmds are absent [H-1, H-2] […]	(UCA-93) Driver performs steering to override, resulting in unintended deactivation and confusion [H-4] (UCA-94) Driver performs steering to deactivate with a steering torque/angle that directs vehicle onto collision path [H-1, H-2] […]	before the new path is clear [H-1, H-2, H-4] […]	[…]
Turn off HTAF	(UCA-114) Driver does not turn off HTAF when HTAF is unable to navigate the current environment and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-115) Driver does not turn off HTAF when HTAF is unable to follow traffic laws or traffic patterns [H-3, H-4] (UCA-116) Driver does not turn off HTAF when exiting traffic/highway environment [H-3, H-4] […]	(UCA-117) Driver turns off HTAF when uncontrolled vehicle trajectory/motion poses an imminent collision danger and manual corrections are not provided (e.g. on a curved road) [H-1, H-2, H-3, H-4] (UCA-118) Driver turns off HTAF inadvertently, resulting in unintended deactivation and confusion[H-4] (UCA-119) Driver turns off HTAF when he/she does not have hands on the wheel and foot over the brake/accelerator pedal [H-1, H-2, H-3, H-4] […]	(UCA-120) Driver turns off HTAF too early before they are in control of lateral and longitudinal manual driving [H-1, H-2, H-3, H-4] (UCA-121) Driver turns off HTAF too early before there is sufficient space to safely bring vehicle to speed of vehicle/ traffic ahead when taking manual control of vehicle [H-1, H-2, H-3] (UCA-122) Driver turns off HTAF too late after violating minimum distance/speed to avoid collision[H-1, H-2, H-3, H-4] (UCA-123) Driver turns off HTAF too late after speed is too high to prevent collision [H-1, H-2, H-3, H-4] […]	[…]

3.7.4 Sample Basic Scenario Generation

Each iteration considers more specific details, and Level 3 is no exception. The scenarios generated at Level 3 may involve more specific conditions, actions, feedback, and other factors compared to Level 2. The same basic process for scenario generation is used at Level 3, but the scenarios include more specifics.

Table 9: Level 3 Basic Scenario Generation

(UCA-88) Driver does not provide steering to deactivate HTAF when vehicle is on imminent collision path and other control measures are absent [H-1, H-2, H-3]

(UCA-105) Driver turns on HTAF when on an entry/exit ramp [H-3, H-4]				
(UCA-78) Driver performs extended braking too late after forward/side minimum safe distance is violated and other control measures are absent [H-1, H-2, H-3, H-4]				
(UCA-80) Driver stops providing extended braking too soon (TBD duration) before HTAF fully deactivates when HTAF is not able to avoid a collision or other hazard [H-3, H-4]				
	UCA type 1: not providing causes hazard (UCA-88)	**UCA type 2: providing causes hazard (UCA-105)**	**UCA type 3: too early, too late, out of order causes hazard (UCA-78)**	**UCA type 4: stopped too soon, applied too long causes hazard (UCA-80)**
Scenario Type 1: Unsafe Controller Behavior	(BS-88.1) Driver does not provide steering to deactivate; driver receives correct indication that vehicle is on imminent collision path and other control measures absent	(BS-105.1) Driver provides "turn on HTAF"; driver has correct indication of if HTAF is enabled and their location	(BS-78.1) Driver provides extended braking to deactivate too late; driver has correct indication that forward/side minimum safe distance is violated and other control measures absent	(BS-80.1) Driver stops providing braking too soon to deactivate; driver has correct indication that HTAF is not deactivated and not able to avoid collision/hazard
Scenario Type 2: Unsafe Feedback Path	(BS-88.2) Feedback received by driver does not indicate imminent collision or absent control measures; vehicle is on a collision path and other control measures are absent	(BS-105.2) Feedback received by driver does not indicate HTAF is enabled, or that vehicle is not in approved location; location is inappropriate for HTAF use	(BS-78.2) Feedback received by driver does not indicate that minimum safe distance is violated and other control measures absent; minimum safe distance is violated and other control measures are absent	(BS-80.2) Feedback received by driver does not indicate HTAF is not deactivated and not able to avoid collision/hazard; HTAF is not deactivated and is not able to avoid collision/hazard
Scenario Type 3: Unsafe Control Path	(BS-88.3) Driver does provide steering to deactivate; steering command to deactivate is not received by vehicle controls	(BS-105.3) Driver does not provide "tun on HTAF "; "turn on HTAF" is received by mode manager	(BS-78.3) Driver provides extended braking to deactivate on time; HTAF does not receive command to deactivate on time before minimum safe distance is violated	(BS-80.3) Driver provides extended braking to deactivate; vehicle controls do not receive adequate extended braking cmd to deactivate
Scenario Type 4: Unsafe Controlled Process Behavior	(BS-88.4) Steering to deactivate is received by vehicle controls; lateral control does not follow manual command or HTAF control does not deactivate	(BS-105.4) Turn on HTAF is not received by mode manager; HTAF is turned on and automated control is initiated	(BS-78.4) HTAF receives extended braking to deactivate on time; HTAF does not deactivate on time before minimum safe distance is violated	(BS-80.4) Extended braking cmd is received by vehicle controls; HTAF does not deactivate or vehicle does not follow manual commands

These Level 3 basic scenarios provide more detailed controller/controlled process elements, and more detailed control actions and feedback than their Level 2 and Level 1 counterparts. For example, (UCA-88) "Driver does not provide steering to deactivate HTAF when vehicle is on imminent collision path and other control measures are absent," now refers to a specific action the driver can take to deactivate, and these changes are propagated throughout the Basic Scenario table. (BS-88.1) "Driver does not provide steering to deactivate; driver receives correct indication that vehicle is on imminent collision path and

other control measures absent," refers to the driver's lack of intervention when the vehicle is unable to react appropriately to an imminent collision (vehicle can only control speed in reaction to a forward collision). The driver sees the collision is about to transpire, and is aware that they could take over control but choose not to. The next step after identifying basic scenarios is to refine them and explain why they might occur.

3.7.5 Sample Human Factors Refinement

As demonstrated in Level 2, the Level 3 human factors refinement process uses the STPA human factors extension model (see Chapter 2) to explain why a human would make decisions to provide unsafe control actions. This step begins with a UCA and the subsequently generated Type 1 basic scenario. Then potential believes that would explain the UCA are entered into the mental models table.

Table 10: Human Factors Refinement: Mental Models

(UCA-88) Driver does not provide steering to deactivate HTAF when vehicle is on imminent collision path and other control measures are absent [H-1, H-2, H-3]		
BS-88.1: Driver does not provide steering to deactivate; driver receives correct indication that vehicle is on imminent collision path and other control measures absent		
	States	**Behaviors**
Controlled Processes	(MM-1) Driver believes HTAF is already deactivated (MM-2) Driver believes other adequate control measures are provided	(MM-3) Driver believes vehicle will prioritize collision avoidance over staying in lane (e.g., will steer to avoid obstacles)
Other Processes	(MM-4) Driver believes there is no imminent collision with an obstacle or the obstacle need not be avoided (e.g. consequence lower than alternative or obstacle will not damage vehicle)	(MM-5) Driver believes approaching obstacle will not move into collision path

Each of the mental model flaws in the above table offers an explanation as to why the driver may perform an unsafe control action; in this case, not steering to avoid collision. For instance, the driver may not steer to avoid collision if they believe that the vehicle has the internal capability to determine whether or not it is better to stay in lane or violate this rule to avoid collision. The next step is to examine the Update Mental Model process and identify why such mental models might reasonably occur.

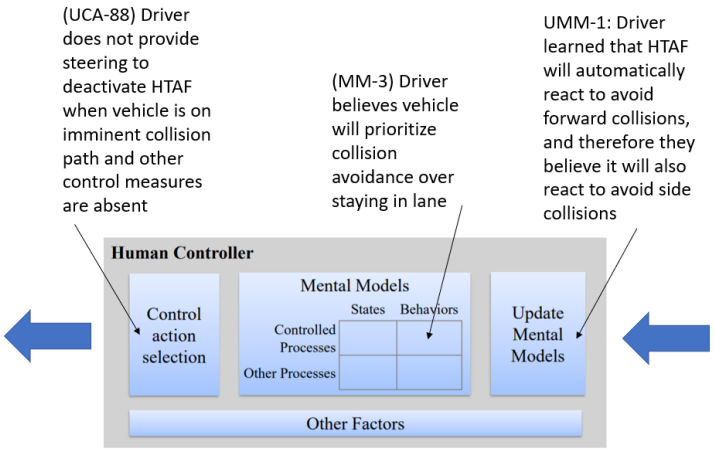

Figure 17: Refining Mental Models for Scenarios III, Graphic Form

Converted into paragraph format, the above scenario might read:

Refined Scenario 1 (RF-88.1.1): *Vehicle is on imminent collision path, and Driver does not provide steering to deactivate HTAF (UCA-88) even though driver has correct indication that vehicle is on collision path and that other control measures are absent (BS-88.1). The driver believes vehicle will provide the necessary steering to prioritize collision avoidance (rather than just staying in lane) (MM-3), and a vehicle to the side swerves over the lane markings. The driver believes the vehicle has this ability because they previously learned that HTAF will automatically react to avoid forward collisions, and therefore they believe it will also automatically react to avoid side collisions (UMM-1). In reality, HTAF has the capability to react to only the vehicle ahead through speed control; all steering performed by HTAF is exclusively used to keep the vehicle in lane even if steering is needed to avoid a collision.*

Like the prior iterations, this refined scenario explains how human factors-derived considerations can explain unsafe control actions, specifically the decision making in response to feedback. Chapter 4 will explore what recommendations and requirements can be developed from this point.

3.8 Driver Attention Cue as a Control Action

One of the notable features of HTAF is that it receives and responds to attention cues from the driver in addition to traditional driver control actions like enable, disable, set configuration options, and temporary manual override of controls. The driver attention cues include factors like whether hands are on the steering wheel (indicated by steering wheel torque) and the direction of the driver's gaze (indicated by live camera monitoring of the driver). When the driver provides sufficient attention cues, HTAF interprets it as appropriate supervision, and as a command to continue to enable the HTAF function. When the driver provides insufficient attention cues, the HTAF automation interprets it as a command to begin a sequence of degraded states and alerts (the escalation sequence) to bring the driver back to their supervisory task.

The attention cues and related interactions can be analyzed using the same STPA process. An example Level 1 UCA is:

(UCA-42) The driver provides sufficient attention cues while vehicle remains on collision course with HTAF engaged [H-1, H-2, H-3, H-4]

Table 11 below shows an example of Level 1 basic scenarios related to the UCA above.

Table 11: Attention Cue Level 1 Basic Scenarios

	UCA type 2: providing causes hazard (UCA-42)
Scenario Type 1: Unsafe Controller Behavior	(BS-42.1) Driver provides attention cues; driver receives indication of collision course and HTAF engaged
Scenario Type 2: Unsafe Feedback Path	(BS-42.2) Feedback received by driver does not indicate collision course or HTAF engaged; vehicle remains on collision course with HTAF engaged
Scenario Type 3: Unsafe Control Path	(BS-42.3) Driver does not provide attention cues; attention cues are received by HTAF
Scenario Type 4: Unsafe Controlled Process Behavior	(BS-42.4) Attention cues are not received by HTAF; HTAF does not disengage or vehicle otherwise continues on collision course

One issue identified above is the possibility of positive driver attention cues even if the driver is not able to intervene in time to prevent a collision. Physical attention cues may not reflect the actual driver attention level or awareness of an undetected danger—even though the automation may be designed to assume the opposite. For example, a mismatch between attention cues and actual attention/awareness could occur due to other mental processes (e.g., driver is "on autopilot", inadvertently daydreaming, deeply immersed in a conversation, etc.), or technical issues (e.g., machine vision algorithms report driver gaze incorrectly), or even intentional manipulation (e.g. a small object placed in the steering wheel to give the appearance of "hands on", a picture of an attentive driver placed in view of the camera, etc.). So, while attention cues as a control action is "measurable," it is important to evaluate whether the measures are an effective evaluation of the driver's supervisory capability.

Throughout the analysis, the driver attention cues have been modeled as a control action and the corresponding HTAF alerts are modeled as feedback to the driver (see UCA collections in Appendices B.2, C.2, D.2). The next chapter considers the opposite interpretation—if the driver attention cues were modeled as feedback while the alerts were modeled as commands to the driver to concentrate and regain focus.

Chapter 4: Evaluation of STPA Applied to "Hands-Off Eyes On" Automation

This chapter provides an evaluation of the analyses performed in Chapter 3. First, an overview of the types of refinement used to iterate the analysis will be discussed and evaluated with respect to scalability for complex systems. Next, the sensitivity of the analysis to certain modeling decisions will be evaluated, such as modeling feedback incorrectly as a control action in the control structure. Another modeling decision that will be examined is the possibility of two controllers who each may have some level of authority over each other, and how this might be modeled as the control structure is refined. Those who wish to skip these nuances related to control structure modeling may skip Sections 4.2 and 4.3, and proceed to the evaluation of refinement, questions encountered, and notable scenario insights.

4.1 Evaluation of the Refinement Types Used to Iterate STPA

The primary focus of this thesis was to demonstrate how refinement could be used to perform STPA iteratively. To do this, three types of refinement as proposed by Thomas [29, 32] were used to iterate from one level of analysis to the next. A sample of each type of refinement applied in the previous chapter is provided here. Note, the order of the methods does not necessarily correlate to their order of appearance in performing STPA.

The **first type of refinement** was to refine the control structure by specifying a higher level of detail within a particular component (subsystem). For example, HTAF is modeled as a black box in Level 1 and is refined into three controllers in Level 2; at Level 3 the Decision Authority and Vehicle controllers are each refined into two and three controllers, respectively.

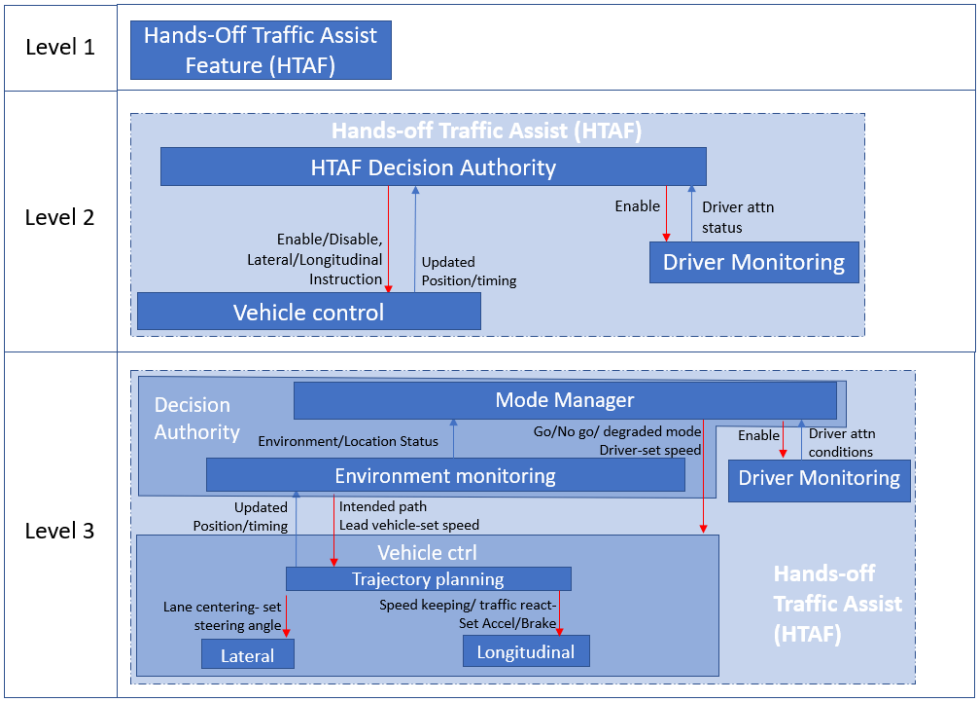

Figure 18: Sample Subsystem Refinement

The **second type of refinement** is to provide greater detail in the context for an Unsafe Control Action. At the Level 1, UCA contexts will involve very broad statements such as:

> "… when vehicle is on collision path."

These broad Level 1 contexts can be refined further to specify exactly when this condition emerges. For example, a collision path can be specified in terms of speed, distance, and direction. Consequently, the lower-level contexts for this UCA may change to:

> "…when [driver's] vehicle violates minimum distance" and "…when [driver's] vehicle is on trajectory towards lead vehicle at speed > lead vehicle speed"

This type of refinement is helpful in identifying specific detectable and preventable conditions which can be used to develop detailed requirements, such as the allowable vehicle speed relative to lead vehicle speed or vehicle deceleration requirements if minimum distance separation is violated.

Table 12: Sample Context Refinement

Level 1	(UCA-22) Driver provides enable HTAF command when in an environment that exceeds HTAF capabilities [H-3, H-4]
Level 2	(UCA-48) Driver turns on HTAF when on a road not approved in the pre-loaded map [H-3, H-4]
Level 3	(UCA-105) Driver turns on HTAF when on an entry/exit ramp [H-3, H-4]

The table above demonstrates this refinement method, starting with Level 1 UCA-22. Note that in addition to the contextual refinement, "provides enable" is refined to "turn on HTAF," which is indicative of the third method (below).

The **third type of refinement** applies to a control action. This type of refinement is done by detailing what specific actions are performed or needed to implement a higher-level command. Figure 18 shows an example. The Level 1 "Disable HTAF" is refined to capture three distinct ways it can be disabled at Level 2—by deactivating, overriding, or turning "off" the system. Level 3 then specifies the exact means by which these commands are implemented, i.e. by different acceleration, braking, or steering control actions. This type of refinement is helpful in connecting broad conceptual commands to specific human actions and identifying possibilities for mode confusion.

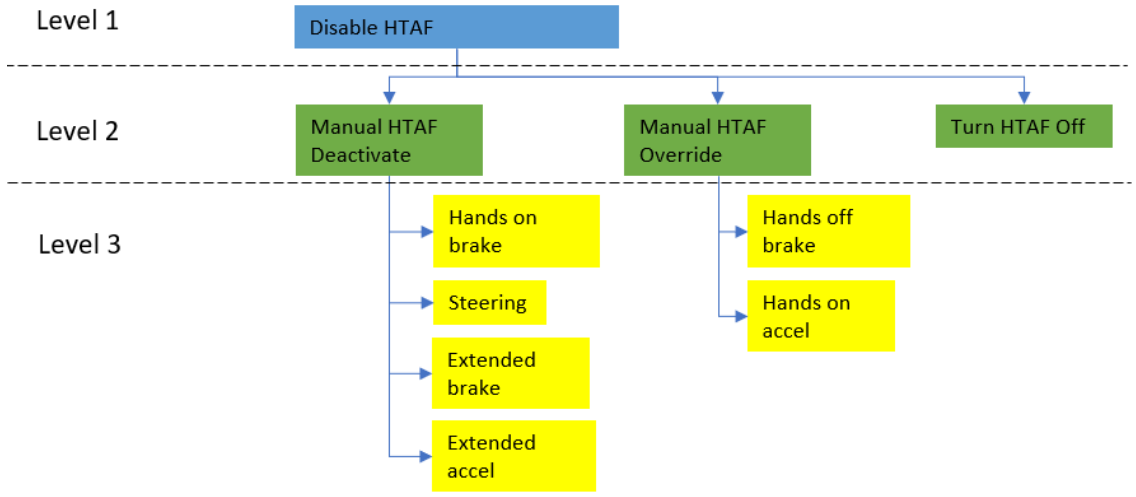

Figure 19: Sample Control Action Refinement

Note that the above figure doesn't include further refinement of the Level 2 control action "Turn HTAF Off". Since that control action is implemented directly with a simple push-button, it is the lowest level of refinement for that control action. To refine the corresponding Level 2 UCAs into Level 3 UCAs, a different type of refinement would need to be used.

These methods were used successfully on each iteration in this analysis, and each step of STPA could be refined. In doing this, it was possible to uncover new insights at each level that were backed by increasing detail. Furthermore, this method proved beneficial for complexity management. Starting with a high-level understanding helped facilitate generation of refined control structures and UCAs by offering a strategic launch point with comprehensive coverage. Furthermore, because the refinements built off of each prior level, there is a high degree of traceability—which is beneficial for generation of justified recommendations and requirements.

4.2 Sensitivity to Control Structure Mistakes: Human Attention and Automation Control

During the construction of the control structure, there may be some discussion among engineers as to who, or what, should be at the top of the control structure. Some might propose that the Driver Monitoring subsystem could be the highest authority, or tied for the highest authority with the driver. Ultimately, in Chapter 3 the mode manager was determined to have authority over the driver monitoring, and the driver had authority over the mode manager in part because the driver had the capability to turn HTAF on and off. These considerations place the driver at the highest point of authority in the system.

However, this discussion begs the question, *what might happen if the analyst opted to place the driver monitoring higher in the control structure such that the feedback it provides to the driver is instead considered to be control actions? Would we be able to identify the same scenarios as a result?* These questions will be answered in this section.

Compounding these questions is the fact that one of the interactions between the driver and the automation involves driver attention monitoring, which raises new questions about how attention monitoring may be modeled in a control structure. If the driver is the highest authority in the control structure, should the driver control action be "providing attention" or should it be more specific? The answer requires a closer look at the concept of a control action in STPA. Among other things, a control action is an observable output of a controller. Control actions do not simply describe the state of the controller or the mental processes within the controller; they are the ultimate result of those processes that are output by the controller. In other words, human control actions are not the human thoughts but the human actions. Therefore Chapter 3 modeled the control action that the driver provides as "attention cues." The attention cues include whether the driver's hands are physically on the wheel, and where they are physically looking, and whether they have taken manual control of the vehicle.

The more general concept of "attention" is much less concrete. Broadly speaking, the driver may provide "attention" the entire time they are driving—whether they are providing forward attention, checking a blind spot, or monitoring gauges on the dashboard. Consequently, the attention that drivers provide under normal operation is very complex. HTAF and other similar attention monitoring systems simplify the concept of "attention" by analyzing the driver's forward eye position when they no longer have manual control of the vehicle's direction or speed. If this condition is not satisfied, feedback to the driver is provided to require more active engagement, such as placing one's hands on the steering wheel and pressing a resume button. Though hand position is not generally thought of as "providing attention," it is how Driver Monitoring evaluates the driver's ability to safely supervise the vehicle. As such, any response needed to keep HTAF engaged, or any response to alerts provided by the monitoring system is considered by HTAF to be *providing attention.* That assumption needs to be carefully considered and potentially challenged by any hazard analysis–especially when generating loss scenarios.

Since the vehicle is providing instruction on how the driver should act, and penalizing them if they do not behave accordingly, it is not inconceivable that someone may mistakenly assign the driver monitoring a higher position of authority. Such a control structure may look like Figure 21. We use Level 2 as the basis for this control structure, as it is the first time the Driver Monitoring subsystem is modeled. Notice how this altered control structure is different from the original control structure used in Chapter 3, which is repeated in Figure 20 below. Figure 20 instead models the audible/visual alert to the driver (escalation sequence) as a control action rather than feedback. Figure 20 also replaces "attention cues" with

"attention status", which is now considered feedback instead of a control action, and models the Driver Monitoring subsystem at a higher level of authority than the driver. The Driver Monitoring subsystem processes the information and provides a control action to the Decision Authority.

