Application of STPA-Sec for Analyzing Cybersecurity of Autonomous Mining Systems

Amardeep Singh Sidhu

Working Paper CISL# 2018-11

February 2019

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Application of STPA-Sec for Analyzing Cybersecurity of Autonomous Mining Systems

by

Amardeep Singh Sidhu

M.S. Mechanical Engineering

Purdue University, 2013

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

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

February 2019

Signature of Author……
System Design and Management Program
October 24, 2018

Certified by……
Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering
Thesis Supervisor

Certified by……
Allen Moulton
Research Scientist, MIT Sociotechnical Systems Research Center
Thesis Supervisor

Accepted by……...
Joan S. Rubin
Director, System Design and Management Program

The work presented here was supported, in part, by the MIT Lincoln Laboratory and the US Army under the "Study of JCIDS Semantic Architecture Framework" project. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not reflect the official policy or position of MIT Lincoln Laboratory, the US Army, or the Department of Defense.

Application of STPA-Sec for Analyzing Cybersecurity of Autonomous Mining Systems

by

Amardeep Singh Sidhu

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management
at the
Massachusetts Institute of Technology

ABSTRACT

Autonomy is seen as the next big thing in the mining industry. For mine operators there are benefits to be gained in terms of higher productivity, inherent safety, lower operational expense, and improved asset management, just to name a few. Original equipment manufacturers (OEM) and dealerships also benefit by gaining the ability to better manage machine lifecycles, adding additional revenue streams from auxiliary products and services like mine operating system (MOS), training, and contracts to run mine autonomy and automation as a service.

For this work, we have selected the autonomous haul truck used in the surface mining operation as the subject. We were motivated primarily by existing OEM efforts on introducing autonomy in the industry through hauling. Various stages of hauling process including the interaction with manually operated MOS and shovel were studied.

Systems-Theoretic Process Analysis for Security (STPA-Sec) method was applied to the loading subsystem of open pit surface mining, where the manually operated shovel and the autonomous haul truck interact. System level safety and cybersecurity hazards were identified, a functional control structure prepared, and a system state model developed. A control action of "autonomous-stop" from the shovel operator and directed towards the autonomous haul truck was analyzed to identify unsecure control actions and corresponding unsecure constraints. Extension to the STPA-Sec framework in the form of modified attack trees was applied to generate rich set of scenarios with the unsafe and unsecure control action as the attack goal. Cybersecurity requirements for the shovel and haul truck subsystem interaction were derived by analyzing scenarios and recommended mitigations.

Results indicated that the STPA-Sec with attack tree performs better than any single method from SAE J3061 based on the process, quality, and quantity of cyber-physical threats identified. In addition, STPA-Sec with attack tree filled an important gap by offering structure and traceability during scenario generation process of STPA. Future work could focus on automating STPA-Sec analysis steps where expert knowledge is not required and integrating the improved STPA-Sec as a hazard analysis and risk assessment framework under ISO26262.

Thesis Supervisors

Stuart Madnick
John Norris Maguire Professor of Information Technologies, MIT Sloan School of Management & Professor of Engineering Systems, MIT School of Engineering

Allen Moulton
Research Scientist, MIT Sociotechnical Systems Research Center

This page intentionally left blank.

ACKNOWLEDGEMENTS

This work would not have been possible without the help and support of few people. I would like thank Allen Moulton and Prof. Stuart Madnick for their guidance and support as my thesis advisors. Their encouragement and feedback have been essential in shaping this work.

I would also like to thank researchers at Vale S.A. in Brazil and the Cybersecurity at MIT Sloan Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (IC)3 for providing me a platform to share my research, sharpening me with their questions, and providing valuable feedback.

Also, important to mention is the support and guidance from Joan Rubin, Prof. Brian Moser, and students from the System Design & Management program at MIT.

Any of this would not have been possible without the love and support of my family. I would like to dedicate this work to my grandmother.

This page intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

NOMENCLATURE

AHS	Autonomous hauling system
AI	Artificial intelligence
AOZ	Autonomous operating zone
ASIL	Automotive safety and integrity level
Auto-ISAC	Automotive Information Sharing & Analysis Center
CAN	Controller Area Network
CAST	Causal Analysis using Systems Theory
CEO	Chief executive officer
CFO	Chief financial officer
CHASSIS	Combined Harm Analysis of Safety and Security for Information Systems
ConOps	Concept of Operations
DGPS	Differential Global Positioning System
DoT	Department of Transportation
ECU	Electronic Control Unit
EH	Electro hydraulic
EPA	Environment Protection Agency
EVITA	E-Safety Vehicle Intrusion Protection Application
FMEA	Failure model and effects analysis
FMECA	Failure Mode, Effects and Criticality Analysis
FMES	Failure Modes and Effects Analysis
FMI	Failure mode indicator
FMVEA	Failure Mode, Vulnerabilities and Effect Analysis
FTA	Fault tree analysis
FuSa	Functional safety
GPS	Global Positioning System
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability Study
HEAVENS	Healing Vulnerabilities to Enhance Software Security and Safety
HMI	Human Machine Interface

I/O	Input/output
IMU	Inertial measurement unit
IoT	Internet of Things
IP	Intellectual property
ISO	International standards organization
IT	Information Technology
LIDAR	Light Detection and Ranging
LIN	Local Interconnect Network
MOS	Mine Operating System
MSHA	Mine Safety and Health Administration
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OEM	Original equipment manufacturer
OPM	Object Process Methodology
OSHA	Occupational Safety and Health Administration
OT	Operational Technology
PNT	Position, Navigation and Timing
RADAR	Radio Detection and Ranging
ROI	Return on Investment
RTK	Real Time Kinematic
SAE	Society of Automotive Engineers
SAHARA	Security-aware hazard analysis and risk assessment
SC	Safety/security constraints
SecL	Security level
SoS	System of Systems
SPS	System Problem Statement
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
STPA-Sec	Systems-Theoretic Process Analysis for Security
STRIDE	Spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege

SVN	Stakeholder Value Network
SyRS	System requirements specifications
TARA	Threat Analysis and Risk Assessment
THROP	Threat and Operability Analysis
TMVA	Threat Modeling and Vulnerability Analysis
TVRA	Threat, Vulnerabilities, and Implementation Risk Analysis
UCA	Unsafe/Unsecure Control Action
VP	Vice president

1. INTRODUCTION

1.1 Motivation

Although mining is a cyclic industry with its booms and busts driven by commodity prices, mine operators have consistently pushed for greater mining automation [1]. Factors such as the need to control costs, gain operational agility and efficiency, and the need to meet safety regulations are important to mine operators. These factors have further accelerated the awareness and development of Internet of Things (IoT)-enabled mining ecosystems that meet operator requirements. The mining value chains includes the following five phases:

- Exploration
- Mine design planning & development
- Operation
    - Extraction
    - Processing
    - Transport
- Trade
- Closure

The impact of digital technologies has been felt across all activities in the value chain. While efficiency and safety at the mine site has improved tremendously due to infusion of technology, the topic of cybersecurity with respect to operational technology (OT) has received relatively little attention.

