A Safety Framework to Assess Autonomous Construction and Mining Equipment

Cynthia Brosque[1] **and Bibhrajit Halder**[2]

[1]Ph.D., Product Manager SafeAI Inc., CA, United States
[2]Ph.D., Founder and CEO SafeAI Inc., CA, United States

cynthiab@safeai.ai, bibhrajit@safeai.ai

Abstract -

Artificial intelligence is set to transform the mining and construction industries by providing greater insights that will eventually create a safer, more productive, and more reliable environment. However, integrating autonomous technology and equipment in the field is still a complex task that necessitates a detailed safety study, analysis, identification, and mitigation of hazards. Before any autonomous operation can be realized, a safety plan needs to be executed by the technology provider and the site operator and/or subcontractors. This plan must be regularly assessed during the development and implementation phases of the technology on site. As the industry evolves to incorporate more autonomous systems, having a comprehensive and consistent safety framework to assess this technology becomes more relevant for innovators in the field. The industry can learn and adapt the analyses developed for other automation uses such as aviation, automobile, nuclear, and defense systems to consider not only the safety of technology, but also the interfaces with human operators and the impact of process changes. The purpose of this paper is to provide an introduction to a safety framework and workflow developed and followed by SafeAI for the application of its autonomous technology in construction and mining. This framework is applied across our global deployments. For example, we highlight its application for our California proving grounds.

Keywords -

Autonomous Ground Vehicle; Safety; Construction; Mining; Hazard Analysis; STPA.

1 Introduction

Increasing demand for safer, zero-entry worksites, higher productivity, and reduced costs are driving the need for innovative solutions across heavy industries, such as mining and construction.

The vision for an autonomous site of the future to achieve these goals involves a higher level of automation. However, the existing Safety frameworks in the industry do not apply the learnings on automation hazard analyses deployed in other fields such as aviation, automobile, nuclear, and defense systems. These industries consider automation as a system, including the interfaces with humans, processes, and change management. As equipment automation strategies evolve in construction and mining applications, so should the approaches for evaluating the hazards and safety of the technology.

SafeAI is a technology start-up based in Santa Clara, California. SafeAI's primary focus is to deliver safe, autonomous vehicle technology and solutions to heavy industry operators through robust computer and perception-based technologies, such as sensor fusion and deep learning, as well as cutting-edge modular and reconfigurable robotics software behavior frameworks.

SafeAI's autonomous solution retrofits existing construction and mining ground vehicles. The manufacturer and vehicle-agnostic solution utilizes a reusable hardware package that can be easily integrated with a broad range of vehicle types. The AI-powered autonomous software is developed to manage and operate vehicles autonomously in the toughest off-road environments (Figure 1).

2 Prior Work

Safety is integral to the development and deployment of autonomous technology at construction and mine sites. Hazard analysis techniques have been widely adopted by transportation industries where safety is critical as the first step to assess risk, i.e., investigating an incident before it occurs [1].

Common hazard analysis techniques involve Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Hazard and Operability Analysis (HAZOP), as well as their variants. FTA [1] focuses on understanding the logic leading to a top undesired event. It assists in designing a system or as a diagnostics tool and was originally developed by the aviation sector in the U.S [2]. Similarly, ETA condenses the FTA to make it more manageable to study complex designs such as nuclear power plants, chemical plants, and spacecraft analysis [3]. HAZOP is often used as a technique to identify operability hazards that can lead to product, environment, or other hazards broken down per module [4].

Figure 1. SafeAI Proving grounds

Failure Modes and Effects Analysis (FMEA) is also used as a bottom-up hazard analysis technique. This method is useful to analyze hardware failures of components like sensors, according to the information provided by their corresponding supplier. The failure modes from each component are associated with a severity scale based on its failure effect, probability of occurrence, and detection scale. However, this method is noted to have limited applicability for safety analysis at a Systems Level [5].

On the other hand, the System Theoretic Process Analysis (STPA) (Figure 2) is a relatively new hazard analysis technique developed by MIT based on an extended model of accident causation [6]. STPA [5] can be used at any stage of the system life cycle and when STPA is performed, it is assumed that the system design exists.