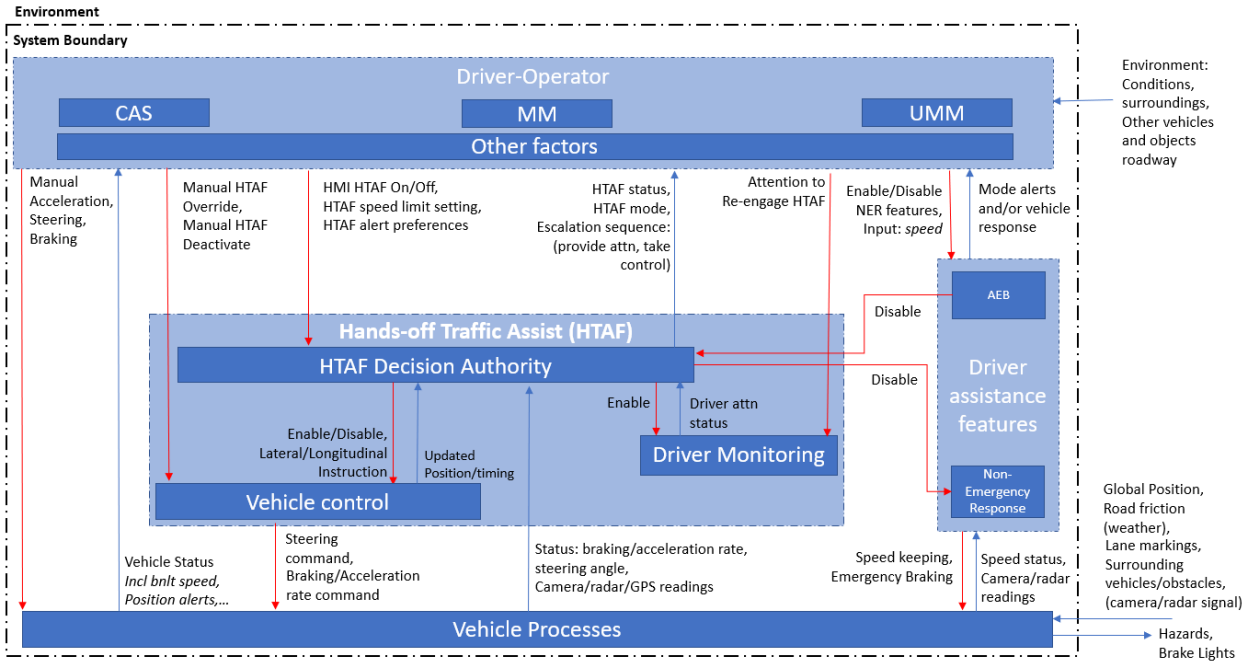

Figure 20: Original (Correct) Control Structure (Level 2)

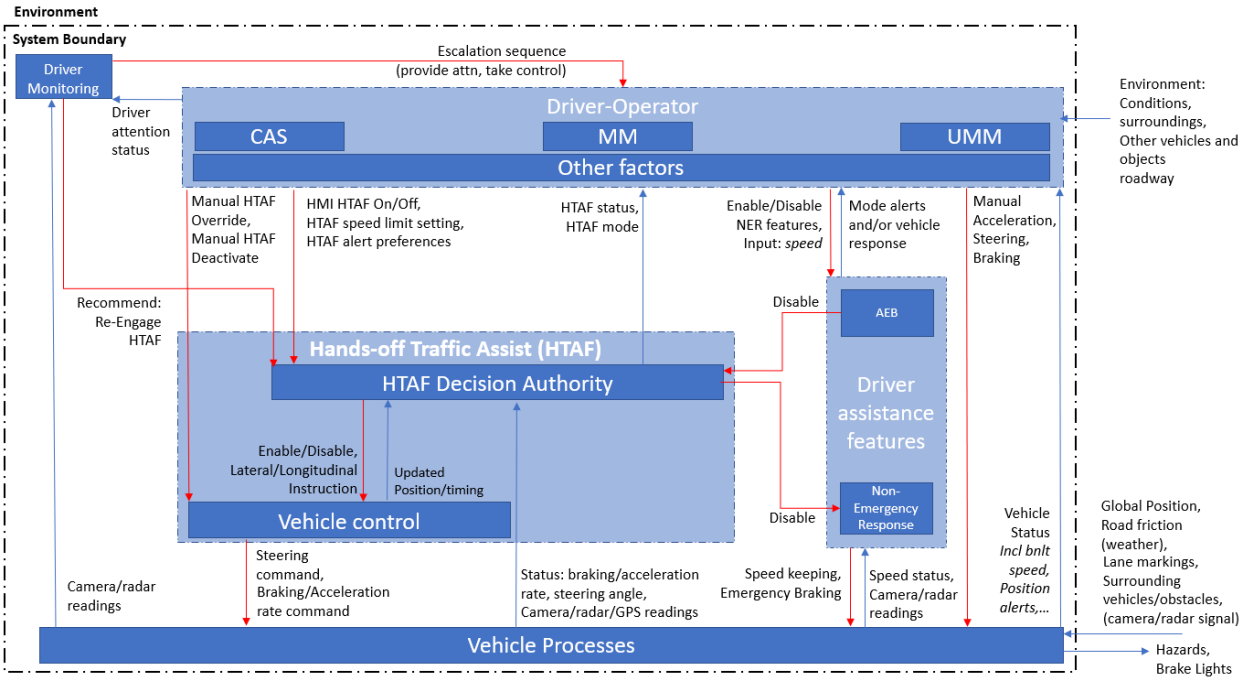

Figure 21: Incorrect (Altered) Control Structure (Level 2)

Table 13 compares the original unsafe control actions from Chapter 3 using Figure 20 against the unsafe control actions that might be derived from the escalation control action from Figure 21. (Enlarged versions of these graphics can be found in Appendix C.1 and Appendix E).

Table 13: Comparison of Upper Level Controller Derived UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Original UCAs – Correct Upper Level Controller				
Attention cues-Re-engage HTAF	(UCA-74) Driver does not provide attention cues to re-engage HTAF while other control measures absent and HTAF degraded mode has put vehicle on collision course (e.g. due to rear approaching vehicles) [H-1, H-2, H-3, H-4] […]	(UCA-75) Driver provides insufficient attention cues (up to and including taking over the controls) to engage HTAF while vehicle is on forward collision course and other control measures are absent [H-1, H-2, H-3, H -4] (UCA-76) Driver provides attention cues to engage HTAF while HTAF is unable to navigate the current environment and other control measures are absent (e.g., HTAF responds to false obstacles and rear vehicles are approaching) [H-1, H-2, H-3, H-4] (UCA-77) Driver provides excessive forward attention cues to engage driver monitoring while vehicle is on collision course with lateral or rear obstacles (resulting in absent attention alerts, further reinforcing driver fwd attention cues away from a rear/side collision) [H-1, H-2, H-4] (UCA-78) Driver provides insufficient attention cues <TBD% of time over HTAF use duration while driver is monitoring environment appropriately (results in inadvertent deactivation/confusion) [H-4] (UCA-79) Driver provides attention cues for ≥TBD% of time over duration of HTAF usage but it is not evenly spaced or otherwise inadequate to observe a collision course (e.g., looking away from the colliding object) [H-1, H-2, H-4] […]	(UCA-80) Driver provides attention cues too late after alert for imminent in-lane collision [H-1, H-2, H-3, H-4] (UCA-81) Driver provides attention cues too late after collision is imminent and no alert is provided [H-1, H-2, H-3, H-4] (UCA-82) Driver provides attention cues in incorrect order to deescalate alerts (resulting in confusion or HTAF degraded mode creating a collision danger) [H-1, H-2, H-4] (UCA-83) Driver provides attention cues too late to resume HTAF use after the third level warning occurs (resulting in confusion or HTAF degraded mode creating a collision danger) [H-1, H-2, H-3, H-4] […]	(UCA-84) Driver stops providing attention cues via hands off or hands on actions too soon before able respond to obstacles in path [H-1, H-2, H-3, H-4] (UCA-85) Driver continues providing attention cues too long after driver is incapacitated (resulting in HTAF operation without driver supervision, potential high-speed collision) [H-1, H-2, H-3, H-4] […]
Alternate Control Structure UCAs – Incorrect Upper Level Controller				
Escalation sequence-provide attention command to driver	(UCA-1) DM does not provide attention command when driver has looked away for TBD duration (or % duration) [H-3, H-4]	(UCA-2) DM provides attention command when driver is looking ahead ≥ TBD duration & no collision is imminent (resulting in driver confusion and frustration) [H-4] (UCA-3) DM provides attention command when driver is already monitoring a potential imminent collision (resulting in interrupting the driver's attention on a critical process,	(UCA-5) DM provides attention command too late after driver attention is lost [H-1, H-2, H-3, H-4] (UCA-6) DM provides attention command too early before driver looks	(UCA-7) DM stops providing attention command too soon before driver attention is regained [H-1, H-2, H-3, H-4]

		like a potential rear collision danger) [H-1, H-2, H-4] (UCA-4) DM provides excessive attention commands when driver is paying attention (resulting in alarm fatigue and driver learns to ignore alerts) [H-1, H-2, H-3, H-4]	away or before attention is lost [H-4]	
Escalation sequence-Take Control command	(UCA-8) DM does not provide Take Control command when HTAF cannot provide sufficient vehicle control to prevent collision [H-1, H-2, H-4] (UCA-9) DM does not provide Take Control command after driver does not heed first warning [H-1, H-2, H-4] (UCA-10) DM does not provide Take Control command when HTAF is unable to navigate the current environment [H-1, H-2, H-3, H-4] […]	(UCA-11) DM provides Take Control command when vehicle is not on collision path (resulting in driver confusion) [H-4] (UCA-12) DM provides insufficient Take Control command when vehicle is on collision course [H-1, H-2, H-4] (UCA-13) DM provides the wrong Take Control command for the driver to be able to correct vehicle path and prevent collision [H-1, H-2, H-4] (UCA-14) DM provides insufficient Take Control command when HTAF is unable to navigate the current environment [H-1, H-2, H-4] […]	(UCA-15) DM provides Take Control command too late after collision is imminent (UCA-16) DM provides Take Control command too early before vehicle is on collision path [H-4] […]	(UCA-17) DM stops providing Take Control command too soon before collision is averted [H-1, H-2, H-3, H-4]

The UCAs are different, which is expected because a control action in the original control structure model is considered feedback in the altered control structure model (so it is not assessed for UCAs). Feedback-related flaws are considered in STPA step 4, so in order to compare the two efforts the scenarios need to be generated and compared.

For the purpose of comparison, UCA-77 from the original control structure and UCA-3 from the altered control structure are brought forward for scenario generation (see Table 14).

Table 14: Comparison of Upper Level Controller Derived Basic Scenarios

(UCA-77) Driver provides excessive forward attention cues to engage driver monitoring while vehicle is on collision course with lateral or rear obstacles [H-1, H-2, H-4]		
(UCA-3) DM provides attention command when driver is already monitoring a potential imminent collision [H-1, H-2, H-4]		
	Original	*Alternate*
	UCA type 2: providing causes hazard (UCA-77)	**UCA type 2: providing causes hazard (UCA-3)**
Scenario Type 1: Unsafe Controller Behavior	(BS-77.1) Driver provides forward attention cues; driver receives correct Driver Monitoring-provided attention/control alerts and awareness of surrounding vehicles	(BS-3.1)Driver Monitoring provides attention commands [alerts]; Driver Monitoring receives correct attention cue response and environment updates

Scenario Type 2: Unsafe Feedback Path	(BS-77.2) Feedback received by driver does not indicate driver attention/control cues needed or position of other vehicles; vehicle/obstacle approach from side/rear is evident	(BS-3.2) Feedback to Driver Monitoring does not indicate that attention cues have been provided or HTAF environment operability; driver attention is not suitable for environment conditions
Scenario Type 3: Unsafe Control Path	(BS-77.3) Driver does not provide forward attention cues [to engage HTAF]; attention cues are received by Driver Monitoring	(BS-3.3) Driver Monitoring does not provide command for attention; attention commands are received by driver
Scenario Type 4: Unsafe Controlled Process Behavior	(BS-77.4) Forward attention cues are not received by Driver Monitoring; decision authority does not provide alert or escalate alert severity	(BS-3.4) Attention commands are not received by driver; driver does not respond or responds with incorrect attention cue

UCA-77 is based on the consequence of the driver providing attention cues, which is that HTAF will remain engaged and neither HTAF nor the driver may notice rear obstacles. The alternate UCAs are based on the consequence of commanding driver attention. What this means is that in the UCAs pulled for scenario generation, UCA-77 refers to attention cues that could include *providing forward attention* all the way through to taking control of the vehicle, while UCA-3 refers to only *low-level attention requests* such as eyes ahead or hands to wheel. However, they are close enough that the scenarios generated provide some points for comparison.

We can approach the comparison in two different ways. The first approach to perform a comparison is to compare specific scenarios and go across the "Scenario Type" line, for instance Type 1:

> "Driver provides forward attention cues; driver receives correct Driver Monitoring-provided attention/control alerts and awareness of surrounding vehicles" (Original) and,
>
> "Driver Monitoring provides attention cue commands [alerts]; Driver Monitoring receives correct attention cue response and environment updates" (Alternate).

These basic scenarios are located in the orange-tinted boxes. At the highest level, these both refer to the idea that the controller and process behaviors are performing as intended, just from opposite perspectives. Ultimately, from either point the analyst could derive a recommendation to address the attention requirements that may cause the driver to not notice environmental dangers on other sides.

To be complete using this first comparison approach, a full set of scenarios for all UCAs must be identified and compared. A different approach to perform a comparison is also possible using a more general analytic view based on the structural changes that were made.

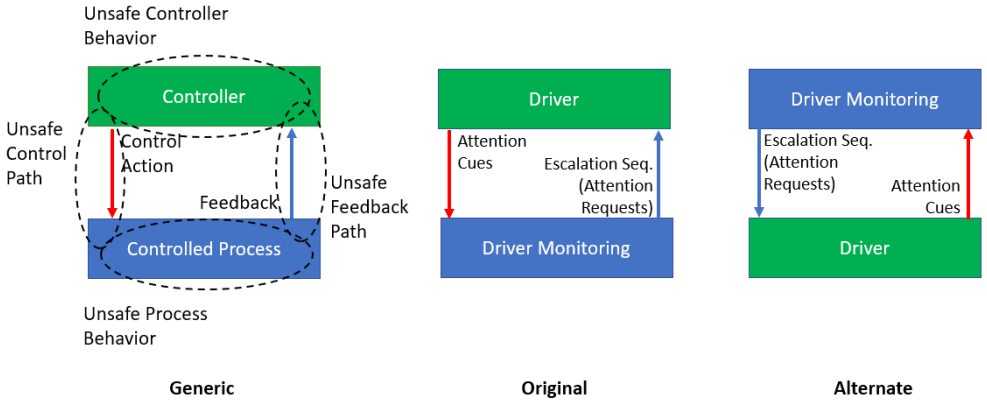

Figure 22: Basic Scenario Generation is Rotated for the Alternate Control Structure

The second approach to perform a comparison is based on how the scenario types for Basic Scenarios are generated. Seen in Figure 22, the Original and Alternate cases have effectively rotated 180 degrees. The content of each model is exactly identical, meaning the exact same content will be reflected in both the

Original and Alternate analyses. The only difference is which category the scenarios fall under—not in the content of the scenarios or the total number of scenarios. So, for every "Original" unsafe controller behavior scenario there will exist a matching "Alternate" unsafe process behavior scenario; similarly, every "Original" unsafe control path scenario will match an "Alternate" unsafe feedback path scenario. A sample from Table 14 is color blocked in yellow.

> "Feedback received by driver does not indicate driver attention/control cues needed or position of other vehicles; vehicle/obstacle approach from side/rear is evident" (Original),
> "Attention commands are not received by driver; driver does not respond or responds with incorrect attention cue" (Alternate).

These basic scenarios demonstrate an obvious correlation in wording, with some moderate changes to the context as they are ultimately pulled from different UCAs.

Though the alternate control structure is incorrect, it does demonstrate that the same scenarios can be derived from a "flipped" control loop, as all the basic content is the same. However, this knowledge should be used with caution as misconceptions about the control structure can have ripple effects and lead the analyst to have incorrect assumptions of how the system works (e.g. driver monitoring having the internal capability to provide operation recommendations to HTAF).

4.3 Horizonal "Other Information" Refinement

This section reflects on an interesting possibility that was observed as control structures evolve from one iteration to the next—it is possible for horizontal "other information" arrows in a control structure to later evolve into distinct control actions and feedback paths in later iterations. This evolution was primarily seen in the transition from Level 1 to Level 2. Level 3 included some changes to the subsystem composition, but did not significantly change the meaning of the arrows between HTAF and DAF (Driver Assistance Features).

At Level 1, the automation boxes were not detailed though to indicate that one has authority over the other. However, we do know that some communication exists between them as they both regulate the vehicle's speed, so some decision is made internally regarding which controller' command is chosen. This horizontal input/output arrow is highlighted in Figure 23 below. Though its presence does not generate UCAs on its own in Level 1, it is an important placeholder as it may be viewed later as a control action once more information is described.

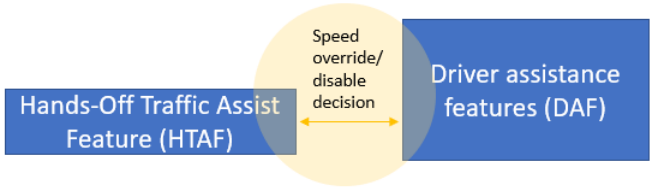

Figure 23: Level 1 HTAF – DAF interaction (horizontal)

The focus of this study was not to perform a full analysis of the future vehicle, but to explore the interactions of HTAF with other controllers in the system. As such, the refined Level 2 control box for DAF is quite simple— see Figure 24. This refined control structure reveals more about the relationship between possible subcomponents of DAF with the operation of automated vehicle control. With the new subcomponents, it is evident that HTAF generally has authority over DAF; when HTAF is enabled, it disables any features that might be automating vehicle control. The notable exception is emergency response features like AEB (Automatic Emergency Braking). These have the capacity to run in parallel with HTAF until AEB is required, at which point AEB may disable HTAF and slow or stop the vehicle. Consequently, though the grouped Level 1 boxes are still parallel, subcomponents like the AEB box can be positioned above HTAF subcomponents. Though these features share sensors and cameras, they operate with different allowable ranges and have different levels of control and authority over each other.

Furthermore, HTAF does not have design control over AEB in this case study—meaning the two are coded separately but must work together.

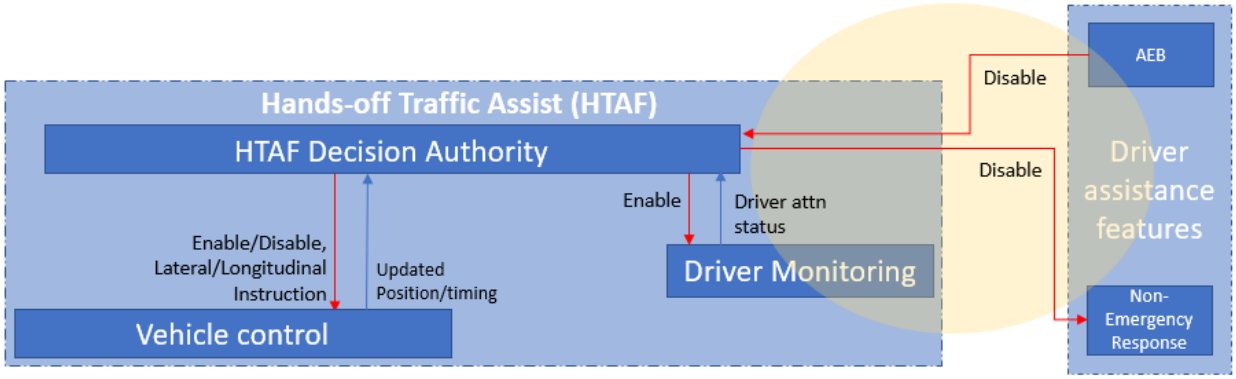

Figure 24: Level 2 HTAF – DAF interaction

This level change to the control structures demonstrates that it is important to consider interactions between parallel subsystems. Vertically traced single control actions generally provide an easily followable path where an action or input leads to a discernable output or consequence. Parallel systems introduce the possibility of conflicting controls acting on the same system element- e.g. if cruise control says maintain speed and HTAF says to slow down to prevent collision. For such a scenario, there needs to be a predetermined response by the system. Not only this, but the operator [driver] needs to be attuned to these mode changes. The predetermined response adds another layer of complexity to the driver's mental model. These control actions between subsystems in particular must be examined carefully as system-level flaws and weaknesses may not be difficult to anticipate, a strength of STPA.

4.4 Evaluation of Refinement Used Throughout STPA

As demonstrated in Chapter 3, refinement is possible at every stage of STPA. This is extremely beneficial for organization and management, as well as for cost and time saving efforts. By starting at the highest level it is possible to begin the analysis very early when few details are known and provide a systematic path forward to capture all controls and interfaces in the system. By working down from this point, the analysis becomes more detailed such that specific recommendations can be provided for system improvements.

Step 1: Losses and Hazards

Providing a more refined hazard list at each level would not have strongly impacted the body of this work and may have complicated the traceability to UCAs. However, taking this extra step can provide more robust and specific system constraints.

Refinement of the hazards is in some ways similar to the refining of control actions and context. Though hazards themselves are not control statements, the actions implied by a hazard statement such as "maintain" in "does not maintain safe distance," can be refined to specify precisely what actions can be performed to maintain—such as acceleration, braking, and steering. Context refinement may also be used to provide more detail about how "safe distance" may differ according to the new control action.

Step 2: Control Structure

The control structure is one of the most obvious candidates for refinement. Due to its graphical nature, the refinements are immediately evident between levels. For a truly comprehensive analysis, all subsystems could be refined from one iteration to the next. However, this is often unnecessary. For example, an analysis could prioritize some areas (such as areas that the project is upgrading or modifying)

while keeping them embedded within the larger overall control structure so as not to lose sight of the higher-level interactions that exist.

Every part of a control structure can be refined. Subsystems in a control structure can be added by "zooming in" on an area. Additional refinement to the control actions may emerge as a result, e.g. a control action from the operator may be refined to reflect the fact that the control action interfaces with 2+ elements instead of one. Alternately, control action refinement may mean that more detail is provided about how the action can be provided, e.g. disable HTAF being refined into multiple actions that detail the specific ways the driver can provide that control action.

Figure 25 and Figure 26 provide a graphical representation of control action refinement. To read these refinement trees, the highest-level controller is shown in white. From there, arrows are drawn to connect the controller to Level 1 control actions, shown in blue. Level 2 control actions (green) appear below their corresponding Level 1 control actions, and Level 3 control actions (yellow) below that. As is evident in both figures, not all control actions were refined in Chapter 3. At Level 3, the most refined version of each control action is analyzed to identify UCAs (e.g. in Figure 24 "HTAF inputs: speed" is seen alongside "Hands on acceleration (Override)").

(For enlarged copies of Figure 25 and Figure 26, see Appendix F.

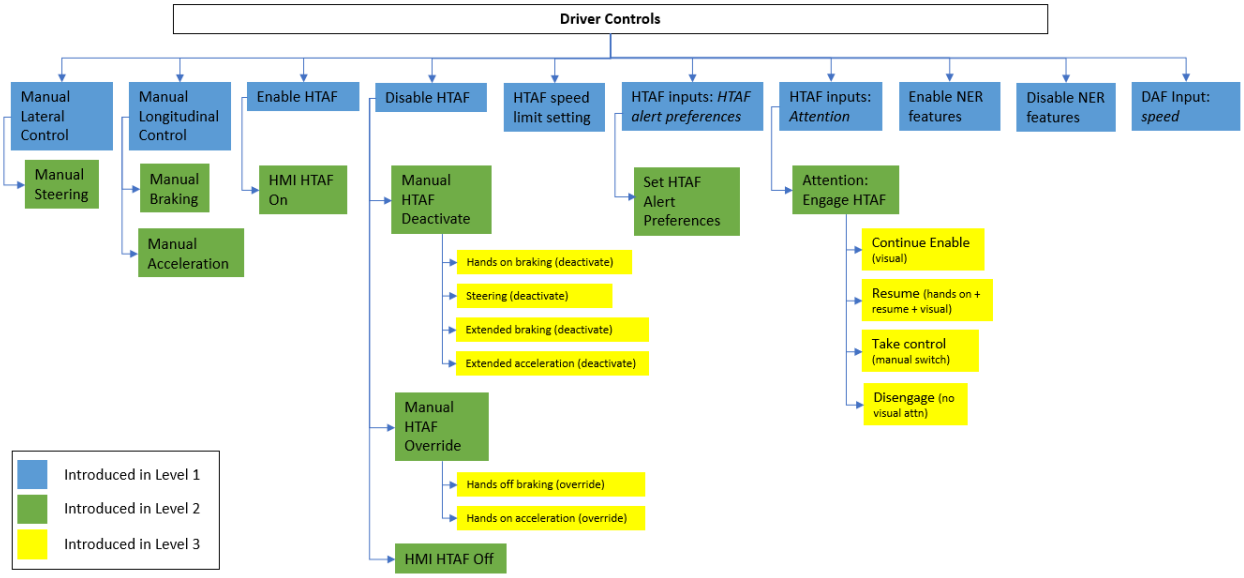

Figure 25: Driver Control Action Refinement Tree

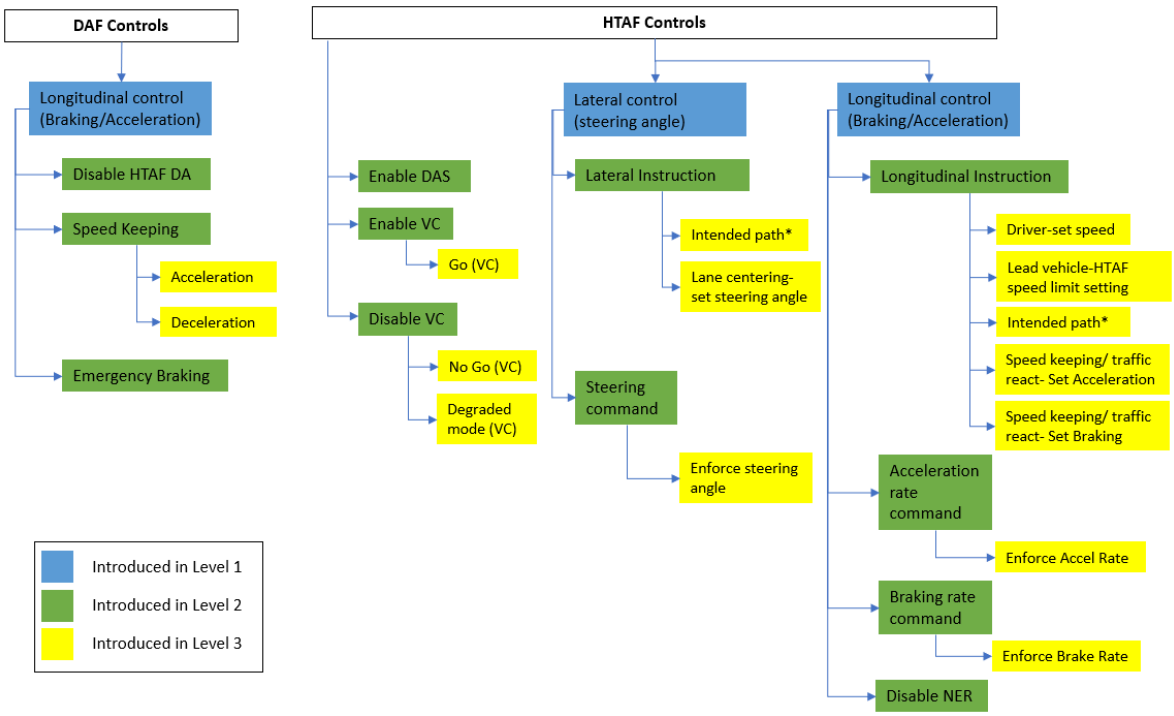

Figure 26: Automation Control Action Refinement Tree[§**]

In Figure 25, no blue box exists over "Enable DAS, Enable VC, Disable VC." This is because these are emergent control actions from the subsystem refinement process, so they are first shown at level two and are internal to the HTAF subsystem. These level 2 control actions exist entirely inside HTAF are not visible at Level 1. Level 1 treats HTAF as a black box and only interactions between HTAF and external entities are visible

Worth mentioning is the rate of increase for control actions throughout the refinement process. At first glance, there is a relatively linear increase between levels for the total number of control actions in each structure (see light blue bars, "All control actions" in Figure 27). However, we must remember that the areas impacted by the refinement was *not* uniformly applied. If we exclusively look at the change to the number of control actions derived from Disable HTAF (seen in dark blue), the increase is actually closer to exponential growth (this is the most extreme increase that emerges as a result of refinement, seen in Figure 25). This does not necessarily mean the workload increases exponentially, as the UCA contexts do not grow in number exponentially (many contexts follow similar patterns) and there is a significant reduction that occurs in the scenario generation step (several UCAs may reference the same basic scenario, which only has to be analyzed once for the group).