For this study, we have focused on an autonomous hauling system of systems (SoS) transforming the link between extraction and processing. Modern hauling systems are complex cyber-physical entities with numerous controllers, networks, and features that use multiple sensory inputs, actuators, and data exchange to haul ore across the mine site. Autonomy of the mining operation further adds to this complexity in a big way through additional support systems. These systems are onboard and outside the vehicle and include both hardware and software required to enable the desired autonomous functionality.

Like most modern systems, autonomous hauling systems are developed using systems engineering's requirements definition process. The purpose of a system requirements definition process is to transform the stakeholder's user-oriented view of desired capabilities into a technical view of a solution that meets the operational needs of the user [2]. System requirements

specifications (SyRS) influence the architecture, design, integration, and verification process that happens downstream. While base machine SyRS can be ported from existing manually operated haul trucks, there are substantial new requirements that need to be written for autonomy functionality, autonomy-base machine interface, system safety, and security. “Base machine” refers to the manually operated haul truck. In this study we will focus on the safety and security requirements of the autonomous hauling system (AHS). While being independent entities, safety and security also exhibit mutual dependence, where loss of security can result in loss of safety and vice versa. Traditional methods of ensuring safety and security include application of causality or chain-of-failure-event models [3] [4] such as fault trees, event trees, hazard and operability study (HAZOP), failure model and effects analysis (FMEA), and failure mode, effects and criticality analysis (FMECA).

These models focus on initial component failures or human error that cascades through a set of other components and results in an unsafe event. While suitable for simple systems, these causality models fail to account for highly complex systems [5] such as autonomous hauling system (AHS), where failure can result from unsafe and unsecure interactions between otherwise safe and secure components. Hence the challenge of developing safety and security SyRS for AHS requires a structured and holistic approach. The systems-theoretic process analysis for security (STPA-Sec) can fulfil that need. The STPA-Sec is an extension of STPA [6] and extends the accident causation model to include unsecure interactions [7].

1.2 Objectives and Approach: outcome, complexity and feasibility, comparison with current methods, and enhancements of STPA

There are four main questions, listed below, that this research study aims to answer.

1.2.1 What would be the outcome of applying STPA-Sec to the mining case?

STPA-Sec has never been applied to the mining case. Like autonomous mobility, autonomous mining is on the rise. But unlike on-road systems, mining provides different sets of challenges that are unique to this application.

1.2.2 What is the complexity and feasibility of STPA-Sec as we tackle the mining case?

1.2.3 How does STPA-Sec compare to industry-recommended cybersecurity and safety analysis methods for connected vehicles?

The Society of Automotive Engineers (SAE) recommends six methods to ensure cybersecurity in connected vehicles. The International Standards Organization (ISO) prescribes

the use of ISO26262, the vehicle functional safety standard for mechatronic systems. One of the goals of this study will be to compare STPA-Sec to SAE and ISO recommended methods.

1.2.4 Can we enhance the applicability and/or outcome from STPA-Sec?

We will go through a use case where one of the recommended methods from the SAE guidebook is combined with STPA-Sec to enhance the framework by providing better traceability during scenario generation.

STPA-Sec is a top-down systems theory approach that starts from high level safety and security losses and ends with unsafe and cyber-vulnerable scenarios which can translate directly to system safety and security requirements. There are numerous low-level goals that need to be achieved for the framework to be applied successfully. These include the following:

- Defining the mining concept-of-operations (ConOps). The ConOps serves the purpose of accurately capturing the stakeholder expectations.
- Defining hauling operation and autonomous haul truck interaction with other systems.
- Applying STPA-Sec on one part of a hauling system and understanding the complexity involved.

Detailed introduction of STPA-Sec, SAE methods, and the ISO standard will be presented in subsequent chapters.

1.3 Thesis Outline

The thesis is divided as follows:

Chapter 2 identifies the needs of the stakeholders in the autonomous hauling system, these needs are explored and value exchange between them are analyzed within the context of cybersecurity to enable prioritization of relationships. Stakeholder needs are then used to define the goal of the autonomous hauling system.

Chapter 3 presents the mining concept of operation along with hierarchical control structure, haul truck architecture, and process flow diagrams. Chapter 3 sets the sociotechnical foundation on which subsequent safety and security analysis is performed in Chapters 5 and 6.

Chapter 4 introduces major safety and security standards, frameworks, and guidelines including ISO26262, SAE J3036 including attack trees, and systems theory-based methods. A summary of literature on these standards, recommendations, and frameworks is shared.

Chapter 5 captures the application of STPA-Sec framework to the autonomous truck-shovel-dispatch subsystem.

Chapter 6 includes the process of scenario generation and requirements identification using attack trees.

Chapter 7 shares the findings from applying STPA-Sec with attack trees on the autonomous truck-shovel-dispatch subsystem. Future research directions are also explored in this chapter.

Appendix A includes a context table for an operator issuing the A-stop command. For the A-stop control command, this table captures all the autonomous truck-shovel-dispatch subsystem states. These system states are generated by the combination of process model variables and autonomous truck -shovel-dispatch functional interactions.

Appendix B includes an updated context table for an operator issuing the A-stop command. The fault inducing system states from the context table are selected and the resulting hazards are mapped by evaluating four conditions namely, “control action hazardous,” “control action hazardous if too late,” “control action hazardous if too early,” and “not providing control action is hazardous.”

Appendix C includes a table of unsafe/unsecure control actions and safety constraints. Using the updated context table and the system control structure, the unsafe and unsecure control actions and safety constraints are derived.

2. OVERVIEW OF AUTONOMOUS MINING IN THE CONTEXT OF CYBERSECURITY

Complex products such as the autonomous hauling system (AHS) are important to multiple stakeholders, each with potentially different needs and priorities. The AHS project may focus on the mine operator as its primary stakeholder, but other stakeholders such as the original equipment manufacturer (OEM) could be influencing the project as an opportunity to test new ideas, features, and services related to autonomous mining. The federal government could see AHS as an opportunity to promote for greener mining and to further improve mine safety. All stakeholders want the AHS to succeed under their differing needs and priorities. The next section focuses on systematic analysis of the needs of these stakeholders to derive the goal of the mining system. The STPA analysis typically starts with talking to the stakeholders to identifying losses, system-level hazards, and safety constraints. The process of "defining the purpose of the analysis" could be strengthened by the use of Kano methodology along with value network analysis [8] to derive what the stakeholders stand to gain and lose, instead of relying on someone's word alone. The mining system operates in a living environment with complex value exchanges based on stakeholder needs, these exchanges are the socio-economic feedback mechanism that are used in the next section to derive the purpose of the STPA analysis. The breakdown of the next section involves identification of different stakeholders involved in the autonomous mining project, prioritizing their needs, and identifying the goal of the AHS project.