STPA [5] offers advantages over other conventional bottom-up safety analysis techniques that have been applied to the safety analysis of partially- or fully automated driving systems. STPA considers the unsafe interactions of system components by human interaction, software, etc. This allows an analysis of complex systems such as those found in aviation, spacecraft, automobile, nuclear, and defense systems.

STPA first identifies the potential for inadequate control of the system that could lead to a hazardous state. A hazardous state is defined as one that violates the norms, rules, or constraints of the system. The method studies how each Unsafe Control Action (UCA) could occur and plans a safety requirement to mitigate or avoid the unsafe action. As the product design evolves, the safety requirements also get more detailed in an iterative process. Complete traceability is established between the requirements and the system deployment, which helps maintain the Quality Assurance (QA) process.

3 Method

Given the fact that automation in construction and mining entails a complex system review, SafeAI has integrated a framework to address a “safety first” approach which begins early in the design phase through to the deployment phase. During the design phase, the flexibility to make changes is at its highest while the cost is at its lowest (Figure 3).

Our Safety Framework is comprised of three main components, with the STPA method as the main foundation for hazard analysis. As far as the authors are aware, STPA has not been consistently applied to analyze Mining or

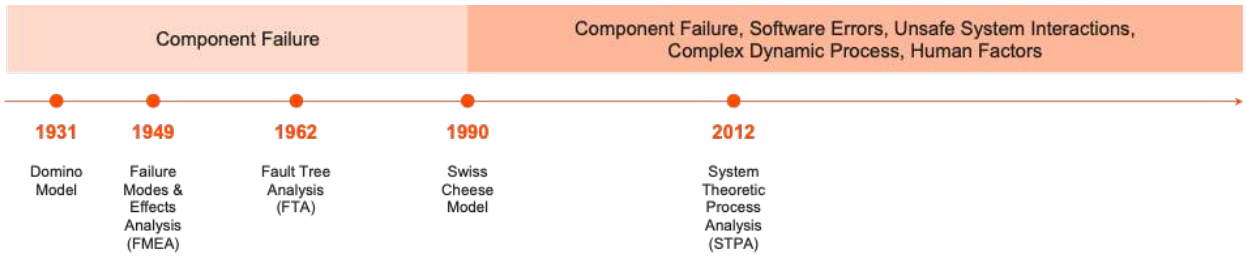

Figure 2. Safety Analysis timeline and type of study

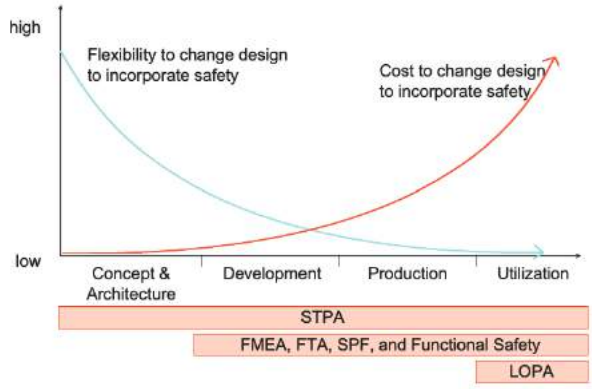

Figure 3. Flexibility to change design to incorporate safety assessment

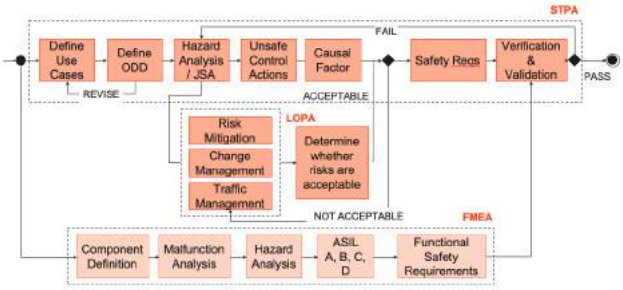

Figure 4. SafeAI Safety Framework

Construction automation strategies. Unlike the traditional hazard analysis methods, this framework can be deployed in early technology development to define safety requirements which can mitigate hazards that would only arise during the operation phase. As the conceptual design is refined and more detailed design decisions are made, STPA maintains complete traceability of the system requirements including the human-in-the-loop analysis.

In addition to STPA, SafeAI implements the bottom-up approach established by FMEA (Figure 4) to study component-level flaws and failures. Finally, it applies a Layer of Protection Analysis (LOPA) focusing on specific mitigation strategies for the risks identified during the Hazard Analysis phase.