§ Intended path is a control action that exists once in the Level 3 diagram, but is distributed to both lateral and longitudinal instruction

** Recall: DAF= Driver Assistance Feature, VC= Vehicle controls, DAS= Driver Attention System, NER= Non-emergency Response [feature(s)]

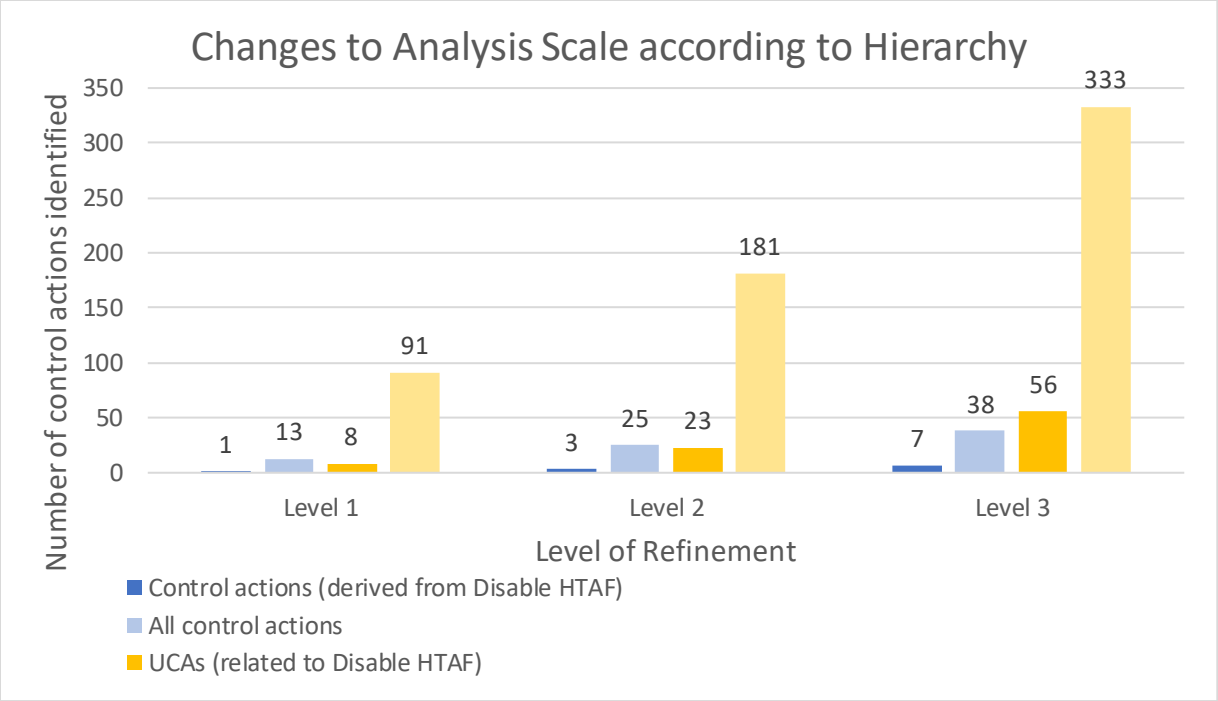

Figure 27: Increasing scale of Control Actions and Unsafe Control Actions

Step 3: Unsafe Control Actions

Unsafe control actions differ between levels of refinement in both quantity and detail. Quantity stems from the control structure changes above, impacted by the inclusion of subsystems and more specified control actions. Increased detail is also impacted by the control action refinement, combined with the contextual refinement. Additionally, though it was not performed in this analysis, refined hazards can be tacked on to the end of each refined UCA.

The approach used in Chapter 3 was to make sure that at least one of the three possible refinement options was applied to each UCA, in each iteration. For example, take "Manual Longitudinal Control." For Level 2, the refinement approach that was utilized was refining the control action itself. So, a Level 1 UCA would look very similar to a Level 2 UCA, except that the UCA for "longitudinal control" was refined into two UCAs, one for a "braking" control action and one for an "acceleration" control action. Moving to Level 3, the UCAs were updated by refining the context, such as specifying a violation of speed or position to replace the broader context of "collision imminence."

Again looking at Figure 27, the increase in total UCAs (light yellow) appears almost linear. When we exclusively look at the UCAs derived from the refinement of the "Disable HTAF" control action (orange), the pattern is a little less clear. This appears to be due to the nature of the refinement application process. Subsystem refinement in the control structure added the most UCAs, as it created more control actions. However, control action refinement and context refinement do not always lead to an increased number of UCAs. For example, in Figure 26, "Enable VC" is refined into "Go VC". This refinement was a 1 to 1 change, but kept Level 2 and 3 at the same level of detail as the corresponding "Disable VC" refinement from Level 2 to 3. Context updates also had a wide range of impacts on the UCA generation; context like "…when not on a highway" can generate many more specifications than "when driver does not have manual control of vehicle."

Step 4: Scenarios

Though UCAs can be used to derive requirements and recommendations for controller constraints to improve system safety, scenarios often provide the most compelling arguments in favor of such changes, as they most clearly demonstrate how and why hazards might realistically occur. The more scenarios that emerge, and the more severe they are perceived to be, the more compelling the argument. As such, it is important to take the final step to refine the scenarios beyond the basic format.

The level of refinement in the basic scenarios is wholly determined by the level of refinement of the UCA they are based upon. The benefit of the basic scenario format is that four simple scenarios can representatively cover all stages of a control/feedback loop where a control may be unsafe. In doing this, the analyst has complete coverage. This also provides an organized foundation for categorical refinement, as each basic scenario type represents the complete set of detailed scenarios that fall under it.

Going from a basic scenario and applying the human factors extension offers a type of contextual refinement for the scenarios. The refined context focuses the analyst (and readers) on *why* the human (driver) may have selected an unsafe control action. These actions may be based on incorrect beliefs about the system's state or behavior. Though a table is used to demonstrate this process, having one belief in each quadrant is not necessarily comprehensive. It should instead be considered a refinement tool for scenario generation assistance.

4.5 Questions Encountered When Applying STPA

Some notable questions were raised and answered during the course of this analysis. The questions are documented here along with the answers that were found during this work.

Can the STPA process be applied beyond traditional safety?

L-1, L-2, and L-3 are very traditional STPA losses. However, given the unique nature of SAE Level 2 automation, where the feature is optional but if used still requires supervision, it was important to explore reasons why the user may not feel comfortable using the automation thereby making it effectively useless. As such, "L-4, Loss or degradation of customer trust" is another important loss. It is a worthwhile consideration because it captures the human perceived value of the system, a lack of which means the system was not successful. In this particular analysis, it is possible for the operator to simply not use the HTAF. This means that unlike the other Losses, it does not necessarily have an immediate traditional safety or financial consequence. However, in future systems where automated features like HTAF may NOT be optional, that is to say it is critical to system operation, this loss scenario may have more immediate impact on the success of the system.

With this new loss, a hazard specific to human interaction with the vehicle automation needed to be captured: "H-4, Vehicle behavior confuses driver or other drivers." When proposing this hazard, it was important to not allude to driver intent; e.g. the driver intends output but a different output occurs. Doing so would be specifying a cause of the hazard and alludes to the incorrect beliefs about system states and behaviors that are analyzed in later steps. By using a term like "confuses," it is possible to indicate the overall state or condition that leads to loss.

Beyond its impact on traditional safety, confusion has implications on driver trust levels and overall satisfaction. These can be factored into UCA generation using the same process. Although phraseology such as "inadvertent" has previously been discouraged from UCA contexts (context should normally reference the underlying condition that makes it hazardous), UCAs related to driver confusion (H-4) may need to use language like "inadvertent." This is because for H-4, the hazard describes a state, or intent, of the driver and not the controlled process directly. With unintended consequences to control actions comes heightened confusion and lowered trust, lowering the effectiveness and value of the feature.

Should all scenarios include beliefs about a system state and a behavior?

While applying the human factors extension a question was raised about whether fully developed scenarios needed to be derived from one incorrect belief about a system state or behavior, or whether they needed to feature an incorrect belief about a system state *and* behavior. In this thesis, examples are generated for both cases, and demonstrate that either derivation is valid. One incorrect belief resulting in a loss may make a strong case to address that mental model flaw; on the other hand, including incorrect beliefs that build upon each other may make for a more robust scenario. Both need to be considered.

Should technical jargon be used to describe human operator beliefs?

The analysis in Chapter 3 found that there is a notable difference in terminology between general human operator beliefs and the actual technical details of the system. Generally speaking, human beliefs don't get down to the component level. Since the human factor scenarios are generally built from Type 1 Basic Scenarios, this largely pertains to the feedback the operator receives and the entity providing it. For example, there may be a high-level name for a subsystem that the operator has familiarity with. An engineer or designer's view of the system will be much more nuanced and, in that way, helpful for developing technical scenarios. Though the explanation on how a belief is ill-conceived may include technical terminology, the operator is most likely not actively making decisions or holding beliefs about how individual components operate. To generate realistic scenarios based on the operator's mental model of the system, it is recommended that the analyst take into account the user's experience and knowledge of the system they are operating. These considerations lead to better human factors design.

Overall, these cumulative insights from the questions above speak to the flexibility and potential capability of STPA as a methodology. STPA was found to apply beyond safety to include factors like driver trust and confusion, and it was found to generate critical human interaction scenarios by using high-level language like operator beliefs about states and behaviors.

4.6 Notable Insights that STPA Identified

To demonstrate what kind of recommendations can result from STPA, a sample of insights produced at every level of this analysis are provided. Notably, even the highest level (lowest detail) analysis uncovered significant insights that could be used to inform design changes. This demonstrates support of the STPA Handbook recommendation that "STPA can be started in early concept analysis to assist in identifying safety requirements and constraints" [13].

Level 1 Analysis Insights

Even at Level 1, it is evident that there is room to accommodate key insights about human interactions to drive high-level decisions. In fact, the high-level basic scenarios identified for HTAF are broadly applicable to many comparable features in other vehicles. For example, Level 1 UCA-42 leads to the following basic scenario; "Feedback received by driver does not indicate attention cues needed or that vehicle is on collision course; vehicle is on collision path." Though this scenario was produced in the HTAF analysis, it is eerily reminiscent of the Tesla case study (Section 2.1.1.1). For Tesla, the requested attention cues were insufficient to generate appropriate supervision levels, and consequently the driver was unable to react in time when the vehicle behavior put them on a collision path.

In continuation on the discussion of this basic scenario, information derived from existing vehicle automation can also be used to inform current design. For example, by test driving another vehicle with a attention monitoring, it was possible to test the escalation strategy in a vehicle where the HMI (user interface, automation alert strategy, etc.) was already designed and in place. When the driver looked away, a colored light flashed on the steering wheel and was meant to bring the driver's attention back to front. Though this may seem like an excellent feedback option on paper, by sitting in the vehicle and looking away to cause the alert, it was noticed that the flashing light was imperceptible if you were looking away! (Particularly in bright daylight conditions). Such an observation is invaluable to

determine appropriate alerts and feedback options for the driver. If the design can't generate an appropriate supervision from the driver, it is more likely that they will be unable to react to an obstacle in their path.

Real world cases can and should inform future designs, even if these features are implemented differently at a lower level. We can determine that alert duration, frequency, and the response needed have significant impact on the success of the design.

Before moving to the refined Level 1 scenario (below), it is helpful to understand the context of the design decisions that went into the most recent version of the HTAF design. HTAF was originally intended to exclusively operate in traffic-heavy highway conditions. To increase the feature's marketability, the feature's speed range was expanded to be operable from 0-50mph (0-80kph)—more akin to the cruise control that most drivers are familiar with. An engineering decision was made that when the driver engages this feature, a speed setting is stored that limits the max speed the vehicle is allowed to accelerate to. Another engineering decision was made that the speed setting should depend on how fast the car is going when the driver engages the feature. If the vehicle is going fast, the current speed is used for the speed setting. If the vehicle is going slow, a fixed default speed is used for the speed setting. Though the exact threshold between fast and slow is proprietary in some current HTAF development efforts, let's assume it is 10 mph (16 kph). If HTAF is engaged under 10 mph (16 kph), the vehicle will rely on the default [max] speed limit setting of 50 mph (80 kph). This design decision means that if the driver is in standstill traffic (or operating at negligible speeds) HTAF can still be engaged and operate in response to the lead vehicle's speed—all the way up to 50 mph (80 kph) if HTAF believes the traffic has largely cleared—without the driver needing to reset the feature.

> Refined Scenario 1 (RF-34.1.1): *Vehicle operates at a speed that is unsuitable for the region. The reason is because the driver did not provide a new speed limit setting when the current speed limit setting was not suitable for the region [UCA-34]. The driver believed that HTAF was using a lower speed limit than it actually was [MM-1]. Although the actual speed limit setting was correctly indicated [BS-34.1], the driver learned from previous experience that turning on HTAF is one way to set the speed limit (the vehicle would not go any faster than the current speed when HTAF was turned on) [MM-2]. Although that is accurate in some cases, the driver did not know that HTAF only behaves that way when the vehicle speed is over TBD mph (10 mph or 16 kph for this analysis) when HTAF is turned on. Otherwise, HTAF will use a default speed limit of 50 mph. The discrepancy may not be obvious because the vehicle would behave no differently as long as the vehicle remains in slow traffic [UMM-1]. If the traffic disappears or picks up speed, the vehicle will unexpectedly accelerate to a speed that may be unsafe (e.g. if is raining or roads are icy, a lower speed will be safer).*

In Chapter 3, STPA identified how these design decisions could lead to the high-level Basic Scenario 1 above. It is possible for the driver to be unsure of the total speed range (0-50mph, or 0-80kph) at which the vehicle is allowed to operate, or unaware of the conditions that result in very different speed settings being stored automatically (10mph vs. 50mph, or 16kph vs. 80kph), or unaware that a default speed setting exists and that it sometimes defaults to the maximum speed possible. These factors can cause the vehicle's behavior to confuse the driver, a H-4 hazard. In a worst case, it could lead to other hazards. The danger here is that the vehicle automatically sets itself to a speed the driver does not approve of.

Additionally, the marketing strategy can be misleading. The average US highway speeds are typically around 65 mph (105 kph). If the feature only operates up to 50 mph (80 kph), lead vehicles will often exit the detectable range and the operator will be asked to take over when the feature is operating at its max possible speed. Because of this, it may not truly be capable of hands-off cruise control in common environments, though the partial capability may lead customers to believe it is.

Potential Recommendation: The HTAF speed setting needs to be visible and adjustable (without having to turn off the feature). Additionally, the driver should be alerted if and when the feature has reached its max speed, as it is not sustainable without the lead vehicle operating at the same speed. Alternatively, the

feature should be exclusively used for traffic assist or be able to operate at the full scale of highway speeds.

Level 2 Analysis Insights

In Level 2, UCAs and scenarios were refined pertaining to deactivation of HTAF. Level 2 began to consider the nuances of different ways to deactivate HTAF, including accidental deactivation, confusion between temporary overriding and full deactivation, and preparedness to take control.

> Refined Scenario 1 (RF-44.1.1): *Driver performs manual deactivate too early before they have taken full manual control, resulting in uncontrolled vehicle steering and speed [UCA-44]. The driver believed that HTAF was still on but it actually wasn't [MM-2], even though the driver has correct indication that full manual control has not occurred [BS-44.1]. The driver learned from previous experience that HTAF is capable of distinguishing between hand placement on the wheel to allow HTAF to remain on (e.g. a response to an attention alert) versus hand placement to deactivate HTAF (e.g. when the driver changes lanes). The driver therefore believes HTAF is capable of distinguishing full manual control from brief inadvertent manual interaction [MM-4]. Although both of those examples are valid, the driver does not realize that torque application is what is critical to deactivate HTAF. The discrepancy may not be obvious, as there is a small range of torque that can be applied that will not deactivate HTAF - this is to prevent accidental nudges from deactivating the system. If the driver's body or clothing was touching the wheel for an extended period of time, they might not immediately notice the deactivation (UMM-1). If this occurs on a curved road, and the vehicle is temporarily without steering or speed control, it will be unable to follow the curvature of the road and may exit its lane and collide with an adjacent vehicle.*

Accidental deactivation does factor into system design; for HTAF, an example is that the steering wheel will not deactivate HTAF unless the action exceeds a certain threshold. This helps prevent unintended nudges from disengaging the automated system. Another factor in this design decision is that steering while HTAF is engaged will only lead to deactivation. Having clear cut, definitive actions for the driver to take to disengage the system might help promote a clearer mental model. Though these are good practices, it is certainly possible to conceive of scenario(s) where this threshold could be exceeded, even accidentally. In this case, the concern is that the system would immediately jump to HTAF deactivation.

Potential Recommendation: The driver should be notified when they have not achieved full control of the vehicle. For example, if steering is applied without acceleration, the seat could provide haptic feedback to the driver that alerts them to the changing behavior of the system. So while the situation is still dangerous, it alerts them that the behavior is occurring where they may have otherwise been unaware.

> Refined Scenario 2 (RF-44.1.2): *Driver performs manual deactivate too early before they have taken full manual control, resulting in uncontrolled vehicle steering and speed [UCA-44]. They are aware they don't have full manual control of the vehicle (steering and speed) [BS-44.1], because they believed that HTAF had only been overridden when HTAF was actually deactivated [MM-1] They believed HTAF would resume once they completed their action. The driver came to have this belief because they have limited experience operating HTAF, so they were unaware that extended control action duration could lead to feature deactivation. The driver did not realize they had exceeded the allotted time for an override by accelerating or braking for >TBD seconds (e.g. 3 seconds) in order to allow a vehicle to merge into their lane. After the merge finished, they released control of acceleration/braking. As a result, HTAF is deactivated, the vehicle does not resume its task to maintain speed, and steering control is lost…*

Next, Driver assistance features are typically designed with some sort of manual overruling capability. This may be a temporary override, or may extend to full feature deactivation. Override helps the driver respond to immediate events, and gives them the opportunity to correct or amend a situation without deactivating the feature. Internally, there may be many more "modes" that are not obvious to the driver. One example is Cadillac's Super Cruise—if the driver deactivates the feature, it actually continues operating until the driver takes manual control (and, if they take control of steering first, it will continue speed control until the driver places their foot on the gas or brake). That said, the driver is usually aware of the concrete actions they can take to affect the system state. For HTAF, there are 7 actions that can be taken that disengage or override the feature (and more combinations of these actions, e.g. hands on

acceleration). This is a large number of options for a driver to process and weigh during the seconds they have to prevent collision. An additional complexity is that the same actions with different durations, or with hands on, lead to different outputs. Furthermore, drivers will enter the system with expectations derived from their own experience. Most drivers have experience with cruise control—for some vehicles, this feature remains on while steering is performed and is disabled with any braking. All of these factors contribute to the driver's beliefs and control action selection.

Potential Recommendation: Decrease the number or complexity of actions the driver can take to override or deactivate. To supplement this action, the design team should consider situations where the driver may wish to override without fully deactivating the system (e.g. lane changes). Additionally, the ruleset should be consistent—if hands on braking results in deactivation, deactivation should occur regardless of the order the driver places their foot on the brake and their hands on the wheel. Finally, the design team should consider the system's similarity to ACC or traditional cruise control—the actions to override and deactivate should not significantly deviate from each other, except to account for differences in functionality.

This leads to the final scenario from Level 2, which is the transition from automated to manual control (Scenario 3). This is tied to Level 2 Scenario 1 above, but instead targets the behavior of the automation rather than the driver.

> Refined Scenario 3 (RF-44.1.3): *Driver performs manual deactivate too early before they have taken full manual control, resulting in uncontrolled vehicle steering and speed [UCA-44]. The driver believed that the vehicle path would not change significantly before they have taken full manual control [MM-3] even though they have correct indication that full manual control has not occurred [BS-44.1]. The driver came to have this belief because though they have correctly used HTAF before, until this instance they always have taken immediate manual control of steering and speed when they deactivate HTAF. Any other deactivation performed may have occurred on a straight road, so their experience demonstrated that the vehicle would be able to continue the current trajectory in the brief interval where the transition to manual control occurs. When they hit the brakes without taking the steering wheel, the steering disengages and the vehicle exits the lane. On a curved road, this is particularly dangerous as the steering wheel may return to center or freeze in its current direction, causing the vehicle to exit its lane and collide with an adjacent vehicle.*

Different vehicles handle this transition in different ways. With regard to the steering mentioned in the scenario, when the automation is turned off it could be programed to: return to center, lock in place, drop all control (no automation even with no manual control either), or continue automated control of steering until driver takes over. There may be an argument for each of these options, but an important consideration is that the driver will likely not know which option actually occurs until they experience the situation themselves. Furthermore, not all of these options are suited for all road conditions. For example, dropping all control will cause the wheel to quickly center itself. On a straight road, this may not have a significant impact on the vehicle steering, but on a curved road this could cause the vehicle to enter other lanes. Continuing with automation until the driver takes over may seem like a promising option, as it could presumably follow the curve of a road while the driver takes over—but what if the transition occurs in an area where there are no lane markings for guidance (e.g. the driver deactivated HTAF where construction was occurring). Depending on whether or not this edge case is covered in the programming, the vehicle could steer to try to center itself in a lane that does not exist.

Potential Recommendation: Vehicle behavior should be predictable—and the average driver would predict that in the brief interval before they take control, the vehicle will proceed along the "intended" path. Ultimately, this will require some level of automated control. Though it should maintain an ability to follow lane markings, edge cases need to be factored in, particularly because edge cases are common when the driver decides (or may even be alerted that) they need to take control. The secondary priority, without adding significant lateral collision avoidance capability, is to enable the vehicle to maintain

current trajectory. Ultimately, the vehicle must be provided with some internal decision-making capability for the transition which assumes the possibility of degraded conditions.

Level 3 Analysis Insights

The Level 3 Scenario 1 is unique in that the design choices leading to this scenario in no way promise this or any similar capability; in fact, it is explicitly a limitation of the system.