2.1 Stakeholder Analysis

Consider AHS as a project that aims to create an autonomous hauling service for the mine operator. AHS project governance is assumed to be co-owned by the OEM and the mine operator. The mining system, within the context of the AHS project, can be divided into beneficiaries and stakeholders [8]. Beneficiaries are those who benefit directly from AHS. AHS produce an outcome that addresses their need. Stakeholders, those who have a stake in the AHS, have an outcome that addresses AHS needs. Stakeholder and beneficiary concepts overlap, as shown in Figure 1.

- Beneficial stakeholders receive value outputs from AHS and provide valued inputs to AHS.
- Beneficiaries that are not stakeholders are called charitable beneficiaries. They provide no returns to AHS, while they derive value from AHS.
- Stakeholders that are not beneficiaries are called problem stakeholders. These are the ones from whom AHS needs something, but there is nothing that the AHS can provide in return.

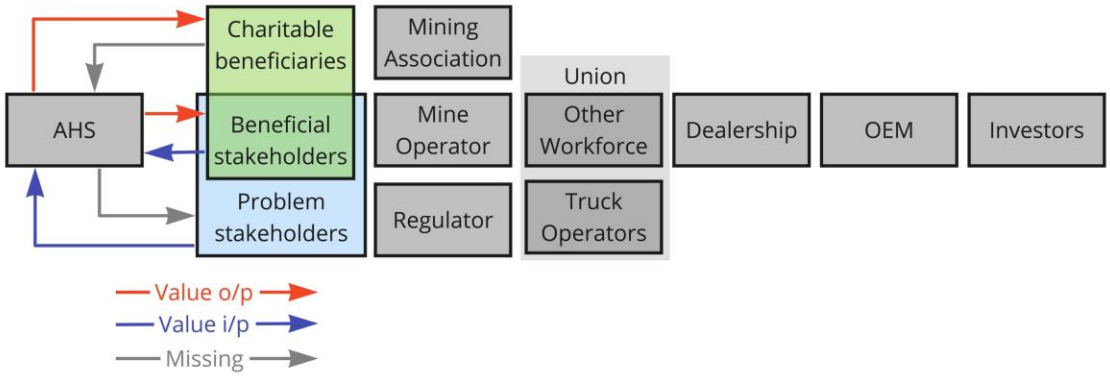

Figure 1 AHS beneficiaries and stakeholders (adapted from [8])

A mine operator is someone who controls the day-to-day operation of the mine. The mine operator takes into consideration numerous operational factors to increase or decrease production, to switch between open pit or underground mining, and to make capacity expansion decisions through technology and equipment investment. Operational factors include events and processes such as changing geology, access to resources such as water, fuel, and consumables, changes in the workforce, and commodity price fluctuations, etc. [9]. Mine operators are beneficial stakeholders because they need autonomous hauling from AHS to improve mining efficiencies. The AHS project needs a mine operator to deploy, operate, and enhance the AHS product.

The OEM develops and sells products and services used by the mine operator. In most cases, a whole catalog of mining equipment, attachments, parts, technology, and services are sold or leased by the OEM through its suppliers. Equipment includes movable machines such as drills, shovels, haul trucks, tractors, and graders. Attachments are subassemblies that connect to the equipment for added versatility or to replace broken or worn out subassemblies. Attachments include blades, winches, rippers, buckets, and more. Parts are used for repair, maintenance, and product enhancement. Technology includes add-on features and services that aid in equipment management and control. These technology offerings include, for example, fleet management systems, grading aids, spotting aids, and payload aids, to name a few. Services offered by the OEM include mine operating systems, trainings, operational safety compliance, and financial and insurance tools. With a growing need for mining efficiency from mine operators, OEMs are increasingly teaming up with preferred mine operators to accelerate the pace of concept to deployment for connected systems. OEMs are beneficial stakeholders because OEMs support AHS

through technology, knowledge, and financial support. In return, AHS provide the OEM with technology innovation, investment in the future, and revenue.

Dealerships usually act as channels between the OEM and the mine operator. Dealers serve as sources of market information and intelligence, as proxies for customers, as consultants, or as problem solvers [10], in addition to be a source of income for the OEM. In return, the OEM provides the dealer with a host of competitive products, a desired inventory of products and parts, financing and leasing options for inventory acquisition, and staff training [11]. In the AHS context, dealerships could provide local support to the project through parts and service for the base machine. In return, the dealerships gather some knowledge and exposure to autonomous hauling, and gain revenue for the hardware and services provided to the AHS project. This makes dealerships beneficial stakeholders since they receive value outputs from AHS and provide value inputs to AHS.

Mining associations are privately funded industry groups that aim to promote safe mining, represent and lobby on behalf of the mining industry, and address the policy needs of the industry including equipment manufacturers [12]. Mining associations are charitable stakeholders because they can leverage AHS as an example of efficient, safe, and environmentally friendly mining. AHS project receives no return from the mining associations that is essential to its functioning.

Unions represent the interests of the mine workforce by negotiating a safer workspace, competitive wages, and benefits [13]. Assuming the hierarchy of needs for organized labor starts with having a job, followed by benefits and safety, it is easy to imagine that the labor unions will be opposed to autonomous hauling. At the same time, it would be far-fetched to consider the unions merely as Luddites. While the AHS can result in loss of jobs for people operating haul trucks, it also provides greater safety and productivity to union members who work outside the haul truck. In other words, haul truck operators are problem stakeholders and the other workforce is a beneficial stakeholder. Haul truck operators are problem stakeholders because they are required by the AHS to test autonomy subsystems and features in haul trucks with L1-L2 autonomy level [14]. For the L3 level of autonomy, haul truck drivers could be required to intervene and perform driver backup in a timely manner.

The United States federal government regulates the mining industry through its agencies such as the Environment Protection Agency (EPA), the Department of Labor’s Mine Safety and Health Administration (MSHA) and the Occupational Safety and Health Administration (OSHA).

Laws are enacted, policies are formulated, and guidance is issued to control the impact of mining operation on air, water, and generation of asbestos, and other waste [15]. Regulations also aim to prevent death, illness, and injury from mining and promote safe and healthful workplaces for miners [16]. While it is surprising to see that cybersecurity is not on the radar for MSHA, other government agencies do facilitate industry-wide efforts to study and design best practices related to cybersecurity. The National Highway Traffic Safety Administration (NHTSA), under the Department of Transportation (DoT), leads cybersecurity efforts in the automotive industry. Mining vehicles share a lot of their technology architecture with and adhere to standards agreed upon by the automotive industry. The NHTSA, for example, recommends the use of cybersecurity best practices, and design principles published by the National Institute of Standards and Technology (NIST) and the Society of Automotive Engineers (SAE). In addition, OEMs and suppliers participate in industry associations such as the Automotive Information Sharing & Analysis Center (Auto-ISAC) for sharing cybersecurity risks and enhancing cybersecurity capabilities [17]. While none of the mining OEMs are part of Auto-ISAC, some suppliers from the mining industry do participate in the consortium. Regulators are problem stakeholders because AHS need to conform to the standards and requires their approval to function. In return, AHS provide environmental protection and a safe workplace, which are important to the regulator but not essential to its functioning.