This paper describes SafeAI Safety Framework for autonomous mining and construction equipment and shows its application in SafeAI's proving grounds quarry site in California.

4 SafeAI Safety Framework

This section addresses in more detail each step of SafeAI's Safety Framework:

1. STPA
2. FMEA
3. LOPA

4.1 STPA

The STPA risk assessment process follows the ISO 12100:2010 guidelines to:

(a) determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof; (b) identify the hazards and associated hazardous situations; (c) estimate the risk for each identified hazard and hazardous situation; (d) estimate the risk for each identified hazard and hazardous situation; (e) evaluate the risk and take decisions about the need for risk reduction

The safety requirements generated from the STPA were directed to a risk reduction process during the development of the autonomous technology and software and are intended to continually occur during the development, operation, and improvement of the autonomous technology.

The risk reduction process according to ISO 12100:2010 aims to:

- determine the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof;
- eliminate the hazard or reduce the risk associated with the hazard by means of protective measures.

Actions (a) to (d) are related to the risk assessment with STPA, while (e) is related to risk reduction or mitigation strategies addressed in the LOPA section.

The key steps of STPA include:

1. Define the Use Case (e.g., Load-Haul-Dump cycles with retrofitted vehicle)
2. Define the Operational Scenarios (i.e., the interactions between the vehicle and other equipment)
3. Define the Operational Design Domain (ODD) in which the AGV can operate
4. Assess potential System-Level Losses and Hazards
5. Identify Unsafe Control Actions that could lead the system to a hazardous state
6. Document 1st Level Safety Requirements
7. Analyze the Causal factors for Unsafe Control Actions
8. Document 2nd Level of Safety Requirements
9. Implement the Safety Requirements in the Development and Testing pipeline
10. Test and Validate Safety Requirements

As new functionality of the system is developed, this process becomes iterative with new layers of Safety requirements that feed into the development and the testing pipeline.

4.1.1 Use Case Definition

The framework begins by defining the Use Case intended for the Autonomous Ground Vehicle (AGV). The description of the Use Case provides inputs for the next steps which involve determining the Operational Scenarios and ODD.

In our case study, the Use Case Definition is focused on one Autonomous Haul Truck (AHT), also referred to as Autonomous Ground Vehicle (AGV) used in Load-Haul-Dump (LHD) cycles at SafeAI's California proving grounds. This site location includes a dedicated space for our Quality Assurance teams to test and progress the Autonomous development.

4.1.2 Operational Scenarios

Within the SafeAI framework, Operational Scenarios include the scenarios in which the autonomous vehicle interfaces with its environment. Adapted from Vehicle Interaction Systems [7], the interactions are defined as interactions between different kinds and types of equipment, obstacles, infrastructure, and/or humans, etc. in the given operational design domain of the AGV (Figure 5).

We identify the following AGV interaction scenarios applicable to the California LHD Use Case:

1. Control of AGV

The AGV movement (forward-backward direction, turns, maneuvers, and speeds) will be restricted to the ODD as described for various steps of the autonomy development.

2. AGV interacting with humans

The personnel involved in the site and task runs are authorized operators to change the mode from manual to autonomous, conduct any required scheduled or unscheduled maintenance and/or repair of the AGV, and act as remote (out-of-AGV) operators while the AGV is performing a task. Duties and responsibilities of all site personnel were detailed in the risk assessment according to the site regulations.

3. AGV interacting with other equipment (staffed or autonomous)

The AGV performs the loading tasks by interacting with a staffed loader via SafeAIFlux (Staffed Vehicle System) and ZENO (Fleet/Autonomous Management System) coordination. Other equipment in or around the task zone was detailed in the corresponding ODD. In this case, a light vehicle is also allowed in the Autonomous Operating Zone.

4. AGV interacting with the environment

The environment in which the AGV can interact within the approved Autonomous Operating Zone (AOZ), including ground conditions, weather, number and types of lanes, lane edges, grade, and obstacles as detailed in the corresponding ODD. Known obstacle types found in the environment are documented and tested in the ODD.

