Safety Report

OCTOBER 2019

CONTENTS

CONTENTS

CONTENTS

CONTENTS

CONTENTS

List of Tables

List of Figures

1. Scope & Goals

Ike is building an automated trucking solution that will save lives, increase freight productivity, and create new opportunities for local communities. This presents two distinct safety objectives: i) Build safe technologies to enable our commercial product at scale and ii) Maintain an exceptional safety track record throughout development. Both objectives require implementing rigorous processes, safety analysis, verification and validation[1] approaches for deployment in both the near and long term.

This document is part of Ike's system safety analysis of our development system, which encompasses Ike's automated driving technology, the in-vehicle operators, the vehicle platform and the

1. As defined in https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook_0.pdf, pp. 11

supporting ecosystem. To date, we have built an automated system that consists of a Class 8 commercial vehicle upfit with development drive-by-wire actuation systems, pre-production autonomy sensors, and compute elements to enable computer control.

While the focus of this document is on a developmental automation solution that requires human supervision, we believe that many of the methodologies and processes described herein are both extensible to a fully driverless product, and necessary prerequisites to public road deployment of any development platform.

More than a year into development, Ike has not yet operated a vehicle under computer control on public roads. There are three reasons for this. First, our extensive simulation and track testing capabilities have enabled rapid development of automated driving competencies, making public road deployment unnecessary. Second, using public roads as a primary testing environment reduces development speed, increases operational costs, and is fundamentally not scalable for a commercially viable product. Third, deploying to public roads comes with non-zero risk - it exposes other road users and our Vehicle Operators to possible hazards caused by misbehaviors and malfunctions of the Automated Driving System (ADS). Trained Vehicle Operators serve as a partial mitigation to these hazards, but they are imperfect.

We seek to primarily test and prove fundamental behavioral competencies in closed track and simulated environments. The combination of these test environments is referred to as offline testing. This approach has resulted in scalable verification and validation technologies that we actively use to improve our automated driving technology. At the same time, we are developing processes and tools to enable public road testing with the highest degree of safety.

The goal of this document is to share Ike's approach to safe automated class 8 truck development and to garner feedback and input from external stakeholders. We are issuing a safety

assessment prior to public road deployment of an automated system, which we believe to be an industry first. Our belief is that close collaboration on safety between government, commercial partners, safety groups, non-profits, and technology developers will result in the strongest possible safety case for an automated trucking solution at scale while minimizing avoidable incidents along the way. We welcome input and feedback on this document. Comments can be sent to safety@ikerobotics.com.

1.1 Developing a Product Safely

Some of the biggest challenges facing the burgeoning vehicle automation industry are related to ensuring safety during technology development, a phase that lasts years. These challenges include: i) the need to use development hardware that has not been qualified to production levels of assurance, ii) rapidly changing hardware and software configurations, iii) the need to demonstrate interim progress to various external stakeholders, and iv) the need to test on public roads to discover rare events that may uncover shortcomings of the ADS.

Our goal is to contain the risk introduced by these challenges by adhering to a few broad principles:

i. We use hardware (actuators and electronic control units) that are intended for automotive development, relying heavily on partnerships with suppliers with well-established safety records.
ii. We minimize our reliance on public road testing for ADS development, instead investing heavily in offline testing technologies for developer feedback, verification and validation.
iii. We likewise minimize our reliance on public road testing for measuring the types and probabilities of events that we will incur within our Operational Design Domain (ODD), instead relying on other proprietary data sources.

iv. We develop meaningful measures of system maturity that do not rely on demonstrations and other anecdotal representations of progress.

We have an enormous responsibility to employ the highest possible safety standards and strict risk mitigation strategies at every stage of development. We take this responsibility extremely seriously, and it guides all parts of our engineering development activities.

1.2 Developing a Safe Product

Our long-term goal of improving highway safety requires employing robust approaches to safe product development. Although our exposure (measured by the number of miles driven by our fleet) is currently limited, we are developing processes and technologies that can be scaled over time to enable a long-term product.

These areas of safety-driven technologies are among our highest priority areas of development. They include:

i. A requirement management and verification tool that enables nightly evaluation of the entire end-to-end autonomy stack.
ii. A simulation pipeline that enables validating vehicle-level planning and decision-making behavior.
iii. Scalable infrastructure to evaluate system performance across large batches of synthetic and logged test cases.
iv. Onboard hardware and software solutions to improve system reliability and enable robust fault management.

Our goal is to evolve and mature all of these approaches over time as our autonomous capabilities and exposure grow.

1.3 Ike's Approach to Development

We actualize our goals of developing a safe product and developing a product safely by structuring our approach to development around building behavioral competencies that grow in complexity over time. For each behavioral competency, we take a waterfall approach whereby each competency progresses through a series of development steps:

Requirement definition: Vehicle-level requirements to satisfy the behavioral competency are defined.

Development: The behavioral competency is developed alongside appropriate testing capabilities required for verification and validation.

Validation: Once developed and passing unit and regression tests, the competency undergoes a battery of validation testing (detailed in Section 8).

Road release: Once a behavioral competency passes all offline validation tests, it may be approved for road release following Operator re-training and approval from appropriate stakeholders.

One critical aspect of Ike's approach to development is to clearly differentiate between behavioral competencies that are under initial development versus those that have been validated for road release. During public road automated driving, it is critical that operators maintain an accurate mental model[2] of the system limitations. The system limitations evolve as new functions are deployed

2 A mental model refers to the intellectual construct maintained by the operator of the controlled process (in this case, the vehicle). For example, an operator's mental model of the system could include braking distance or the expected response to a cut-in by another actor.

and so must the appropriate operator training. Similarly, Ike will update appropriate external stakeholders on the current deployed behavioral competencies.

1.4 Document Overview

This document is structured as follows: We begin by broadly describing the scope, goals and challenges of the system under development. Next, we describe the major system components and their interaction. Sections 4 - 15 address the Voluntary Safety Self-Assessment elements as defined in *National Highway Traffic Safety Administration (NHTSA) Voluntary Guidance – Automated Driving Systems 2.0: A Vision for Safety*.[3] Particular emphasis is given to the System Safety analysis and Ike's unique verification and validation methodology. Finally, we present current challenges and future work.

3 https://www.nhtsa.gov/automated-driving-systems/voluntary-safety-self-assessment

2. Problem Statement

A safe, automated driving product that does not require human supervision has been an industry goal for over a decade and as of this writing has yet to be realized. Despite this, we believe that improving highway safety by automating long-haul freight transportation is a technical challenge that can be achieved. At the same time, significant challenges remain. Below we broadly outline the primary challenges that our safety approach is intended to address.

2.1 System Complexity

The ADS is a complex combination of sensors, actuators, compute elements, a physical platform, and software. Any of these elements by themselves represent years of diligent engineering and safety analysis, and in combination present even more complexity. Additionally, human-machine interaction, learned (machine learning

and neural network) software techniques, and unconstrained operating environments present significant challenges for system design, validation, and safety assurance of automated driving.

Because of this complexity, our analysis relies heavily on abstraction, which is the standard approach taken in many industries developing highly complex systems. The system as a whole is considered a group of components united by common goals, aligned to our product definition.

Common automotive safety analysis practices are necessary but not sufficient for evaluating the potential hazards and risks to such a system. Similarly, a number of new risk mitigation strategies must be considered, including operational constraints, training, and post-deployment testing.

2.2 Class 8 Trucks

In addition to this system complexity, class 8 trucks introduce unique challenges to automation. The first among them is mass. At highway speed, an 80,000 lb vehicle presents an enormous potential hazard. This necessitates an incredibly high bar for safety, and further underscores the need for extensive analysis and testing prior to public road deployments. There are likewise key differences between passenger vehicles and class 8 trucks that require specific attention and safety analysis for automation. These include pneumatic braking systems, articulated vehicle dynamics, limited baseline driver assist capabilities, highly complex transmission systems, and a large physical footprint.

These challenges and the trucking industry's remarkable safety record notwithstanding, class 8 trucks present the most compelling automation opportunity for safety in the near future.

Driving a truck is a tough job and a tough lifestyle. Truckers spend

many nights away from home,[4] have limited options for healthy food and exercise, and put themselves in harm's way with every mile they drive. Driving a truck is one of the deadliest jobs in the United States.[5] The result is a historic shortage of available truck drivers, high annual turnover,[6] and an aging workforce.[7]

Research has shown that fatigue harms driving reaction times,[8] and that driving performance degrades significantly with each hour behind the wheel.[9] Historically, many drivers are forced to choose between meeting regulatory requirements and making a living wage. Truck accidents often involve slowed reaction times,[10] contributing to the thousands of fatal truck-related accidents that occur every year.

Ike is developing automation technology to directly address these challenges, presenting a compelling opportunity to improve highway safety and truckers' livelihoods.

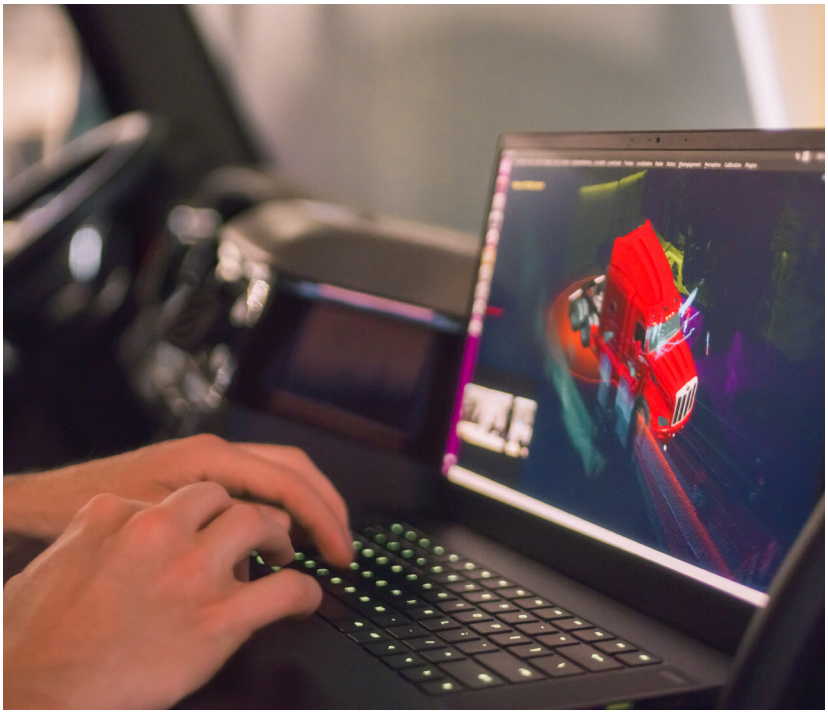
2.3 Exposure & Test Environments

Ike relies on three test environments to validate vehicle-level functionality: public roads, simulation, and closed test tracks. Subsystem and module functionalities also use lab and virtualized environments. Each environment presents specific limitations, safety considerations, and operational challenges. As we will describe in subsequent sections, with clear requirement traceability and function allocation we are able to both reduce our dependence on public road miles and limit the risk of discovering module-level malfunctions during vehicle-level testing.

4 https://www.nytimes.com/2018/08/11/opinion/sunday/the-trouble-with-trucking.html
5 https://www.bls.gov/iif/oshwc/cfoi/cftb0313.htm
6 https://www.ttnews.com/articles/driver-turnover-rises-4-large-truckload-fleets-ata-reports
7 https://www.npr.org/2018/01/09/576752327/trucking-industry-struggles-with-growing-driver-shortage
8 https://www.ncbi.nlm.nih.gov/books/NBK384963/
9 https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/docs/2011_HOS_Final_Rule_RIA.pdf, Figure 4-13
10 https://www.fmcsa.dot.gov/safety/research-and-analysis/large-truck-crash-causation-study-analysis-brief, Table 2

PROBLEM STATEMENT

A persistent challenge to the entire automated vehicle development effort is the necessity to perform some level of testing on public roads. Historically, public road testing has been required in order to capture both the training data and test data to improve automation capabilities. To mitigate the risk associated with deploying development systems on public roads, companies have traditionally relied on trained Vehicle Operators. Even with vigilant Vehicle Operators and well-performing ADSs, there is still inherent risk associated with large public road deployments of test vehicles during development. For this reason, Ike's safety strategy relies on minimizing our public road operational footprint during development. Toward this end, Ike has developed a number of powerful offline validation tools, described further in Section 8.



3. System Description & Control Structure

In this section, we broadly describe the design and the control structure of the system under analysis. We model the system as an assemblage of control elements. We analyze not just the vehicle, sensors, and controllers required for automated driving, but also human elements such as Operators, Fleet Operations (including operator training), and Engineering. This allows us to identify and mitigate losses associated with complex interactions that extend beyond simple component failures. Additionally, we describe safety-relevant contextual factors that span the system as a whole (and do not appear as an explicit control element within the model). This control structure modeling is a key component to the Systems-Theoretic Process Analysis (STPA) that serves as the foundation of our approach to systems safety (described in Section 4).

SYSTEM DESCRIPTION & CONTROL STRUCTURE

The model of the system as a controlled process is a powerful tool for identifying the control actions that may lead to accidents. This also allows us to identify missing control interfaces or feedback loops and establish new processes, sensors, or inspections to ensure adequate control and prevent accidents. An overview diagram of our control structure is provided in Figure 1.