Investors are beneficial stakeholders because they provide capital for the AHS project either directly or through the OEM and/or the mine operator. Mining is an expensive business with most of the operations run by large organizations. Due to the cyclic nature of the industry and large capital required for exploration, most of the mining companies and OEMs are publicly traded. Investors, in return, expect return on investment (ROI), strategic influence, and risk minimization.

Beneficiaries and stakeholders have needs which are product/system attributes such that the autonomous hauling system is built to meet those needs. Needs of beneficiaries and stakeholders are identified in the next section.

2.2 Needs Analysis

The needs of the beneficiaries and stakeholders are captured and represented in the format of Object Process Methodology (OPM) language [18] using the OPCAT software tool [19] and are shown in Figure 2. The symbol of a solid triangle inscribed in an empty triangle represents “exhibition.” For example, the mine operator exhibits the need for revenue, mining efficiency, etc.

Also, it is important to note that the needs are represented in decreasing order of importance to the stakeholder or beneficiary. For example, for the mine operator, mining safety is more important than mining efficiency, which in turn is less important than revenue. In other words, the mine operator does not get into the mining business to gain mining safety; instead, the primary need of the mine operator is to increase revenue, lower expenses, and maximize profit. Once the system is designed to meet that need, next in line is to ensure mining safety.

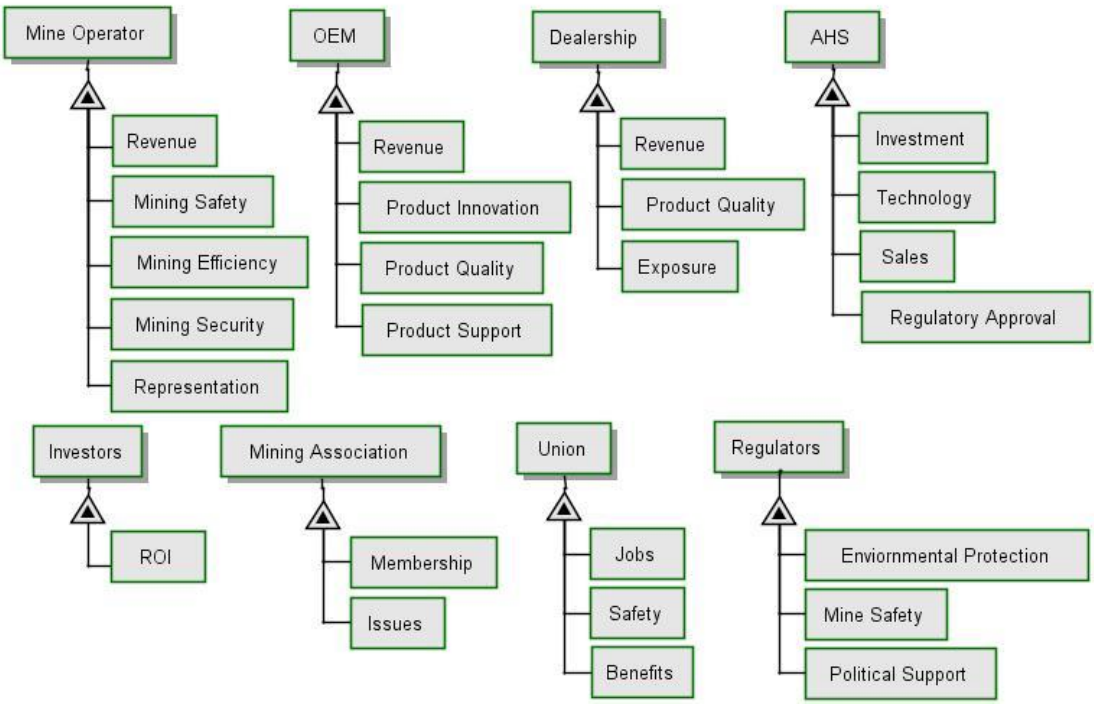

Figure 2 Stakeholder and beneficiary needs

The mine operator desires higher revenue, a good mine safety record, greater mining efficiency to increase profits, along with security related to his/her Information Technology (IT) and OT systems. The mine operator also desires representation to push for their own and industry interests at the state, national, and international level.

The OEM also desires higher revenue, technology leadership by providing innovative products and services, high product quality to improve bottom line, and good product support to improve customer satisfaction and generate ideas for product enhancement.

The dealership desires high revenue by supporting mine operators with products and services. Higher product quality is also important to the dealership because lower quality drives

too much rework and could lead to loss of customer confidence. Exposure to new and upcoming mining technology allows the dealership to plan and prepare for new products and services.

The AHS as a project desires investment of time, money, and resources from the mine operator and the OEM. A long-term need of the project is also to generate revenue for the OEM through commercialization and sale of AHS to other mine operators as a product, service, or both. AHS also need technology from the OEM and suppliers to realize its goal of implementing autonomous hauling. Regulatory approval is also needed to certify that the AHS is safe, secure, and environmentally friendly.

Investors invest in the AHS through the mining company and the OEM. Investors expect good ROI. Mining associations need membership and common issues that impact mining. Unions need jobs, followed by safe working conditions, and good benefits for their members. Regulators need the mining industry to ensure environmental protection and mine safety. In addition, regulators need political support to draft and enforce regulations. These stakeholders and their needs are interrelated. In the next section, the stakeholder and beneficiary exchanges will form a system.

2.3 Stakeholder Map

The stakeholder and beneficiary relationships are an exchange. Beneficial stakeholders produce outputs that are important to the AHS. In return, AHS provide valued inputs to beneficial stakeholders. Problem stakeholders provide valuable input to the AHS, but there is nothing that they need that can be provided by AHS in return. Charitable beneficiaries receive valued input from the AHS, but they provide no return to the AHS. Overlaying these exchanges with the individual needs identified in the previous section, a stakeholder map for the AHS, as shown in Figure 3, is created. Based on Kano methodology, the links or the value flows are divided into three types, namely- Must Have, Should Have, and Might Have [8].

- Must Haves are absolutely crucial, and their absence would be devastating.
- Should Haves are important, and their absence is bad.
- Might Haves are important, but their absence will not be a big issue.

This categorization captures the importance of a flow with regards to the successful operation of the AHS project. Must Haves originating from the OEM and directed towards AHS include sharing of technology and investment of resources: capital, human, and time. Other Must Haves for the AHS come from the mine operator and the regulator. The mine operator commits to

the AHS by investing capital, human resources, and time. Regulators provide AHS project with regulatory approval to develop, test, and deploy autonomous hauling. Must Haves flowing out of the AHS project include enhanced mine safety and efficiency for the mine operator, compliance to regulatory requirements, and at least similar or enhanced mine safety for the operational workforce involved in the AHS effort. Mine operator's compliance and regulator's approval are also crucial to the smooth operation of the AHS.