Figure 5. Illustration of Autonomous Ground Vehicle Operational Scenarios based on EMESRT[7]

4.1.3 Operational Design Domain

Operational Design Domain (ODD) specifies the boundary in which the AGV can safely operate. There-

fore, ODD provides the design constraints of the AGV. Per SAE J3016 [8] ODD is defined as the "operating conditions under which a given driving automation system or feature is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics."

Defining an ODD early in the design process identifies the functional scope of the AGV and what conditions it should be able to handle safely. The ODD definition identifies where changes in system capabilities are required and can aid in generating AGV test cases with varying levels of complexity.

For our ground proving site in California, we designated an initial ODD where the vehicle is allowed to operate. This first ODD was defined as the tightest boundary or radius in which the AGV has been designed and tested to operate. By passing out a series of milestones, the AGV can operate in increasingly complex scenarios or areas of the site. ODD compliance is monitored during the operations to ensure that the AGV is working within the set boundaries.

In our example, the ODD includes:

- Private off-road, geo-fenced area with a Load Zone, a Dump Zone, and hauling roads defined for autonomous operation
- Operating hours between 8am to 5pm according to site shift (running only one shift at the moment with no night operations)
- Site maximum grades are less than 15 degrees
- Drivable area surface is loose gravel
- Drivable area features do not include icy, flooded or muddy surfaces on this site
- Fixed road structures include site office, storage container, and vegetation
- No low clearance areas in AOZ
- AGV can operate in rainfall as permitted by staffed site operations
- Minimum and maximum temperature allowed for operations are the same as for staffed operations
- Traffic rules according to USA and California driving code. Mining rules apply including radio communication and left-hand driving
- Site speed limit 15mph
- No humans allowed in vehicle path while the vehicle is in autonomous mode.
- Interacting road users are authorized mining and construction vehicles

4.1.4 Assess Potential System-Level Losses and Hazards

Defining System-Level Losses in the framework introduces the concept of unacceptable losses to internal and external stakeholders. These losses are documented for the ODD in which the AGV tasks take place.

Losses include cases where the AGV causes an unsafe, unplanned, or undesired scenario. For this use case, the scenarios identified are the damage to the autonomous vehicle, another entity, the environment, and humans or coming dangerously close to causing damage to the autonomous vehicle, another entity, the environment, and humans.

A System-level Hazard is defined as a set of conditions that together with a set of environmental conditions could lead to an accident or loss as defined above. Hazards are linked to each possible Loss to provide insights into the conditions or circumstances that could lead to unacceptable scenarios.

4.1.5 Identify Unsafe Control Actions

The next step of the framework identifies potential Control Actions in the autonomous system that may lead to the hazardous state(s) disclosed above, hence called Unsafe Control Actions (UCA). Hazardous states could result from such potential control actions because:

- A control action required for safety is not provided or not followed;
- An unsafe control action is provided;
- A potential safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence;
- A control action required for safety is stopped too soon or applied too long.

Table 1 illustrates the analysis of Unsafe Control Actions within the context of the autonomous hauling task in our proving grounds in California. In this example, the unacceptable loss is identified as AGV nearly colliding with one or more obstacles, terrain, or infrastructure. The hazardous circumstance that leads to the potential loss is that the AGV does not stop for obstacles in the road during the Load-Haul-Dump (LHD) cycle.

4.1.6 Safety Requirements (1st Level)

Completing the UCA analysis is useful to express a list of safety requirements for the AGV following established safety standards and prevention thresholds. Under SafeAI's framework, these requirements or Safety Conditions (SC) were implemented during product and software development workflow.

From the previous example, high-level safety requirements were elaborated as follows:

SC2.1: AGV shall maintain a minimum distance from other equipment/vehicle of at least 20m in zones. **SC2.2:**

Table 1. Unsafe Control Action (UCA) Analysis

Control Loop/Action	CA not provided	UCA Provided	CA too late/early	CA delivered incorrectly
Stop for Obstacle in haul road	AGV does not stop for obstacle	AGV accelerates with obstacle	AGV stopped too late Min distance violation	AGV engages wrong brake to stop

AGV shall maintain a minimum distance from other obstacles of at least 20m. **SC2.3:** AGV shall maintain a safe distance from vulnerable road users according to the Use Case and ODD. **SC2.4:** AGV shall obey and follow the site rules.