> Refined Scenario 1 (RF-88.1.1): *Vehicle is on imminent collision path, and Driver does not provide steering to deactivate HTAF (UCA-88) even though driver has correct indication that vehicle is on collision path and that other control measures are absent (BS-88.1). The driver believes vehicle will provide the necessary steering to prioritize collision avoidance (rather than just staying in lane) (MM-3), and a vehicle to the side swerves over the lane markings. The driver believes the vehicle has this ability because they previously learned that HTAF will automatically react to avoid forward collisions, and therefore they believe it will also automatically react to avoid side collisions (UMM-1). In reality, HTAF has the capability to react to only the vehicle ahead through speed control; all steering performed by HTAF is exclusively used to keep the vehicle in lane even if steering is needed to avoid a collision..*

The internal capability is confined to (1) staying in lane, (2) maintaining speed, and (3) preventing *forward* collision[††]. Instead, it explores how the driver may come to have incorrect beliefs about the system's capabilities, which might lead them to perform unsafe control actions. In this particular instance, the driver may be aware they *can* steer or deactivate HTAF to avoid collision, but may choose not to because they think the action is unnecessary.

Potential Recommendation: Provide means to ensure driver has accurate understanding of system capabilities and limitations. Though the long-term fix may be to provide a capability which *is* capable of performing this level of action prioritization (avoiding collision versus staying in lane), minimally consider external interfaces beyond operation, such as dealerships and advertisers, and provide explicit lists of limitations so no false claims are made. Alternatively, consider providing supplementary training (beyond providing a driver's manual)- such as a video the owner can watch to learn how to operate the system. Lastly, we again might consider adding steering to the list of allowable overrides, so the consequence of a minor correction is less severe.

How relevant are these insights for real automotive systems?

These recommendations demonstrate that STPA is effective at identifying human factors issues, at all levels of refinement. Though the scenarios created refer to more detailed parts of the design as they are iterated, the recommendations drawn can be looked at from both a high and low level. At level 1, the recommendation alludes to a high level decision on what capability the feature should include. At a low level, it offers a specific solution like the speed limit setting being viewable and adjustable. Similarly, level 3 refers to a high level concept of ensuring accurate conveyance of system capability, while also offering specific solutions based on the scenario. The scenarios created make it easier to generate realistic and applicable solutions that are directly traceable to a specific hazard and loss. It should be noted that the example recommendations in this work are not meant to give a definitive answer to the best possible automation design, as they are just meant to provide examples of how to follow the process.

The HTAF system analyzed in Chapter 3 is a fictional system, but it was created to closely align with real development efforts by major automotive companies currently developing these systems. Approximately 20 hours of interviews were conducted with engineers at various companies to collect information and produce the representative HTAF system analyzed in this thesis, in addition to individual reading and interactions with similar systems. Some of system details were proprietary, so there are gaps which have been filled either with known behaviors of systems that are already in production or with proposals by

[††] Preventing forward collision is not an intended HTAF function - the vehicle will slow if the lead vehicle slows, and AEB will work in tandem to assist in collision prevention, but the driver is expected to take control if needed.

others that have not yet made it to production. This does not diminish the validity of the scenarios, as the recommendations that emerged as a result are still pertinent.

Many aspects of the fictional HTAF system reflect real decisions and assumptions made well before the design was finalized and made production-ready. Many of the issues uncovered in this analysis have since been raised with the manufacturers or suppliers and addressed before the design was finalized. Therefore, the analysis and system weaknesses identified in this thesis are not necessarily a reflection or a criticism of any specific production vehicle. Instead, this thesis should be seen as a demonstration of how such issues can be uncovered early before the design is finalized.

4.7 STPA Approach of Human Factors Issues

In systems where we are changing the role of the operator, it is important to understand how these changes affect their control actions and decision making. For vehicle automation, this an especially important consideration for SAE Levels 2 and 3, as the operator is not exclusively a driver or passenger.

STPA inherently considers human factors issues more comprehensively than other methodologies because the human is considered to be a part of the system as another controller element; that is to say human factors issues are incorporated within a larger analysis of the whole system. This means that they can contribute to system-level weaknesses and are critical to the total success of the system. The body of this analysis focused on human-derived control actions, and how the refinements of these actions propagate themselves within each iteration.

That said STPA is not exclusively a human factors analysis, akin to how it is not exclusively a software or automation analysis. The human factors extension maintains this holistic approach that is central to STPA, while focusing on providing insights that inform design for human use. Because this extension is largely assigned to scenario generation, the analysis that was performed was distributed across all control actions by all system elements, and not solely focused on human factor related insights until refined scenarios were produced.

The STPA approach integrates consideration of human factors within the context of the rest of the analysis, while giving equal consideration to the other interactions in the system. This balanced approach can be applied as a major improvement over other methods that miss important interactions by considering human factors separately from other considerations.

Chapter 5: Conclusions

5.1 Key Takeaways

This work demonstrated and evaluated an iterative analysis and refinement of complex human-automation systems using STPA. This process enables the analyst to rapidly provide recommendations based on comprehensive system understanding, and to demonstrate the types of recommendations that may be provided in subsequent levels of refinement. The application to HTAF-equipped vehicles found that this methodology is both feasible and beneficial for analysis of complex automation.

To perform this analysis, refinement was applied at every step of the STPA procedure. General types of refinement were employed including that of subsystems and the resulting emergence of additional subsystem controllers, control actions, and contexts of the control actions. The most meaningful changes were demonstrated between iterations of the control structure and UCAs, as well as from basic to detailed scenarios whereby the quantity or quality was markedly increased. The detail available at each level of analysis, seen in the control structure, determined the specificity of the resulting UCAs and scenarios. Potential risks and recommendations could be provided at every level.

This work benefits the body of STPA research by demonstrating how iteration affects all parts of the STPA process. It also demonstrates the basic scenario generation process for a new automotive application. Furthermore, it demonstrated that the human factors extension can be used as the refinement method for basic scenarios that involve a human controller—another application for the existing body of work.

STPA has already been established as a valuable method for capturing system-level hazards, including the inclusion of the operator as an important element of the system. Though the transition from a high-level overview to a low-level detailed depiction of the system has been alluded to in the STPA methodology and existing guidance (STPA Handbook [13]) with short examples, there has not been a public demonstration and evaluation of each step of the method through three levels of iteration. This contribution demonstrates additional guidance and traceability that is possible through multiple iterations, of control structures, UCAs, and scenarios. Iterative use of STPA would prove valuable for any application requiring rapid and ongoing recommendations, especially since this analysis can grow with the system as it is designed and developed.

Though every effort was made to provide a realistic and accurate analysis of the HTAF system, there are some limitations to this study. This system is based on interviews and descriptions of real systems in development and in production. Different models were used to supplement the understanding of the automation for the benefit of the reader and the analyst, and to demonstrate the methods indicated in this work. Furthermore, this is not a complete analysis; a selection of scenarios was chosen to demonstrate hazards pertaining to human factors, but more would need to be created to be truly comprehensive.

STPA is an excellent method for hazard analysis, and the extensions applied in this work were found to provide scalability as system complexity increases as well as demonstrating how human factors insights can be gained from a holistic perspective. The method is intended to guide, not replace, the contributions from the team of engineers and other experts involved. To successfully perform STPA, the analyst will need sufficient training and a basic understanding of the system being analyzed which will be dependent on their own knowledge or that which can be collected from experts. Furthermore, when representing the mental model of an actual user, extra care needs to be taken to ensure their understanding of the system is accurately depicted to get the best results. This will likely only include a high-level comprehension of how the subsystem works, especially as compared to the engineer or analyst's knowledge.

Key findings:

- Three basic refinement methodologies (subsystem controllers, control actions, and contexts of the control actions) can be applied to provide iterative analyses on a system and manage complexity as the analysis grows
- Control actions and feedback (between a controller and controlled process) are cyclical, so an inverted (incorrect) control loop interpretation does not invalidate an analysis
- Iterative refinement can provide the context needed to refine horizontal "other information" arrows into distinct control actions and feedback paths
- Refinement can be applied at every step of STPA
- The comprehensive and inclusive nature of applying STPA promotes the generation of new extensions for more specific uses of the analysis
- Even at the highest level (lowest detail) of system analysis, STPA will produce insights and recommendations
- The STPA approach to human factors allows the analyst to provides valuable human factors insights without compromise to the analysis of other interactions in the system

5.2 Recommendations and Future Work

"Self-driving" vehicle subsystems today do not have clear and consistent expectations for the driver/automation interface. As the number of accidents caused by or involving automated vehicles increases, it is becoming evident that changes to the HMI can have substantial impact on the success of the system. This increase in data indicates that there are many human factors which need to be addressed—such as what is an acceptable way to govern and ensure sufficient driver supervision and attention, how to promote straightforward decision making, how to quantify acceptable reaction time as the driver moves from supervisor to controller, and how to ensure the HMI supports all these elements.

It is possible to utilize STPA to address these gaps. By utilizing the hierarchical structure, it is possible to quickly hone in on these factors while maintaining the benefits of a system level analysis. It is hoped that this analysis has helped to demonstrate the benefits of the iterative process, and that it will provide more companies with incentive to use this method to improve the capability of their risk management methods. Furthermore, the hierarchy management demonstrated should promote better organization, processing of results, and savings to cost and schedule by providing the analyst with tools to have a comprehensive analysis that can be focused to the areas requiring immediate guidance. This particular work was used to demonstrate the importance of human centered design, derived from shortcomings evident though scenario creation.

Moving forward, it would be valuable to demonstrate a side by side iterative refinement of two automated subsystems which superficially perform similar functions, but have been implemented differently at lower levels. Such an analysis would provide greater insight to the hierarchy management process, as comparisons can be drawn between the systems to see where the differences in implementation emerge to provide nuanced recommendations. Additionally, further work could be done to analyze how the different refinement methods affect the scale of UCAs output at each level. This analysis demonstrated a sample of the possible expansion, but it would be of particular value to be applied to a complete STPA analysis, where every subsystem is equally refined at every level of iteration. This information would help future analyst manage complexity and growth expectations of the work scale.

The analysis in this work ended up touching on a number of nuances, any of which could be expanded and studied in future work. In particular, the "incorrect" control structure generated significant insight on the rotational quality of the control structure. Further analysis (outside of the one changed control/feedback loop) could be performed to explore and evaluate possible ripple effects of such a change. To eliminate possible bias, it may benefit the analysis to have two different people create UCAs

based on the different control structures. This work would help offer guidance into creating successful control structures by providing definitive knowledge on how and why incorrect assumptions could affect the analysis.

Appendices

Appendix A: Super Cruise Automation Description

The Super Cruise automation feature will be used in this thesis as a point of reference and comparison for the HTAF system. Super Cruise is a "hands free" SAE level 2 feature available in select 2018-2020 Cadillac models.

Similar to HTAF, Super Cruise is intended for highway use and operates via a pre-loaded map system used in conjunction with environment monitoring sensors and cameras, which allows it to react to traffic patterns according to forward vehicle position/speed (range: 0 mph-ACC limits). Super Cruise can be used for cruise control and as a traffic assist feature by providing lane-centering capabilities and adaptive speed control based on the driver-set speed. It is built to supplement and enhance the adaptive cruise control (ACC).

The driver is expected to keep their eyes on the road, else be subjected to the series of driver attention warnings. Unlike HTAF, this system is on the market so the HMI and alert escalation strategy will be detailed below. Upcoming models of Super Cruise will feature automated lane change capability.

Limitations/Assumptions

Super Cruise will only operate on highways as defined in the preloaded maps. This may include alerting drivers to place hands on steering wheel in states where hands free driving is prohibited, though the driver is expected to abide by traffic laws regardless of alert capabilities. Though Super Cruise has the capability to come to a full stop, it should not be depended on for emergency braking (AEB may assist but human monitoring and control is intended). Though the vehicles have sensors and cameras on all sides of the vehicle, only the forward sensors are used for highway speed control. ACC must be enabled to be able to turn on Super Cruise.

Similar to HTAF, the driver is assumed to be licensed and their ability to drive is not compromised. It is not assumed that they have read the driver's manual.

Influence of environmental factors on vehicle function

Vehicle speed is set by the driver but will react to the forward vehicle position and speed. GPS tracks the vehicle's position relative to the pre-loaded maps and if the road is appropriate for feature use, HTAF can be enabled. Road/lane markings are sensed and processed by the vehicle for the purposes of lane centering and to determine if manual control is necessary. Performance may be degraded at night or in inclement weather due to limitations of the sensors and cameras. If performance is detected to be degraded, the operator will be instructed to take control of the vehicle via the systems escalation system.

Escalation strategy

Escalation indicators (feedback options) include visual, audial, and/or haptic feedback. Reasons why Super Cruise disengaged or will not engage are provided to the driver in a brief text format. Duration of/between warnings is on the scale of seconds, and occurs at fixed time (dependent on vehicle speed).

- Engaged and operating: Light bar on steering wheel is steady green color
- Engaged but overridden: Light bar on steering wheel is flashing blue color
- 1st warning- eyes on road: Light bar on steering wheel will flash green
- 2nd warning- take over steering and reengage feature: Light bar flashing red plus audio or haptic feedback (beeping sound or seat vibration)
- 3rd warning- take control or car comes to stop in lane with hazards on (requires restart to operate HTAF again): Light bar flashing red plus voice command to take control. If no control is taken vehicle will slow to stop in lane and signal brake lights/hazards to other vehicles.

The driver can take control at any point in the escalation strategy, however if it reaches the 3rd warning the driver will need to cycle the ignition before they can turn on HTAF again.

Turn on Super Cruise

The vehicle must be on highway for the system to become engageable, and the vehicle should not be too close to any vehicle ahead. Next, ACC must be enabled. When Super Cruise is available, a designated symbol (matching the button on the wheel) appears on the display behind the wheel. At that point, the driver may press the button, and the light display on the wheel will turn blue if the driver is applying torque to the wheel. Once the vehicle is centered in lane, the light display will turn green and the driver may release control of the wheel, and continue monitoring the road. Super Cruise will not engage if the system is not in good health (capable of diagnosing and detecting faults), or capable of monitoring the ODDs (e.g. certified highway roads, lead vehicle, and more). While the system is engaged, if driver monitoring determines the driver has looked away for too long it will engage the escalation strategy. Lastly, the driver can change the set speed while Super Cruise is engaged by pressing +/- arrows on the steering wheel to change the speed seen in the heads-up display.

Turn off Super Cruise

When the driver wishes to exit a highway environment or take manual control of the vehicle, they may turn off Super Cruise by applying braking or by pressing either the Super Cruise button or the ACC button (which will disengage ACC and consequently Super Cruise). Unless the driver brakes, ACC will remain on when Super Cruise is disengaged. When Super Cruise is disengaged, it remains on in a degraded mode until the driver takes

Super Cruise steering can always be overridden, at which point the steering wheel light will turn blue. The driver can also accelerate and change lanes to override while Super Cruise is engaged. Braking results in a takeover request.

Failure to provide attention for extended periods will result in feature deactivation- the stop in lane function. If the driver monitoring subsystem or vehicle sensors become blocked, manual control will be requested. The driver should be able to wear sunglasses, but some facial coverings (like sanitary face masks) may result in compromised ability to monitor the driver's face/eyes. Certain ODDs may result in ABS or ESC engagement, or sensor degradation, at which point the driver will be asked to take control. The driver will need to take over when construction is present and when there is a lack of lane markings. Getting off the highway results in takeover request.

Appendix B.1: Enlarged Level 1 Control Structure

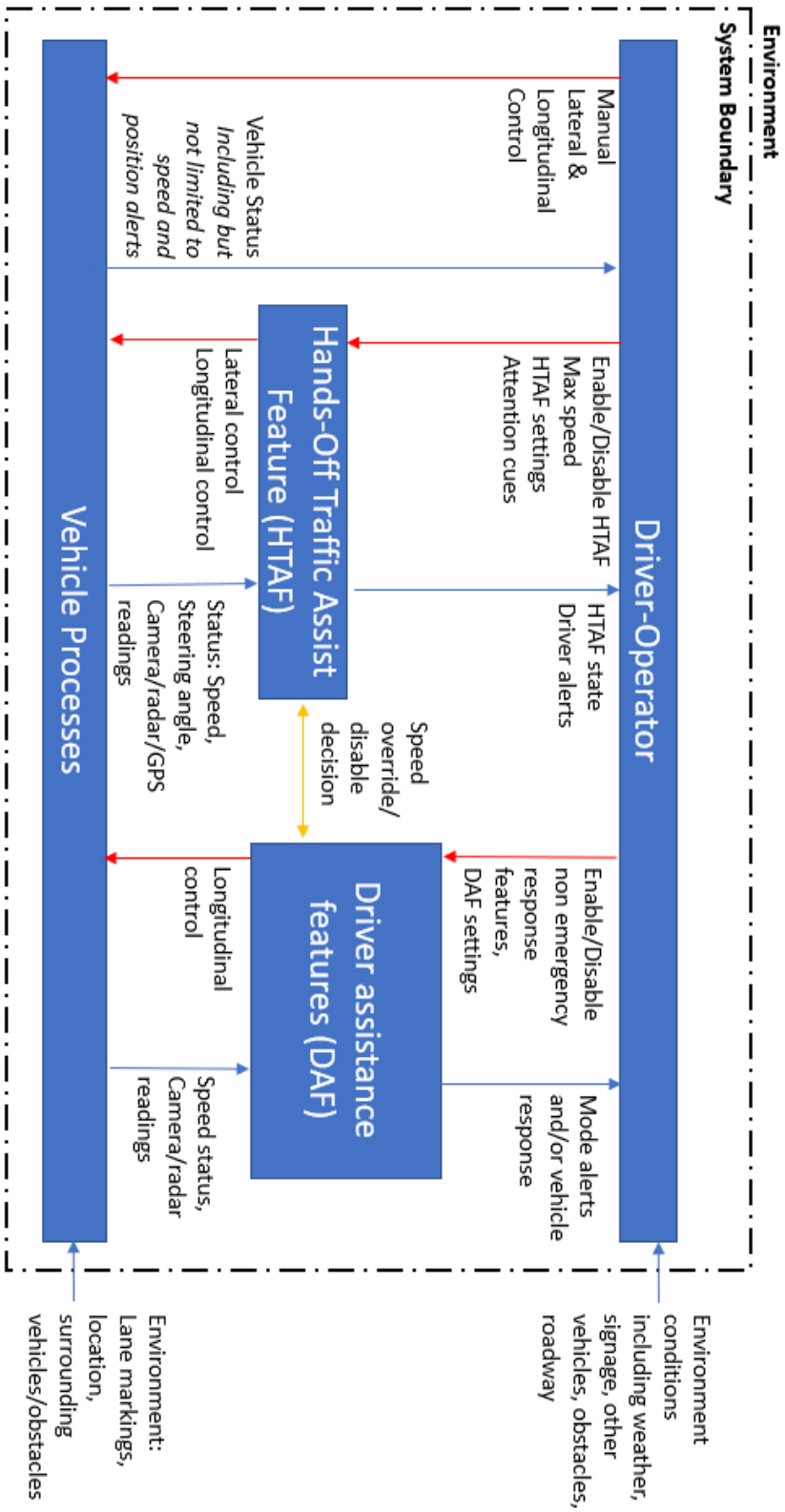

Figure 28: Enlarged Level 1 Control Structure

Appendix B.2: Level 1 UCAs

Note: For this UCA table and all following, Human Controlled Actions are colored in blue, HTAF controlled are colored in grey, and DAF controlled are colored in yellow. Furthermore, these are exploratory draft UCAs produced during the analysis, and not meant to be final UCAs. They are provided in this appendix to help interested readers follow the original thought process as the analysis was conducted.

Table 15: Level 1 UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Manual Longitudinal Control	(UCA-1) Driver does not provide longitudinal control to adjust speed of vehicle when vehicle is on collision path [H-1, H-2, H-3] (UCA-2) Driver does not provide longitudinal control to keep speed within legal limits [H-3]	(UCA-3) Driver provides longitudinal control that moves vehicle into collision path [H-1, H-2, H-3] (UCA-4) Driver provides incorrect longitudinal control to amend speed when vehicle speed is not at legal speed limits [H-3] (UCA-5) Driver provides longitudinal control that is insufficient to avert collision [H-1, H-2, H-3]	(UCA-6) Driver provides longitudinal control too late after collision is unavoidable [H-1, H-2, H-3] (UCA-7) Driver provides long-itudinal control too early before vehicle is on imm-inent collision path [H-1, H-2, H-3]	(UCA-8) Driver stops providing longitudinal control too soon before collision is averted [H-1, H-2, H-3] (UCA-9) Driver applies longitudinal control too long after vehicle enters collision path [H-1, H-2, H-3]
Manual lateral control	(UCA-10) Driver does not provide lateral control to steer vehicle when vehicle is on collision path [H-1, H-2, H-3] (UCA-11) Driver does not provide lateral control to keep vehicle within lane markings [H-3]	(UCA-12) Driver provides lateral control that steers vehicle into collision path [H-1, H-2, H-3] (UCA-13) Driver provides lateral control that steers vehicle in violation of traffic guidance [H-1, H-2, H-3] (UCA-14) Driver provides lateral control that is insufficient to steer vehicle from path with obstacle [H-1, H-2, H-3] (UCA-15) Driver provides excessive lateral control that steers vehicle into collision path [H-1, H-2, H-3]	(UCA-16) Driver provides lateral control too early before verifying vehicle is not on collision path (OR) in violation of traffic guidance [H-1, H-2, H-3] (UCA-17) Driver provides long-itudinal control too late after collision is unavoidable [H-1, H-2, H-3]	(UCA-18) Driver stops providing lateral control too soon before obstacle is avoided [H-1, H-2, H-3] (UCA-19) Driver applies lateral control too long after turn is completed [H-1, H-2, H-3]
Enable HTAF	(UCA-20) Driver does not provide enable HTAF command to transition to automated driving when relinquishing manual controls [H-1, H-2, H-3, H-4]	(UCA-21) Driver provides enable HTAF command when operating manually [H-1, H-2, H-3, H-4] (UCA-22) Driver provides enable HTAF command when not in hig-hway driving setting [H-3, H-4] (UCA-23) Driver provides enable HTAF where prohibited by law [H-3]	(UCA-24) Driver provides enable HTAF command too early before lead vehicle is in appropriate range [H-1, H-2, H-3, H-4]	(UCA-25) Driver stops providing enable HTAF command too soon before mode change is applied [H-1, H-2, H-3, H-4]

Disable HTAF	(UCA-26) Driver does not provide disable HTAF command when transitioning to manual driving [H-1, H-2, H-3, H-4] (UCA-27) Driver does not provide disable HTAF command to take control when HTAF is on and not responding to obstacle(s) in path [H-1, H-2, H-3, H-4] […]	(UCA-28) Driver provides disable HTAF command when driver is unable to mitigate an imminent collision but HTAF is [H-1, H-2, H-4] (UCA-29) Driver provides disable HTAF command when driver preparedness to take control is low [H-1, H-2, H-3, H-4] (UCA-30) Driver performs insufficient action to disable HTAF when transitioning to manual driving [H-1, H-2, H-3, H-4] […]	(UCA-31) Driver provides disable HTAF command too early before they are ready to take manual control [H-1, H-2, H-3, H-4] (UCA-32) Driver provides disable HTAF command too late after vehicle is on collision path [H-1, H-2, H-3, H-4] […]	(UCA-33) Driver stops providing disable HTAF command too soon before mode change is applied [H-1, H-2, H-3, H-4] […]
HTAF Speed Limit Setting	(UCA-34) Driver does not provide speed limit setting to regulate longitudinal control when the hands off feature speed limit is not suitable for the region (e.g. legal limits) [H-3, H-4]	(UCA-35) Driver provides speed limit setting that is too large for full stop when following vehicle [H-1, H-2, H-3, H-4] (UCA-36) Driver provides speed limit setting to regulate longitudinal control while driving <TBD kph [H-1, H-2, H-3, H-4]	(UCA-37) Driver sets speed limit setting too late after HTAF is engaged [H-1, H-2, H-3, H-4]	(UCA-38) Driver [takes too long to] provide speed limit setting via acceleration/ deceleration when HTAF is engaged [H-1, H-2, H-3, H-4]
HTAF settings	(UCA-39) Driver does not provide HTAF settings when they have limitations in their perception of audio/haptic feedback [H-1, H-2, H-3, H-4]			(UCA-40) Driver provides incomplete (stops too soon) HTAF settings while configuring vehicle and they have sensory limitations [H-1, H-2, H-3, H-4]
Provide Attention	(UCA-41) Driver does not provide attention cues to monitor vehicle while obstacles are in vehicle path [H-1, H-2, H-3, H-4]	(UCA-42) The driver provides sufficient attention cues while vehicle remains on collision course with HTAF engaged [H-1, H-2, H-3, H-4] (UCA-43) Driver provides attention cues that responds to alerts when no obstacles are present [H-4] (UCA-44) The driver provides excessive attention cues to the environment when vehicle control is needed in response to obstacles in path [H-1, H-2, H-3, H-4]	(UCA-45) Driver provides attention cues too late after collision is imminent [H-1, H-2, H-3, H-4]	(UCA-46) Driver provides attention cues too long after imminent collision requires manual intervention (e.g. driver is not aware of environment) [H-1, H-2, H-3, H-4]