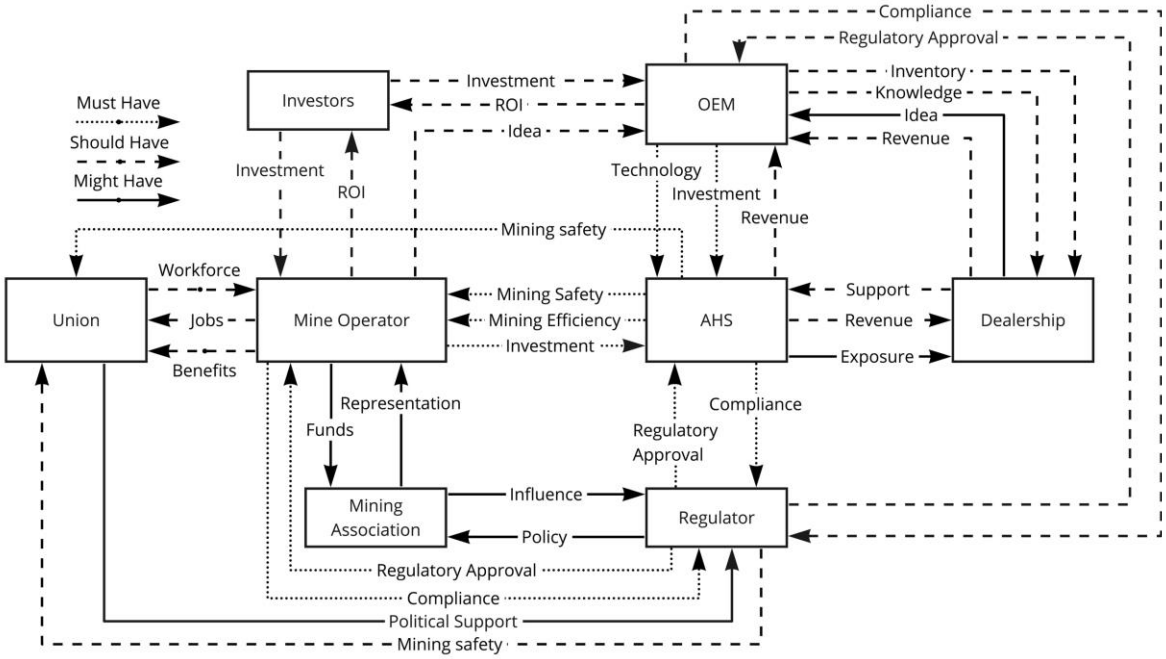

Figure 3 AHS stakeholder value network

Should Have links include revenue for the OEM from the AHS, generated through operating AHS as a service. Should Have flows between the mine operator and the union include availability of workforce from the union to the mine operator, secure jobs, and attractive benefits for the workforce. Additional Should Haves include investment into OEM and mine operators by investors for innovative projects like the AHS. Investors would also get attractive returns on their investment. The OEM requires regulatory approval for the base machine- for example, approval after meeting emission norms. The regulator would require compliance from the OEM for regulations related to the base machine and other subsystems. Dealerships make available products and part inventories along with expertise to support the AHS at the mine site. OEMs have revenue coming in from dealerships for consumables used in supporting the AHS project. A dealership generates revenue from the AHS project based on its timely support in the form of hardware,

technology, and expertise. The mine operator's feedback and ideas regarding AHS and shared with the OEM are also important and characterized as a Should Have. Regulators ensure mining safety for the workforce.

Value exchanges for Might Haves include: feedbacks and ideas for enhancement of the AHS coming from the dealership and directed at the OEM; mine operator support for mining associations; mining association representation of industry interests at the state and federal level; mining association influence on regulators and highlighting of industry issues, concerns, and success related to the AHS; regulator response with policy which benefits the mine operator, OEM, and the AHS project; dealership exposure to the AHS; and union influence on regulators through political support or lack thereof.

Impact of cybersecurity on each value link can be overlaid on the stakeholder map of Figure 3. The resulting stakeholder map gives an idea of high priority value links. Links with 'must have' connectivity along with high impact from cyberthreat are the ones that could be prioritized across the system. Figure 4 shows a representative example of a stakeholder map with overlaid cybersecurity impact information.

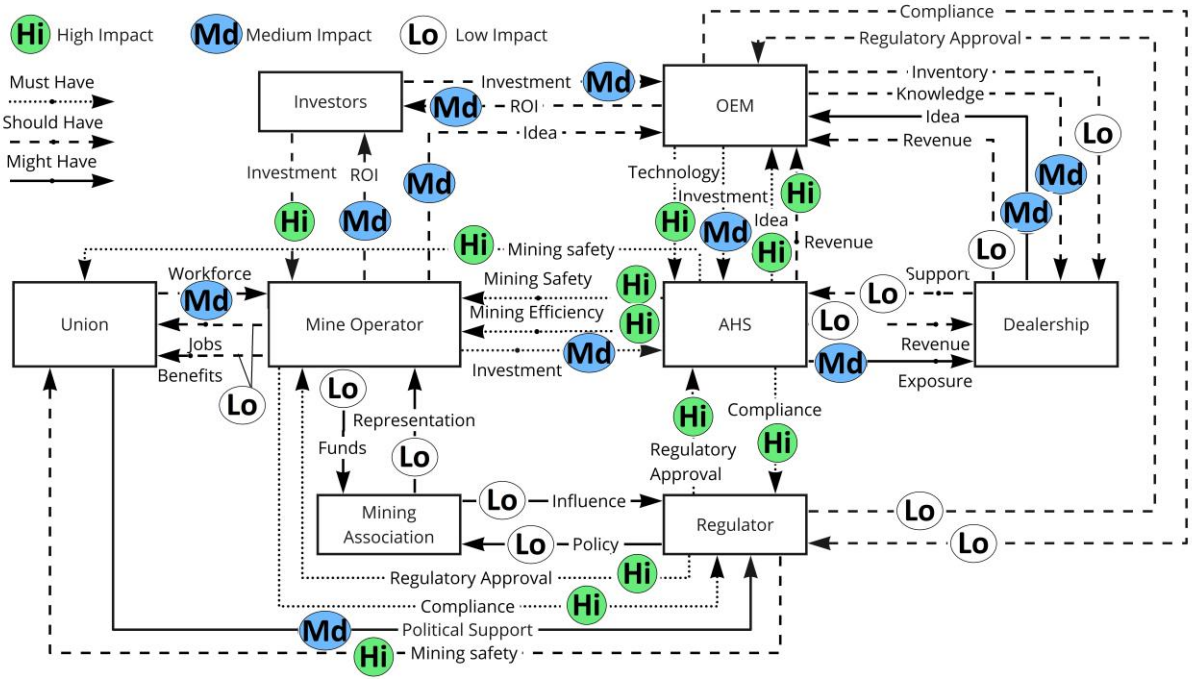

Figure 4 AHS stakeholder value network with impact of cybersecurity

The impact of cyberattacks on a mine site could manifest themselves in three possible ways, given by:

- Loss of production
- Loss of safety
- Loss of intellectual property (IP) or other critical information

These losses have high potential of impacting the mine operator. With respect to the value network from Figure 4, mine safety and efficiency value links from the AHS to the mine operator are susceptible to the impact of a cyberthreat. Technology and idea links between the OEM and the AHS will also experience high pressure to rectify and enhance the cyber-safety and security of the AHS. Since the AHS does not completely remove the need for human agents in other mining functions, mine safety value link from the AHS to the union is expected to experience high impact. Regulators in the mining industry currently do not actively monitor autonomy initiatives, but that is likely to change in the future. Cyber-initiated accidents are bound to have a high impact on regulations directed at the AHS and the mine operator. In response, compliance will also see high degree of change. To meet the expectation of the people, mining safety as a value link from regulator to union could also see high impact.

2.4 The Goal

The goal for the AHS is connected to the needs of its stakeholders. We have seen that the stakeholders have different needs, satisfied by the AHS project or other members of the mining system. We have also implemented kano methodology along with categorizing cyber impact on value exchange to filter needs that are important to the AHS. The subset of needs that should be represented by the goal of the AHS are listed below:

- Union needs safety when working with AHS project
- AHS project needs from the OEM, technology to implement AHS
- OEM needs feedback from the AHS project to innovate in autonomous mining
- Mine operator needs safe AHS
- Mine operator needs high operational efficiency
- Regulator needs mine safety and environmental protection from both the AHS project and the mine operator

Using the system problem statement (SPS) approach [8] to define a high-level goal and establish the boundary of the system, we get:

To run a safe, sustainable, and profitable mining business

By efficiently removing minerals from the earth

Using autonomous mining systems

2.5 Summary

Needs are in the hearts and minds of the stakeholder, goals on the other hand are defined by the enterprise with the intent of meeting them [8]. These two important concepts, needs and goals, are connected through stakeholders and the exchanges between them. As the system grows due to the addition of stakeholders and greater value exchanges between them, mapping from needs to goal becomes difficult. To make this process more manageable, various stakeholders and beneficiaries associated with the AHS project are identified and their motivations explored. Next step was to identify the needs of these stakeholders and beneficiaries and rank them based on importance. Value links between the players in the mining system were identified and prioritized based on a two-step method. Value links are categorized based on importance and cyberthreat impact. ‘Must Have’ links with ‘High’ impact from cyber threat are selected as high value. These high value exchanges are then used for defining the goal for the AHS.

3. CONCEPT OF OPERATION

The objective of the concept-of-operation (ConOps) is to ensure that all stakeholders fully understand the expectations and how they may be satisfied by a project, and that understanding has been agreed to by all stakeholders [20]. ConOps in the STPA context serves two objectives: first by defining the operational concept of the autonomous mining system and hence capturing in detail what is expected out of the system, and second as the source of the multiple control structures desired by the STPA analysis downstream.

3.1 Mining System

The ConOps shown in Figure 5 includes the complete mine system, of which AHS is a part. It is clearly a system-of-systems involving complex machine systems, human systems (organizations), and communication systems. Emergence in the form of greater production, safer work, increased knowledge, and connected worksite is derived from such a complex system through the set of entities and their relationships, where the combined functionality is greater than the sum of the individual.

A mine site may have one or more mine pits. Each mine pit, a group of mine pits, or the complete mine site may have its own control center that monitors and controls the mining operation in that area. Local control centers are connected with the mine operator corporate management directly and/or through the service providers. Service providers enable the processing and sharing of information related to assets on the ground.

The global positioning system (GPS) is used for ascertaining asset position navigation and timing (PNT) information anywhere on the mine. Mining operations have heavy dependence on GPS; from surveying the landscape to material removal and processing. The GPS system provides continuous global positioning capability by designing a scheme to orbit sufficient number of satellites so that four satellites are always electronically visible [21]. While the final user accuracy from GPS depends on satellite geometry, signal blockage, atmospheric conditions, and receiver design, the US Government commits to user range error of ≤ 0.715m or 2.3ft, 95% of the time [22]. Commercially available GPS systems, for example, offer final user accuracy of less than 10 meters [23].