4.1.7 Analyze Causal Factors

Each UCA is linked to one or more causal factors (CF). This process of determining causal factors is further broken down from the system level to the functional block level, until the algorithmic level.

For example, for our UCA "AGV does not stop for an obstacle in forward path", we identified the CF involving the software functional block of the Perception module as follows:

CF1.1: Perception did not identify the obstacle. **CF1.2:** Perception did not check for static objects in the path. **CF1.3:** Perception did not check for dynamic objects entering around/in the path. **CF1.4:** Perception did not identify dynamic objects entering around/in the path. **CF1.5:** Perception did not register the position of the objects in the path ahead.

4.1.8 Safety Requirements (2nd Level)

Based on the causes described in the previous subsection, a second level of safety requirements or constraints was defined specific to the Perception functions.

See the following requirement definition:

REQ-1: *AGV shall perform a normal stopping procedure (e.g., retarder activation) when AGV reaches a minimum safe distance of 20m from an obstacle in a zone.* **REQ-1.1:** Perception shall identify static equipment in the path within 80-40m limit. **REQ-1.2:** Perception shall check for static objects in the path within 80-40m limit. **REQ-1.3:** Perception shall check for dynamic entering around/in path within 80-40m limit. **REQ-1.4:** Perception shall identify for dynamic entering around/in path within 80-40m limit. **REQ-1.5:** Perception shall register position of the objects in path ahead within 80-40m limit.

As observed in this section, SafeAI has integrated STPA iterative approach in the Safety framework wherein we continue to identify a deeper causal factors for each identified causal factor that could lead to a hazardous state. Each new causal factor layer triggers the definition of new levels of safety requirements which are incorporated into the development pipeline.

4.2 FMEA

FMEA is deployed in the Safety Framework to assess hardware performance such as sensors and Drive-by-Wire. FMEA establishes Failure Mode Identifiers (FMI) for each component of the Autonomous kit.

This standard analysis established a *Severity Scale* for each component failure from very high/catastrophic to low or insignificant, the *Probability of Occurrence* of the failure according to the number of failures per day, month, or year, and finally the *Detection Scale* of the failure, i.e., the likelihood of the defect being detected by process controls or reported by the system.

FMEA guided the hazard analysis of individual component failures on the AGV system and provided controls or safety requirements to be implemented to prevent or detect the failure. For example, if the compute unit loses power, the potential effect of failure is loss of vehicle control, and hence the safety requirement is: *AGV shall detect compute unit loss and stop immediately*.

4.3 LOPA

As an outcome of the hazard analysis delineated in the STPA and FMEA subsections, we determine additional risk mitigation strategies to identify, plan, manage, reduce, or eliminate potential risks associated with each identified hazard.

The Layers of Protection Analysis (LOPA) [9] is a semi-quantitative risk evaluation method that builds on a hierarchy of controls (as shown in Figure 6). Several safety systems or controls are arranged in a format from more effective and protective to less effective or reliant on human behavior.

One of AGV's key benefits for the Use Case involves moving the equipment operators out of the vehicle and the equipment operation zone. The risk to the driver is eliminated, which is the highest level of protection identified by the National Institute for Occupational Safety and Health (NIOSH) [10]. However, other operators, such as loading unit operators, ancillary unit operators, drilling operators, and technical services staff may need to access or operate within the autonomous operating zone. Therefore, it is recommended by the Department of Mines, Industry

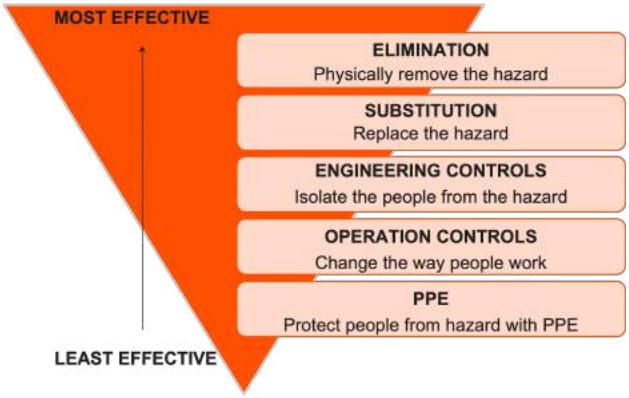

Figure 6. NIOSH [10] Hierarchy of Controls

Regulation and Safety (DMIRS) that additional primary controls such as elimination and substitution be put in place to reduce risks to these employees [11]. SafeAI has integrated LOPA into the Safety framework to define protective layers for identified system-level hazard scenarios, and implement the protective layers as independent safeguarding barriers.