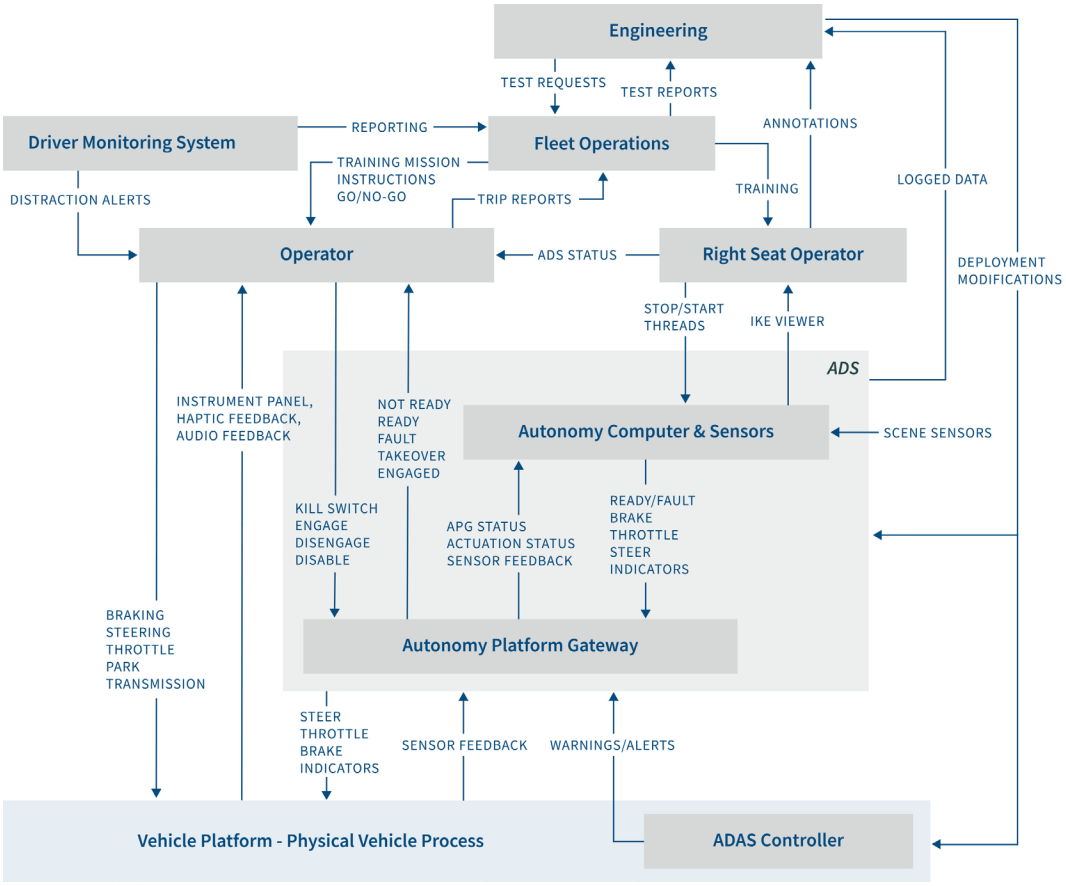


Figure 1: Control structure of the Ike system under analysis. As per STPA, control hierarchy decreases from top to bottom (controllers at the top have the most control authority). Individual control elements are described below.

3.1 Safety Ecosystem

While not explicitly called out in the control structure, all of our system development and engineering occurs within a safety ecosystem. This ecosystem influences day-to-day engineering activities both directly and indirectly. It is critical for building an environment for class-leading safety development.

COMPANY LEADERSHIP

Curating a successful safety ecosystem begins with company leadership. At Ike, prioritizing safety is not only in line with our corporate values but also critical to building a successful product.

We allocate specific requirements to company leadership to foster a robust safety culture. Company leadership is required to directly and indirectly incentivize actions and decision-making that facilitate safety and foster a robust safety culture throughout the company. Examples of Ike's approach to safety leadership include:

i. Rewarding employees for making choices in support of a safe development process (e.g. public recognition of an employee for excellence in safety)
ii. Encouraging transparency and hand-raising for safety concerns through bi-monthly pulse surveys
iii. Frequent leadership-level discussions about practices and blind spots that may add risk to our development process
iv. Scrutinizing development milestones to assure that team goals do not encourage "band-aid" solutions, safety compromises, or bypassing safety processes

Ike's leadership team has broad experience and deep expertise in shipping products in safety-critical industries, and has been exposed to a wide variety of safety cultures in many different industries. Collectively, Ike's engineering leadership team across systems, software, and hardware engineering has decades of

experience working in industries such as aviation, aerospace, medical devices, semiconductors, networking, consumer electronics, passenger automobiles, heavy duty commercial vehicles, and robotics. This provides a strong baseline to build a team culture and a technical development process rooted in safety. We likewise are able to draw from standards, architectures, and best practices across diverse industries to develop novel solutions to address new safety challenges presented by automated driving.

RECRUITING

Ike's approach to building a strong safety ecosystem includes building a team with a firm consensus on the importance of safety. We make a safety mindset an explicit part of the candidate evaluation process. Additionally, we continue to build our team from a diverse set of technical backgrounds in systems safety. We set purposeful hiring goals to continue to increase the diversity of the team's technical background.

SYSTEMS ENGINEERING

Systems engineering is both a centralized and distributed role within our safety ecosystem. Systems engineering performs formal analyses to assess both the safety and the risk of the system as a whole. The systems engineering team is also responsible for generating and collecting verification and validation artifacts for safety mitigations. In addition to this centralized function, every engineer at Ike has a critical role to ensure safety by understanding the context of their work and the potential safety implications of engineering decisions. These responsibilities include peer-review of software and hardware, raising safety concerns, and adhering to best-practice instructions (e.g. safety best practices in the garage bay). We continuously remind and empower engineers to play this critical role by requiring peer-review for software commits, polling engineering for safety concerns, and distributing best-practice instructions.

Poor or non-existent systems engineering analysis can have far-reaching implications for the safety ecosystem. The systems engineering team works to deploy effective analysis by:

i. Attending and hosting workshops in systems safety analysis tools (e.g. STPA)
ii. Employing an analysis and requirement review process that requires at least one approver for requirement changes
iii. Regularly reviewing requirements for both coverage and traceability
iv. Capturing and tracking assumptions that underpin requirements directly in our requirement tracking tool

Similar to company leadership, requirements allocated to systems engineering can be challenging to verify. To help mitigate this, the systems engineering team relies heavily on education, iteration, and peer-review. Peer-review includes expertise both internal and external to Ike.

TOOLS

Tools for analysis, documentation, traceability, and monitoring are key to building a robust safety ecosystem. Here we highlight a few of the tools that Ike has developed to help pave the way for industry-leading approaches to safety.

Requirement Tracking: Requirement tracking is handled by Ike's internally developed requirement tracking tool. While a number of commercial requirement software packages exist, we developed our own tool to enable configurable bindings between requirements and the autonomy software stack. This enables fast and iterative requirement validation. When an existing requirement value is modified and committed (following peer-review), the autonomy software is assessed against this new value automatically in the behavioral evaluation of the system (see Section 8.1). This ensures that the autonomy software and corresponding requirements are evolving in lockstep, preventing developers from

working toward stale or deprecated requirements. It also ensures that the results of testing are always up to date and removes the risk of multiple sources of information for requirements.

When new requirements are introduced to the system, our requirement tracking tool automatically tracks the validation status, highlighting any requirements that are either failing verification, validation or lacking assessment. Our requirement tool also makes use of bindings to our verification and validation software. This makes it possible to specify requirements that apply to individual messages or software modules to ensure a one-to-one correspondence in testing.

Configuration management: Ike employs well-established version control tools for requirements, hardware, and software. When there is a change to the upfit hardware configuration, an Engineering Change Request is created. The change request identifies the rationale for the change, the hardware subsystems affected, and how new and existing requirements will be met. Subsystem designs and installation procedures go through the Hardware Release Process (see Section 8.4) and are verified through analysis or test before approval for vehicle integration. After installation, all potentially impacted subsystems are inspected and tested for proper installation and operation prior to the release of the truck. The hardware subsystem configuration status and resulting approved uses are tracked for all trucks. This process generates an explicit understanding and traceable record of each truck's capability based on its configuration.

Verification and Validation: We have created internal tools for testing, displaying, and tracking the verification and validation status of our system to accompany our internal requirement tracking tool. Our verification and validation software consists of both backend and frontend components. The backend consists of a suite of algorithms that is used to assess whether requirements are being met by the appropriate subsystem (see Section 8.1). The frontend is used to provide a dashboard view showing requirement

pass/fail status for each software release. Additionally, these tools allow for automated detection and reporting of regression, which occurs when a previously passing requirement fails after a new software release.

3.2 Engineering

In the context of the Control Structure of the system (see Figure 1), the engineering team's role is to develop and deploy hardware and software to meet system requirements.

The Control Actions available to Engineering are Deployment (of a new software release or hardware module), Modification (to an existing module on the system), and Test Requests. Additionally, Engineering provides information to Fleet Operations and Vehicle Operators about the current capabilities of the system and any changes made to the system configuration or system behavior.

Of all the control elements contained within the system, Engineering presents one of the highest levels of risk by virtue of having the most control authority over the system. Engineering can make Unsafe Control Actions (UCAs) through poor design, poor execution, or poor engineering judgement that are extremely difficult for downstream processes to mitigate . For this reason, system documentation, traceable engineering decisions, peer-review, and standardized processes are critical to preventing deployments or modifications that can lead to hazards.

One such process is the release of a truck build and software release for use on public roads. Robust release processes are required to assure that released hardware and software adhere to strict safety constraints. These release processes are described in Section 8.4.

3.3 Fleet Operations

The Fleet Operations team is responsible for managing Vehicle Operators, fleet deployment, operator training, and Go/No-Go decisions for test execution. Similar to the Engineering team, Fleet Operations resides near the top of the control structure and plays a critical role in the safe execution of vehicle operations.

Fleet Operations interfaces with Engineering, Vehicle Operators (including Right Seat Operators), and In-Vehicle Monitoring Systems. Control Actions taken by Fleet Operations, such as changing operating procedures or grounding the fleet can serve as powerful Loss Scenario mitigations. To ensure that these mitigations are effective, feedback between the Vehicle Operators, Engineering, and In-Vehicle Monitoring Systems is critical. This allows Fleet Operations to maintain an accurate understanding of how vehicles are being operated in the field.

Fleet Operations interfaces with the Vehicle Operator via Training Modules and Mission Instructions. Training Modules serve to provide context, operational best practices, safety procedures, and inspection instructions to all Vehicle Operators. A full overview of all training modules is included in Appendix C. Fleet Operations also provides Mission Instructions to Vehicle Operators based on the Test Requests received from Engineering and the ODD restrictions imposed on the system. Mission Instructions and corresponding Go/No-Go decisions are critical control actions as they determine whether or not a vehicle is in operation at all. These are described in Section 16.1.

3.4 Operators

We require two operators in the cab of trucks during all development missions that engage the ADS (today on closed tracks, and in the future on public roads). The operator responsible for driving the vehicle is referred to as the Vehicle Operator (or sometimes

simply the Operator). The operator responsible for the management of the Autonomy Computer (described in Sections 3.6 and 6) is referred to as the Right Seat Operator. The roles and responsibilities of each operator are described below.

VEHICLE OPERATORS

The Vehicle Operator is responsible for executing the Dynamic Driving Task (DDT)[11] during manual operation and supervising the vehicle behavior when the vehicle is under computer control. This effectively means the Vehicle Operator acts as a rationality monitor. Vehicle Operators are instructed to reestablish manual control when they believe there is risk that i) vehicle control actions may violate safety constraints or ii) the vehicle may exit the intended operational domain (e.g. weather conditions change).[12]

Operators interface with Fleet Operations, the ADS, the Right Seat Operator, the Vehicle Platform, and the In-Vehicle Monitoring System. A few key interfaces are highlighted below.

Ike development vehicles use In-Vehicle Monitoring Systems (described in Section 3.5). The In-Vehicle Monitoring System plays audio alerts to the Operator when it detects distracted or drowsy driving. These alerts themselves may be distracting, so we tested multiple monitoring systems to find the one with the highest precision and recall.

The Vehicle Operator interfaces with the ADS via the discrete actions and status feedback described in Section 3.6. Conventional class 8 trucks require truck drivers to manage a large number of interfaces and negotiate complex scenarios during the course of a journey. By incorporating additional components onto the vehicle platform, the Operator is tasked with managing even more inter-

11 Defined as per SAE International, J3016 June 2018, pg 6., 3.13.

12 Mental model accuracy and updating beliefs regarding the operation and operating domain of the system is a key challenge for all operators of partially- or fully-automated systems. This is a major analysis topic within our STPA Loss Scenarios.

faces, resulting in a higher baseline cognitive workload. For this reason, minimizing the tasking and eliminating unnecessary alerts to the Vehicle Operator is required to maximize the Operator's efficacy. We designed the interfaces from the ADS to the Operator to be as simple as possible, providing information that may be seen at a glance with unambiguous interpretation. See Section 9 for more details.

Another critical Vehicle Operator interface is to the Vehicle Platform itself. Inputs to the Vehicle Platform are identical to those of a conventional Class 8 tractor as is the feedback from the instrument panel and ADAS system. Ike's integration of the ADS onto the Vehicle Platform in no way modifies or interferes with the standard Vehicle Operator interfaces and by design does not interfere with the ADAS functionality of the stock vehicle. To further reduce the cognitive load on Operators, all vehicles within the Ike fleet are the same model with near-identical control interfaces to the vehicle.

RIGHT SEAT OPERATORS

The primary function of the Right Seat Operator is to manage the Autonomy Computer (described in Sections 3.6 and 6) in order to reduce the cognitive workload of the Vehicle Operator.

The primary interface of the Right Seat Operator is the Ike Viewer. This program runs on a laptop connected to the Autonomy Computer. Data from the Autonomy Computer is streamed to the laptop so that the Right Seat Operator may view sensor data, visualize the planned motion of the vehicle, view perceived and tracked objects in the scene, and view any diagnostic messages that may arise due to warnings or errors from the Autonomy Computer.

During manually driven data-collect missions, the Right Seat Operator starts and stops data logging, creates real time "tags" to denote objects or behaviors of interest (e.g. #motorcycle, #cutin), and monitors the status of autonomy threads that are executing.

In addition to the responsibilities above, during automated driving missions the Right Seat Operator actively monitors the viewer for missed detections, false detections, unsuitable motion plans, and poor data quality. The Right Seat Operator is instructed to call out ADS misbehavior to the Vehicle Operator so the Vehicle Operator can take over driving responsibilities before a hazardous situation emerges. Online monitoring functions can be reliable at detecting and diagnosing component-level issues. Nonetheless, the Right Seat Operator provides an additional means by which misbehaviors of the ADS may be prevented or mitigated.

Control over the Autonomy Platform Gateway (APG, described in Section 3.6) for computer control engagement, disengagement, arming/disarming or activating the kill switch is held by the Vehicle Operator and not the Right Seat Operator. This is enforced through training and best practices.

3.5 In-Vehicle Monitoring Systems

All Ike vehicles are outfitted with off-the-shelf In-Vehicle Monitoring systems that perform several tasks including logging for Federal Motor Carrier Safety Administration (FMCSA) compliance, driver distraction alerts, and video recording of the cabin and region in front of the truck.

FMCSA logging compliance is achieved via the Electronic Logging Device (ELD) and Hours of Service (HOS) features built into the system. The system sends information to the Fleet Operations team about how often the truck is driven and by whom.