Enable non-emergency driver assist features (DAF)	(UCA-47) Driver does not enable DAF when relinquishing control of corresponding manual feature and obstacles are in path [H-1, H-2, H-3, H-4]	(UCA-48) Driver enables DAF while not in appropriate environment settings (as determined by manufacturer) [H-1, H-2, H-3] (UCA-49) Driver enables DAF while HTAF is enabled and their hands are not at the wheel and/or foot not on gas/brake [H-1, H-2, H-3, H-4]	(UCA-50) Driver enables DAF too early before they reach their intended speed [H-4] (UCA-51) Driver enables DAF too early before path is safe [H-1, H-2]	
Disable non-emergency driver assist features (DAF)	(UCA-52) Driver does not disable DAF when there are changes to road speed or conditions [H-1, H-2, H-3, H-4] (UCA-53) Driver does not disable DAF when transitioning to manual driving [H-1, H-2, H-3, H-4] (UCA-54) Driver does not disable DAF when vehicle does not respond to obstacle(s) in path [H-1, H-2, H-3, H-4]	(UCA-55) Driver provides disable DAF command when feature is already disabled and HTAF is on [H-1, H-2, H-3, H-4] (UCA-56) Driver provides disable DAF command when driver control preparedness is low [H-1, H-2, H-3, H-4]	(UCA-57) Driver disables DAF too early before foot is on gas/brake [H-1, H-2, H-3, H-4] (UCA-58) Driver disables DAF too late after vehicle is on collision path [H-1, H-2, H-3, H-4]	
Set DAF speed		(UCA-59) Driver sets excessive speed that is too large for full stop to prevent forward collision [H-1, H-2, H-3] (UCA-60) Driver sets speed while in violation of legal speed limit [H-1, H-2, H-3] (UCA-61) Driver sets speed while vehicle is operating at low speeds and following vehicles are present (forgets after acceleration to override and vehicle suddenly slows down) [H-1, H-2, H-3, H-4]	(UCA-62) Driver sets speed too late after DAF is already engaged [H-1, H-2, H-4]	
Lateral control	(UCA-63) HTAF does not provide lateral control to steer vehicle when obstacles are in path [H-1, H-2, H-3, H-4] (UCA-64) HTAF does not provide lateral control to steer vehicle when lane markings are	(UCA-65) HTAF provides lateral control that steers vehicle to violate lane markings [H-1, H-2, H-3, H-4] (UCA-66) HTAF provides lateral control that steers vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-67) HTAF provides lateral control when there is no guidance	(UCA-70) HTAF provides lateral control too late after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-71) HTAF provides lateral control too early before verifying vehicle is not on	(UCA-72) HTAF provides lateral control too long after turn is completed that steers vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-73) HTAF stops providing lateral control too

	present [H-1, H-2, H-3, H-4]	(lane markings, etc.) [H-1, H-2, H-3, H-4] (UCA-68) HTAF provides insufficient lateral control to steer vehicle when obstacle is in path AND/OR to keep vehicle within lane [H-1, H-2, H-3, H-4] (UCA-69) HTAF provides excessive lateral control that steers vehicle into collision path [H-1, H-2, H-3, H-4]	collision path (OR) in violation of traffic guidance [H-1, H-2, H-3]	soon before obstacle is avoided [H-1, H-2, H-3, H-4]
Longitudinal control	(UCA-74) HTAF does not provide longitudinal control to adjust speed of vehicle when vehicle is on collision path [H-1, H-2, H-3, H-4]	(UCA-75) HTAF provides longitudinal control when the driver is manually controlling vehicle [H-1, H-2, H-4] (UCA-76) HTAF provides excessive longitudinal control that adjusts speed beyond the set limit range [H-3, H-4] (UCA-77) HTAF provides longitudinal control that moves vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-78) HTAF provides longitudinal control that is insufficient to avert collision [H-1, H-2, H-3, H-4]	(UCA-79) HTAF provides longitudinal control too late to adjust speed after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-80) HTAF provides longitudinal control too early before collision is imminent [H-1, H-2, H-3, H-4]	(UCA-81) HTAF stops providing longitudinal control too soon before collision is averted [H-1, H-2, H-3, H-4] (UCA-82) HTAF applies longitudinal control too long after vehicle enters collision path [H-1, H-2, H-3, H-4]
Longitudinal Control	(UCA-83) DAF does not provide longitudinal control to adjust speed when collision is imminent [H-1, H-2, H-3, H-4] (UCA-84) DAF does not provide longitudinal control when driver is not attending speed controls manually [H-1, H-2, H-4]	(UCA-85) DAF provides longitudinal control that moves vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-86) DAF provides longitudinal control when there is no obstacle or limit in path [H-1, H-2, H-4] (UCA-87) DAF provides longitudinal control that is insufficient to avert collision [H-1, H-2, H-3, H-4]	(UCA-88) DAF provides longitudinal control too late to adjust speed after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-89) DAF provides longitudinal control too early before collision is imminent [H-1, H-2, H-3, H-4]	(UCA-90) DAF stops providing longitudinal control too soon before collision is averted [H-1, H-2, H-3, H-4] (UCA-91) DAF applies longitudinal control too long after vehicle enters collision path [H-1, H-2, H-3, H-4]

Appendix C.1: Enlarged Level 2 Control Structure

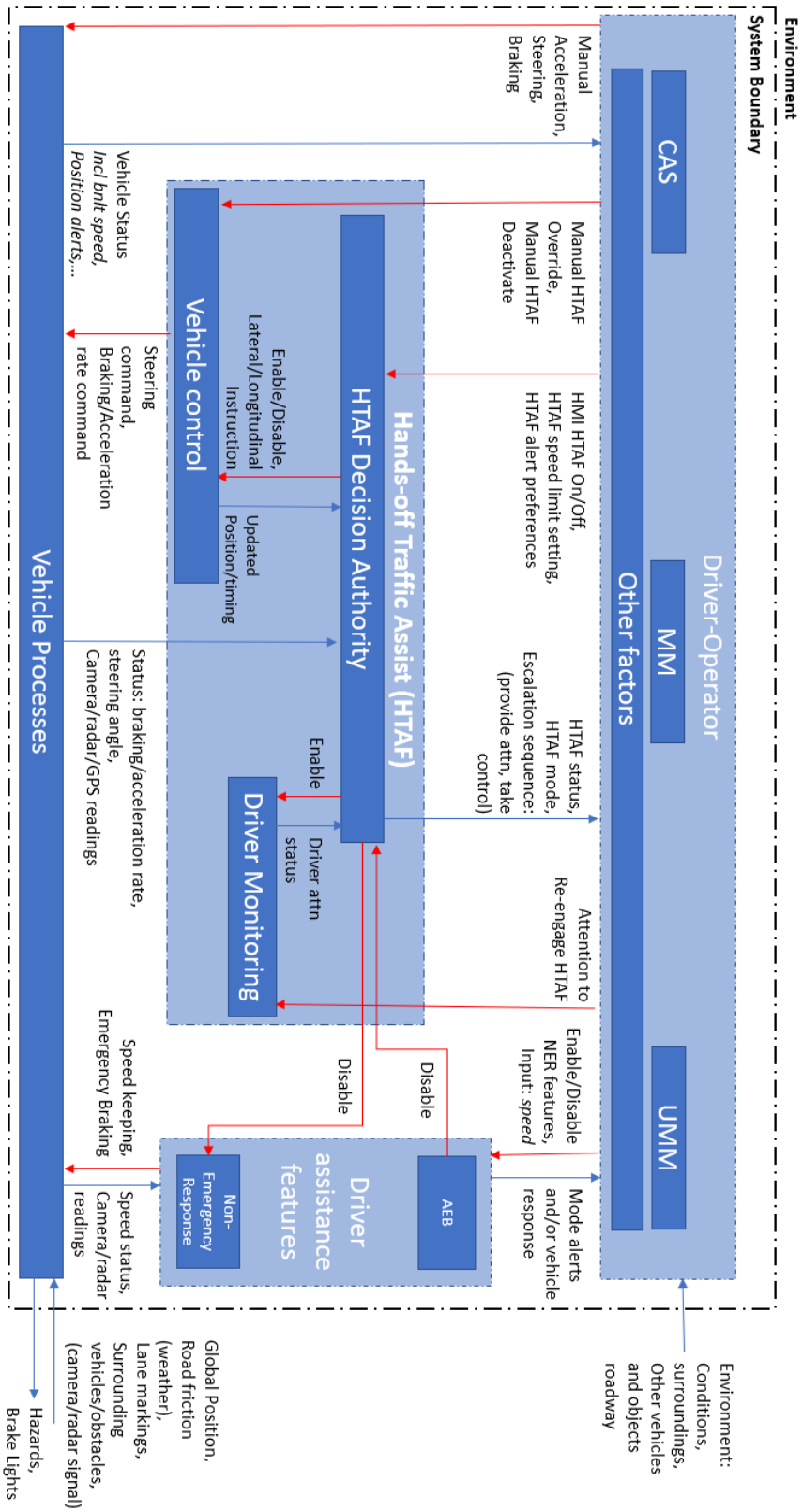

Figure 29: Enlarged Level 2 Control Structure

Appendix C.2: Level 2 UCAs

Note: For this UCA table and all following, Human Controlled Actions are colored in blue, HTAF controlled are colored in grey, and DAF controlled are colored in yellow. Furthermore, these are exploratory draft UCAs produced during the analysis, and not meant to be final UCAs. They are provided in this appendix to help interested readers follow the original thought process as the analysis was conducted.

Table 16: Complete Level 2 UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Acceleration	(UCA-1) Driver does not provide acceleration command to adjust speed of vehicle when vehicle is on collision path [H-1, H-2, H-3] (UCA-2) Driver does not provide acceleration command to keep speed within legal limits [H-3]	(UCA-3) Driver provides acceleration command that moves vehicle into forward collision path [H-1, H-2, H-3] (UCA-4) Driver provides acceleration command that increases the vehicle speed above legal speed limits [H-3] (UCA-5) Driver provides acceleration command that is insufficient to avert collision [H-1, H-2, H-3]	(UCA-6) Driver provides acceleration command too late after rear/side collision is unavoidable [H-1, H-2, H-3] (UCA-7) Driver provides acceleration too early before forward path is clear [H-1, H-2, H-3]	(UCA-8) Driver stops providing acceleration command too soon before side/rear collision is averted [H-1, H-2, H-3] (UCA-9) Driver applies acceleration command too long after vehicle enters forward collision path [H-1, H-2, H-3]
Steering	(UCA-10) Driver does not provide steering to change vehicle direction to prevent collision with slowed or stopped obstacles/ vehicles in lane [H-1, H-2, H-3] (UCA-11) Driver does not provide steering to change vehicle direction to prevent collision with obstacles in adjacent lane(s) [H-1, H-2, H-3] (UCA-12) Driver does not provide steering to keep vehicle centered between lane markings [H-3]	(UCA-13) Driver provides steering that changes vehicle direction to a collision path [H-1, H-2, H-3] (UCA-14) Driver provides steering that changes vehicle direction to violate traffic guidance [H-3] (UCA-15) Driver provides insufficient steering to keep vehicle within lane and/or change vehicle direction from path with obstacle [H-1, H-2, H-3] (UCA-16) Driver provides excessive steering to change vehicle direction into collision path [H-1, H-2, H-3]	(UCA-17) Driver provides steering too early before verifying vehicle is not on collision path (OR) in violation of traffic guidance [H-1, H-2, H-3] (UCA-18) Driver provides steering too late after collision is unavoidable [H-1, H-2, H-3]	(UCA-19) Driver stops providing steering too soon before obstacle is avoided [H-1, H-2, H-3] (UCA-20) Driver provides steering too long after turn is completed [H-1, H-2, H-3]
Braking	(UCA-21) Driver does not provide braking to	(UCA-24) Driver provides braking that moves vehicle	(UCA-27) Driver provides braking too	(UCA-29) Driver stops

	slow/stop vehicle when vehicle is on collision path [H-1, H-2, H-3] (UCA-22) Driver does not provide braking to keep speed within legal limits [H-3] (UCA-23) Driver does not provide braking to slow/stop vehicle when there is a change to the road conditions that affects performance [H-2, H-3]	into collision path [H-1, H-2, H-3] (UCA-25) Driver provides braking when vehicle speed is below legal limits [H-3] (UCA-26) Driver provides insufficient braking to avert forward/side collision [H-1, H-2, H-3]	late after forward/side collision is unavoidable [H-1, H-2, H-3] (UCA-28) Driver provides braking action too early before vehicle is on collision path [H-1, H-2, H-3]	providing braking too soon before forward/side collision is averted [H-1, H-2, H-3] (UCA-30) Driver applies braking too long after reacting to obstacle [H-3]
Manual Override HTAF	(UCA-31) Driver does not provide manual override when HTAF is not responding to prevent a collision [H-1, H-2, H-3, H-4]	(UCA-32) Driver provides manual override to change vehicle speed while hands are on the wheel (resulting in unintended deactivation and confusion) [H-4] (UCA-33) Driver provides manual override to change vehicle speed while applying torque to the steering wheel (resulting in unintended deactivation and confusion) [H-4]	(UCA-34) Driver performs override too late after vehicle is on collision path [H-1, H-2, H-3, H-4] (UCA-35) Driver performs override too early before they are ready to take temporary manual control [H-1, H-2, H-3, H-4]	(UCA-36) Driver continues providing manual override too long (3s) until system deactivates when driver is temporarily overriding [H-1, H-2, H-3, H-4] (UCA-37) Driver provides manual override too long until vehicle enters collision path [H-1, H-2, H-3] UCA-38) Driver stops providing manual override too soon before collision is averted [H-1, H-2, H-3]
Manual Deactivate HTAF	(UCA-39) Driver does not provide manual deactivate to change vehicle speed/direction when vehicle is on collision path [H-1, H-2, H-3, H-4] (UCA-40) Driver does not provide manual deactivate to change vehicle speed/direction when HTAF is unable to supervise the vehicle	(UCA-41) Driver provides manual deactivate when vehicle is on collision path and driver is unable to mitigate [H-1, H-2, H-3, H-4] (UCA-42) Driver provides manual deactivate to take manual control of speed/direction when their hands are off the wheel or their foot is off the gas/brake [H-1, H-2, H-3, H-4] […]	(UCA-43) Driver performs manual deactivate too late after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-44) Driver performs manual deactivate too early before they have full manual control [H-1, H-2, H-3, H-4] […]	(UCA-45) Driver stops performing manual deactivate too soon before HTAF is fully deactivated [H-1, H-2, H-3, H-4] […]

	effectively [H-1, H-2, H-3, H-4] […]			
Turn HTAF On	(UCA-46) Driver does not turn on HTAF to transition to automated driving when relinquishing control of steering wheel, gas pedal, and brake pedal [H-1, H-2, H-3, H-4]	(UCA-47) Driver turns on HTAF while continuing to operate lateral and/or longitudinal control [H-1, H-2, H-3, H-4] (UCA-48) Driver turns on HTAF when on a road not approved in the pre-loaded map [H-3, H-4] (UCA-49) Driver turns on HTAF where hands free driving is prohibited by law (see local guidance) [H-3] (UCA-50) Driver turns on HTAF when not in advised traffic context [H-3]	(UCA-51) Driver turns on HTAF too late after lead vehicle is too far ahead [H-4] (UCA-52) Driver turns on HTAF too early before lead vehicle is far enough away [H-1, H-2, H-3, H-4]	(UCA-53) Driver stops providing turn on HTAF command too soon before mode change is applied (switch not engaged or lead vehicle not in correct position) [H-1, H-2, H-3, H-4]
Turn Off HTAF (via control panel)	(UCA-54) Driver does not turn off HTAF to take over control when vehicle does not respond to obstacle(s) in path [H-1, H-2, H-3, H-4] (UCA-55) Driver does not turn off HTAF when road/environmental conditions are too degraded for continued HTAF use [H-1, H-2, H-3, H-4]	(UCA-56) Driver turns off HTAF, putting vehicle on a collision path when no collision was imminent [H-1, H-2, H-3, H-4] (UCA-57) Driver turns off HTAF when driver is not attending manual controls [H-1, H-2, H-3, H-4] (UCA-58) Driver turns off HTAF when driver is not monitoring road conditions [H-1, H-2, H-3, H-4]	(UCA-59) Driver turns off HTAF too late after already deactivating via manual controls [H-1, H-2, H-3, H-4] (UCA-60) Driver turns off HTAF too late after collision is unavoidable [H-1, H-2, H-3, H-4] (UCA-61) Driver turns off HTAF too early before they are prepared to take manual control [H-1, H-2, H-3, H-4]	
HTAF Speed Limit Setting	(UCA-62) Driver does not provide speed limit where lead vehicle's speed is greater than speed limit but less than or equal to 80kph [H-3, H-4] (UCA-63) Driver does not provide speed limit when HTAF is initiated at <kph, and lead vehicle accelerates over 80kph [H-3, H-4]	(UCA-64) Driver provides excessive speed limit that is too large to enable full stop according to following distance [H-1, H-2, H-3, H-4] (UCA-65) Driver provides speed limit while driving <TBD kph and lead vehicle is present [H-3, H-4] (UCA-66) Driver provides speed limit while driving <TBD kph and no lead vehicle is present [H-3, H-4]	(UCA-68) Driver sets speed limit (via acceleration/deceleration) out of order, after HTAF is engaged [H-1, H-2, H-3, H-4] (UCA-69) Driver provides speed limit too early before a lead vehicle is in position [H-3, H-4]	(UCA-70) Driver sets speed limit but applies gas too long (does not remove pressure) to keep HTAF engaged [H-1, H-2, H-3, H-4] (UCA-71) Driver sets speed limit but applies brake too long (does not remove pressure) to keep HTAF

		(UCA-67) Driver provides excessive speed limit while driving >80 kph [H-3, H-4]		engaged [H-1, H-2, H-3, H-4]
Set HTAF alert preferences	(UCA-72) Driver does not set alert preferences when they have limitations in their perception of audio/haptic feedback [H-1, H-2, H-3, H-4]	(UCA-73) Driver provides incomplete set alert preferences while configuring vehicle and they have sensory limitations [H-1, H-2, H-3, H-4]		
Attention cues- Re-engage HTAF	(UCA-74) Driver does not provide attention cues to re-engage HTAF while other control measures absent and HTAF degraded mode has put vehicle on collision course (e.g. due to rear approaching vehicles) [H-1, H-2, H-3, H-4]	(UCA-75) Driver provides insufficient attention cues (up to and including taking over the controls) to engage HTAF while vehicle is on forward collision course and other control measures are absent [H-1, H-2, H-3, H -4] (UCA-76) Driver provides attention cues to engage HTAF while HTAF is unable to navigate the current environment and other control measures are absent (e.g., HTAF responds to false obstacles and rear vehicles are approaching) [H-1, H-2, H-3, H-4] (UCA-77) Driver provides excessive forward attention cues to engage driver monitoring while vehicle is on collision course with lateral or rear obstacles (resulting in absent attention alerts, further reinforcing driver fwd attention cues away from a rear/side collision) [H-1, H-2, H-4] (UCA-78) Driver provides insufficient attention cues <TBD% of time over HTAF use duration while driver is monitoring environment appropriately (results in inadvertent deactivation/confusion) [H-4] (UCA-79) Driver provides attention cues for ≥TBD% of time over duration of HTAF usage but it is not evenly spaced or otherwise inadequate to observe a collision course (e.g., looking	(UCA-80) Driver provides attention cues too late after alert for imminent in-lane collision [H-1, H-2, H-3, H-4] (UCA-81) Driver provides attention cues too late after collision is imminent and no alert is provided [H-1, H-2, H-3, H-4] (UCA-82) Driver provides attention cues in incorrect order to deescalate alerts (resulting in confusion or HTAF degraded mode creating a collision danger) [H-1, H-2, H-4] (UCA-83) Driver provides attention cues too late to resume HTAF use after the third level warning occurs (resulting in confusion or HTAF degraded mode creating a collision danger) [H-1, H-2, H-3, H-4]	(UCA-84) Driver stops providing attention cues via hands off or hands on actions too soon before able respond to obstacles in path [H-1, H-2, H-3, H-4] (UCA-85) Driver continues providing attention cues too long after driver is incapacitated (resulting in HTAF operation without driver supervision, potential high-speed collision) [H-1, H-2, H-3, H-4]

		away from the colliding object) [H-1, H-2, H-4]		
Enable non-emergency driver assist features (DAF)	(UCA-86) Driver does not enable DAF to maintain speed and relinquishes control of acceleration and braking when rear vehicles are on collision imminent path [H-1, H-2, H-3, H-4]	(UCA-87) Driver enables DAF while not paying attention to objects in current lane and surrounding lanes [H-1, H-2, H-3] (UCA-88) Driver enables DAF while not in appropriate environment (as determined by manufacturer) [H-1, H-2, H-3] (UCA-89) Driver enables DAF to maintain speed when collision is imminent [H-1, H-2, H-3, H-4] (UCA-90) Driver enables DAF while HTAF is enabled and their hands are not at the wheel and/or foot not on gas/brake [H-1, H-2, H-3, H-4] (UCA-91) Driver enables DAF to maintain speed and relinquishes steering control [H-1, H-2, H-3, H-4]	(UCA-92) Driver enables DAF too early before they reach their intended speed [H-3, H-4]	
Disable non-emergency driver assist features (DAF)	(UCA-93) Driver does not disable DAF when there are changes to posted road speed or road conditions [H-1, H-2, H-3, H-4] (UCA-94) Driver does not disable DAF when there are changes to traffic speed or traffic conditions [H-1, H-2, H-3, H-4] (UCA-95) Driver does not disable DAF when switching to manual driving [H-1, H-2, H-3, H-4] (UCA-96) Driver does not disable DAF when vehicle does not change speed for obstacle in path [H-1, H-2, H-3, H-4] (UCA-97) Driver does not disable DAF when vehicle does not steer	(UCA-98) Driver disables DAF to operate with HTAF when feature is already disabled and HTAF is on [H-1, H-2, H-3, H-4] (UCA-99) Driver disables DAF to operate manually when feature is already disabled and HTAF is on [H-1, H-2, H-3, H-4] (UCA-100) Driver provides disable DAF command when driver is inattentive [H-1, H-2, H-3, H-4] (UCA-101) Driver provides disable DAF command when driver does not have manual controls ready to take over [H-1, H-2, H-3, H-4]	(UCA-102) Driver disables DAF too late after forward/side collision is imminent [H-1, H-2, H-3, H-4] (UCA-103) Driver disables DAF too early before foot is on gas/brake [H-1, H-2, H-3, H-4]	

	from obstacle in path [H-1, H-2, H-3, H-4]			
Set DAF speed		(UCA-104) Driver sets excessive speed that is too large for full stop to prevent forward collision [H-1, H-2, H-3, H-4] (UCA-105) Driver sets excessive speed that is >lead vehicle's speed (cruise control) [H-1, H-2, H-3, H-4] (UCA-106) Driver sets speed while in violation of legal speed limit [H-3] (UCA-107) Driver sets speed while vehicle is operating at speeds > (min threshold) kph but less than speed limit and following vehicles are present [H-1, H-2, H-3, H-4] (UCA-108) Driver sets speed while vehicle is operating at speeds < (min threshold) kph [H-3]	(UCA-109) Driver sets speed too late to speed greater than current speed after DAF is already engaged [H-1, H-2, H-4] (UCA-110) Driver sets speed too late to a speed less than current speed after DAF is already engaged [H-1, H-2, H-4]	
HTAF DA Enable monitoring	(UCA-111) DA does not enable driver monitoring when HTAF is turned on [H-1, H-2, H-3, H-4]	(UCA-112) DA enables driver monitoring while in manual or DAF modes [H-1, H-2, H-3, H-4]	(UCA-113) DA enables driver monitoring too late after automation sequence has already begun [H-1, H-2, H-4] (UCA-114) DA enables driver monitoring too early before automation sequence has begun [H-4]	(UCA-115) DA enables driver monitoring and stops too soon before duration of the HTAF-on driving period is complete [H-1, H-2, H-3, H-4] (UCA-116) DA enables driver monitoring too long after the duration of HTAF use is complete [H-1, H-2, H-3, H-4]
HTAF DA Enable VC	(UCA-117) DA does not enable vehicle controls to transition to automated driving while HTAF is engaged [H-1, H-2, H-3, H-4]	(UCA-118) DA enables VC when driver has not performed enable HTAF action [H-1, H-2, H-3, H-4] (UCA-119) DA enables VC when safety overrides are attempted by driver/DAF [H-1, H-2, H-3, H-4]	(UCA-120) DA provides enable VC too late after automated control was initiated by driver [H-1, H-2, H-3, H-4]	(UCA-121) DA provides enable VC but stops too soon before duration of HTAF use is complete [H-1, H-2, H-3, H-4] (UCA-122) DA continues enable of VC too long after duration of