The first step in risk mitigation for the Use Case is to ensure that any form of risk or hazard is first prevented. The prevention process involves complying with applicable California and United States regulations, international safety standards as applicable, and site procedures defined by the site operation and management prior to the initiation of work with autonomous equipment at the site. The site requirements are periodically revised to ensure SafeAI management is up to date with the site requirements.

The standard ISO 17757:2019 [12] was referred to and studied for safety analysis and assessments for the deployment of the autonomous equipment at the site. This standard requires a risk assessment process for Autonomous and Semi-Autonomous Machine System Safety (ASAMS), which conforms to the principles of ISO 12100 [13] wherein, all identified risks shall be mitigated to acceptable risk levels. ISO 17757 also requires that safety-related parts of control systems shall comply with the appropriate functional safety performance level. Examples include ISO 13849 [14], ISO 19014 [15], or IEC 62061 [16].

The following risk mitigation steps included:

- **Identification of risks:** Risks associated with potential hazards are identified as part of the STPA and FMEA, and per risk, the process of prevention is followed.
- **Compliance checks:** The system must comply with international and local regulations (when applicable), and safety standards relevant to the system as a whole or to any system part.
- **Planning:** The system, its processes, and interactions are planned to ensure the prevention of each identified risk.
- **Verification:** The system is verified to ensure it meets the safety requirements, safe fallback actions and plans are in place, and it is prepared for ongoing maintenance implications. Fallback options include built-in redundancies to ensure that if one component or process fails, there is at least one method to bring the AGV to stop.

Each layer of protection integrated into the system should be independent of each other for effective risk reduction.

SafeAI defines layers of protection for each Use Case and Release from development to production (Figure 7). These layers are related to operational procedures or protection measures, as detailed by the corresponding Job Safety Analysis, handed to the Site Operator. Engineering controls arranged as layers of protection as mentioned in ISO 17757 and included in our Use Case in California are:

1) Site Procedures and Regulations
2) Remote Autonomous Stop (A-Stop)
3) Situational Awareness (AGV Perception)

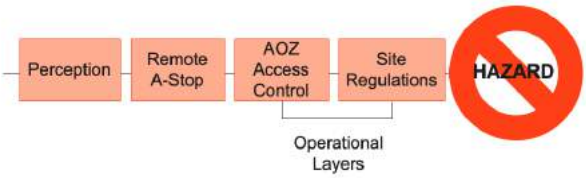

Figure 7. Layers of Protection Analysis

4.4 Implement Safety Requirements

The last step of the Safety framework is to implement the requirements in the system design and validate that the requirements are passed. The requirements are documented internally along with the expected pass/fail criteria. The test results are linked to the requirements and any discrepancies are highlighted as part of this process. A decision on discrepancies might either be continued validation or issue a change request. The following section further details the testing and validation of the requirements as part of the SafeAI Safety Framework for the case study.

4.4.1 Verification and Validation

We have implemented rigorous verification and validation processes to ensure that our system meets the specifications outlined in our safety requirements. These activities are vital in developing autonomous products that

are verifiable and traceable at all levels of analysis. Our SafeAI and testing site personnel are regularly trained in the latest iteration of these procedures and informed of their responsibilities concerning these activities.

Our verification and validation processes have incorporated the expectations outlined in relevant industry and safety standards. We also consult the regional safety regulations of our customers and recommendations from industry-specific organizations such as Earth Moving Equipment Safety Round Table (EMESRT) and Mine Safety and Health Administration (MSHA). As new guidelines are discussed and introduced, we reassess and realign our existing procedures accordingly.

The requirements we established at the beginning of the production lifecycle primarily inform our verification and validation activities at the site. Our quality assurance team then planned and coordinated the relevant tests for the system, module, and unit levels. These tests analyzed all levels of the component, from interfaces and boundary values to operational use cases and dependent failures.

Our verification strategy followed a process similar to that outlined by the "V-model" of development for functional safety (Figure 8). Software requirements fed into software specification, which detailed the system design, module design, unit design, and overall implementation.