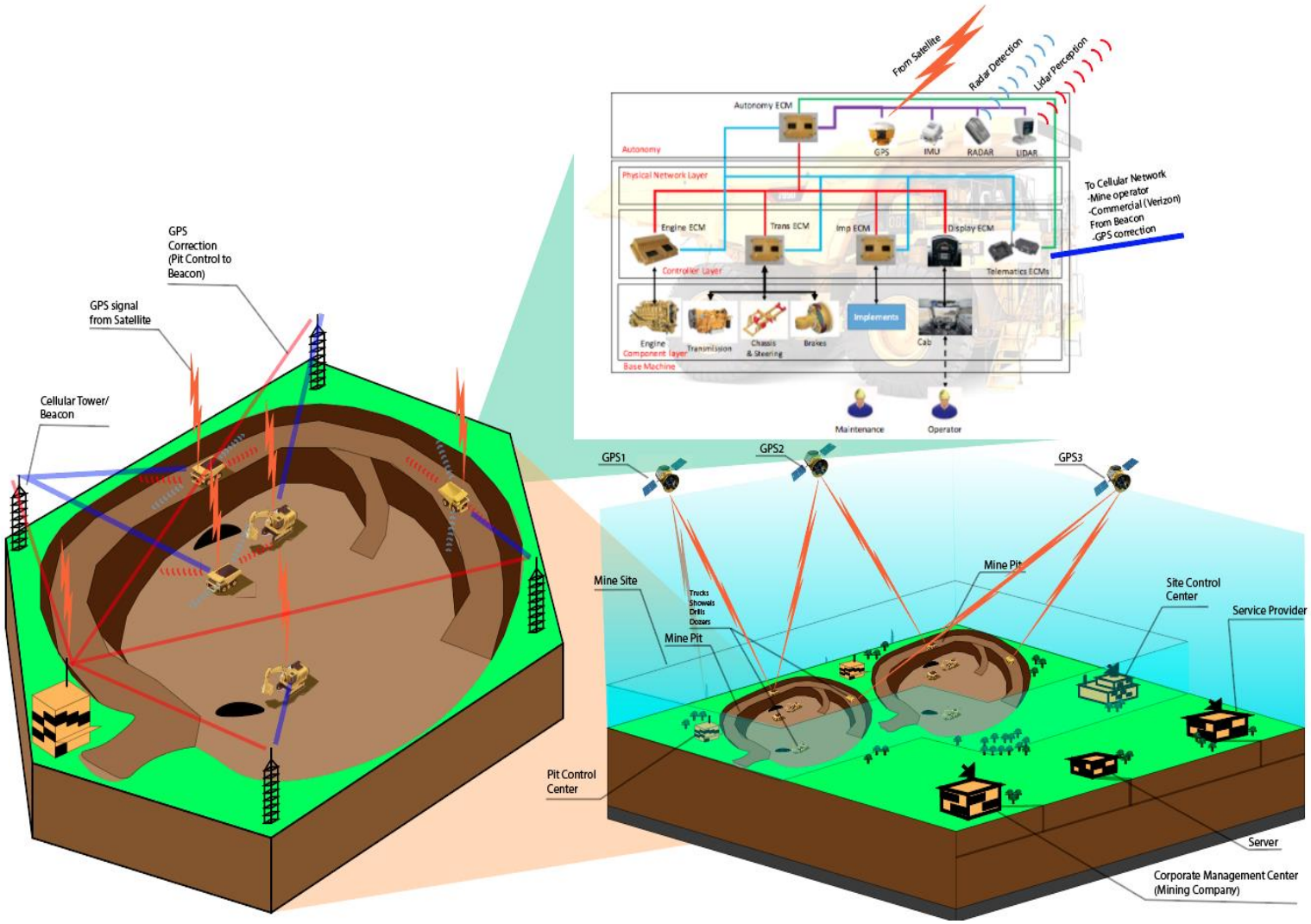

Figure 5. Mining operation ConOps

For certain applications, such as precision mining and autonomously operating machines, PNT systems with better accuracy could be desired. Differential GPS (DGPS) is one of the augmentation techniques which improves positional accuracy. DGPS requires setting up of a base station and comparing the base station's known location with the one determined using GPS satellites to deduce the error correction, which is then shared with the rover station. The distance between the base station and the rover station is limited by the requirement that both stations need to see the same constellation of GPS satellites for the correction to be accurate.

Multiple vehicles operate within a mine pit. There are drills drilling precise holes for blasting, shovels handling lose material and loading it on the haul trucks, haul trucks carry the material from the mine pit and dumping it at the dumping site. In addition, there are support vehicles such as water tankers for dust control and service trucks for onsite repair and service. Most of these vehicles have some form of onboard perception sensors that aid the driver or the autonomy controller in operating the machine. These sensors may include rear view cameras, RADARs, LIDARs and more.

The vehicle is a system with multiple controllers, actuators, sensors, and networks. There are dedicated controllers for the engine, implements, transmission, telematics, and more. Vehicle controllers accept dedicated hardware and network communication inputs through their input/output (I/O) pins. The information is processed and an appropriate control action, if required, is issued in real-time through the I/O pins connected to dedicated or network actuators. The pins are referred to as I/O because some pins on the controllers can function as both input and output, for example, controller area network (CAN) pins are used for listening, receiving, broadcasting, and addressing messages from and to other controllers and network sensors and actuators.

3.2 Command and control

The functional organization structure of the mine operator is developed based on consultation with Luis Uzeda from Vale Inc. and is as shown in Figure 6. It has the CEO at the top, followed by the vice presidents (VP) of logistics, finance, and other VP positions based on the mineral being mined.