				HTAF use is complete [H-1, H-2, H-3, H-4]
HTAF DA Disable VC	(UCA-123) DA does not disable VC when HTAF is deactivated [H-1, H-2, H-3, H-4] (UCA-124) DA does not disable VC when safety override occurs [H-1, H-2, H-3, H-4]	(UCA-125) DA disables VC when control is not transitioned to DAF of driver [H-1, H-2, H-3, H-4]	(UCA-126) DA provides disable VC too late after when driver control was needed for imminent collision [H-1, H-2, H-3, H-4]	
Lateral instruction	(UCA-127) HTAF does not provide lateral instruction to direct vehicle when collision is imminent [H-1, H-2, H-3, H-4] (UCA-128) HTAF does not provide lateral instruction to direct vehicle when vehicle is in violation of lane guidance [H-1, H-2, H-3, H-4] (UCA-129) HTAF does not provide lateral instruction to direct vehicle when no lanes are present [H-1, H-2, H-4]	(UCA-130) HTAF provides lateral instruction to direct vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-131) HTAF provides lateral instruction to direct vehicle to violate lane markings [H-1, H-2, H-3, H-4] (UCA-132) HTAF provides excessive/ insufficient lateral instruction when no lane markings are present [H-1, H-2, H-3, H-4]	(UCA-133) HTAF provides lateral instruction too early before sensing/processing environment input [H-1, H-2, H-3, H-4] (UCA-134) HTAF provides lateral instruction too late after collision is imminent [H-1, H-2, H-3, H-4]	
Longitudinal instruction	(UCA-135) HTAF does not provide longitudinal instruction to direct vehicle when collision is imminent [H-1, H-2, H-3, H-4] (UCA-136) HTAF does not provide longitudinal instruction to direct vehicle when no lead vehicle is present [H-1, H-2, H-3, H-4]	(UCA-137) HTAF provides longitudinal instruction to direct vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-138) HTAF provides longitudinal instruction that the driver or lead vehicle did not set [H-3, H-4]	(UCA-139) HTAF provides longitudinal control too early before sensing/processing environment [H-1, H-2, H-3, H-4] (UCA-140) HTAF provides longitudinal instruction too late when collision is imminent [H-1, H-2, H-3, H-4]	
Enforce Steering command	(UCA-141) VC does not enforce steering to change vehicle direction when obstacles are in path [H-1, H-2, H-3, H-4] (UCA-142) VC does not enforce steering to change vehicle	(UCA-143) VC enforces steering to change vehicle direction in violation of lane markings [H-1, H-2, H-3, H-4] (UCA-144) VC enforces steering to change vehicle direction that puts vehicle	(UCA-145) VC enforces steering to change vehicle direction too late after collision is imminent [H-1, H-2, H-3, H-4] (UCA-146) VC enforces steering to change vehicle	(UCA-147) VC enforces steering in violation of instruction (steers too long or stops too soon) when vehicle is on path with

	direction according to lane guidance [H-1, H-2, H-3, H-4]	onto collision course [H-1, H-2, H-3, H-4]	direction too early before receiving instruction [H-1, H-2, H-3, H-4]	obstacle [H-1, H-2, H-3, H-4]
Enforce Braking command	(UCA-148) HTAF does not enforce braking to slow/stop vehicle when forward/side collision is imminent [H-1, H-2, H-3, H-4]	(UCA-149) HTAF enforces braking to slow/stop vehicle that moves vehicle into collision path [H-1, H-2, H-4] (UCA-150) HTAF enforces excessive/ insufficient braking in violation of instruction when vehicle is on collision path [H-1, H-2, H-4]	(UCA-151) HTAF enforces braking too late to slow/stop vehicle when collision is imminent [H-1, H-2, H-3, H-4] (UCA-152) HTAF enforces braking to slow/stop vehicle too early before receiving instruction [H-1, H-2, H-3, H-4]	(UCA-153) HTAF stops enforcing braking to slow/stop vehicle too early before collision is averted [H-1, H-2, H-3, H-4]
Enforce Acceleration command	(UCA-154) HTAF does not provide acceleration to move vehicle when rear/side collision is imminent [H-1, H-2, H-3, H-4]	(UCA-155) HTAF enforces acceleration that moves vehicle into collision path [H-1, H-2, H-3, H-4] (UCA-156) HTAF enforces excessive/ insufficient acceleration in violation of instruction when vehicle is on collision path [H-1, H-2, H-3, H-4]	(UCA-157) HTAF enforces acceleration too late to move vehicle when collision is imminent [H-1, H-2, H-3, H-4] (UCA-158) HTAF enforces acceleration to move vehicle too early before receiving instruction [H-1, H-2, H-3, H-4]	(UCA-159) HTAF stops enforcing acceleration too early before collision is averted [H-1, H-2, H-3, H-4]
Disable NER	(UCA-160) DA does not disable NER to control vehicle when HTAF is engaged (especially when they have conflicting commands) [H-1, H-2, H-3, H-4]	(UCA-161) DA disables NER to change control of vehicle when HTAF is not engaged [H-1, H-2, H-3, H-4] (UCA-162) HTAF DA disables NER to control vehicle when HTAF is turned on (driver expects it to resume) [H-4]	(UCA-163) DA disables NER too early before engaging its own controls [H-1, H-2, H-3, H-4] (UCA-164) DA disables NER too late after engaging its own controls [H-1, H-2, H-3, H-4]	
Speed Keeping	(UCA-165) DAF does not provide speed keeping to move vehicle according to set rate [H-3, H-4] (UCA-166) DAF does not provide speed keeping when driver is not attending speed controls [H-1, H-2, H-3, H-4]	(UCA-167) DAF provides speed keeping that moves vehicle into collision path [H-1, H-2, H-4]		(UCA-168) DAF provides speed keeping for longer than DAF is engaged (too long after DAF is terminated) [H-1, H-2, H-3, H-4] (UCA-169) DAF provides speed keeping for less time than DAF is

				engaged [H-1, H-2, H-3, H-4]
Emergency Braking	(UCA-170) DAF does not provide emergency braking when forward collision is imminent and HTAF is not responding [H-1, H-2, H-3, H-4] (UCA-171) DAF does not provide emergency braking when forward collision is imminent and driver is not responding [H-1, H-2, H-3, H-4]	(UCA-172) DAF provides emergency braking to slow/stop when no obstacle is ahead [H-1, H-2, H-3, H-4] (UCA-173) DAF provides insufficient emergency braking to slow/stop vehicle when collision is imminent	(UCA-174) DAF provides emergency braking to slow/stop too late after collision is imminent [H-1, H-2, H-3, H-4] (UCA-175) DAF provides emergency braking to slow/stop vehicle too early before collision is imminent [H-1, H-2, H-3, H-4]	(UCA-176) DAF stops providing emergency braking too soon before collision is averted [H-1, H-2, H-3, H-4]
Disable HTAF	(UCA-177) AEB does not disable HTAF when forward collision is imminent [H-1, H-2, H-3, H-4]	(UCA-178) AEB disables HTAF when a forward collision is imminent and no feature resumes vehicle control [H-4] (UCA-179) AEB disables HTAF when no forward collision was imminent [H-1, H-2, H-3, H-4]	(UCA-180) AEB disables HTAF too early before engaging its own controls [H-1, H-2, H-3, H-4] (UCA-181) AEB disables HTAF too late after engaging its own controls [H-1, H-2, H-3, H-4]	

Appendix D.1: Enlarged Level 3 Control Structure

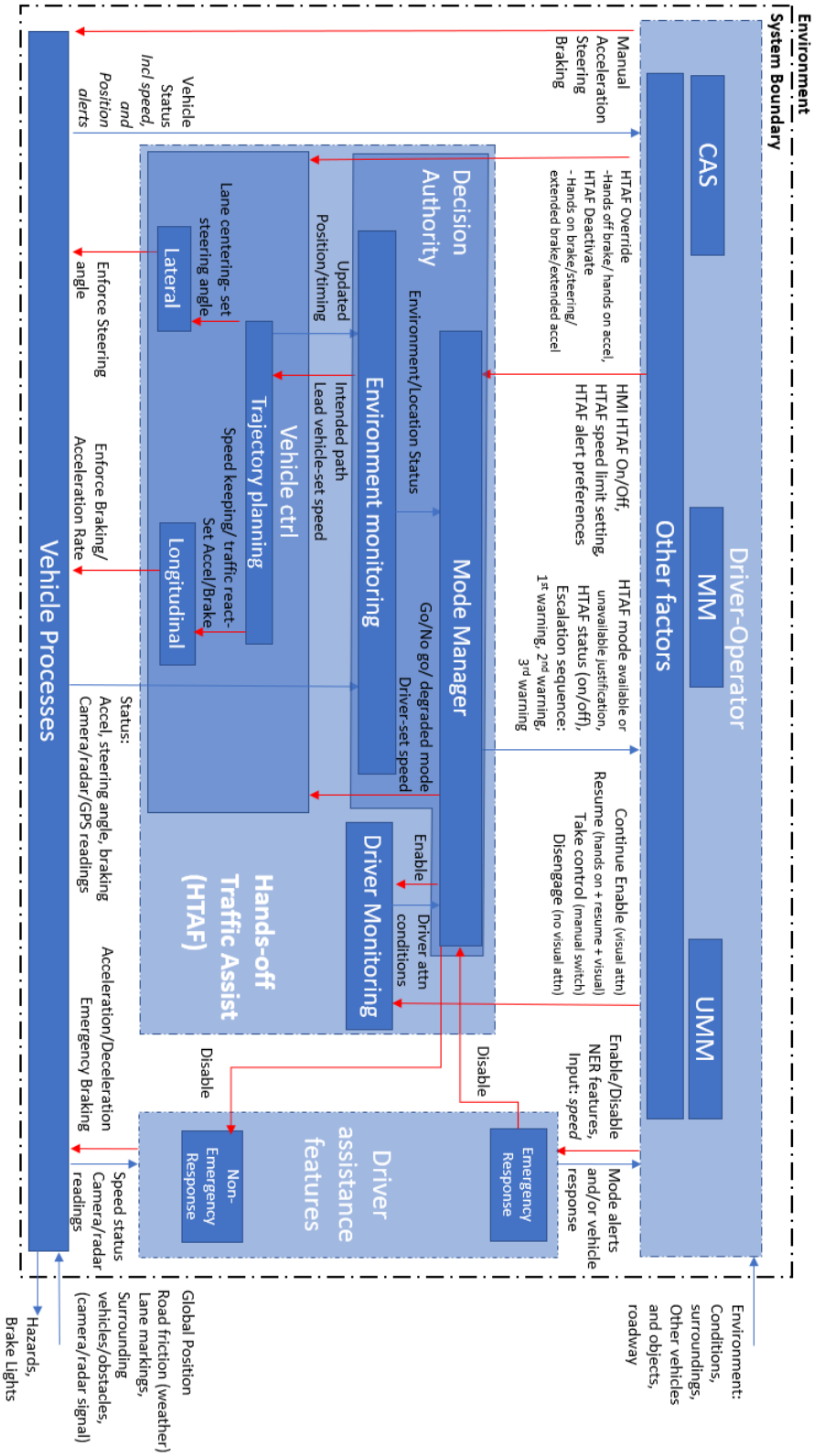

Figure 30: Enlarged Level 3 Control Structure

Appendix D.2: Level 3 UCAs

Note: For this UCA table and all following, Human Controlled Actions are colored in blue, HTAF controlled are colored in grey, and DAF controlled are colored in yellow. Furthermore, these are exploratory draft UCAs produced during the analysis, and not meant to be final UCAs. They are provided in this appendix to help interested readers follow the original thought process as the analysis was conducted.

Table 17: Complete Level 3 UCAs

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Too Early, Too Late, Out of Order	Stopped too Soon, Applied too Long
Acceleration	(UCA-1) Driver does not provide acceleration command to adjust speed when vehicles at rear or side violate minimum distance [H-1, H-2, H-3] (UCA-2) Driver does not provide acceleration command to adjust speed when vehicles at rear or side are on trajectory towards driver's vehicle at speed > driver's [H-1, H-2, H-3] (UCA-3) Driver does not provide acceleration command to maintain speed limit [H-3] (UCA-4) Driver does not provide acceleration command to keep pace with other drivers in traffic [H-3]	(UCA-5) Driver provides acceleration command greater than obstacle in forward path while remaining in lane [H-1, H-2, H-3] (UCA-6) Driver provide acceleration command to move vehicle forward when minimum distance threshold between vehicles is met [H-1, H-2, H-3] (UCA-7) Driver provides excessive acceleration command at rate above legal speed limits [H-3] (UCA-8) Driver provides excessive acceleration command above speed of surrounding cars [H-3] (UCA-9) Driver provides acceleration command that is insufficient to increase speed or maintain safe distance between itself and side/rear obstacles [H-1, H-2]	(UCA-10) Driver provides acceleration command too late after approaching vehicles are travelling at a speed greater than that of the driver [H-1, H-2, H-3] (UCA-11) Driver provides acceleration command too late after approaching vehicles violate minimum distance [H-1, H-2, H-3] (UCA-12) Driver provides acceleration too early before forward path has at least minimum following distance between vehicles/obstacles [H-1, H-2, H-3]	(UCA-13) Driver applies acceleration command duration (foot on gas) too long after vehicle violates forward minimum distance [H-1, H-2, H-3] (UCA-14) Driver stops applying acceleration command too soon before vehicle has increased distance between itself and a rear/side car to avert collision [H-1, H-2, H-3]
Steering	(UCA-15) Driver does not provide steering to change vehicle direction to prevent collision with slowed or stopped obstacles/ vehicles in lane [H-1, H-2, H-3] (UCA-16) Driver does not provide steering to change vehicle direction to prevent collision with obstacles in adjacent lane(s) [H-1, H-2, H-3]	(UCA-19) Driver provides steering to change lanes and moves vehicle onto collision path [H-1, H-2, H-3] (UCA-20) Driver provides steering to change direction when both sides of the vehicle are blocked [H-1, H-2, H-3] (UCA-21) Driver provides steering to cross over solid line lane indicators [H-3]	(UCA-27) Driver provides steering too early, before verifying that new direction will not violate minimum distance between vehicles [H-1, H-2, H-3] (UCA-28) Driver provides steering too early, before evaluating changes to lane markings (type/direction) [H-1, H-2, H-3]	(UCA-30) Driver stops providing steering too soon before vehicle is centered in lane [H-1, H-2, H-3] (UCA-31) Driver stops providing steering too soon before vehicle clears obstacle and is a safe lateral distance

	(UCA-17) Driver does not provide steering to keep vehicle centered between lane markings [H-3] (UCA-18) Driver does not provide steering to change vehicle direction to follow curve of road [H-1, H-2, H-3]	(UCA-22) Driver provides steering to move vehicle outside of lane without signaling to other drivers [H-3] (UCA-23) Driver provides steering to change vehicle direction that violates sign navigation guidance [H-3] (UCA-24) Driver provides steering that violates temporary lane guidance (e.g. construction, accident, lane closure, etc) [H-3] (UCA-25) Driver provides insufficient steering to keep vehicle within lane and/or change vehicle direction from path with obstacle [H-1, H-2, H-3] (UCA-26) Driver provides excessive steering to change vehicle direction into collision path [H-1, H-2, H-3]	(UCA-29) Driver provides steering too late after vehicle is on collision path without sufficient distance to navigate around obstacle [H-1, H-2, H-3]	away [H-1, H-2, H-3] (UCA-32) Driver provides steering too long after curvature of road straightens [H-1, H-2, H-3] (UCA-33) Driver provides steering too long after vehicle enters a lateral collision path and violates safe distance between itself and the obstacle [H-1, H-2, H-3]
Braking	(UCA-34) Driver does not provide braking to slow/stop vehicle when vehicle is on collision path and speed of obstacle ahead is <driver's speed [H-1, H-2, H-3] (UCA-35) Driver does not provide braking to slow/stop vehicle when vehicle merges into driver's lane and violates minimum distance [H-1, H-2, H-3] (UCA-36) Driver does not provide braking to lower speed to limit OR maintain speed [H-3] (UCA-37) Driver does not provide braking to slow vehicle when driving on a curve [H-1, H-2, H-3] (UCA-38) Driver does not provide braking to slow vehicle when	(UCA-40) Driver provides braking action to slow/stop vehicle when vehicle(s) to the rear are travelling faster than driver [H-1, H-2, H-3] (UCA-41) Driver provides braking action to slow/stop vehicle when vehicle(s) to the rear are violating minimum following distance [H-1, H-2, H-3] (UCA-42) Driver provides braking to slow vehicle below set speed limits [H-3] (UCA-43) Driver provides braking to slow vehicle below speed of traffic flow [H-3] (UCA-44) Driver provides insufficient braking to match lead vehicles speed and/or increase distance between vehicles to prevent collision [H-1, H2]	(UCA-45) Driver provides braking action too late after driver's starting speed is greater than lead vehicle's speed to prevent collision [H-1, H-2, H-3] (UCA-46) Driver provides braking action too late to prevent collision after driver has gotten too close to lead vehicle [H-1, H-2, H-3] (UCA-47) Driver provides braking action too early before minimum distance is violated [H-1, H-2, H-3]	(UCA-48) Driver stops providing braking action too soon to adjust speed to <= lead vehicle's speed and prevent collision [H-1, H-2] (UCA-49) Driver stops providing braking action too soon to remain a safe distance away from lead vehicle [H-1, H-2] (UCA-50) Driver provides braking action for too long after collision is avoided and forward path is clear[H-3]

	weather/lighting impairs vision [H-1, H-2, H-3] (UCA-39) Driver does not provide braking when construction or temporary blockage is present [H-1, H-2, H-3]			
Hands off braking (Override)	(UCA-51) Driver does not provide hands off braking to override HTAF when sensors are degraded/ malfunctioning [H-1, H-2, H-3, H-4] (UCA-52) Driver does not provide hands off braking to override HTAF when obstacle enters from side and other control measures are absent [H-1, H-2, H-4]	(UCA-53) Driver provides hands-off braking to override and moves vehicle onto collision path [H-1, H-2, H-3, H-4] (UCA-54) Driver provides hands-off braking to override and maintain safe distance from forward vehicle while torque is applied to the wheel (e.g. clothing, knees, etc.) [H-1, H-2, H-3, H-4] (UCA-55) Driver provides hands-off braking to override while on a curved road [H-1, H-2, H-3, H-4]	(UCA-56) Driver performs hands-off braking to override too late after forward minimum distance is violated [H-1, H-2, H-3, H-4] (UCA-57) Driver provides hands-off braking to override too early before they have monitored environment [H-1, H-2, H-3, H-4]	(UCA-58) Driver continues performing hands-off braking to override too long after override sequence duration is exceeded (resulting in feature deactivation) [H-1, H-2, H-3, H-4] (UCA-59) Driver stops performing hands-off braking to override too soon before safe minimum distance is achieved between vehicles [H-1, H-2, H-3, H-4]
Hands on acceleration (Override)	(UCA-60) Driver does not provide hands on acceleration to override HTAF when following vehicle or side vehicle violates minimum distance between vehicles and other control measures are absent [H-1, H-2, H-4]	(UCA-61) Driver provides hands on acceleration to override when there is a forward obstacle travelling at a slower speed and below a minimum distance [H-1, H-2, H-4] (UCA-62) Driver provides hands on acceleration to override while inadvertently applying torque to steering wheel (resulting in unintended behavior and confusion) [H-4]	(UCA-63) Driver performs hands on acceleration to override too late after rear/side minimum distance is violated [H-1, H-2, H-3, H-4] (UCA-64) Driver provides hands-on acceleration to override before checking lateral vehicles' position [H-1, H-2, H-3]	(UCA-65) Driver continues providing hands on acceleration to override too long after override duration sequence is exceeded [H-1, H-2, H-3, H-4]
Hands on braking (Deactivate)	(UCA-66) Driver does not provide hands on braking to deactivate HTAF when vehicle is on forward or lateral collision path and other	(UCA-68) Driver applies hands on braking that moves vehicle onto collision path (e.g.	(UCA-71) Driver performs hands on braking too late after forward/ lateral minimum distance is violated and other control measures	

	control measures are absent [H-1, H-2, H-3, H-4] (UCA-67) Driver does not provide hands on braking to deactivate HTAF when HTAF is unable to supervise the vehicle effectively [H-1, H-2, H-3, H-4]	rear/side) [H-1, H-2, H-3, H-4] (UCA-69) Driver applies hands on braking to override while inadvertently applying torque to steering wheel (applies hands on instead of hands off braking, resulting in unintended deactivation and confusion) [H-4] (UCA-70) Driver performs hands on braking while something other than hands are applying torque to the steering wheel (e.g. knee or other object) [H-1, H-2, H-3, H-4]	are absent [H-1, H-2, H-3, H-4] (UCA-72) Driver performs hands on braking too early before checking rear environment [H-1, H-2, H-3, H-4] (UCA-73) Driver performs hands on braking out of order, braking before placing hands on wheel [H-1, H-2, H-3, H-4]	
Extended braking (Deactivate)	(UCA-74) Driver does not provide extended braking to deactivate HTAF when vehicle is on forward or lateral collision path and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-75) Driver does not provide extended braking to deactivate HTAF when HTAF is unable to supervise the vehicle effectively [H-1, H-2, H-3, H-4]	(UCA-76) Driver provides extended braking with hands off the wheel to deactivate HTAF while on a curved road [H-1, H-2, H-4] (UCA-77) Driver applies extended braking when steering is better suited to prevent collision [H-1, H-2]	(UCA-78) Driver performs extended braking too late after forward/side minimum safe distance is violated and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-79) Driver performs extended braking to deactivate too early before Driver is ready to take lateral control [H-1, H-2, H-3, H-4]	(UCA-80) Driver stops providing extended braking too soon (TBD duration) before HTAF fully deactivates when HTAF is not able to avoid a collision or other hazard [H-3, H-4] (UCA-81) Driver applies extended braking too long after it's deactivated when there is a rear-end collision danger [H-1, H-2, H-3]
Extended acceleration (Deactivate)	(UCA-82) Driver does not provide extended acceleration to deactivate HTAF when vehicle is not responsive to a rear-approaching or lateral collision path [H-1, H-2, H-3]	(UCA-83) Driver provides extended acceleration with hands off the wheel while on a curved road [H-1, H-2, H-3, H-4] (UCA-84) Driver applies extended acceleration to increase speed when there is a forward obstacle travelling at a slower speed and below a minimum distance [H-1, H-2, H-3, H-4]	(UCA-85) Driver performs extended acceleration to deactivate too late after rear or lateral obstacle violates minimum distance and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-86) Driver performs extended acceleration to deactivate too early before there is sufficient space to	(UCA-87) Driver stops providing acceleration too early before TBD duration triggers change from override to deactivate [H-3, H-4]

			complete command without violating minimum distance [H-1, H-2, H-3, H-4]	
Steering (Deactivate)	(UCA-88) Driver does not provide steering to deactivate HTAF when vehicle is on imminent collision path and other control measures are absent [H-1, H-2, H-3] (UCA-89) Driver does not provide steering to deactivate HTAF when [H-1, H-2] (UCA-90) Driver does not provide steering to deactivate when HTAF does not detect in-lane obstacle and other deactivation cmds are absent [H-1, H-2]	(UCA-91) Driver applies steering torque that inadvertently causes HTAF to deactivate when there is no obstacle (resulting in unintended behavior and confusion) [H-4] (UCA-92) Driver performs steering to deactivate when Driver is not prepared to take longitudinal control [H-1, H-2, H-3, H-4] (UCA-93) Driver performs steering to override, resulting in unintended deactivation and confusion [H-4] (UCA-94) Driver performs steering to deactivate with a steering torque/angle that directs vehicle onto collision path [H-1, H-2]	(UCA-95) Driver performs steering too late after obstacle violates minimum distance and other control measures are absent [H-1, H-2, H-4] (UCA-96) Driver performs steering to deactivate and change direction too early before the new path is clear [H-1, H-2, H-4]	(UCA-97) Driver stops providing steering to deactivate too soon before TBD torque is achieved to transition to manual control when HTAF is unable to navigate the current environment [H-1, H-2, H-3, H-4]
Turn on HTAF	(UCA-98) Driver does not turn on HTAF to transition to automated driving when stopping manual control of direction via steering wheel [H-1, H-2, H-3, H-4] (UCA-99) Driver does not turn on HTAF to transition to automated driving when stopping manual control of speed via gas/brake pedals [H-1, H-2, H-3, H-4]	(UCA-100) Driver turns on HTAF to transition to automated driving while continuing to operate steering [H-1, H-2, H-3, H-4] (UCA-101) Driver turns on HTAF to transition to automated driving while continuing to operate gas/brake [H-1, H-2, H-3, H-4] (UCA-102) Driver turns on HTAF to transition to automated driving while sensors (internal/external) are or become blocked/ non-functional [H-1, H-2, H-3, H-4] (UCA-103) Driver turns on HTAF when not on highway [H-3, H-4] (UCA-104) Driver turns on HTAF when on a road is under construction (changes to lane markings,	(UCA-109) Driver turns on HTAF too late after lead vehicle is providing speed >80kph [H-1, H-2, H-3, H-4] (UCA-110) Driver turns on HTAF too late after driver is <TBD distance from lead vehicle [H-1, H-2, H-4] (UCA-111) Driver turns on HTAF too early before lead vehicle is a safe distance away (TBD) [H-1, H-2, H-4] (UCA-112) Driver turns on HTAF too late after relinquishing steering and/or speed control [H-1, H-2, H-3, H-4]	(UCA-113) Driver stops providing turn on HTAF too soon before (1) following vehicle and/or (2) not applying enough pressure to “on” button when relinquishing lateral and/or longitudinal controls [H-1, H-2, H-3, H-4]