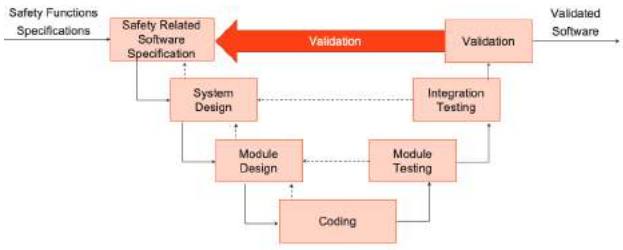

Figure 8. V Development Model

Developers documented their work through issue tickets and merge requests. We utilized a number of methods to verify the code at all stages, such as: • An automated continuous integration and continuous development (CI/CD) pipeline that checks all pushed commits for compliance with Motor Industry Software Reliability Association (MISRA) and AUTomotive Open System ARchitecture (AUTOSAR) code guidelines and code styling rules; • A manual review and approval process with developers designated to have an appropriate degree of independence from the code in question; • Unit-level tests such as inspection, fault injection, and extended functional testing; • Branch coverage and multiple condition/decision coverage (MC/DC); and • Analyses of interfaces and resource usage.

When possible, we have also implemented tools that have been designated as safety certifiable to our desired standards and frameworks.

If errors or non-compliant code was detected at any stage, the request in question was blocked. All development occurs on separate branches and cannot be merged into production unless it has successfully passed the above checks and received all required approvals. Once all verification checks have been completed, safety requirements and goals were validated at the vehicle level to evaluate any residual risk that could potentially trigger hazardous behavior of the overall system. We performed validation in two main stages: initial simulation and on-site vehicle testing.

Simulation provided an opportunity to thoroughly test entire systems and/or sub-systems for adequate performance before deployment and testing on the real vehicle at the site. Simulation also provided unique features that would otherwise be extremely hard to achieve, such as edge cases and future prediction. SafeAI utilized the topology and map of the AGV actual working location in California to create the simulation environment. We then tested various operational scenarios over thousands of hours to ensure that the vehicle will encounter safety-critical scenarios multiple times under a variety of conditions.

5 Site Operation and Established Work Procedures

Safety in mining and construction operations is the top priority of all personnel and support teams. This includes all personnel directly or indirectly engaged in supporting autonomous solutions. It is critical that the autonomous solution deployment at construction and mining sites not only addresses existing safety rules and regulations, but also helps end-users increase safety performance with in-built features, processes, and technology.

This section outlines safe work practices and procedures for the California proving grounds. Any deviations from the safe work procedures, required a job safety or hazard analysis to capture the hazards of the task and ensure that adequate controls or change management actions are implemented and communicated.

Safe work practices included education and training, access to the AOZ, mode change procedures, and emergency response.

5.1 Education and Training

All supervisory and operating personnel were instructed on the system functionality and specific tasks to be undertaken, including the hazards and risks, the controls to be applied, and the job steps necessary to complete the tasks safely and correctly. Training (manuals, specifications, and instructions) covered the different job skills required, the operation's policies, applicable legislation and stan-

dards, site requirements for monitoring machine performance, and incident reporting.

All personnel successfully demonstrated evidence-based assessment of competency before working without supervision.

5.2 Access to the Autonomous Operating Zone (AOZ)

A clear visual indication of the AOZ was provided at each designated entry and exit point. The AOZ access control system was monitored, with appropriate actions in case of failure, based on safety plans and controls. Anyone entering the AOZ underwent a required AOZ induction and/or was escorted according to the risk assessment.

5.3 Mode Change Procedures

Manual to Autonomous mode change was represented and indicated to site personnel by clearly visible mode lights. Transitioning to Autonomous mode requires a series of gateways and steps, both in the vehicle or remotely (in close proximity) starting from the Manual mode to prevent a single human error from transitioning the vehicle to autonomous mode. The required steps were defined in the operating procedure for the site.

5.4 Emergency Response

All personnel must be familiar with the emergency response strategy, muster points, and emergency contacts before entering any site. Emergency response planning for autonomous operations was integrated into the comprehensive site emergency response planning.

In addition to the work procedures summarized above, reporting and communication execution, inspections, traffic management, and practices to monitor the environment were developed by SafeAI together with the site management to ensure a safe working environment for all.