Driver distraction alerts are a critical function of the In-Vehicle Monitoring System. Studies suggest that in the absence of a secondary task (e.g. use of a smartphone), Vehicle Operators are equally capable of responding to a critical event whether they are actively

performing the DDT or supervising an automated system.[13] These same studies, however, suggest that incorporating automation may increase the likelihood of engaging in secondary tasks when the operator is not fully engaged in the DDT.[14] Use of the driver distraction alert system increases the likelihood that a Vehicle Operator will be ready to react when an intervention is needed and allows Fleet Operations to audit for Operator distractions.

Video recording of the cabin and region in front of the truck provides a redundant method for reconstructing events, including during non-ADS missions. In the event of an accident or near miss, the video from the In-Vehicle Monitoring System allows Ike to reconstruct the event and understand the situational context. This helps us prevent similar situations from occurring in the future.

3.6 Automated Driving System (ADS)

The ADS is the system responsible for performing the DDT while the vehicle is under computer control. Our current development ADS requires human supervision. The ADS consists of two primary controllers: the Autonomy Platform Gateway and the Autonomy Computer.

AUTONOMY PLATFORM GATEWAY (APG)

The APG serves as a safety gateway between the Autonomy Computer and the Vehicle Platform. It also drives the Human-Machine Interface (HMI) that informs the Vehicle Operator about the state of the system.

We have included the APG in our architecture for several reasons. First, high-performance compute elements required for development that meet the environmental qualifications and redundancies

13 http://eprints.whiterose.ac.uk/86236/1/Highly%20automated%20driving%20secondary%20task%20performance%20and%20driver%20state_final_for%20web.pdf

14 While Vehicle Operators are explicitly prohibited from using smartphones while driving, other secondary tasks may arise during testing.

consistent with automotive standards do not yet exist. Second, modern stock class 8 trucks do not include standard drive-by-wire interfaces, which means some drive-by-wire functionality must exist within the ADS.

The APG consists of two modules: an automotive-grade control module that utilizes a tri-core safety processor as well as an automotive-grade display screen that acts as the HMI to the driver. We note specific interfaces of interest below.

Operator Interface: The APG reports the status of the ADS to the Operator via large simple text, colored screens, and audio cues (see Figure 1). The Operator can issue the following control actions to the APG:

i. Arm/Disarm - A latching switch that acts as a “hard” disable of computer control, preventing unintentional engagement of computer control
ii. Engage/Cancel - A momentary switch that transitions the system between manual and computer control
iii. Kill- A latching mushroom button on the dash that electrically severs power to the APG and prevents any computer control (also called an E-Stop button)

Autonomy Computer Interface: The APG receives READY/FAULT status from the Autonomy Computer and prevents computer control if the Autonomy Computer does not report READY. The APG also receives actuation commands generated by the Autonomy Computer including brake, throttle, steering, and indicator commands. The APG reports the current state of the APG state machine back to the Autonomy Computer along with actuation status and sensor feedback.

Vehicle Platform Interface: The APG issues actuation commands to the Vehicle Platform, including steering, throttle, braking, and indicator commands. The APG receives a number of sensor inputs from the vehicle CAN network, such as wheel speed, brake pressure

and engine RPM (revolutions per minute). These signals are used for various safety protections and driver intervention detections within the APG.

AUTONOMY COMPUTER & SENSORS

The Autonomy Computer, sensors, and software together generate motion control requests to the APG. The Autonomy Computer interfaces with the APG as described in the preceding section. The Autonomy Computer also interfaces with the Right Seat Operator, as described in Section 3.4. Details describing the operation of the Autonomy Computer & Sensors are in Section 6.

3.7 Vehicle Platform

The Vehicle Platform control element represents the class 8 tractor that serves as the actuation platform for the ADS. It is effectively the plant of the controls system. The Vehicle Platform is largely unmodified from a stock class 8 tractor with a few critical exceptions: i) a steering actuator that allows steer-by-wire control, ii) a pneumatic actuator and changes to the truck air system that allows brake-by-wire control, iii) bracketry to accommodate externally and internally mounted ADS components, iv) power systems to support the electrical loads of ADS components, v) splices into the CAN bus to allow communication between the vehicle, the ADS components, and the actuators.[15]

In defining the control structure of the system, we choose to represent the drive-by-wire actuators as part of the Vehicle Platform rather than discrete control structure elements. In the future we anticipate that Tier 1 suppliers will provide drive-by-wire actuation systems that will be installed onto the Vehicle Platform at the factory and will be highly integrated with the rest of the tractor.

15 ADS components are "gatewayed" such that ADS CAN messages are isolated from the rest of the stock vehicle CAN bus, preventing bus corruption and message collisions.

This abstraction also allows us to accommodate future arbitration strategies (for example, steer-by-brake solutions for steering redundancy).

The interfaces to and from the Vehicle Platform are described in Sections 3.4 and 3.6.

DRIVE-BY-WIRE ACTUATORS

Ike vehicles are equipped with drive-by-wire actuators that enable execution of motion commands from the APG while preserving Vehicle Operator control authority. These actuators consist of production-intent hardware, which include firmware that enables drive-by-wire operating modes. The hardware is installed onto the vehicle platform either by the Tier 1 supplier or by Ike technicians according to supplier documentation. After installation, all actuator functionality is tested prior to vehicle release. This includes testing manual control, auxiliary systems, and driver assist (collision mitigation) systems to confirm full functionality.

A principal design requirement for drive-by-wire actuators is that they preserve manual control paths in all operating modes. Below we describe implementation details as to how manual control authority is ensured for each of the primary actuators.

Steering: The steering system detects and responds to steering inputs from the Vehicle Operator and disengages computer control when manual input is detected. Additionally, the APG constantly monitors for manual steering input (through multiple, redundant means) and triggers mode transitions accordingly.

Braking: The brake actuator ensures manual application authority in hardware: pneumatic pressure from manual application via the foot pedal is applied regardless of the operating mode of the actuator, APG, or autonomy computer. Multiple sensors are used to detect inputs via the brake pedal by the APG, providing redundant means for driver intervention detection.

Throttle: Multiple inputs are used to detect manual throttle pedal input, providing redundant means for driver intervention detection. Manual control is restored on detection.

A drawback of the current generation of actuators is that they rely on human intervention as a mitigation for many malfunctions or failures (e.g. power loss). As such, they are not suitable for use for fully driverless applications without additional redundancies and protections.

4. System Safety

Our System Safety approach relies heavily on System-Theoretic Process Analysis (STPA).[16] STPA offers key advantages over other conventional safety analysis techniques that have been applied to the safety analysis of partially- or fully-automated driving systems.[17] These include: i) the ability to analyze both intended and unintended functionality, ii) the ability to consider complex human interactions including Vehicle Operator inattention and engineering decision-making, iii) the ability to identify losses from complex system interactions that may not result from simple component-level failures.

Our application of STPA broadly follows the STPA Handbook,[18] with some customization to Ike's application. Our application of STPA

16 http://sunnyday.mit.edu/safer-world.pdf
17 For example ISO 26262 (https://www.iso.org/standard/68383.html).
18 https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

is still in progress, and we expect it will remain a living analysis throughout our development. While we present a few examples of outputs from our analysis, a full description of the analysis is outside of the scope of this document. For a complete description of the methodology associated with each of these steps, we refer the reader to the STPA Handbook.

4.1 System-Level Losses

We begin by identifying system-level losses (loss of something of value to internal or external stakeholders), which are defined as follows:

ID	Title	Notes
L1	Bodily Harm (injury or death)	Including vehicle occupant, occupants of other vehicles, vulnerable road users, and Ike personnel working on or around the vehicle
L2-1	Property damage	Including road infrastructure, Ike facilities, Ike vehicle, or other vehicles
L2-2	Loss of mission	Including failure to perform the experiment, collect data, etc.
L2-3	Loss of highway utilization	Including traffic jams, slowdowns, or other traffic delays to other road users
L2-4	Loss of critical data	Including data required for motor-carrier compliance, event recorders for accident reconstruction, or other safety compliance data
L2-5	Citation or other legal action from enforcement or regulatory body	Including traffic citations (e.g. for operating a truck with expired plates)

Table 1: Ike's system-level loss definitions. We use "L1" to specify safety-related losses and "L2" to specify business-related losses (property damage, loss of mission, legal action, and etc.). While STPA is a powerful tool for identifying potential causes of loss to business, our primary focus in this document is safety-related (e.g. Level 1) losses.

4.2 System-Level Hazards

Next, we identify system-level hazards, defined as the conditions under which, given worst-case circumstances, a loss is realized. While our long-term product focus is divided interstate highways, in this analysis we include all of the environments in which the vehicle will operate in either manual or computer control. This is critical, as it allows us to consider a much wider range of safety issues that may arise during development than those strictly related to testing the ADS. We believe this comprehensive view is necessary to ensure the highest possible safety bar through all stages of development.

ID	Description	Related Losses
H1	Violation of buffer zone around another vehicle	L1 - Potential bodily harm to ego vehicle occupants or other vehicle occupants
H2	Violation of buffer zone around a vulnerable road user	L1 - Potential bodily harm to vulnerable road user
H3	Violation of buffer zone around stationary object	L1 - Potential bodily harm to vehicle occupants or other road occupants
H4	Debris from vehicle or trailer	L1 - Potential bodily harm to vehicle occupants or other road occupants
H5	Inadequate data capture for event reconstruction	L2-4 Loss of critical data
H6	Violation of traffic laws	L2-5 Citation or legal action from enforcement or regulatory body
H7	Exposure of personnel to potentially harmful effects and/or health hazards (e.g. light, heat, exhaust, FOD, or electricity)	L1 - Bodily harm to Ike personnel

Table 2: Ike's system-level hazard definitions. Hazards describe the conditions in which a loss occurs.

4.3 Unsafe Control Actions

An Unsafe Control Action (UCA) is a term used in STPA to describe a control action that may lead to a hazard (and in turn, a loss) given a set of worst-case circumstances.[19] Significant complexity of this system is due to the multiple systems that have authority to command and execute Control Actions. In order to provide clarity to the control authority (and thus the system state and resulting context), we separately consider UCAs taken by the Operator, the ADS, and the ADAS controller (in the case of braking). As described in the subsequent sections, this designation is particularly powerful in identifying Loss Scenarios, in which mode confusion can result in UCAs.

4.4 Loss Scenarios

Loss Scenarios define causal factors that lead to a UCA.[20] We broadly consider four categories of causal factors, which leverages the STPA approach of modeling the system as a control structure:

i. Controller: Causal factors related to the systems (Operator, ADS, or ADAS) that have control authority to execute the Control Action. (These causal factors may be related to the controller inputs, the controller's internal process model, the algorithm or decision-making behavior of the controller, or the controller's physical hardware.)
ii. Feedback: Causal factors related to the feedback to the controller to confirm that a control action was executed correctly and on time
iii. Actuator: Causal factors related to electromechanical systems (e.g. steering actuator) responsible for converting commands into control actions

19 https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf, pp. 35
20 https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf, pp. 42

iv. Plant: Causal factors related to the physical plant of the controlled system (i.e. the Vehicle Platform)

4.5 Mitigations & Requirement Allocation

For each of the Loss Scenarios identified, we consider potential mitigations to prevent the scenario from occurring and/or mitigating the loss. These mitigations are framed as requirements that are allocated to (and subsequently fulfilled by) vehicle subsystems or connected controllers (e.g. Vehicle Operators, Engineering, or Fleet Operations).

In some cases, we identify the Loss Scenario as Not Applicable or Acceptable, and as such, does not require mitigation. An assessment of non-applicability is generally when a scenario is deemed not possible within our applicable ODD. Critical to this step is to clearly identify any assumptions about our ODD so that these assumptions may be revisited over time. Loss Scenarios identified as Acceptable are usually the result of an assessment that the loss does not require explicit mitigation at our stage of development (e.g. transportation delays).[21]

After any mitigations have been identified, the resulting requirement is allocated to the appropriate control element. These requirements are then migrated to our proprietary requirement tracking tool (see Section 3.1), where implementation of the requirement is tracked.

In this way, STPA acts as a requirement-generation process. It serves as an effective means by which we can analyze the system with a high level of abstraction and consider, with the broadest possible scope, all the ways in which the system may suffer or induce losses. From this high level, we are able to generate detailed

21 We recognize that specifying a Loss Scenario as *Not Applicable* or *Acceptable* presents a risk that an opportunity to prevent that Loss Scenario will be missed. At the same time, imposing constraints and de-prioritizing non-safety-related losses are critical to enabling a tractable analysis.

engineering requirements that trace to vehicle-level losses. This does not result simply from component-level failures, but also from human interactions, system misuse, poor design, or inadequate implementation.

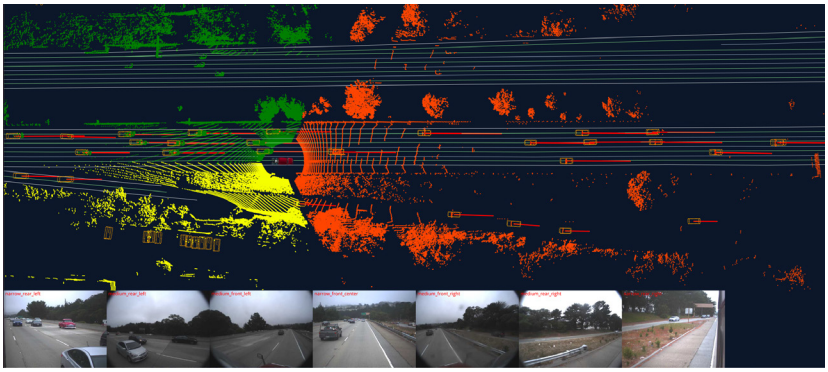
One of the challenges of using any safety analysis process is that there is no explicit way to guarantee completeness of the requirements (complete in the sense that all possible Loss Scenarios have been identified). For this reason, it is critical that STPA is a living analysis, whereby all levels of analysis are continually revisited. The analysis must also be updated when near, partial, or complete losses are incurred. Near losses in particular must be analyzed thoroughly to update the system analysis, thereby preventing partial or complete losses.

4.6 System Safety Analysis Example

The example below illustrates the application of the methodology presented in the previous sections.