		blocked lanes, etc) [H-3, H-4] (UCA-105) Driver turns on HTAF when on an entry/exit ramp [H-3, H-4] (UCA-106) Driver turns on HTAF where hands free driving is prohibited by law (see local guidance) [H-3] (UCA-107) Driver turns on HTAF when no lead vehicle is present [H-3, H-4] (UCA-108) Driver turns on HTAF when moving >80kph [H-3, H-4]		
Turn off HTAF	(UCA-114) Driver does not turn off HTAF when HTAF is unable to navigate the current environment and other control measures are absent [H-1, H-2, H-3, H-4] (UCA-115) Driver does not turn off HTAF when HTAF is unable to follow traffic laws or traffic patterns [H-3, H-4] (UCA-116) Driver does not turn off HTAF when exiting traffic/highway environment [H-3, H-4]	(UCA-117) Driver turns off HTAF when uncontrolled vehicle trajectory/motion poses an imminent collision danger and manual corrections are not provided (e.g. on a curved road) [H-1, H-2, H-3, H-4] (UCA-118) Driver turns off HTAF inadvertently, resulting in unintended deactivation and confusion [H-4] (UCA-119) Driver turns off HTAF when he/she does not have hands on the wheel and foot over the brake/accelerator pedal [H-1, H-2, H-3, H-4]	(UCA-120) Driver turns off HTAF too early before they are in control of lateral and longitudinal manual driving [H-1, H-2, H-3, H-4] (UCA-121) Driver turns off HTAF too early before there is sufficient space to safely bring vehicle to speed of vehicle/ traffic ahead when taking manual control of vehicle [H-1, H-2, H-3] (UCA-122) Driver turns off HTAF too late after violating minimum distance/speed to avoid collision [H-1, H-2, H-3, H-4] (UCA-123) Driver turns off HTAF too late after speed is too high to prevent collision [H-1, H-2, H-3, H-4]	
Set HTAF speed limit	(UCA-124) Driver does not provide HTAF speed limit setting where lead vehicle's speed is greater than speed limit but less than or equal to 80kph [H-3, H-4] (UCA-125) Driver does not provide HTAF speed	(UCA-126) Driver provides HTAF speed limit setting that is too large for full stop when following vehicle due to vehicle's position/timing [H-1, H-2, H-3, H-4] (UCA-127) Driver provides HTAF speed limit	(UCA-131) Driver sets HTAF speed limit setting (via acceleration/ deceleration) out of order by not releasing pressure to pedals after HTAF is engaged [H-1, H-2, H-3, H-4]	(UCA-135) Driver sets HTAF speed limit but applies gas too long to keep HTAF engaged [H-1, H-2, H-3, H-4]

	limit setting when HTAF is initiated at <min kph, and lead vehicle accelerates over 80kph [H-3, H-4]	setting that is too large for full stop when vehicle merges ahead of driver [H-1, H-2, H-3, H-4] (UCA-128) Driver provides HTAF speed limit setting while driving <min TBD kph or stopped and lead vehicle is present [H-4] (UCA-129) Driver provides HTAF speed limit setting while driving <80 kph and no lead vehicle is present [H-3, H-4] (UCA-130) Driver provides HTAF speed limit setting while driving >80 kph [H-3, H-4]	(UCA-132) Driver sets HTAF speed limit setting out of order by releasing pressure to pedals before HTAF is engaged [H-3, H-4] (UCA-133) Driver tries to increase/decrease HTAF speed limit setting too late after HTAF is engaged [H-1, H-2, H-3, H-4] (UCA-134) Driver provides HTAF speed limit setting too early before operating at (1) a speed that allows enough time for the vehicle to take over control and respond to vehicle ahead, and (2) a position within TBD range (distance from lead vehicle) [H-1, H-2, H-3, H-4]	(UCA-136) Driver sets HTAF speed limit but applies brake too long to keep HTAF engaged [H-1, H-2, H-3, H-4] (UCA-137) Driver sets HTAF speed limit but stops too soon before they reach their desired speed [H-3, H-4]
Set HTAF alert preferences	(UCA-138) Driver does not set alert preferences when they knowingly have limitations in their perception of audio/haptic feedback [H-1, H-2, H-3, H-4] (UCA-139) Driver does not set alert preferences when they unknowingly have limitations in their perception of audio/haptic feedback [H-1, H-2, H-3, H-4] (UCA-140) Driver does not set alert preferences before using HTAF [H-1, H-2, H-3, H-4]	(UCA-141) Driver provides incomplete set alert preferences by (1) selecting the wrong option, (2) not saving their changes while configuring vehicle and they have sensory limitations [H-1, H-2, H-3, H-4]		
Attention-continue enable	(UCA-142) Driver does not provide attention cues to the road ahead for TBD% of use duration and no obstacle is ahead [H-4] (UCA-143) Driver does not provide attention cues to the road ahead for TBD% of use duration and collision is	(UCA-145) The driver provides forward attention cues but vehicle remains on forward collision course [H-1, H-2, H-3, H-4] (UCA-146) Driver provides forward attention cues to engage driver monitoring but does not monitor side/rear [H-1, H-2, H-4]	(UCA-151) Driver provides attention cues too late after violating minimum distance at side/rear [H-1, H-2, H-3, H-4] (UCA-152) Driver provides attention cues too late after sensor(s) did not detect obstacle(s) [H-1, H-2, H-3, H-4]	(UCA-155) Driver stops providing attention cues too soon before vehicle enters collision course (speed/distance) [H-1, H-2, H-4]

	imminent [H-1, H-2, H-3, H-4] (UCA-144) Driver does not provide attention cues in response to HTAF escalation sequence first warning by returning eyes to road ahead [H-1, H-2, H-3, H-4]	(UCA-147) Driver provides insufficient forward attention cues <TBD% of time over duration of HTAF usage to remain alert and keep HTAF engaged [H-1, H-2, H-4] (UCA-148) The driver provides insufficient attention cues to the environment when road conditions/traffic patterns change [H-1, H-2, H-3, H-4] (UCA-149) The driver provides sufficient forward attention cues and vehicle enters collision course with obstacles in adjacent lane(s) or to rear [H-1, H-2, H-3, H-4] (UCA-150) Driver provides attention cues for TBD% of time over duration of HTAF usage but attention is not evenly spaced or in correct direction to be aware of imminent collision [H-1, H-2, H-4]	(UCA-153) Driver provides attention cues too late after vehicle provides alert [H-1, H-2, H-4] (UCA-154) Driver provides attention cues too late to prevent second warning [H-1, H-2, H-4]	
Attention-Resume	(UCA-156) Driver does not provide attention cues to the road ahead for TBD% of use duration, TBD time has elapsed since first warning, and vehicle is not responding to in lane obstacle [H-1, H-2, H-3, H-4] (UCA-157) Driver does not provide attention cues to resume automation control after the second escalation by returning eyes to road ahead, placing hands on steering wheel, and pressing "resume" [H-1, H-2, H-4]	(UCA-158) The driver provides attention cues to resume after second warning but vehicle remains on forward collision course [H-1, H-2, H-3, H-4] (UCA-159) Driver provides attention cues to resume after second warning but does not respond to imminent side/rear collision [H-1, H-2, H-4]	(UCA-160) Driver provides attention cues too late after forward collision is imminent [H-1, H-2, H-3, H-4] (UCA-161) Driver provides attention cues too late after alert to put hands on wheel is provided [H-1, H-2, H-3] (UCA-162) Driver provides resume cue before making sure it is safe leave HTAF in control [H-1, H-2, H-4] (UCA-163) Driver provides attention cues to resume sequence out of order, or missing steps, after the second escalation [H-1, H-2, H-3, H-4] (*see UCA-167*)	(UCA-165) Driver stops providing attention cue sequence too soon before HTAF automation resume occurs [H-1, H-2, H-3, H-4]

			(UCA-164) Driver provides attention cues to resume automation too late after the 3rd escalation is provided [H-1, H-2, H-3, H-4]	
Attention-take control	(UCA-166) Driver does not provide take over vehicle control cues to switch to manual control of vehicle to prevent collision [H-1, H-2, H-4] (UCA-167) Driver does not provide take over vehicle control cues when requested by HTAF or after the 3rd escalation [H-1, H-2, H-3, H-4]	(UCA-168) Driver takes control of vehicle when sensors trigger alerts for false obstacles [H-4] (UCA-169) Driver takes control of vehicle but remains on collision course [H-1, H-2, H-3, H-4] (UCA-170) The driver provides insufficient attention to respond to obstacles detected and undetected by controls [H-1, H-2, H-3, H-4]	(UCA-171) Driver takes control too late after vehicles to rear/adjacent lanes violate minimum distance [H-1, H-2, H-3, H-4] (UCA-172) Driver takes control too late to respond to obstacle sensor did not detect [H-1, H-2, H-3, H-4] (UCA-173) Driver takes control too late after 3rd escalation to have resume HTAF available without vehicle restart or to prevent stop in lane [H-4]	
Attention-Disengage	(UCA-174) Driver provides forward attention cues that does not disengage HTAF when driver is looking forward but mentally or physically unable to monitor vehicle or respond to environment [H-1, H-2, H-4]	(UCA-175) Driver attention cues provided disengages HTAF when vehicles are approaching from rear and there is not adequate space to avoid collision [H-1, H-2, H-3, H-4] (UCA-176) Driver attention cues disengages HTAF when vehicles are approaching from rear and they cannot see the stopped vehicle [H-1, H-2, H-3, H-4] (UCA-177) Driver attention cues disengages HTAF before reaching a safe point to stop by not finishing maneuver (hill, curve) [H-1, H-2, H-3, H-4] (UCA-178) Driver attention cues disengages HTAF and prevents driver from resuming use of HTAF without restarting vehicle [H-4]			
Enable non-emergency	(UCA-179) Driver does not enable DAF to	(UCA-180) Driver enables DAF while eyes are	(UCA-185) Driver enables DAF too early	

driver assist features (DAF)	maintain speed but removes pressure from gas pedal or brake pedal and vehicle violates minimum distance from the side/rear [H-1, H-2, H-3, H-4]	inattentive and hands are not on steering wheel [H-1, H-2, H-3, H-4] (UCA-181) Driver enables DAF while not in appropriate environment (as determined by manufacturer) e.g. used in heavy traffic [H-1, H-2, H-3] (UCA-182) Driver enables DAF while HTAF is enabled and their hands are not at the wheel and/or foot not on gas/brake [H-1, H-2, H-3, H-4] (UCA-183) Driver enables DAF to maintain speed and relinquishes control of steering, and vehicle is directed into collision path with vehicles or obstacles in adjacent lanes [H-1, H-2, H-3, H-4] (UCA-184) Driver enables DAF to maintain speed and moves vehicle onto collision path when following distance is too close, or following speed is too high [H-1, H-2, H-3, H-4]	before they reach their intended speed [H-3, H-4] (UCA-186) Driver enables DAF too late after they take their foot off braking/acceleration and stop maintaining safe following distance [H-3, H-4]	
Disable non-emergency driver assist features (DAF)	(UCA-187) Driver does not disable DAF when there are changes to posted road speed or road conditions that would require frequent changes to vehicle speed to prevent collision [H-1, H-2, H-3, H-4] (UCA-188) Driver does not disable DAF when there are changes to traffic speed or traffic conditions such that the speed is lower than the set DAF speed [H-1, H-2, H-3, H-4] (UCA-189) Driver does not disable DAF via HMI or manual deactivation	(UCA-192) Driver disables DAF when feature is already disabled and HTAF is on, and driver does not have manual speed/steering controls ready to prevent collision [H-1, H-2, H-3, H-4] (UCA-193) Driver provides disable DAF command when driver is not paying attention to road conditions including: road speed, road conditions, traffic speed, traffic conditions, obstacle presence [H-1, H-2, H-3, H-4] (UCA-194) Driver provides disable DAF command when driver does	(UCA-197) Driver disables DAF too late after minimum distance is violated to prevent forward/side collision [H-1, H-2, H-3, H-4] (UCA-198) Driver disables DAF too late after speed increases to above that of the lead vehicle to prevent forward/side collision [H-1, H-2, H-3, H-4] (UCA-199) Driver disables DAF too late after vehicle merges into lane to maintain safe following distance and prevent collision [H-1, H-2, H-3, H-4]	

	(acceleration, braking, steering, as determined by manufacturer) when transitioning to manual driving such that NE DAF resumes after manual control is relinquished [H-1, H-2, H-3, H-4] (UCA-190) Driver does not disable DAF when vehicle does not slow for obstacle in path after minimum distance is violated [H-1, H-2, H-3, H-4] (UCA-191) Driver does not disable DAF when vehicle does not steer from obstacle in path after vehicle does not change speed or preserve minimum distance separation [H-1, H-2, H-3, H-4]	not have hands at wheel [H-1, H-2, H-3, H-4] (UCA-195) Driver provides disable DAF command when driver does not have foot at breaks [H-1, H-2, H-3, H-4] (UCA-196) Driver provides disable DAF command while steering (e.g. merging, on a curved road) [H-1, H-2, H-3, H-4]	(UCA-200) Driver disables DAF too early before foot is on gas/brake [H-1, H-2, H-3, H-4]	
Set DAF speed		(UCA-201) Driver sets excessive speed that is too large for full stop when lead vehicle(s) is stopped [H-1, H-2, H-4] (UCA-202) Driver sets excessive speed that is too large to maintain safe following distance when lead vehicle(s) is travelling at rate < that of driver [H-1, H-2, H-4] (UCA-203) Driver sets speed while in traveling above legal speed limit [H-1, H-2, H-3] (UCA-204) Driver sets speed while in below legal speed limit [H-1, H-2, H-3] (UCA-205) Driver sets speed while vehicle is operating at speeds > (min threshold) kph but less than speed limit moves vehicle to violate forward or rearward minimum following distance [H-1, H-2, H-3, H-4]	(UCA-207) Driver sets speed too late by accelerating to speed or manually inputting speed greater than current speed after DAF is already engaged [H-1, H-2, H-3, H-4] (UCA-208) Driver sets speed too late to move vehicle from collision path by changing set speed while driving [H-1, H-2, H-4] (UCA-209) Driver sets speed too late to a speed less than current speed after speed limit drops or vehicle exits highway [H-3]	

		(UCA-206) Driver sets speed while vehicle is operating at speeds < (min threshold) kph [H-3, H-4]		
MM Enable monitoring	(UCA-210) MM does not enable driver monitoring to provide alerts when driver turns on HTAF and driver is not providing attention unprompted [H-1, H-2, H-3, H-4] (UCA-211) MM does not [resume] enable driver monitoring to provide alerts after manual override is performed [H-1, H-2, H-3, H-4]	(UCA-212) MM enables driver monitoring to provide attention alerts while transitioning to and operating under automated driving but sensor is compromised [H-1, H-2, H-3, H-4] (UCA-213) MM enables driver monitoring while driver is controlling vehicle manually [H-1, H-2, H-3, H-4] (UCA-214) MM enables driver monitoring while driver is using DAF and manual controls [H-1, H-2, H-3, H-4]	(UCA-215) DA enables driver monitoring too late after automation sequence has already begun and does not provide attention alerts [H-1, H-2, H-4] (UCA-216) DA enables driver monitoring too early before automation sequence has begun and provides alerts [H-4]	(UCA-217) DA enables driver monitoring and stops too soon before driver deactivates or turns off HTAF [H-1, H-2, H-3, H-4] (UCA-218) DA enables driver monitoring too long after driver deactivates or turns off HTAF [H-1, H-2, H-3, H-4]
MM Enable VC	(UCA-219) MM does not enable VC while HTAF is on and driver is "hands off eyes on" [H-1, H-2, H-3, H-4] (UCA-220) MM does not enable VC while HTAF is on and driver is "hands off eyes off" [H-1, H-2, H-3, H-4]	(UCA-221) MM enables VC when driver does not turn on HTAF [H-1, H-2, H-3, H-4] (UCA-222) MM enables VC after driver has taken control or vehicle has come to stop after 3rd escalation, before vehicle has been restarted [H-4] (UCA-223) MM enables VC when safety overrides are attempted by driver and/or DAF to maintain safe following distance or speed [H-1, H-2, H-3, H-4] (UCA-224) MM provides insufficient enable vehicle controls intermittently through automation usage [H-1, H-2, H-3, H-4]	(UCA-225) MM provides enable vehicle control too late after HTAF enable was initiated by driver and driver has relinquished manual control of vehicle [H-1, H-2, H-3, H-4]	(UCA-226) MM stops providing enable vehicle control too soon before driver overrides, deactivates, or turns off HTAF [H-1, H-2, H-3, H-4] (UCA-227) MM continues providing enable vehicle control too long after driver deactivates or turns off HTAF, or after DAF overrides automation [H-1, H-2, H-3, H-4]
MM Disable VC	(UCA-228) MM does not temporarily disable VC when HTAF is deactivated through manual override [H-1, H-2, H-3, H-4] (UCA-229) MM does not disable VC when HTAF is deactivated	(UCA-232) MM disables vehicle controls while HTAF is enabled and driver is not physically engaged (hands/foot) [H-1, H-2, H-3, H-4]	(UCA-233) MM provides disable VC too late after minimum distance was violated [H-1, H-2, H-3, H-4] UCA-234) MM provides disable VC too early before driver or DAF	

	through manual deactivate [H-1, H-2, H-3, H-4] (UCA-230) MM does not disable VC when HTAF is deactivated through turn HTAF off [H-1, H-2, H-3, H-4] (UCA-231) HTAF DA does not disable VC when safety (DAF) override occurs [H-1, H-2, H-3, H-4]		take over VC [H-1, H-2, H-3, H-4]	
MM Degrade VC	(UCA-235) MM does not enable degraded VC while HTAF is on and attention was not provided after the 3rd escalation [H-1, H-2, H-3, H-4]	(UCA-236) MM degrades VC when driver attention is sufficient and degradation moves vehicle onto collision path [H-1, H-2, H-3, H-4]	(UCA-237) MM enables degraded VC too early before and/or too late after the 3rd escalation alert [H-1, H-2, H-3, H-4]	
Driver-set speed	(UCA-238) MM does not convey driver's desired max speed to VC when HTAF was enabled at speed over TBD minimum threshold [H-3, H-4]	(UCA-239) MM conveys driver's desired max speed to VC when no lead vehicle is present to regulate speed [H-3, H-4]	(UCA-240) MM conveys driver's desired max speed to VC before driver has achieved desired speed [H-3, H-4]	
Plan intended path	(UCA-241) Environment monitoring (EM) does not plan intended path according to obstacles detected in from the localization module and/or perception module [H-1, H-2, H-4]	(UCA-242) EM plans intended path in response to obstacles from the localization module and/or perception module when sensors are degraded [H-1, H-2, H-4] (UCA-243) EM performs path planning that instructs the vehicle to violate minimum distance [H-1, H-2, H-3, H-4] (UCA-244) EM provides path planning for only lateral or longitudinal control and not both [H-1, H-2, H-3, H-4]	(UCA-245) EM provides path plan too early before updating/ processing environment changes [H-1, H-2, H-3, H-4] (EM-246) EM plans intended path too late to respond to prevent violation of minimum distance [H-1, H-2, H-3, H-4]	
Default set speed (lead vehicle)	(UCA-247) EM does not set default max speed when HTAF is engaged and vehicle is operating at <TBD kph [H-3, H-4]	(UCA-248) EM sets default max speed settings when HTAF was engaged while operating at >TBD kph [H-3, H-4] (UCA-249) EM sets default max speed settings when		

		no lead vehicle is within TBD range [H-4]		
Set Steering angle	(UCA-250) Trajectory planning (TP) does not set a steering angle/torque to direct vehicle out of minimum distance violation [H-1, H-2, H-3, H-4] (UCA-251) TP does not set a steering angle/torque in response to lane markings (pattern/direction) [H-1, H-2, H-3, H-4] (UCA-252) TP does not set a steering angle/torque when driver does not provide lateral control [H-1, H-2, H-3, H-4]	(UCA-253) TP sets steering angle that causes vehicle to violate min distance [H-1, H-2, H-4] (UCA-254) TP sets a steering angle that directs vehicle to turn when obstacles are present on both sides of vehicle [H-1, H-2, H-3, H-4] (UCA-255) HTAF sets a steering angle to direct vehicle to cross over dashed or solid lane markings [H-1, H-2, H-3, H-4] (UCA-256) HTAF sets an excessive/insufficient steering angle to keep vehicle within lane guidance & off collision path [H-1, H-2, H-3, H-4] (UCA-257) HTAF sets steering angle that overrides driver-provided steering angle [H-1, H-2, H-3, H-4]	(UCA-258) TP sets steering angle too soon before sensing/ processing environment [H-1, H-2, H-4] (UCA-259) TP sets steering angle too late after vehicle has violated forward/lateral minimum distance [H-1, H-2, H-3, H-4]	
Set Accel rate	(UCA-260) TP does not set acceleration rate and causes the vehicle to violate minimum distance from the rear or side of vehicle [H-1, H-2, H-3, H-4] (UCA-261) TP does not set acceleration rate when lead vehicle is present and within TBD distance or driving less than 80 kph [H-3, H-4] (UCA-262) TP does not set acceleration rate when lead vehicle is not present and vehicle requests manual takeover [H-1, H-2, H-3, H-4]	(UCA-263) TP sets acceleration rate that is greater than that of the lead vehicle, or provides a correct speed for too long of duration and causes it to violate minimum distance [H-1, H-2, H-3, H-4] (UCA-264) TP sets acceleration rate that is higher than the max provided by the driver or higher than the current lead vehicle's speed OR higher than 80kph (max HTAF) [H-3, H-4] (UCA-265) TP sets acceleration rate that overrides manual longitudinal instruction [H-1, H-2, H-3, H-4]	(UCA-266) TP sets acceleration rate before monitoring environment or before reviewing updates to the environment including introduction of new obstacles or new traffic speed [H-1, H-2, H-3, H-4] (UCA-267) TP sets acceleration too late to prevent collision from rear when rear vehicle's speed is greater than vehicle's and no obstacle is present ahead [H-1, H-2, H-3, H-4]	
Set Brake rate	(UCA-268) TP does not set brake rate when vehicle ahead is	(UCA-271) TP sets brake rate that decelerates the vehicle more rapidly than	(UCA-274) TP sets brake rate too early before vehicle has violated	

	travelling at speed less than that provided by VC [H-1, H-2, H-3, H-4] (UCA-269) TP does not set brake rate when lead vehicle lowers speed or violates minimum distance (exiting lead vehicle or merged vehicle) [H-1, H-2, H-3, H-4] (UCA-270) TP does not set brake rate to enforce max speed when no lead vehicle is present [H-1, H-2, H-3, H-4]	the vehicle behind it or applies braking for incorrect duration and vehicle violates minimum distance separation [H-1, H-2, H-3, H-4] (UCA-272) TP sets brake rate that overrides manual longitudinal instruction [H-1, H-2, H-3, H-4] (UCA-273) TP sets brake rate when there is no obstacle in forward path (OR) response is disproportional (speed/time) to obstacle in path (e.g. should not stop for plastic bag) [H-3, H-4]	minimum distance [H-1, H-2, H-3, H-4] (UCA-275) TP sets brake rate too late to prevent violation of minimum distance to the front or sides of vehicle [H-1, H-2, H-3, H-4] (UCA-276) TP sets brake rate before monitoring environment or before reviewing updates to the environment [H-1, H-2, H-3, H-4]	
Enforce Steering	(UCA-277) Lat ctrl does not enforce steering to move vehicle when obstacles are approaching violation of min distance [H-1, H-2, H-3, H-4] (UCA-278) Lat ctrl does not enforce steering to keep vehicle centered in lane when lane markings are present [H-1, H-2, H-3, H-4]	(UCA-279) Lat ctrl enforces steering in violation of lane markings [H-1, H-2, H-3, H-4] (UCA-280) Lat ctrl enforces steering to move vehicle to violate minimum distance between vehicles or into path of obstacle [H-1, H-2, H-3, H-4] (UCA-281) Lat ctrl enforces excessive/ insufficient steering when there is no guidance (lane markings, etc.) and the driver has not assumed control of the vehicle [H-1, H-2, H-3, H-4]	(UCA-282) Lat ctrl enforces steering too late after vehicle violates minimum distance or after vehicle exits lane [H-1, H-2, H-3, H-4] (UCA-283) VC enforces steering to change vehicle direction too early before receiving instruction from TP sensing/processing to acknowledge changes to vehicle collision imminence [H-1, H-2, H-3, H-4]	(UCA-284) Lat ctrl stops enforcing steering too soon before instruction is completed [H-1, H-2, H-4] (UCA-285) Lat ctrl provides steering too long after instruction is completed and vehicle moves onto [new] violation of minimum distance [H-1, H-2, H-4]
Enforce Braking	(UCA-286) Long ctrl does not enforce braking to slow/stop vehicle when speed exceeds lead vehicle speed or forward minimum distance is violated [H-1, H-2, H-3, H-4]	(UCA-287) Long ctrl enforces braking to slow/stop vehicle when speed is within limits and minimum distance has not been violated [H-1, H-2, H-3, H-4] (UCA-288) Vehicle provides excessive/ insufficient braking (in violation on instruction) to prevent violation of minimum distance [H-1, H-2, H-3, H-4]	(UCA-289) Long ctrl enforces braking too late after vehicle's speed is > lead vehicle or vehicle has violated minimum distance [H-1, H-2, H-3, H-4] (UCA-290) HTAF enforces braking to slow/stop vehicle too early before receiving rate/duration [H-1, H-2, H-3, H-4]	(UCA-291) Long ctrl stops enforcing braking too soon to slow/stop vehicle when vehicle violates forward minimum distance [H-1, H-2, H-3, H-4]
Enforce Acceleration	(UCA-292) Long ctrl does not enforce	(UCA-294) Long ctrl enforces acceleration to	(UCA-296) Long ctrl enforces acceleration too	(UCA-298) HTAF stops