6 Conclusions

Given the industry need to assess the impact of automation in construction and mining to increase safety and productivity, this document outlined a Safety Framework for comprehensive and systematic assessment of the safety hazards in Construction and Mining operations with Autonomous vehicles. The framework is mainly based on STPA, taking into account the latest approach developed for industries like automobile and aviation automation. Additionally, FMEA, and LOPA are integrated into the comprehensive safety approach. The requirements from this assessment and relevant local and international norms feed into SafeAI's product development and testing procedures.

Application of the framework into our proving ground site is provided as an example of the practices SafeAI carries out at each new mine or construction site across the world. The risk mitigation strategies addressed in this document ensure a phased approach to a fully autonomous site while taking care of the development, operations, and QA teams on the field.

In sharing this framework, our goal is to advance the industry approach to evaluate the safety of new autonomous equipment.

References

[1] Federal Aviation Administration. *Safety Risk Management Policy*, volume Order 8040.4A. U.S. Department of Transportation, https://www.faa.gov/documentLibrary/media/Order, 2012.

[2] R. A. Evans. *Engineering Design Handbook Design for Reliability*, volume AMCP-706-196. US Army Materiel Command, https://apps.dtic.mil/dtic/tr/fulltext/u2/a027370.pdf, 1976.

[3] Reactor safety study. an assessment of accident risks in u. s. commercial nuclear power plants. executive summary: main report. [pwr and bwr]. 1975. doi:10.2172/7134131.

[4] IEC. *Hazard and Operability Studies (HAZOP studies) – Application Guide. International Standard IEC 61882 (2.0 ed.)*, volume AMCP-706-196. International Electrotechnical Commission, ISBN 978-2-8322-3208-8, 2016.

[5] J.P. Leveson, N.; Thomas. *STPA Handbook*. MIT Partnership for Systems Approaches to Safety and Security (PSASS), https://psas.scripts.mit.edu, 2018.

[6] MIT. Mit partnership for systems approaches to safety and security (psass). On-line: `http://psas.scripts.mit.edu/home/`, Accessed: 12/15/2023.

[7] EMESRT. Vehicle interaction. On-line: `https://emesrt.org/vehicle-interaction/`, Accessed: 12/15/2023.

[8] On-Road Automated Driving (Orad) Committee. Taxonomy definitions for operational design domain (odd) for driving automation systems j3259. *SAE International Standards*, 2021. doi:https://www.sae.org/standards/content/j3259/.

[9] Ronald J. Willey. Layer of protection analysis. *Procedia Engineering*, 84:12–22, 2014. doi:https://doi.org/10.1016/j.proeng.2014.10.405.

[10] The National Institute for Occupational Safety and Health (NIOSH). Hierarchy of controls. On-line: https://www.cdc.gov/niosh/topics/hierarchy/default.html/, Accessed: 12/15/2023.

[11] Mining Industry Advisory Committee, Work Health, and Safety Commission. *Mine safety management system: Code of practice, Department of Mines, Industry Regulation and Safety*. Government of Western Australia, ISBN 978 1 922873 01 9, 2022.

[12] International Organization for Standardization. Earth-moving machinery and mining autonomous and semi-autonomous machine system safety. Requirements with guidance for use (ISO Standard No. 17757:2019) https://www.iso.org/standard/76126.html/, 2019.

[13] International Organization for Standardization. Safety of machinery. general principles for design. risk assessment and risk reduction. Requirements with guidance for use (ISO Standard No. 12100:2010) /https://www.iso.org/standard/51528.html, 2010.

[14] International Organization for Standardization. Safety of machinery. safety-related parts of control systems part 1: General principles for design. Requirements with guidance for use (ISO Standard No. 13849-1:2023) /https://www.iso.org/standard/73481.html, 2023.

[15] International Organization for Standardization. Earth-moving machinery. functional safety. part 1: Methodology to determine safety-related parts of the control system and performance requirements. Requirements with guidance for use (ISO Standard No. 19014-1:2018) /https://www.iso.org/standard/70715.html, 2018.

[16] International Electrotechnical Commission. Safety of machinery - functional safety of safety-related control systems. Requirements with guidance for use (IEC No. 62061:2021) /https://webstore.iec.ch/publication/59927, 2021.