Element	Description
System Losses	L1-1: Bodily harm (injury or death) L2-1: Infrastructure damage L2-2: Damage to vehicle
Hazards	H1: Vehicle violates buffer zone around another vehicle H2: Vehicle violates buffer zone around a vulnerable road user H3: Vehicle violates buffer zone around a stationary object H6: Vehicle violates traffic laws
Unsafe Control Action (UCA)	UCA-48: Steering from ADS is applied too long when vehicle is under computer control and performing a steering maneuver (e.g. lane change or lane keeping) with other actors in adjacent lanes and the Vehicle Operator does not disengage computer control
Loss Scenario	LS-379: An APG software release is deployed that disables or otherwise interferes with Vehicle Operator intervention via steering (This could be by, for example, modifying the state machine transition logic or the steering intervention detection logic.)
Mitigation or Requirement	MT-379: All APG software commits impacting state machine transition logic shall undergo peer-review. MT-380: All APG software commits impacting Vehicle Operator intervention shall be track-tested prior to road release. MT-381: The APG release process shall include a hardware-in-the-loop formal software verification routine to determine if the intervention logic has different behavior than the last road-released version and to test whether the intervention logic meets requirements. MT-382: The automated APG initialization procedure shall include a check to assure that steering, braking, and throttle intervention mechanisms are operational prior to enabling computer control.

Table 3: Example of a single end-to-end execution of STPA applied to Ike's development ADS. Mitigations or requirements can be traced back to system-level losses. Ensuring safety equates to ensuring that loss scenarios do not occur.



5. Operational Design Domain (ODD)

During development, Ike defines three different types of ODDs. Multiple ODD definitions are required because different operational restrictions are imposed to enable development. For example, we may need to transport a truck or collect data in regions outside of the approved ODD for the ADS. Our three ODDs are as follows:

- **Manual Control**: ODD for the vehicle to operate under manual control (data collection or transportation)
- **Computer Control on Closed Test Tracks**: ODD for the vehicle to operate under computer control on closed test tracks
- **Computer Control on Public Roads**: ODD for the vehicle to operate under computer control (with human supervision) on public roads with other road users

The detailed description of our ODDs is provided in Appendix B.

6. Object & Event Detection & Response (OEDR)

We present our OEDR capabilities as an abstraction of an underlying architecture whose detailed description is in part described in Section 3. The OEDR capabilities are represented broadly through the common abstraction of Perception, Prediction and Planning, and Actuation.

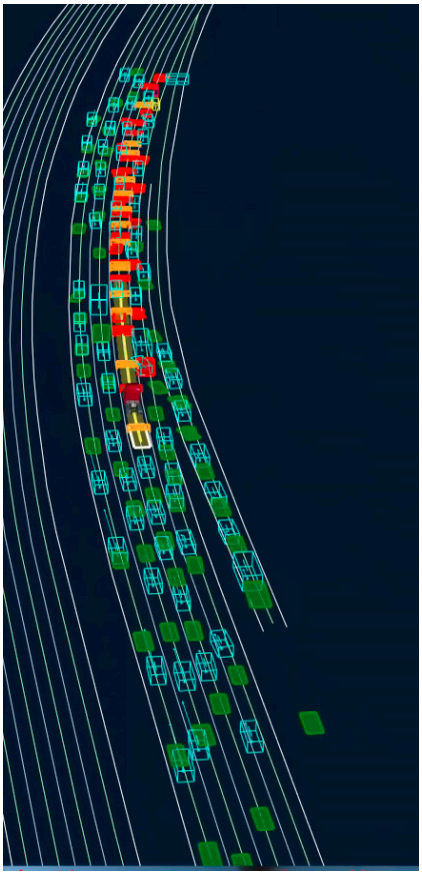
6.1 Perception

Ike's focus on class 8 trucks on highways presents a few key sensing challenges. Long-range detection is required to handle the long braking distances and operating speeds of the vehicle. The tractor and trailer combination presents challenges for blindspot minimization and self-occlusion (where the line of sight to an object is obstructed by the ego vehicle). To address these challenges, we utilize radar, lidar, and cameras with overlapping fields of view. Sensors are integrated into the vehicle fairing to achieve a high vantage point for minimal occlusion in traffic from other actors as well as into the vehicle bumper and side skirts to eliminate blindspots close to the vehicle.

OBJECT & EVENT DETECTION & RESPONSE (OEDR)

Ike's sensor constellation is designed to achieve two development goals. First, we utilize our collected data for model training and offline evaluation. Toward this end, we require multi-modal data to support these data-collection efforts. Second, we utilize our current constellation to perform sensitivity analyses, architecture trade studies, and detection experiments to test hypotheses to validate our fully driverless vehicle architecture. While our current constellation is adequate for our current development goals, we anticipate that future changes to our sensor constellation may be required prior to public road deployment of a driverless system.

Raw sensor data is used by Ike's perception and tracking algorithms to produce objects with associated trajectories and semantic labels. We evaluate these trajectories, predictions and labels via offline testing.



6.2 Prediction & Planning

Given the location and orientation of the ego vehicle, the perceived detected objects and contextual information from the map, we generate predictions for objects in the vicinity of the ego vehicle. These predictions are evaluated offline prior to public road deployment for all software releases.

The motion planner is responsible for generating trajectories based on the predicted objects and the route associated with the specific mission. The motion planner must obey a number of constraints to ensure various Loss Scenarios are prevented. Conformance to these constraints is likewise evaluated during offline testing through a large number of test cases prior to public road deployment.

6.3 Actuation

The trajectory generated by the motion planner is converted to actuation commands, which in turn are passed to the drive-by-wire actuators of the vehicle. In the Ike architecture, there are two controllers. The first is a high-level controller on the Autonomy Computer that is used to generate actuation commands based on the current vehicle state, vehicle position and vehicle orientation. There is an additional lower-level controller residing on the APG that is used to ensure that various dynamic constraints are in place.

A challenge associated with having multiple vehicle controllers on the vehicle is to satisfy seemingly conflicting actuation requirements to address different Loss Scenarios. For instance, we require that sudden, unnecessary hard braking of the vehicle be prevented to reduce the likelihood of a rear-end collision (another actor colliding with the rear of the ego vehicle) or a loss of dynamic stability (trailer jackknife). At the same time, we require that the vehicle applies the necessary braking to avoid forward collisions (which may include hard braking). While there are a number of mitigations in place to reduce false positive detections that would result in unnecessary hard braking, the low-level controller also limits the braking available to the ADS to prevent extreme braking maneuvers. In this way, the likelihood of inducing a rear-end collision is reduced.

While this serves as a mitigation for the rear-end collision Loss Scenario, it increases the likelihood of a front-end collision from under braking. To address this, we additionally require that the ADS alerts the Vehicle Operator when the brake demand from the Autonomy Computer exceeds the limits imposed by the APG. The Vehicle Operator is trained to reestablish manual control via brake application to supplement as needed.

This serves as an example of the type of actuation optimization that we believe is required prior to public road actuation develop-

ment and an instance in which simply ensuring Vehicle Operator control authority is insufficient for preventing Loss Scenarios.

6.4 Assessment, Testing, & Validation of Behavioral Competencies

Ike's approach to Assessment, Testing, and Validation of the behavioral competencies associated with OEDR are described in Section 8. Some of the core behavioral competencies include following other vehicles, reacting to cut-ins by other vehicles, staying in lane, adhering to speed limits, and maintaining buffers around nearby vehicles. While there is still much work to be done to complete our verification and validation in terms of coverage and statistical significance, we do have substantial test coverage of our core behavioral competencies. At the sub-module level, examples of offline testing include perceiving vehicles ahead of and behind the ego vehicle, predicting and planning for the behavior of other vehicles, and localization. Most of these behaviors are tested using logged data simulation and synthetic simulation as described in Section 8.1. These examples are non-exhaustive, and the number of systems and behaviors under test is constantly increasing.

6.5 Crash Avoidance Capability - Hazards

The vast majority of our automated capability requirements are drawn from Loss Scenarios that ultimately trace to crash-related hazards. As such, crash avoidance capabilities are embedded into our requirements for all of our vehicle-level behaviors.

We extensively test two common crash scenarios involving class 8 trucks: stopped or slowed traffic just ahead of the vehicle and sudden cut-ins of other vehicles into the ego vehicle lane. To test vehicle behaviors in these scenarios, fully synthetic simulations can be executed with no risk of injury. Extreme scenarios involving behaviors that are rarely observed on public roads may also be simulated and parametrically varied.

OBJECT & EVENT DETECTION & RESPONSE (OEDR)

Through the process of requirement decomposition and allocation, we can test applicable subsystem requirements that are traced to a vehicle crash avoidance capability without having to test the subsystem requirement in a crash scenario. As an example, braking for stopped vehicles (that may have been previously occluded) requires both detection and prediction of stationary vehicles. We extensively measure stationary vehicle-detection performance by testing perception against manually collected scenes that involve vehicles on the shoulder. These occur frequently in day-to-day driving. As such, we are able to test perception requirements required for crash avoidance without testing in real-world crash scenarios.

As we continue to develop behavioral competencies, crash avoidance will remain central to verification and validation. As noted above, this is due to the fact that these behavioral competencies are developed according to system requirements that are drawn from Loss Scenarios.

7. Fallback (Minimal Risk Condition)

In the current stage of development, the response to ADS malfunction or degraded function is to transition the vehicle to manual control (as opposed to having the system perform an emergency pullover). This requires the Vehicle Operator to respond to a transition to manual control (with accompanying audible/display alerts, and in some instances the system may provide an advance alert for the operator to intervene). While fallback to manual control is not a viable mitigation in a fully driverless architecture, it remains the safest mitigation while emergency pullover capabilities are still under development.

There are several conditions that will result in a fallback to manual control. The detection and response to each of these events may vary. Transitions to manual control may occur via a "hard transition" of an immediate transition with an accompanying alert, or a "soft transition" where a takeover is requested of the Vehicle Operator. Note that while system fault-detection and response capabilities are currently under development, we use the following guidelines to set requirements for vehicle-level responses to fallback scenarios for public road release.[22]

22 Throughout development, our Vehicle Operators are trained to reestablish manual control whenever they deem it necessary. By improving the onboard capability of the system to detect fallback scenarios, we reduce the dependency on the operator.

Fallback Scenario	Detection mechanism	Response
Exit ODD	Operator (e.g. high wind) or ADS (e.g. end of map)	Request takeover or operator takeover
Hard system fault (e.g. loss of power)	ADS/Vehicle Platform monitors	Hard transition to manual
Soft system fault (e.g. message timeout)	ADS algorithms, process monitors	Request takeover
System misbehavior, diagnosed	System (e.g. lane crossing)	Request takeover
System misbehavior, undiagnosed	Operator	Operator takeover
False-positive interventions	Operator	Operator takeover
End of mission	Operator	Operator takeover

Table 4: Summary of Fallback Scenarios and corresponding detections/mitigations currently under development. "Request takeover" indicates that the ADS is responsible for detection and requests that the Vehicle Operator reestablish manual control. "Operator takeover" indicates that the Vehicle Operator is responsible for detection and responds by reestablishing manual control.

7.1 Detecting Fallback Scenarios

The timely detection of conditions that require a fallback response remains an enormous challenge in automated driving technologies. For both near-term and long-term development, computer detection and response to fallback scenarios is preferred over relying on the Vehicle Operator. A necessary prerequisite for fully driverless automated driving is to make the ADS fully capable of self-diagnosis.

During development, the Vehicle Operator plays a crucial role in detecting fallback scenarios for exiting the ODD, undiagnosed system misbehaviors, and false-positive interventions.

FALLBACK (MINIMAL RISK CONDITION)

In the first case, the Vehicle Operator is responsible for judging when environmental conditions have degraded to the point that manual driving is necessary. Fleet Operations is responsible for evaluating if the weather conditions are suitable for executing a mission in the first place. Even so, it is possible for environmental conditions to change rapidly during a mission, which may require a transition to manual control of the vehicle.

In the second case, the Vehicle Operator is responsible for detecting system misbehaviors that are not diagnosed by the onboard system. The primary goal of our offline verification and validation efforts is to minimize the likelihood of these misbehaviors. Similarly, the primary goal of our online monitoring software is to detect degraded system and subsystem performance to minimize undiagnosed misbehaviors.

Finally, in our current stage of development, the Vehicle Operator is responsible for false-positive intervention detection, in which the onboard system detects an intervention from the Vehicle Operator that did not occur. This may be due to an accidental tap of the throttle or a large bump in the road (which may appear as a steering intervention). In such scenarios, the HMI alerts the Vehicle Operator that an intervention has been detected and immediately transitions to manual control. Currently, intervention detectors are tuned to ensure that all true interventions are appropriately detected while accepting some non-zero false intervention rate. While false-positive transitions are not themselves hazardous, they do cause brief gaps between computer and manual control due to the Vehicle Operator's finite response time. To further minimize the associated risk, Ike is developing novel approaches to suppress even the rare false interventions while still ensuring that every true intervention is correctly detected.

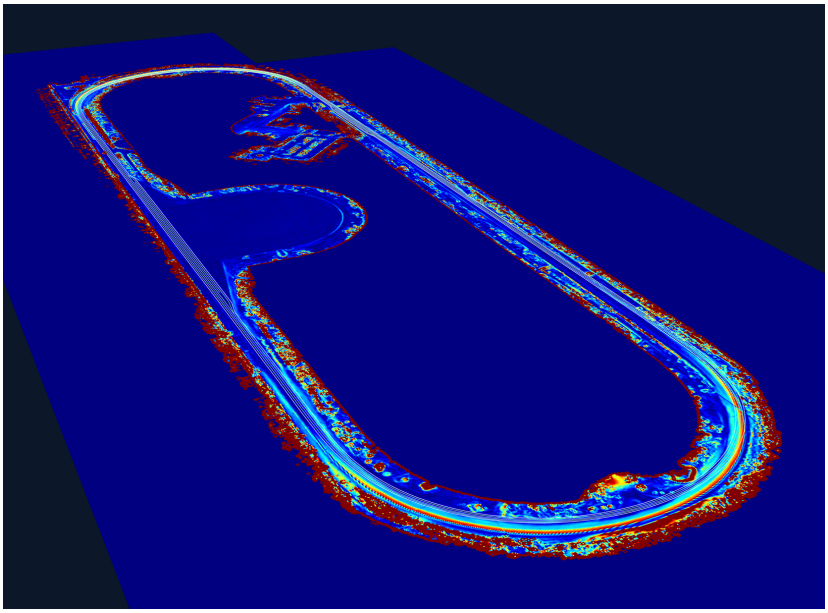
7.2 Responding to Fallback Scenarios

While normally routine and safe, transitions between computer and manual control are not without risk. This is due in part to the fact that the reaction of a Vehicle Operator to a mode transition is not instantaneous. Similarly, there is risk of mode confusion that may result in uncertainty as to the state of the vehicle. To address this risk, our HMI is explicitly designed to minimize mode confusion (described in Section 9). Since risks related to mode transitions remain for any supervised automated system, especially in an emergency situation, requesting an operator takeover is preferred (rather than a hard transition to manual) in all but hard-fault scenarios.