	acceleration to keep vehicle a safe forward distance from rear vehicle [H-1, H-2, H-3, H-4] (UCA-293) Long ctrl does not enforce acceleration to maintain speed set by driver or lead vehicle [H-3, H-4]	increase speed when obstacle/vehicle ahead is at equal or lower speed [H-1, H-2, H-3, H-4] (UCA-295) Long ctrl enforces excessive/ insufficient acceleration in violation of speed/duration set by driver or lead vehicle [H-1, H-2, H-3, H-4]	late after vehicle's distance from rear-approaching vehicle is too small when no obstacle is ahead [H-1, H-2, H-3, H-4] (UCA-297) HTAF enforces acceleration to move vehicle too early before receiving speed and duration of application [H-1, H-2, H-3, H-4]	enforcing acceleration too early when traffic is operating at speed > vehicle's speed [H-1, H-2, H-3, H-4]
Disable NER	(UCA-299) HTAF DA does not disable NER longitudinal controls when HTAF is turned on [H-1, H-2, H-3, H-4]	(UCA-300) HTAF DA disables NER longitudinal controls when HTAF is not turned on and driver is not operating gas/brake [H-1, H-2, H-3, H-4] (UCA-301) HTAF DA disables NER when HTAF is turned on and vehicle speed >80kph [H-1, H-2, H-3, H-4]	(UCA-302) HTAF DA disables NER before engaging its own acceleration/braking to maintain speed and minimum distance spacing [H-1, H-2, H-3, H-4] (UCA-303) HTAF DA disables NER too late after engaging its own acceleration/braking and there are conflicting longitudinal commands [H-1, H-2, H-3, H-4]	
Acceleration	(UCA-304) DAF does not provide acceleration when engaged and performing below the set speed [H-1, H-2, H-3, H-4] (UCA-305) DAF does not provide speed keeping when driver is not attending gas pedal to keep minimum separation [H-1, H-2, H-3, H-4]	(UCA-306) DAF provides acceleration that moves vehicle to violate minimum distance separation when driver does not have hands on/eyes on readiness [H-1, H-2, H-3, H-4] (UCA-307) DAF provides excessive acceleration beyond what is required preserve set speed [H-3, H-4]	(UCA-308) DAF provides acceleration too late after vehicle falls below set speed [H-3, H-4]	(UCA-309) DAF provides acceleration for too long after driver disables feature [H-1, H-2, H-3, H-4] (UCA-310) DAF stops providing acceleration too early before driver disengages feature [H-1, H-2, H-3, H-4]
Deceleration	(UCA-311) DAF does not provide deceleration when engaged and performing above the set speed [H-1, H-2, H-3, H-4] (UCA-312) DAF does not provide speed keeping when driver is not attending brake to	(UCA-313) DAF provides deceleration to keep speed and moves vehicle to violate minimum distance separation when driver does not have hands on/eyes on readiness (e.g. such that the time needed to move foot to brakes is less than the time until	(UCA-315) DAF provides deceleration too late after vehicle operates above set speed [H-3, H-4]	(UCA-316) DAF provides deceleration for too long after driver disables feature [H-1, H-2, H-3, H-4] (UCA-317) DAF stops providing deceleration too

	keep minimum separation [H-1, H-2, H-3, H-4]	collision at current speed) [H-1, H-2, H-3, H-4] (UCA-314) DAF provides excessive/insufficient deceleration beyond what is required preserve set speed [H-3, H-4]		early before driver disengages feature [H-1, H-2, H-3, H-4]
Emergency Braking	(UCA-318) DAF does not provide emergency braking when vehicle is traveling faster than lead vehicle or violates minimum distance [H-1, H-2, H-3, H-4] (UCA-319) DAF does not provide emergency braking to full stop when obstacle ahead is stopped [H-1, H-2, H-3, H-4] (UCA-320) DAF does not provide emergency braking when HTAF and/or driver does not provide sufficient braking control [H-1, H-2, H-3, H-4]	(UCA-321) DAF provides emergency braking when there is no violation of minimum distance, or object is not a threat to vehicle (e.g. plastic bag) [H-1, H-2, H-3, H-4] (UCA-322) DAF provides insufficient emergency braking to slow/stop vehicle to reduce speed or amend violation of minimum distance [H-1, H-2, H-3, H-4] (UCA-323) DAF provides emergency braking when there is not enough distance left for full stop and lateral control would avoid collision [H-1, H-2, H-3, H-4] (UCA-324) DAF provides emergency braking that overrides driver-provided alternate control (steering/acceleration) [H-1, H-2, H-3, H-4]	(UCA-325) DAF provides emergency braking too late to prevent collision when vehicle has violated TBD following distance [H-1, H-2, H-3, H-4] (UCA-326) DAF provides emergency braking to slow/stop vehicle too early before vehicle violates minimum distance [H-1, H-2, H-3, H-4]	(UCA-327) DAF stops providing emergency braking too soon before vehicle reaches same speed as lead vehicle [H-1, H-2, H-3, H-4]
Disable HTAF	(UCA-328) AEB does not disable HTAF when vehicle violates forward minimum AEB response distance TBD [H-1, H-2, H-3, H-4]	(UCA-329) AEB disables HTAF when vehicle violates min AEB distance TBD and does not engage AEB [H-3, H-4] (UCA-330) AEB disables HTAF when there is no violation of minimum distance, or object is not a threat to vehicle [H-3, H-4] (UCA-331) AEB disables HTAF when accident prevention did not require TBD AEB minimum following distance or AEB braking rates [H-4]	(UCA-332) AEB disables HTAF too early before engaging emergency braking [H-1, H-2, H-3, H-4] (UCA-333) AEB disables HTAF too late after engaging its own controls and HTAF is providing conflicting commands (accelerate, steer) [H-1, H-2, H-3, H-4]	

Appendix E: Enlarged Incorrect Upper Level Controller Diagram

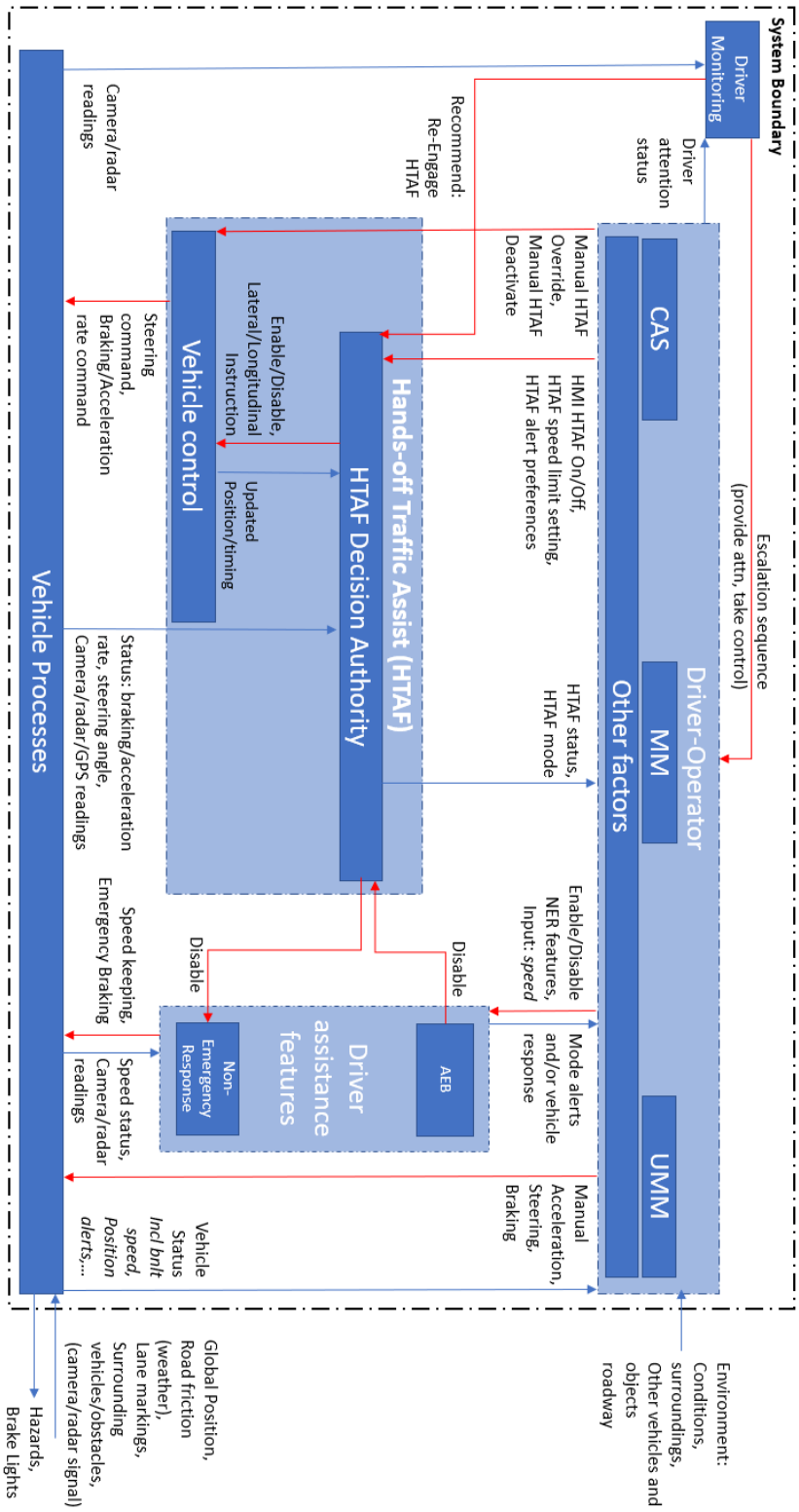

Figure 31: Enlarged Incorrect Upper Level Controller Level 2 Diagram

Appendix F: Enlarged Control Action Refinement Trees

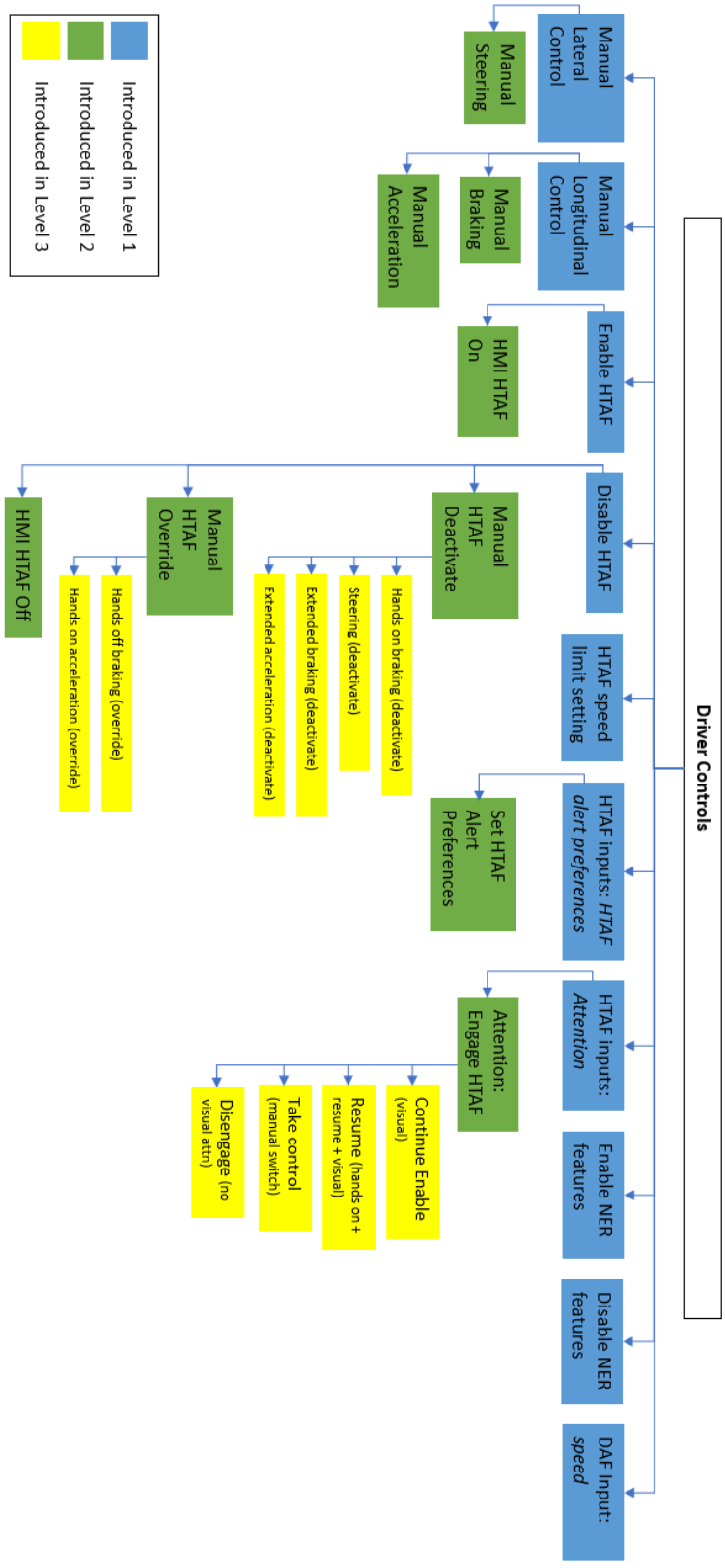

Figure 32: Enlarged Driver Control Action Refinement Tree

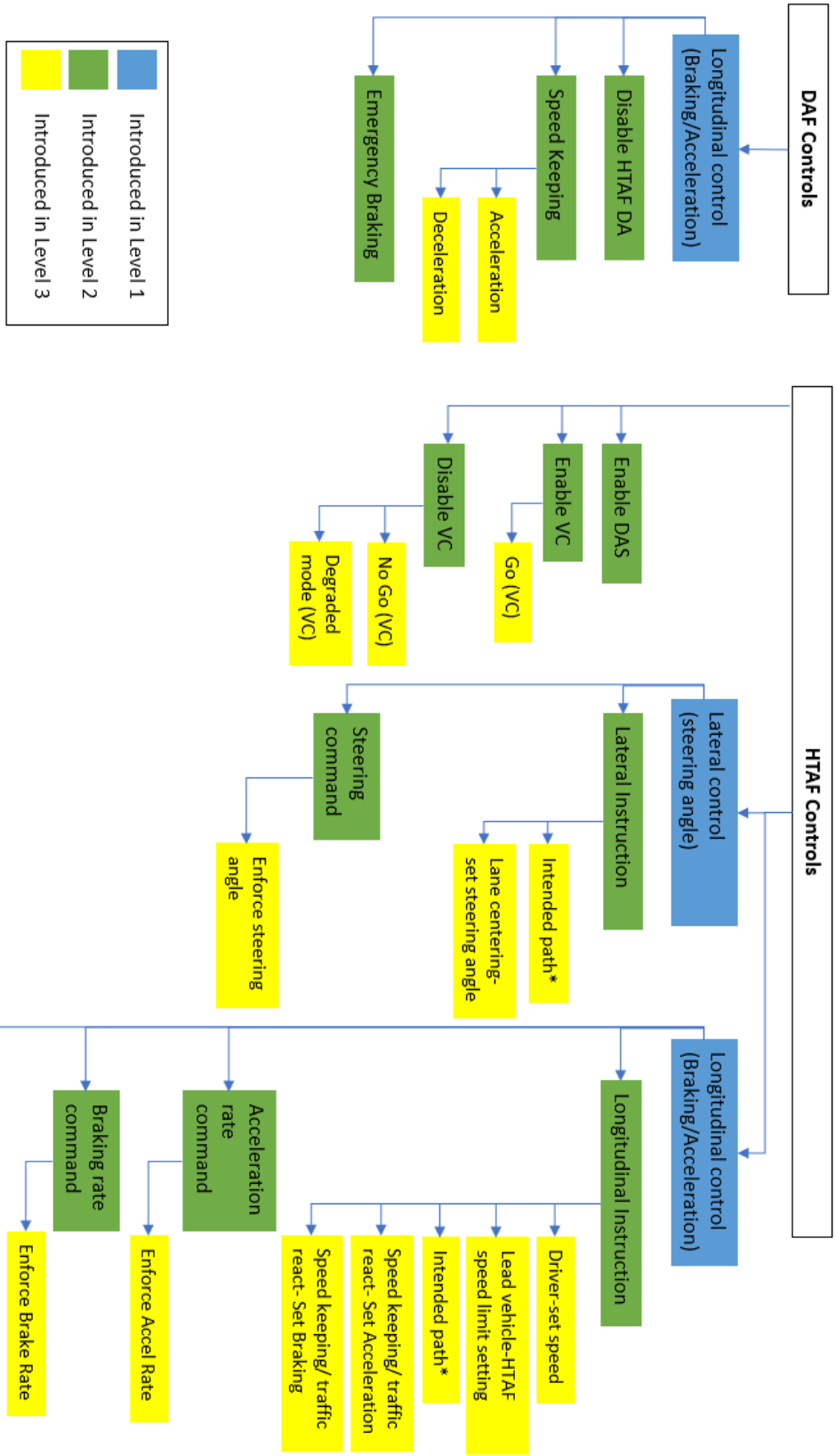

Figure 33: Enlarged Automation Control Action Refinement Tree

Works Cited

[1] Czarnecki, K. "Operational Design Domain for Automated Driving Systems–Taxonomy of Basic Terms." *Waterloo Intelligent Systems Engineering (WISE) Lab, University of Waterloo, Canada* (2018).

[2] Diamond, D.M., Campbell, A.M., Park, C.R., Halonen, J., Zoladz, P.R. "The temporal dynamics model of emotional memory processing: a synthesis on the neurobiological basis of stress-induced amnesia, flashbulb and traumatic memories, and the Yerkes-Dodson law." *Neural Plast.*. 2007. Web. https://pubmed.ncbi.nlm.nih.gov/17641736/

[3] Endsley, Mica R. "Design and evaluation for situation awareness enhancement." *Proceedings of the Human Factors Society*, vol. 32, no. 2, pp. 97-101. Sage CA: Los Angeles, CA: SAGE Publications, 1988.

[4] Forster, Y., Hergeth, S., Naujoks, F., Krems, J., & Keinath, A. (2019). "User Education in Automated Driving: Owner's Manual and Interactive Tutorial Support Mental Model Formation and Human-Automation Interaction." *Information*. 10.4. (2019).

[5] France, Megan E. "Engineering for Humans: A New Extension to STPA." Master's Thesis. Massachusetts Institute of Technology, 2017. Web. Jul 2020.

[6] Furley, Memmert, Daniel. "The role of working memory in sport." *International Review of Sport and Exercise Psychology*. 171-194. Web.

[7] Guszcza, J. & Schwartz, J. "Superminds, not substitutes: Designing human-machine collaboration for a better future of work." *Deloitte Review 27*. July 28, 2020.

[8] Huber, Jeffrey J. "Applying educational psychology in coaching athletes." *Human Kinetics*, 2012.

[9] International Organization for Standardization. (2018). *Electrical and electronic components and general system aspects—Road Vehicles – Functional Safety*. (ISO/FDIS Standard No. 26262).

[10] International Organization for Standardization. (2019). *Road vehicles— Safety of the Intended Functionality*. (ISO/WD Standard No. 21448).

[11] Lee, J.D., See, K.A. (2004). *Trust in Automation: Designing for Appropriate Reliance*. https://pdfs.semanticscholar.org/8525/ef5506ece5b7763e97bfba8d8338043ed81c.pdf

[12] Leveson, N., Pinnel, L. D., Sandys, S. D., Koga, S., & Reese, J. D. "Analyzing software specifications for mode confusion potential." *Proceedings of a workshop on human error and system development*. Glasgow Accident Analysis Group, 1997.

[13] Leveson, N. G., and J. P. Thomas. "STPA Handbook." (2018). https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf . (2019)

[14] McCausland, P. "Self-driving Uber car that hit and killed woman did not recognize that pedestrians jaywalk." *NBC News*. Nov 9, 2019. Web. https://www.nbcnews.com/tech/tech-news/self-driving-uber-car-hit-killed-woman-did-not-recognize-n1079281

[15] Militello, Laura G., and Robert JB Hutton. "Applied cognitive task analysis (ACTA): a practitioner's toolkit for understanding cognitive task demands." *Ergonomics* 41.11 (1998): 1618-1641.

[16] National Transportation Safety Board. "Rear-End Collision Between a Car Operating with Advanced Driver Assistance Systems and a Stationary Fire Truck, Culver City, California, January 22, 2018." *Highway Accident Brief HAB1907*. 2018.

[17] National Transportation Safety Board. "Preliminary Report Released for Crash Involving Pedestrian, Uber Technologies, Inc., Test Vehicle." *NTSB News Release*. May 24 2018. Web. https://www.ntsb.gov/news/press-releases/Pages/NR20180524.aspx

[18] Norman, D. "The Design of Everyday Things." *Basic Books*. 2013.

[19] Oxstrand, J., J. O'Hara, K. L. LeBlanc, A. M. Whaley, J. C. Joe, and H. Medema. "Development of an Initial Model of Human-Automation Collaboration--Results from a Needs Analysis." *SMR/ICHMI/INL/TR-2013/01, INL/EXT-13-28682*. Idaho Falls, ID: Idaho National Laboratory (2013).

[20] Parasuraman, R. & Riley, V.A. "Humans and automation: Use, misuse, disuse, abuse," *Human Factors,* vol. 39, pp. 230–253.

[21] Peters, G.A. & Peters, B.J. "Human Error: Causes and Control." *CRC Press*. 2006.

[22] Proctor, R. & Van Zandt, T. "Human Factors in Simple and Complex Systems." *CRC Press*. 3rd ed. 2018.

[23] Rasmussen, J. "Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models." *IEEE transactions on systems, man, and cybernetics*. (1983). Pp. 257-266.

[24] Reason, J. "Human Error: Models and Management." *BMJ: British Medical Journal*, vol. 320, no. 7237, 2000, pp. 768–770. *JSTOR*.

[25] Reason J. "Human Error." *Cambridge University Press*, 1990.

[26] SAE On-Road Automated Driving Committee. SAE J3016. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. tech. rep., SAE International, 2018.

[27] Stewart, J. "Why Tesla's Autopilot Can't See a Stopped Firetruck." *Wired*. Aug 27 2018. Web. https://www.wired.com/story/tesla-autopilot-why-crash-radar/

[28] Thomas, J. "A New Extension for STPA: Engineering for Humans", MIT Research Lecture, April 2015

[29] Thomas, J., Leveson, N., Ishimama, N. Katahira, M., Hoshino, N., Kakimoto, K. "A Process for STPA: STAMP Accident Model of HITOMI and Expansion to Future Safety Culture", MIT PSAS, 2017

[30] Thomas, J. "Enhancing Human Factors Analysis with STPA", MIT STAMP/STPA Workshop. March 2019.

[31] Thomas, J. "Extending an Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis", Diss. Massachusetts Institute of Technology, 2013. p139

[32] Thomas, J. “Improving STPA Step 2”, 2016. (also from MIT PSAS)

[33] Thomas, J. Personal Communication. May 2020.

[34] Thompson, K. “Google's driverless cars are getting into accidents for an unexpected reason.” *Business Insider*. Sept 2 2015. Web. https://www.businessinsider.com/google-driverless-cars-are-getting-in-accidents-because-of-human-error-2015-9

[35] Wasson, C. S. “System Engineering – Analysis, Design, and Development.” 2nd ed. *Wiley*. 2016.

[36] Wentink, M., Stassen, L., Alwayn, I., Hosman, R., & Stassen, H. “Rasmussen's model of human behavior in laparoscopy training.” *Surgical endoscopy*. 17. 2003. Web.

[37] Ziegler, C. “A Google self-driving car caused a crash for the first time.” *The Verge*. Feb 29 2016. Web. https://www.theverge.com/2016/2/29/11134344/google-self-driving-car-crash-report