7.3 Assuring Vehicle Operator Control Authority

The development vehicle platform has multiple means by which the Vehicle Operator may reestablish manual control, the most common being braking, steering, and applying throttle. To ensure manual takeovers are correctly detected and result in the proper mode transitions, we have implemented an initialization procedure on the APG for verification.

At key-on and while stationary, the Vehicle Operator is instructed to provide various manual inputs into the system. The initialization routine verifies correct sensor readings and proper transitions between computer and manual control. This initialization procedure protects against a large number of potential issues that may interfere with interventions, including sensor malfunctions, latent hardware faults, and missing or corrupt messages. Only after this initialization procedure has been completed may computer control be engaged. In the event of an initialization failure, the APG latches into a faulted state, preventing computer control prior to the truck leaving the vehicle bay.



8. Validation Methods

Developing robust validation technology and tools is a core part of Ike's development. We believe this is key to successfully developing a scalable automated driving solution. We apply our validation methods to various safety mitigations that address identified Loss Scenarios (see Section 4.4).

Rarely is it the case that mitigations are as simple as component-level redundancy or improved module-level reliability. Instead, successful mitigations may include a wide range of solutions like design optimizations, operational best practices, engineering leadership, code reviews, or build-and-release processes. Employing a diverse set of mitigations encourages more robust coverage of our losses and focuses our technology development on scalable safety solutions.

Similar to a diverse set of mitigation strategies, we likewise employ a number of verification and validation methods to assure that requirements are valid and satisfied. We use verification and vali-

dation method definitions of Test, Analysis, Inspection and Demonstration as defined in the NASA Systems Engineering Handbook.[23]

While the complete list of all possible Loss Scenarios (and their corresponding mitigation) is beyond the scope of this document, we can broadly categorize Loss Scenarios according to the method that is used to verify that the requirement has been met and validate the efficacy of the mitigation:

- **Behavioral Competencies:** Requirements that are satisfied at the system level via statistically significant empirical tests
- **Operations/Process:** Requirements that may be satisfied via training, best practices, or following prescribed processes
- **Hardware Module:** Requirements that are satisfied by discrete, standalone hardware modules and validated via component-level test
- **Software Module:** Requirements that are satisfied by discrete, standalone software modules and validated via deterministic evaluation of outputs from prescribed inputs or by regression tests that measure module-level performance

8.1 Behavioral Competencies

Assessing the behavioral competencies and system capabilities of the ADS is critical for both long-term product deployment and near-term development. This is especially true for class 8 trucks operating at highway speed. We believe that ensuring the Vehicle Operator's ability to reestablish control of the vehicle is necessary but not sufficient for road release of the system even during development. Instead, ADS capabilities must be thoroughly tested prior to every public road release to ensure a high degree of behavioral competency. This reduces the burden on operators to monitor for

23 https://www.nasa.gov/sites/default/files/atoms/files/nasa_systems_engineering_handbook_0.pdf pp. 93

behavioral shortcomings and reduces the likelihood of ADS-related Loss Scenarios.

Unlike software and hardware module verification and validation described elsewhere in this section, it is often infeasible to verify system behaviors with unit tests, regression tests, corner case scenarios, or formal software verification methods. The system is complex, interacts with its environment, and includes modules that rely on classical machine learning and deep neural networks. Formal software verification techniques that utilize a discrete set of inputs to verify a known set of acceptable outputs are untenable for learned algorithms, though new verification methodologies are an area of active research.[24, 25]

Gauntlet testing (an "obstacle course" that tests discretized capability) or rare-event testing is likewise insufficient to verify and validate system capabilities. Automated driving behaviors may be easily tuned to pass these scenarios but fail even with small changes to the test design, the environmental conditions, or the test execution. Practically speaking, the breadth of such gauntlet tests is extremely limited since they must be performed at a private test facility and require significant time to set up and execute.

We rely on empirical validation of our system behaviors over a statistically significant suite of test cases that span the parameter space of our ODD. The required statistical significance required for each system behavior is dependent on a number of factors including: i) the test environment, ii) the exposure of the overall fleet, determined by the number of vehicles and the number of miles driven, iii) the frequency of the conditions in which a particular system behavior may be demanded (e.g. debris on the road) and finally, iv) the ability of the Vehicle Operator to mitigate a system behavior shortcoming.

24 https://arxiv.org/pdf/1702.01135.pdf
25 https://arxiv.org/pdf/1803.06567.pdf

VALIDATION METHODS

Below is an example of how verification and validation of behavioral competencies are used to assure that mitigations are in place to address Loss Scenarios.

UCA	Loss Scenario	Mitigation (Requirement)	Verification/ Validation
Braking from ADS is too late after an imminent collision with a vehicle or object ahead has become unavoidable.	ADS does not maintain appropriate headway distance. This would introduce risk that an imminent collision with a vehicle ahead would be unavoidable in a hard braking or suddenly revealed stopped-vehicle scenario, requiring intervention from the Vehicle Operator that is not satisfied.	The ADS shall preserve a velocity-dependent distance to vehicles ahead, where the headway distance accounts for the potential deceleration of the ego vehicle, the vehicle ahead, and relevant system latencies.	Synthetic and logged data simulation. Synthetic scenarios and manually collected data are run against the latest autonomy software release; any instances of prolonged headway violations are flagged as failures.
		The ADS shall restore appropriate headway distance in the event of a cut-in.	Synthetic and logged data simulation. Logged data containing instances of vehicle cut-ins are run against the latest autonomy software release. Any instances in which the ADS does not restore headway distance in the prescribed amount of time are flagged as failures.

Table 5: A UCA line item taken from Ike's STPA related to late braking as an example of how ADS behavioral competencies are critical mitigations for Loss Scenarios (even with a Vehicle Operator). Synthetic and logged data simulations, spanning many test instances, are used to assess behavioral competencies before each road release.

VALIDATION METHODS

Ike is actively using and developing three primary methods to make empirical validation possible at scale: requirement decomposition, simulation, and structured track testing.

REQUIREMENT DECOMPOSITION & ALLOCATION

Requirement decomposition and allocation is the process by which we trace how various modules on the vehicle contribute to emergent vehicle-level behaviors. Decomposed requirements may be validated at the module level, reducing the test burden after system integration. This is critical for reducing the dependency on real-world closed-loop testing.

This approach to requirement decomposition is accompanied by a general philosophy that we only utilize full system tests for validating vehicle-level requirements. Using full system tests to discover module-level issues is both inefficient and unscalable. As a simple example, virtually all onboard hardware requires verification that durability requirements (e.g. shock, vibration, temperature, etc) are met. This can be performed efficiently through accelerated life testing in test labs rather than on-vehicle. As a less trivial example, localization accuracy may be verified entirely using manually driven data so long as regions driven manually fully cover all regions that may be driven autonomously. We therefore do not use automated driving on public roads to test our localization solution. This is efficient, reduces the risk of an accident, and scales by enabling new software releases to be tested without driving millions of new miles.

SIMULATION

Simulation has been a central part of Ike's technology development efforts since the founding of the company. Because the required statistical significance for road release of system behaviors demands thousands of test cases, simulation is required both for scalability and rapid iteration. Our simulation tools are architected to address exactly this need.

VALIDATION METHODS

Synthetic Simulations are virtual scenarios that may be either designed from scratch in our scenario editor or automatically extracted from recorded data. Once created, they may be parameterized and varied to create unique scenes. These have the advantage of scalability: infinite combinations of road geometry, initial conditions, and actor behaviors may be explored. Nonetheless, these simulations lack the fidelity necessary to validate some sub-system requirements, especially camera-based perception and non-linear dynamics in the plant model.

Logged data simulations (colloquially referred to as "LogSims") utilize previously collected data, which is then "replayed" against the latest software release. These LogSims are inherently open-loop, which make them unsuitable for validating closed-loop functions (e.g. control algorithms). They are, however, a powerful tool for validating vehicle-level world modeling, perception, tracking, and decision making. Leveraging previously logged data to test new software releases effectively means that our data collection efforts are cumulative over time.

The simulation tools we use are wholly developed and owned by Ike rather than third parties. This has several advantages. For one, it allows us to easily keep our tools up to date as we improve our onboard software and offboard infrastructure. It also allows us to quickly iterate on improvements to the fidelity of the simulation that increase the correlation between test results in simulation and reality.

Ike operates manually driven vehicles on public roads at a regular cadence for data collection. We are able to collect large volumes of relevant scenes to be used in validation while still maintaining a small operational footprint. Relevant scenes are cut from vehicle logs using human annotations from the Right Seat Operator or from algorithms that identify actor behaviors, environmental conditions, or events of interest. These "Scenes" are then added to our Scene Database and used for LogSim. The pipeline of scene collection to offline validation is displayed in Figure 2.

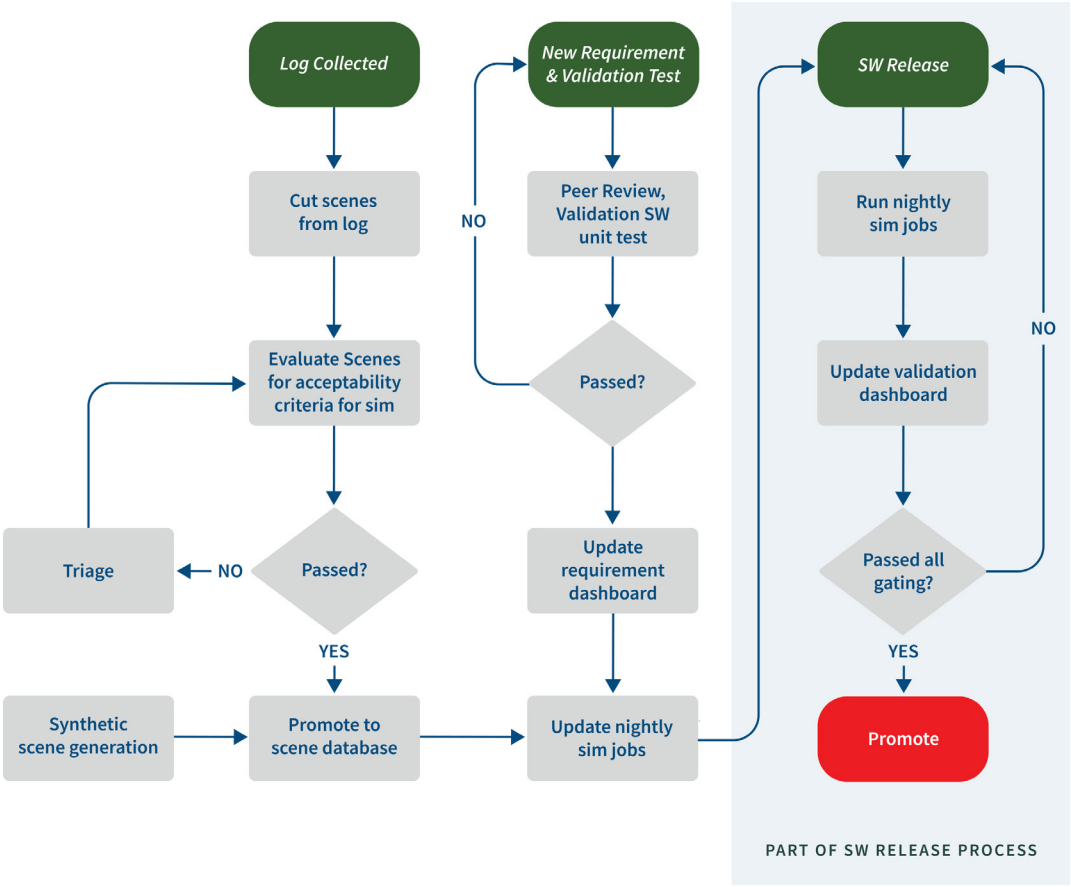


Figure 2: Overview of Ike's validation workflow. Real-world data collected on Ike trucks are passed through an automated processing pipeline where scenes of interest are cut from the log. These are evaluated for acceptability for sim (the open-loop nature of LogSim means some scenes will not work in simulation) and then promoted to a Scene Database which also contains synthetically generated scenes. New requirements and associated verification test software that have passed through the review process are promoted to the requirement dashboard. The nightly sim job list (executed in a containerized cloud framework) is updated to include new scenes and requirement validation routines. After execution, results are aggregated and published on the Ike Validation Dashboard. Sometimes, we find a requirement to be invalid, which creates a feedback loop to the Systems Team to update the requirement. Other times, requirements are not met, which results in rejecting the candidate software release. Only when all vehicle-level requirements[26] are satisfied is the release promoted to Candidate Release.

26 Some subsystem/module requirement failures are non-blocking for road release. As an example, requirements exist for detecting and correctly classifying objects of various types in the scene. Not every requirement violation (missed detection) results in a Loss Scenario. As such, a subsystem requirement may fail for a particular scene, but the vehicle-level safety constraint is still satisfied. In most cases, this is an indication that the requirement decomposition requires further development.

STRUCTURED TRACK TESTING

Test tracks enable closed-loop development in a constrained environment and structured testing to prescribed scenarios. A challenge in this test environment is scalability - each test variation must be manually configured via the placement of actors, signage, and etc. Additionally, the test track environment severely restricts the variety of vehicles, actor behaviors, road geometries, road surfaces, and environmental factors to which the system under test is exposed. Despite these restrictions, closed tracks are a critical test environment. To make them more efficient and repeatable, structured track tests may be combined with virtual simulation.

TEST COVERAGE

Ensuring that our offline validation suite spans our ODD is a highly complex problem and an active area of research at Ike. There are several key considerations. First, the parameterization of a particular scene or scenario is non-obvious in many cases. Some parameters, such as ambient light conditions, road geometry, and geographic location may be readily measured and correlated to system-level behavioral metrics. Other factors, such as the behavior of other actors on the roadway, are both difficult to parameterize and difficult to correlate to system-level behavioral metrics. We believe that as we grow our test scenario suite through manually driven data collection, structured track testing, and simulation we will be able to improve our understanding of this key aspect of our validation test suite.

8.2 Hardware Modules

Discrete hardware failures of a controller, a sensor used for feedback, an actuator, or in the plant itself can give rise to Loss Scenarios. Tracing hardware failures to system-level Loss Scenarios is a well-understood process that has been a major focus of automotive safety engineering for decades. Ike employs many of the

same verification and validation techniques commonly employed within automotive engineering; a non-exhaustive list includes testing via Hardware-in-the-Loop (HIL) and a structured design review and release process. Ike's hardware verification and validation process will change as hardware capabilities are added.

While hardware malfunctions or misbehaviors that directly impact the performance of the system remain a critical focus of our technology development efforts, many other safety risks arise during engineering development. These include injury to engineering personnel by unsecured components within the cab, electrical fires due to improperly fused components, or Foreign Object Debris (FOD) from improperly secured components on the exterior of the vehicle. Addressing even these basic safety risks with a high degree of engineering rigor is critical to our goal of excelling in safety during all stages of development.

An example of our approach to mitigation and validation is shown below. Here, we consider a Loss Scenario caused by a hardware malfunction of the HMI.

UCA	Loss Scenario	Mitigation (Requirement)	Verification/ Validation
Braking from ADS is not provided when a forward collision is imminent.	Human-Machine Interface (screen that displays the state of autonomy control to the Vehicle Operator) becomes unresponsive and hangs, potentially displaying incorrect state to Vehicle Operator. Vehicle Operators lacks feedback on the state of computer/manual control of the vehicle platform and does not supplement control inputs after a manual control transition. This leads to missing braking.	The APG shall monitor the HMI display for message counters, checksums, and screen state, and shall raise a latching fault (and a corresponding transition to manual control) in the event of a timeout, counter error, checksum failure, or commanded/reported screen state mismatch.	HIL - counter error, checksum, error, screen state mismatch, timeout. Observe correct behavior on APG.
		The APG shall utilize an audio alert module independent of the HMI screen control.	Design requirement validated via inspection
		The APG audio alert shall utilize a unique repeated tone sequence in the event that the APG transitions to a faulted state.	Demonstration - part of initialization sequence

Table 6: Illustrative example extracted from Ike's STPA of how UCAs may be addressed via requirements allocated to hardware modules. Verification of these requirements is achieved through a combination of analysis, demonstration, and test.

8.3 Software Modules

As with discrete hardware failures, discrete software failures can give rise to Loss Scenarios that may have severe safety implications. There is often confusion about what constitutes software module versus behavioral verification or validation. We use vastly different testing for each. Behavioral capabilities are validated through statistically significant empirical testing described above, which relies on execution of tests on representative hardware in a representative test environment (i.e. a high level of integration). Software module assessment, on the other hand, may be executed with a high degree of independence of other system components, (e.g. on a development computer or virtualized container).

VALIDATION METHODS

Software module verification may be asserted after a single successful test when the number and range of inputs and outputs is known.

For software module development, we rely on well-established means to gate releases. This includes unit testing, peer-review of code, regression tests, and Hardware-in-the-Loop testing.

In the example below, we consider two mitigations to address the same Loss Scenario. The implementation of the first mitigation is allocated to a discrete software module and the required output may be verified in a single test that does not require the full vehicle. The second implementation is via an ADS behavior; the full integrated vehicle with representative sensing, maps, vehicle dynamics, and environmental interactions is needed to verify and validate the requirement.

UCA	Loss Scenario	Mitigation (Requirement)	Verification/ Validation
Excessive steer - ADS: Excessive steering from ADS is provided when vehicle is in either computer or manual control and there are other vehicles/VRUs present in adjacent lanes.	Localization error results in vehicle sensing that it is not centered in lane, resulting in corrective steering that causes a lane change/vehicle buffer zone violation.	The Autonomy Computer shall monitor the localization solution covariance and trigger an autonomy disengagement or takeover in the event of the lateral localization error growing to exceed 0.3 m.	Unit test: demonstrate that when localization covariance exceeds threshold, the APG interface module is observed to broadcast the appropriate disengagement/takeover message to the APG.
		The ADS shall achieve a localization lateral standard deviation of 0.05 m and a longitudinal standard deviation of 0.5 m in all lanes on all routes within the ODD.	Empirical test: Reprocess previously logged data and demonstrate across the entirety of our ODD that the localization error is within specified bounds.

Table 7: A UCA line item from Ike's STPA that is used to illustrate the different roles of unit testing and empirical testing. Generally, unit tests are used to confirm that outputs are achieved when specific input conditions are met. Empirical tests instead test many instances of the software running against both real and synthetic data to confirm that statistical variations are within acceptable bounds.

8.4 Operations & Process

Operations and Process includes operational policies and best practices for vehicle deployment and day-to-day driving. Operations and Process can be powerful mitigations as the associated control elements have enormous control authority. For example, Operations and Process can prevent Loss Scenarios by determining whether the vehicle should even be on the road. While they can be powerful, assuring that human-dependent processes are executed properly can be a challenge. Processes may not be followed to the letter and best practices may be forgotten or skipped. To mitigate these risks, Ike implements a variety of workflows, training, and tools.

Operations and processes are implemented in a variety of ways. Training modules cover a wide range of Operator requirements and best practices (see Appendix C) and Ike implements strict processes for hardware and software release, as described below.

HARDWARE RELEASE PROCESS

The hardware release process describes review, release, and version control procedures that apply to hardware documents. This process applies to all documents used in the analysis, fabrication, assembly, inspection, commissioning, and verification testing of upfit hardware components and assemblies. Engineers can also use the hardware release process to place reference documents under version control if desired.

The hardware release process workflow is separated into three states: *Work in Process*, *For Review*, and *Released*. *Work in Process* documents are not controlled and are only used as reference during hardware development. *For Review* documents are used to create evaluation hardware that can be used to determine hardware upfit readiness but cannot be permanently upfit onto Ike vehicles. *Released* documents are used for all on-vehicle hardware.

For a document to be promoted from *Work in Process* to *For Review*, it must be peer-reviewed by other engineers to address development intent. This is managed at the discretion of the organizing engineer. For a document to be promoted from *Work in Process* or *For Review* to *Released*, or to change the version of a *Released* document, it must be peer-reviewed by a cross-functional panel of engineers who consider development history, detailed key decisions and justifications, and all analyses or test results. Required approvers and associated roles are identified on *Released* documents. If any document undergoes heavy revision, it reverts to the *Work in Process* state.

SOFTWARE RELEASE PROCESS

The autonomy software release process workflow is diagrammed in Figure 3. Software commits are landed onto a development branch after passing unit tests and a set of regression tests that are module-specific. Development branches undergo offline behavioral competency evaluation via our validation workflow (see Figure 2). Next, the candidate release is deployed for Hardware-in-the-Loop testing to confirm performance on the target hardware. After this, closed-course, full-vehicle validation occurs through structured track testing. After passing these structured track tests, the software is released to the fleet. Mechanisms are in place to enable bug fixes that do not invalidate earlier stages of testing. These can present significant challenges, as it is often difficult to assure that a given code change does not invalidate earlier results. For this reason, we use bug fix branches sparingly, and only for minor changes.

VALIDATION METHODS

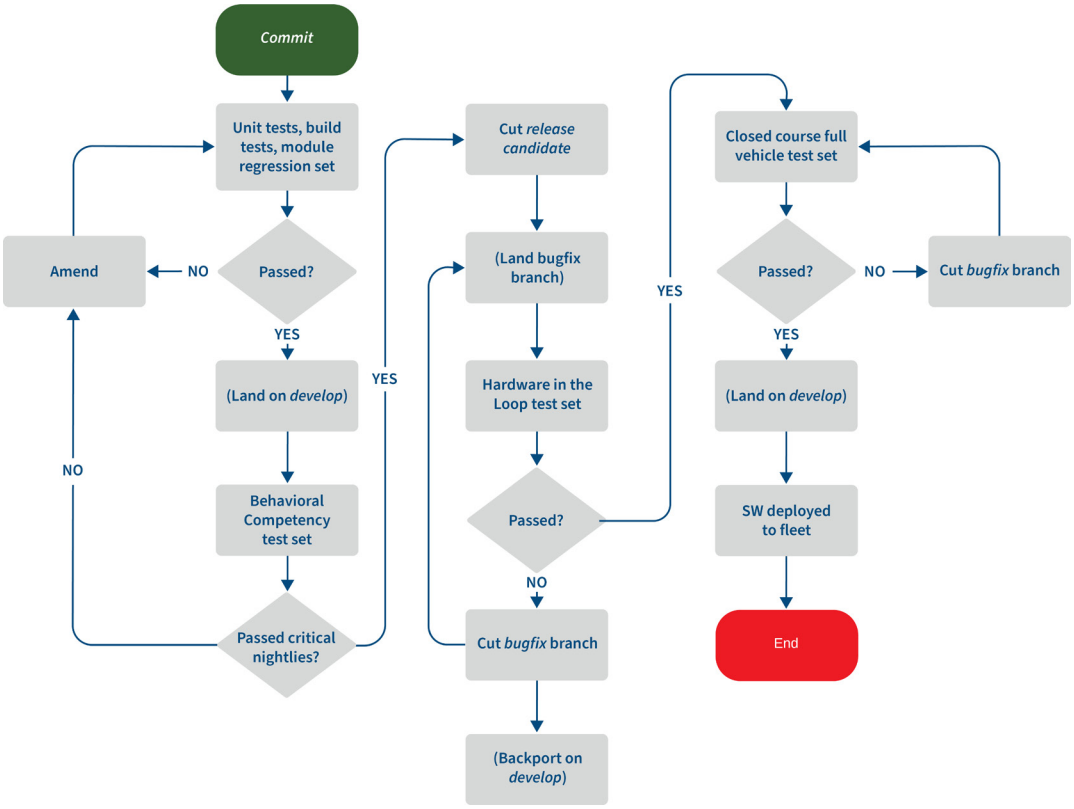


Figure 3: Workflow of Ike's development autonomy release process. Gates are staged at critical integration points to maximize the likelihood of catching bugs and requirement violations early. This workflow is under active development and will continue to evolve over time as our test coverage and preparations for road release evolve.

The APG software release process differs from the autonomy software release process in a few ways. Because there are no emergent behaviors from the APG, no behavioral competencies are evaluated for the APG. Safety-critical functions achieved by the APG must be evaluated in Hardware-in-the-Loop testing prior to road release. Additionally, not all APG software changes require closed-course testing. However, when changes are made that impact the intervention or command-limiting behavior of the APG, the software release must undergo a test suite that checks some or all of the intervention logic, takeover request logic, and vehicle controls.

OPERATOR TRAINING

Operating safely is a core value for our team. We have implemented an intensive screening process to train and test candidates that includes a background check on every individual's criminal, driving, and DOT history (including FMCSA's Pre-employment Screening Program), and a pre-employment drug screening. All candidates must complete and pass a safety-focused vehicle inspection and driving interview with a veteran Vehicle Operator who observes the candidate under normal driving conditions while operating a manually driven class 8 truck during a road test. Newly hired operators spend their first three weeks in an intensive in-house training program.

The training program is broken up into two distinct roles: Vehicle Operator and Right Seat Operator. Each trainee begins as a Right Seat Operator responsible for supporting a Vehicle Operator. Once the trainee demonstrates competency in right seat operation and passes the necessary tests, they are trained and tested as a Vehicle Operator. Our training is designed to create a culture and practice of safe vehicle operation and includes a variety of methods to ensure each trainee augments their existing record of safe vehicle operation with familiarity and comfort with our processes, policies, and best practices. Throughout the three-week training program, trainees participate in active observation, classrooms, and closed-

course track-training. The majority of this time is dedicated to training in vehicles with veteran Operators. Employment as an Operator is contingent upon passing all modules in our training program. A full list of our current operator training modules may be found in Appendix C.

Trainees are tested throughout the program. Tests are designed to measure the trainee's understanding of Ike's software, hardware, and operating system, how to properly communicate the system's intent, and how to safely operate the system under normal and adverse circumstances in manual and automated modes. The trainee must pass check points before being granted daily Operator responsibilities. Each member of the operations team receives continuous feedback and training refreshers throughout the year. Furthermore, all operators agree to monitoring and are expected to follow all company policies in and out of our vehicles.

Our goal is to develop safety-minded and confident operators who exude technology and industry know-how while demonstrating professionalism and a willingness to learn throughout the training program and beyond.

Below we capture an example of a Loss Scenario mitigation via operator training. As in other examples above, this represents only one Loss Scenario among many associated with this particular UCA. (We do not include some non-operational mitigations in place to address this specific Loss Scenario.)

Unsafe Control Action (UCA)	Loss Scenario	Mitigation (Requirement)	Verification/ Validation
Steering release - ADS: Steering from ADS is stopped too soon before a steering maneuver has been completed to stay in lane and steering is not supplemented by Vehicle Operator.	The E-Stop button is activated by the Vehicle Operator, ceasing computer commands to steering, momentarily releasing steering before the Vehicle Operator has reestablished control.	The Operations Team shall train Drivers to disengage computer control using the brake pedal with a light brake tap and with hands on the steering wheel.	Verification via inspection of operator training modules. Validation via Vehicle Operator training on a closed test track

Table 8: Illustrative example of an analysis of a UCA related to steering release. In this case, the mitigation is implemented via training and best practices. This requires the inspection of training modules as well as Vehicle Operator training at a closed test track.

9. Human-Machine Interface (HMI)

Because our current development platform may be under computer or manual control, the HMI design is crucial to communicating the status of the vehicle platform and the ADS to the Vehicle Operator. Through the application of STPA, many Loss Scenarios have been identified and associated with process model flaws of the Vehicle Operator. Examples include believing that the system is still under computer control when it is not or believing that the system is operating correctly when a fault has occurred. Poor HMI design can also lead to mode confusion. For example, if the state of computer control is indicated via colored lights, an operator could misinterpret the meaning of a particular light color or flash pattern.

Ike uses an automotive grade display to indicate the state of computer control to the Vehicle Operator. The display contains minimal information, indicating only the system state to both operators. This is used instead of an LED panel in order to minimize the potential for mode confusion. The display utilizes an automotive-grade microcontroller rather than a consumer-grade tablet to reduce the likelihood of a hung process resulting in a frozen display. Examples of HMI display screens are provided in Figure 4.

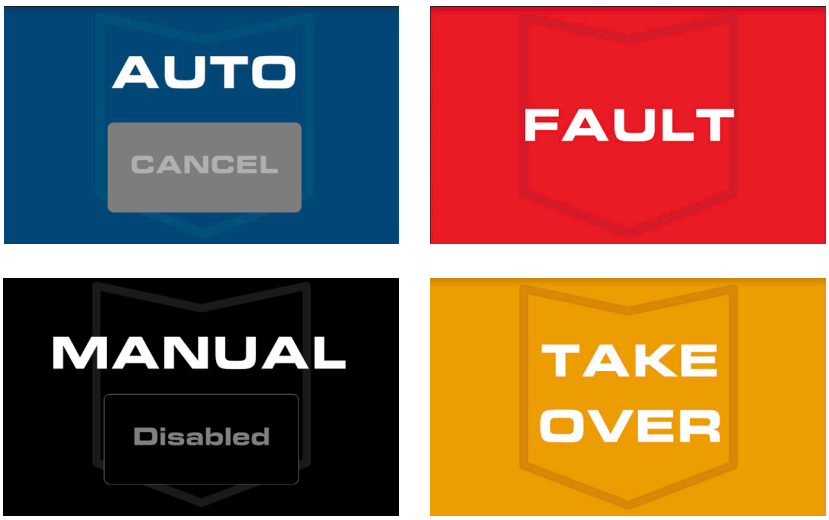


Figure 4: Ike's HMI display screens as seen by the Vehicle Operator. Vehicle Operators at a glance may understand the operating state of the vehicle.

HUMAN-MACHINE INTERFACE (HMI)

Even with a highly reliable display, there is still risk that the display will not update, will go blank, or will otherwise fail to accurately indicate the state of computer control to the Vehicle Operator. To mitigate this risk, we also utilize an audible alert system that is independent of the display screen, controlled by a separate safety co-processor. Even if the HMI screen enters a faulted state, the Vehicle Operator is still warned via audible alerts.

10. Vehicle Cybersecurity

To protect our system from malicious attacks, we rely heavily on operational best practices and limiting physical access to our system. As examples, there are no wireless access points to the ADS, and all physical access points are tightly enforced by limiting physical access to the vehicle. Furthermore, our Vehicle Operators are trained to inspect for physical intrusion and detect anomalies in system behavior.

We expect that vehicle cybersecurity will require significant technology development in order to deploy a product at scale. Our approach will be to use as a starting point and improve upon the state of the art as recommended by NHTSA, NIST, Auto-ISAC, and SAE. Future versions of this document will include additional details and updates on these fronts.

11. Crashworthiness

Crashworthiness is assessed for all development vehicles for the protection of both road users and vehicle occupants.

11.1 Structural Integrity

In the design process, all ADS mounts are evaluated using simulation, as well as best-practice hand calculations when appropriate. Design standards are used in the selection of materials, fabrication processes, and fasteners. Shock load values representative of crashworthiness are based upon information provided by industry stakeholders and are specific to the mount location on the vehicle. Fatigue load estimates are based upon ISO standards for on-road class 8 trucks with a suspended cab.[27]

11.2 Vehicle Occupant Protection

Due to the mass and size of class 8 tractors, the biggest risk to vehicle occupants in the event of a crash is from improperly secured objects within the cabin rather than cabin encroachment. To mitigate this risk, upfit components within the vehicle cabin are designed to withstand worst-case crash loads. All fasteners are torqued to a specified load and marked during the build process. Additionally, the vehicle cabin is inspected for loose objects as part of the pre-trip inspection for every mission.

11.3 Protection of Other Road Users

Our externally mounted components are carefully designed to take into consideration the protection of other road users. Protru-

27 https://www.iso.org/obp/ui/#iso:std:iso:16750:-1:ed-3:v1:en section 4.1.2.8

sions from the front or sides of the vehicle can present significant hazards to pedestrians, cyclists, and motorcyclists. For this reason, externally mounted components conform to the A-surface of the stock vehicle wherever possible. Sensors that protrude from the A-surface are kept as close to the vehicle as possible. Sensors that protrude more than 10 cm from the stock vehicle are mounted above the lowest height of the side mirrors, minimizing the risk to vulnerable road users.

12. Post-Crash ADS Behavior

The current development platform relies on human operation to return the ADS to a safe state after a crash. Operator training includes standard procedures in the event of a crash (under either manual or computer control), such as disarming or disabling the ADS and navigating to a safe location.

In the event of a crash, the vehicle is transported to a maintenance facility and inspected and appropriately repaired prior to returning to the road for manual operation. All ADS components are likewise inspected and recalibrated as necessary whenever damage occurs.

Future versions of this document will describe technologies under development that will detect and respond to various crash scenarios.

13. Data Recording

The onboard system records data generated by both the ADS (described in Section 3.6) as well as the In-Vehicle Monitoring System (described in Section 3.5). These two systems are independent, which allows for data-recording even in the event of power loss or hardware failure. In addition to signals needed for conventional Event Data Recorders, Ike development vehicles record interior and exterior camera data and vehicle CAN network busses at all times, whether the vehicle is driven manually or under computer control.

14. Education & Training

Ike is engaged in a number of outreach activities with relevant stakeholders to provide education on both the capabilities and limitations of automated trucking technologies. While Ike does not offer automated driving solutions to consumers, we feel obliged to continue to educate the broader public on the technologies under development.

The deployment and commercial use of automated trucks powered by Ike's technology will have wide-ranging implications. Companies in the logistics industry will adjust their operational models to take advantage of the benefits created by Ike's technology. Individuals working in the industry will see their work change in some ways, either shifting their workflows to integrate with automated trucks (such as a truck driver handing off a trailer for a long-haul journey by an automated truck) or building new skills and expertise (such as calibrating automated vehicle sensors in a transfer hub, maintaining new vehicle components, or remotely supporting automated operations). While these changes will not be drastic, new training and certifications will be necessary to ensure high reliability and commercial value. Ike is already working with a number of companies in the industry to develop a foundation for various training and certification efforts. More work will be needed as the technology matures and approaches commercial viability.

In addition to commercial training, education and outreach for public road users will also be necessary to ensure safe deployment of automated trucks. Much more can be done today to provide more transparency and accountability by companies developing these technologies. Our Safety Report is part of a broader effort toward this goal, including disclosures involving our current fleet, geography of operation, and DOT safety and compliance metrics.

As automation technology approaches commercial viability in coming years, Ike expects to invest heavily in broader public

education to help road-users better understand our technology and how we assure safety. Education will help minimize misconceptions and reduce erratic or other risky driving involving vehicles powered by our technology. This will require collaboration with many stakeholders, including government, commercial partners, and safety groups.

15. Federal, State, & Local Laws

Ike is committed to complying with current laws, regulations, and guidance from all levels of government. Additionally, Ike is committed to participating in the future development of regulations and standards that will help ensure safe deployment of automated class 8 trucks throughout the industry. Ike is well-positioned to help establish these standards going forward to ensure the highest degree of highway safety.

15.1 Federal Regulatory Engagement

As indicated in the Department of Transportation's (DOT) 2018 guidance[28] and the Federal Motor Carrier Safety Administration's (FMCSA) recent Advanced Notice of Proposed Rulemaking,[29] current regulations may need to be revised to accommodate for the deployment of automated class 8 trucks. Ike is actively involved in this process. Most recently, Ike provided comments to FMCSA on the ANPRM[30] and will continue to engage with DOT, FMCSA, and NHTSA to develop safety regulations and standards for automated class 8 trucks.

15.2 State Regulatory Engagement

Ike engages with relevant state Departments of Motor Vehicles (DMVs), Highway Patrols (HPs) and DOTs to provide state and local law enforcement and emergency responders the opportunity to ask questions and learn about current capabilities and best practices.

28 Automated Vehicles 3.0, Preparing for the Future of Transportation, October, 2018.
29 FMCSA ANRPM, Safe Integration of Automated Driving Systems-Equipped Commercial Motor Vehicles, 84 FR 24449, May 28, 2019.
30 See Ike filing here: https://www.regulations.gov/document?D=FMCSA-2018-0037-0286

15.3 Regulatory Compliance

Ike is obligated to adhere to all regulations imposed on traditional motor carriers, including keeping records to document compliance with relevant safety regulations. We meet all DOT and State requirements to maintain a valid, interstate motor carrier authority:

- Drug & Alcohol Testing
- Driver Qualifications
- Hours of Service via Electronic Logging Devices (ELDs)
- Vehicle Inspection, Repair, and Maintenance
- Registration and Insurance
- Roadside Inspection

15.4 Local Traffic Laws

Whether under manual or computer control, Ike vehicles are designed to adhere to applicable traffic laws. One of the unique opportunities afforded by automated driving technologies is the ability to encode federal, state and local laws directly into the vehicle behavior to ensure that vehicles conform at all times. Adherence to traffic laws is assessed as part of our offline behavioral competency validation, as described in Section 8.1. Additionally, through the use of ELDs, Right Seat Operators, and operations training, Ike can reduce the risks of speed-limit violations, drowsy, impaired driving, and distracted driving.

15.5 Future Engagement

Ike will continue to engage with all relevant regulators, legislators, and other external stakeholders, including the Commercial Vehicle Safety Alliance, to ensure compliance with existing laws and regulations and to help develop appropriate laws and regulations where needed to ensure the safe operation of automated commercial vehicles on our public highways.

16. Roadworthiness Criteria

Unlike well-established industries such as aviation and conventional passenger vehicles that manufacture and operate safety-critical systems, automated class 8 trucks currently lack roadworthiness criteria. This is the case both for vehicles in development and for production vehicles. While some standards may be used to certify hardware and software modules that are used in an ADS, no behavioral certification exists for the ADS itself.

For this reason, Ike is developing roadworthiness criteria to ensure that Ike vehicles on public roads meet strict safety constraints. These are drawn from a combination of Euro NCAP test protocols,[31] Federal Aviation Administration Certification Procedures for Experimental Aircraft,[32] behavioral certification from internal learnings, and current FMCSA regulations.[33]

16.1 Roadworthiness Criteria for Development ADS

In this context, a "Development ADS" is a conventional vehicle that has been upfit with sensors, compute elements, software, and actuators to enable automated driving. A Development ADS is supervised by a Vehicle Operator who has control authority at all times. The system is considered developmental when installed components are not part of the original vehicle build or when development software is used. All current Ike vehicles match these criteria.

Below is Ike's current list of internal elements for establishing roadworthiness, which is non-exhaustive and subject to changes throughout development. Some of these are specific to a particular truck, software release, or even individual mission (i.e. test request)

31 https://cdn.euroncap.com/media/32290/euro-ncap-sas-test-protocol-v20.pdf
32 14 CFR 21.193
33 49 CFR 392

while others are common to all development vehicles operated by Ike. Documentation of these elements is part of the road release process.

Elements:

i. DOT number, Vehicle identifier, and proof of insurance
ii. Vehicle Operator/Right Seat Operator
iii. Description and purpose of experiment (test request/ ticket), including estimated duration (number of miles, number of vehicles)
iv. Description of the trailer/cargo, if any
v. Geographic and environmental constraints for computer control
vi. Operating instructions
vii. Proof of maintenance and pre-trip inspection
viii. Summary of modifications made to the vehicle and proof of installation according to supplier/manufacturer's guidance
ix. Summary of track testing and simulation testing of the vehicle and software release (for both Autonomy Computer and APG software)
x. Summary of driver intervention methods and how control authority of the Vehicle Operator is assured
xi. Proof of ADS behavioral competency through offline validation, for example:
    - Lane-keeping
    - Speed-keeping and speed-limiting
    - Preserving headway distance for slow traffic ahead
    - Appropriate deceleration for cut-ins and merging vehicles

MISSION GO/NO-GO

Once all roadworthiness criteria have been satisfied, the Fleet Operations team is responsible for making Go/No-Go decisions as to whether test requests and experiments may be executed. The Go criteria are primarily based on analysis of the roadworthiness

elements above. Below are illustrative examples of such criteria, which may include:

- Is the experiment within the ODD?
- Is the system capability consistent with current operator training?
- Is the vehicle behavior consistent with current operator training?
- Has the truck been released by Engineering?
- Have the Autonomy Computer and APG software versions been released by Engineering?
- Have the vehicle behaviors under test been released by Engineering?
- Have the operators been briefed, release notes reviewed, and clear test plan(s) with success criteria provided?
- If using other actors on a closed track, is there any risk to operators of other vehicles?

16.2 Roadworthiness Criteria for Production ADS

Establishing clear roadworthiness criteria for a fully driverless, production ADS will require both technology development and collaborative partnerships throughout industry and government. While these criteria are under development, Ike must develop the technology and tools necessary to demonstrate adherence to safety constraints toward our eventual goal of operation without human supervision.

Due to a number of differences between automated driving for class 8 trucks as compared to last-mile delivery or passenger-vehicle applications, we expect different roadworthiness criteria to be appropriate for production. For example, future automated class 8 trucks will carry no occupants, so occupant-protection will be a non-factor. As such, the roadworthiness criteria applicable to automated class 8 trucks on specific highway segments will not be directly applicable to other automated driving applications.

ROADWORTHINESS CRITERIA

Ike is actively developing not only the ADS capabilities but also tools to test roadworthiness criteria. In particular, Ike is developing the means by which to assess behavioral competency across a statistically significant set of test scenarios that span our ODD (see Section 5). In the future, these test results will be at the core of our roadworthiness criteria for public road release of automated class 8 trucks that do not require human supervision.

17. Challenges, Limitations, & Future Work

In this section, we describe the challenges and limitations of our current safety approach. Many of these challenges are not specific to Ike's technology or product aspirations. The goal of sharing these challenges more broadly is to encourage collaboration on solutions that may be shared between developers of automated driving technologies.

Our mitigations to some current system limitations are either operational or involve human supervision or management. For example, we rely on Vehicle Operators to reestablish manual control when weather conditions deteriorate. These types of solutions may be sufficient for a small fleet during development, but are not possible to implement and validate for a driverless product at scale. These and other limitations to our current safety approach must be addressed prior to deploying a commercial product at scale.

17.1 Offline Testing Validation Representativeness

As described in Section 8.1, we validate behavioral competencies using a battery of offline tests developed from real-world logs and fully synthetic simulation. Through the evaluation of our performance throughout this test suite, we can guarantee that behavioral competencies satisfy requirements. This guarantee relies on the test suite being statistically representative of our operating domain. In some cases, this is straightforward: we can measure the location, time of day, weather conditions, and lighting conditions throughout the test suite and compare these to our target ODD. In contrast, measuring the distribution of actor behaviors and comparing them to our target deployment lane presents a significant technical challenge.

We require a parameterization framework that encompasses the primary scenario variables brought under test for a specific validation. This work is ongoing and will benefit from collaboration with other technology developers in this space. A shared parameterization framework would be an important early step toward commonizing validation.

17.2 Simulation Validation

As described in Section 8.1, fully synthetic simulation is a powerful tool for validation, as it allows for procedurally generated variants that can span a wide range of scenarios and behaviors. The challenge is to assure that test results in simulation have strong correlation with real-world testing. That "realism" challenge can be broken down into two parts: the realism of the scenario (simulating driving behaviors of real actors) and the realism of the simulator (sufficient fidelity to prove real-world performance). Ike has developed a virtualization technology (colloquially called "Virtualization") to address both challenges.

Virtualization is the ability to automatically extract a virtual scenario from real data. Ike's implementation is designed to be agnostic to the data source and format. Human-generated labels, GPS trajectories, or our own logs can be processed and combined to create parameterized and editable scenarios.

Bootstrapping our virtual scenario creation process with Virtualization has the immediate advantage of streamlining the otherwise labor-intensive process of scenario design. Combining with parameterized variations enables the creation of large volumes of realistic and representative virtual scenarios.

Central to the iterative process of evaluating and improving the fidelity of the simulator is the ability to execute identical scenarios in simulation and the real world. Executing a repeatable real-world test with several high-speed actors is a non-trivial task. Instead, we

perform a test at our real-world test track and rely on Virtualization to create the corresponding simulation scenario. From these direct comparisons, we can understand the system requirements that can be faithfully validated via virtual simulation, while also detecting gaps between simulation and reality.

17.3 Driverless Validation & Performance Indicators

While the scope of the safety measures described herein is primarily to address safety considerations for a development platform with human supervision, Ike is currently developing the technology necessary to qualify an ADS for public road release with no Vehicle Operator.

At a minimum, two criteria must be satisfied in order to qualify a fully driverless automated class 8 truck for road release: First, a class 8 truck fleet operating with the ADS must be proven to be less likely to generate losses (as defined in Section 4.1) compared to a human driven fleet operating in the same region. Second, the ADS must be proven to lose no safety performance by removing the Vehicle Operator. There is reason to expect that in the future, the ADS will be made safer by removing the Vehicle Operator, principally by removing Loss Scenarios associated with mode confusion, false-positive interventions, and etc.

Ike is developing a validation pipeline capable of precisely measuring behavioral competencies, efficiently identifying potential behavioral requirement violations, and qualifying new software releases with limited public road testing. Key to this technology is the validation foundation described in Section 8 as well as accompanying proprietary tools and statistical models. Similarly, Ike is developing the system architecture necessary to operate without a human operator.

Ike is also developing performance indicators to provide a statistically significant measurement of the system's overall likelihood of

incurring a Loss Scenario. This is a critical step toward establishing qualification criteria for road release of a fully driverless platform.

17.4 Leading Indicators for Increasing Risk

A key aspect of operational risk management is identifying the potential for a safety constraint violation to occur before an accident happens.[35] Toward this end, we adopt the approach of utilizing assumption-based indicators, as defined in the STPA handbook:[36] "An assumptions-based leading indicator is defined as a warning sign that can be used in monitoring a process to detect when an assumption is broken or dangerously weak or when the validity of an assumption is changing." Examples of assumptions that impact our safety analysis include the level of effectiveness of mitigations against Loss Scenarios (e.g. the Vehicle Operator will respond to specific takeover requests), environmental conditions within our geography, and the principles of operation of driver-assist features.

35 https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf, pp. 101
36 https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf, pp. 103

Appendix

A. Glossary

A Surface: The exterior cosmetic surface of the vehicle

ADAS: Advanced Driver Assistance System

ADS: Automated Driving System, defined as per SAE J3016[37]

APG: Automated Platform Gateway

ANPRM: Advance Notice of Proposed Rulemaking

Auto-ISAC: Automotive Information Sharing and Analysis Center

Autonomy Computer: The computer responsible for generating motion commands to the vehicle platform based on sensor inputs

Buffer Zone: The allowable minimum distance to other nearby road occupants, stationary objects, or vulnerable road users

CAE: Computer Aided Engineering

CAN: Controller Area Network

CHP: California Highway Patrol

Class 8: In the United States, commercial truck classification is determined based on the vehicle's gross vehicle weight rating (GVWR). Class 8 is the classification of a heavy duty truck with a GVWR that exceeds 33,000 pounds.

Computer Control: A state of operation where the ADS is commanding control actions to the vehicle platform

DDT: Dynamic Driving Task, defined as per SAE J3016[37]

DFMEA: Design Failure Mode and Effect Analysis

Disengagements: transitions from computer to manual control

37 https://www.sae.org/standards/content/j3016_201806/

DMV: Department of Motor Vehicles

DOT: Department Of Transportation

Drive-by-wire actuators: Use of electrical or electro-mechanical systems for performing vehicle actuation traditionally achieved by mechanical linkages. Steer-by-wire refers specifically to steering control and brake-by-wire refers specifically to braking control.

E-Stop: A latching mushroom button on the dash that electrically severs power to the APG and prevents any computer control

Ego vehicle: Refers to the vehicle under control of the Automated Driving System

ELD: Electronic Logging Device

Euro NCAP: European New Car Assessment Programme

FMCSA: Federal Motor Carrier Safety Administration

FOD: Foreign Object Debris

GPS: Global Positioning System

HIL: Hardware-in-the-Loop

HMI: Human-Machine Interface

HOS: Hours of Service

HP: Highway Patrol

Interventions: events when the Vehicle Operator reestablishes control over the vehicle platform

ISO: International Organization for Standardization

LED: Light Emitting Diode

Logged Data Simulations (also known as "LogSims"): Simulations that utilize previously collected data to replay against the latest software release.

Loss Scenario: A term used in System-Theoretic Process Analysis (STPA) defined as a causal factor that can lead to an Unsafe Control Action (UCA)

Manual control/operation: A state of operation where the Vehicle Operator is commanding control actions to the vehicle platform

NIST: National Institute of Standards and Technology

NHTSA: National Highway Transportation Safety Administration

ODD: Operational Design Domain, the definition of the environment that an ADS is designed to operate in

OEDR: Object and Event Detection and Response

Offline testing: The combination of testing that occurs in a simulated or closed test track environment

Right Seat Operator: The operator responsible for the management of the Autonomy Computer

SAE: Society of Automotive Engineers

STPA: System-Theoretic Process Analysis

Structured track testing: Testing to prescribed scenarios in a controlled environment

Synthetic Simulations: Virtual scenarios, that may be either designed from scratch in our scenario editor or automatically extracted from recorded data.

Tier 1 Supplier: Tier 1 suppliers are companies that supply parts or systems directly to truck manufacturers, also known as Original Equipment Manufacturers (OEMs)

Tractor: The unit that is part of a semi-trailer (also known as a tractor-trailer) that contains the engine responsible for motive power to haul a load

UCA: Unsafe Control Action

Vehicle Operator: The operator responsible for driving the vehicle

VRU: Vulnerable Road User (e.g. pedestrians, cyclists)

B. Operational Design Domain (ODD) Summary

The following table (page 91) is a summary of our current Operational Design Domain (ODD) for operation under manual control, computer control on closed test tracks, and computer control on public roads. Note that these are design constraints. As noted previously, we do not currently operate on public roads under computer control. Do Not Operate means that the vehicle is not approved to operate in this domain. Do Not Operate/Return to Base means that should the vehicle enter the specified domain, the Vehicle Operator is to cease operations and return to base. Return to Manual means that the Vehicle Operator is to return the vehicle to manual control should the vehicle inadvertently enter this ODD under computer control. Note that we implement multiple methods to impose ODD restrictions. Operations Allowed means that the vehicle is approved to operate in the specified ODD.

	Domain Parameter	Design Constraints for Manual Control	Design Constraints for Computer Control on Closed Test Tracks	Design Constraints for Computer Control on Public Roads
Road Type	Residential	Do Not Operate	N/A	Do Not Operate
	Surface street (truck route)	Operations Allowed	N/A	Return to Manual
	Highway	Operations Allowed	N/A	Operations Allowed
	On/off ramp	Operations Allowed	N/A	Operations Allowed
	Steep grade (>6%)	Operations Allowed	N/A	Return to Manual
	Construction zones	Operations Allowed	N/A	Return to Manual
	Scales, tolls	Operations Allowed	N/A	Return to Manual
Temperature	Extreme cold (<-10 C)	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base
	Nominal (-10 C – 40 C)	Operations Allowed	Operations Allowed	Operations Allowed
	Extreme heat (> 40 C)	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base
Time of Day	Daytime	Operations Allowed	Operations Allowed	Operations Allowed
	Dawn/Dusk	Operations Allowed	Operations Allowed	Return to Manual
	Nighttime	Operations Allowed	Operations Allowed	Return to Manual
Visibility	Low visibility	Do Not Operate/ Return to Base	Operations Allowed	Do Not Operate/ Return to Base
	Moderate visibility	Operations Allowed	Operations Allowed	Return to Manual
	High visibility	Operations Allowed	Operations Allowed	Operations Allowed
Precipitation	Light rain	Operations Allowed	Operations Allowed	Operations Allowed
	Moderate rain	Operations Allowed	Operations Allowed	Return to Manual
	Heavy rain	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base
	Light snow	Operations Allowed	Operations Allowed	Return to Manual
	Moderate snow	Do Not Operate/ Return to Base	Operations Allowed	Do Not Operate/ Return to Base
	Heavy snow	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base	Do Not Operate/ Return to Base
Road Condition	Ice	Do Not Operate/ Return to Base	Operations Allowed	Do Not Operate/ Return to Base
	Wet roads/ standing water	Operations Allowed	Operations Allowed	Return to Manual
	Dry roads	Operations Allowed	Operations Allowed	Operations Allowed
Geography	CA - Unmapped	Operations Allowed	N/A	Return to Manual
	CA - Mapped	Operations Allowed	N/A	Operations Allowed
	Out of State	Operations Allowed	N/A	Return to Manual

Table 9: ODD parameter descriptions and design constraints for Ike's current system under development. Manual and computer control are subject to different constraints that include geography, road types, and weather conditions. These are subject to change over time.

C. Operator Training Modules

Below we include a subset of relevant training modules included in our Operator onboarding and training process.

Ike Internal Training	
Ike Company Overview	An introduction to Ike's technology and the company's history.
Training Program Overview	High-level summary of Ike's Training Program and expectations. Basic overview of the responsibilities in the Vehicle Operator and Right Seat Operator roles.
Best Practices & Safe Driving Policy	Ike's policies for safety and best practices.
Ike Viewer	An introduction to Ike Viewer - the Right Seat Operator's console for ADS monitoring and logging.
Ike Software Use	How to use all software modules.
SW/HW Start-up & Shut-down Procedures	End-to-end lessons covering how to properly start up and shut down all ADS hardware and software.
Driver & Co-Driver Communication & Hashtags	How the Vehicle Operator and Right Seat Operator communicate. Callouts, Comments, & Hashtags: What they are and how they are used.
Troubleshooting/Escalating Issues	How to troubleshoot and escalate issues. Communication and importance of teamwork.
Review of Relevant Vehicle Code/Traffic Laws to ODD	Review with Operators their responsibility to obey all provisions of the Vehicle Code and local regulations applicable to the operation of motor vehicles, regardless of whether the vehicle is in autonomous mode or manual mode, except when necessary for the safety of the vehicle's occupants and/or other road users.
System Limitations & Operational Design Domain	Inform the Operators of the limitations of the ADS so they can safely handle the vehicle in all conditions under which the vehicle is tested.
Public Interface Guidelines	What Operators can expect while operating our vehicles in public spaces and how to talk about our technology.
Emergency & Escalation Procedures	Steps that must be followed in the event of an emergency.
Grounding & Stand-Down Policy	Ike's internal stand-down policies and their levels.
In-Vehicle Monitoring System - Dash Cam Policy	Read, review, and consent to our In-Vehicle Monitoring System.
In-Vehicle Monitoring System - Distracted/ Fatigued Driving Examples & Demonstration	Demonstration of the features of our deployed In-Vehicle Monitoring System.
Workplace Safety & Security for Drivers	Tips for drivers to stay safe on the road or in the office.
Mapping Data Collection & Map QA	How to operate Ike's mapping vehicle and the Map QA process.
Sensor Calibration	Explanation and procedures for ADS sensor calibration.
Mission Debriefing Tips	How to write mission debriefs.
Daily Debrief Tips	How to summarize mission debriefs and communicate them to engineers and other teams.

CMV Driver Training	
Drug & Alcohol Testing Policy	Read, review, and consent to Ike's FMCSA-compliant drug and alcohol screening program.
Hours of Service Regulations - Property-Carrying Vehicles	Overview of the hours-of-service expectations for drivers, including prohibition of coercion.
Using our Electronic Logging Device (ELD)	Training on ELD use.
Vehicle Inspections & Checklists	How to complete a vehicle inspection and use the appropriate checklists.
Training in Fatigue Management & Prevention	Educate drivers on how to manage fatigue while operating. Included is guidance on FMCSA tips on fatigue and wellness awareness.
Driver Health & Fitness	How to stay healthy, off and on the road.
Distracted Driving	FMCSA tips on avoiding distractions and NSC tips about how to avoid distractions and other drivers who are distracted.
Defensive Driving	Train drivers to be aware of other drivers and situations and to practice proper speed and space management. Includes proactive activities like hazard-awareness and mountain driving and discusses special considerations for urban and rural driving environments.
Cornering	Techniques for driving around corners.
Evasive Maneuvers	Common emergency maneuvers for drivers.
Backing	Techniques for safe backing maneuvers.
Coupling and Uncoupling	Ike's tractor/trailer coupling and uncoupling procedure that complies with CHP/DOT expectations.
CSA Training	Educate drivers about the ways the FMCSA categorizes unsafe driving.
Cargo Securement	How to properly secure cargo when driving with a load.

Final Review	
Final Review	A final review of both CMV driver and Ike internal training , from in-vehicle training to the classroom presentations. Vehicle Operators will need to pass this at the end of the training to be eligible to operate any Ike vehicle.