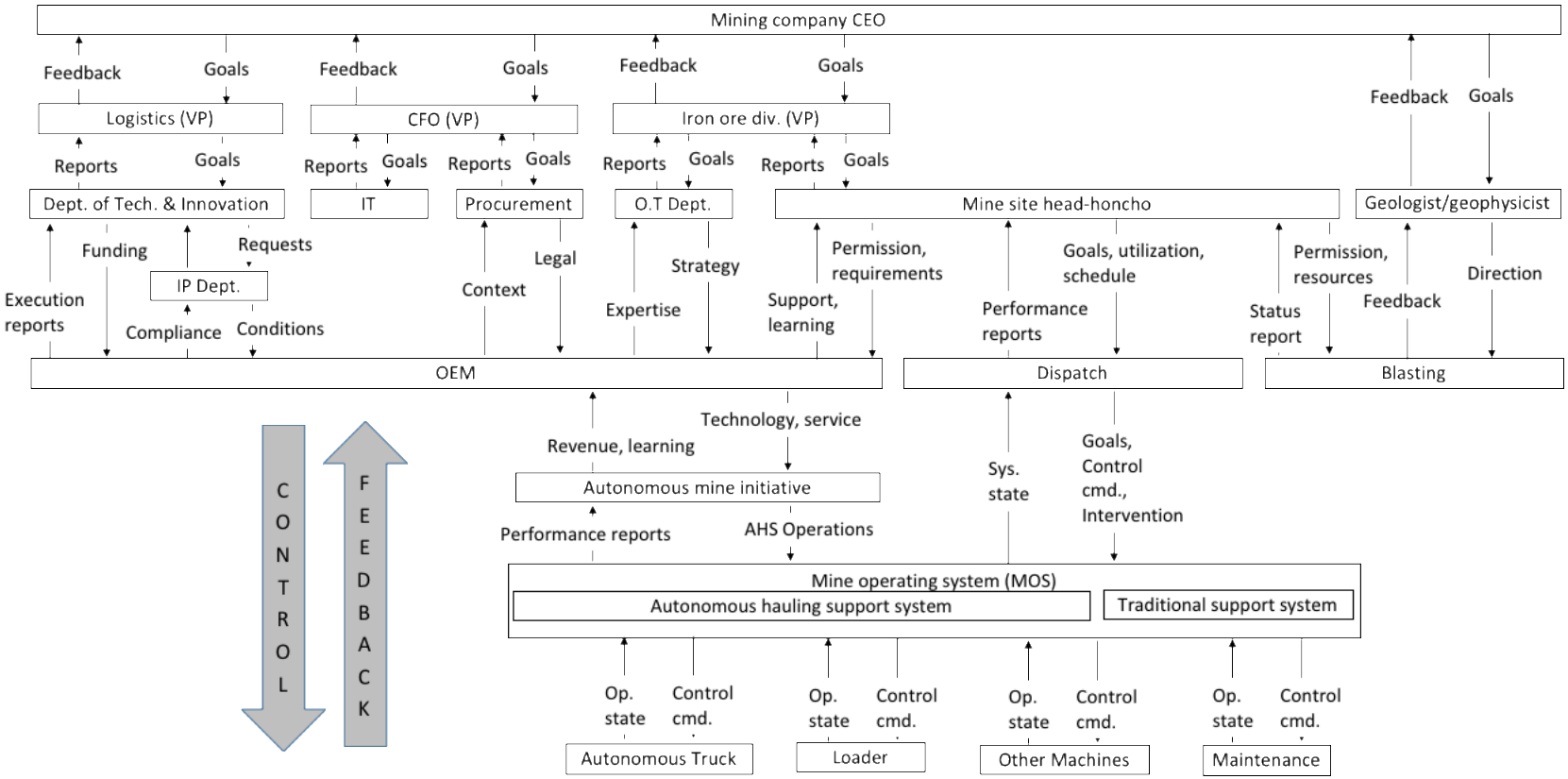

Figure 6 Mine operator organization structure

Under vice presidents are the various departments such as technology and innovation, IT, procurement, operations, and mine site head. Geologist may report directly into CEO or into a senior VP overseeing extraction of multiple mineral ores. The OEM and mine operator joint effort at autonomous mining is embedded in mine operator's functional organization structure. Different departments interact with the OEM to enable the planned implementation of AHS. Autonomous mining is mostly a joint effort from the OEM and the mine operator to develop, implement, operate, and maintain autonomy in various mining operations. Autonomous mining impacts the mine operating system (MOS), which includes equipment and software used for efficiently managing autonomous, semi-autonomous, and manually operated mining assets. Mine operation is controlled by the dispatch based on the state of mine shared with the dispatch through the MOS. Some information processing and decision making could be performed by the MOS on its own, while majority of oversight and control is performed by the dispatch. The dispatch reports into the mine site head who plans and oversees site operations such that the production targets and safety standards are met. The mine site head is also in contact with the blasting team to coordinate resources and aid in efficient blasting operation.

The mine, at any given time, employs machines with different levels of autonomy. As shown in Figure 7, there are four main ways in which these machines are controlled. First is the traditional way and involves a human operator controlling the machine based on his/her sensory inputs, mental model and training. While this control mode always requires human in the cab during operation, new machines are offering low level autonomy with assist features that aid the operator in repetitive and precision tasks. The second mode of control is the remote control (RC). In this mode, the operator is outside the machine and operates the machines through a body mounted console. The operator always maintains visual contact with the machine and receives some critical machine parameters on the console. Since RC mode is built on top of the base machine, most RC capable machines can also be operated in mode one, i.e. with operator in cab. This makes RC control functionality very attractive when machine operation with an operator in cab could be considered dangerous, for example over unstable surface for asset recovery efforts [24]. Beyond line of sight operation with the look and feel of being in a real cab is achieved through the third mode of machine control called the operator station. In this mode, the operator, sitting in an office building far away and detached from the harshness of the mining environment and machine vibrations, operates the machine. Information on machine environment and other critical

parameters is shared on a screen. The operator, based on his/her metal model and training, moves control levers, pedals, and switches to efficiently control the machine. In the fourth and final mode of machine control, the machine operates autonomously with little interruption from the dispatch. The machine is equipped with multiple sensors, PNT information acquisition devices, and digital map of the mine to aid in perception and localization. Based on the constraints, referred to as operational programming in Figure 7, mode four requires initial setup by the dispatch at the start of the shift including but not limited to motion planning. The planned motion is executed using the vehicle platform (onboard) controllers.

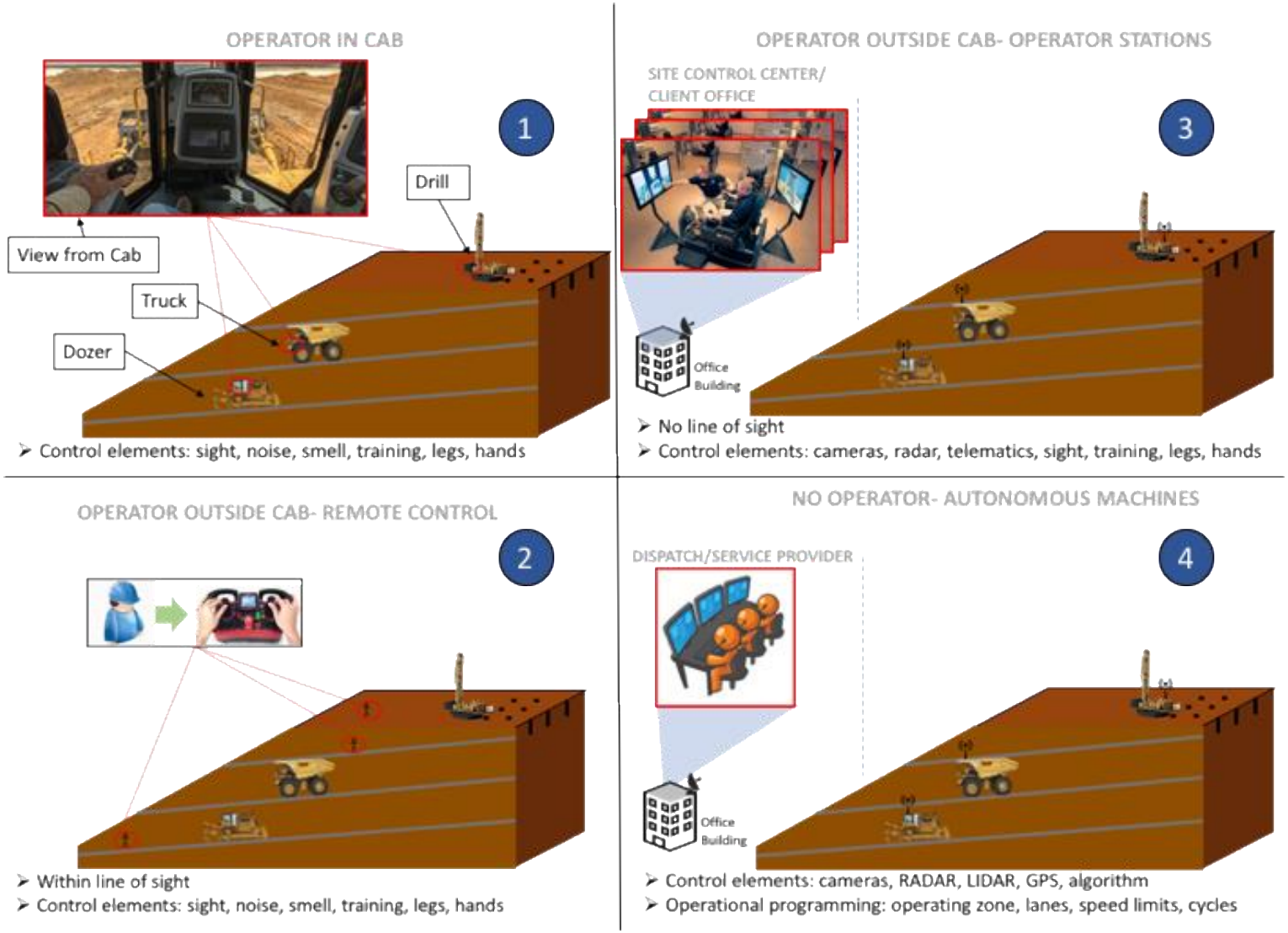

Figure 7 Machine control

3.3 Autonomous hauling function

Hauling is the operation that involves moving valuable material from the point of extraction in the mine to another point for further processing. For this study, we have assumed that the mining operation is running in a surface metalliferous mine.

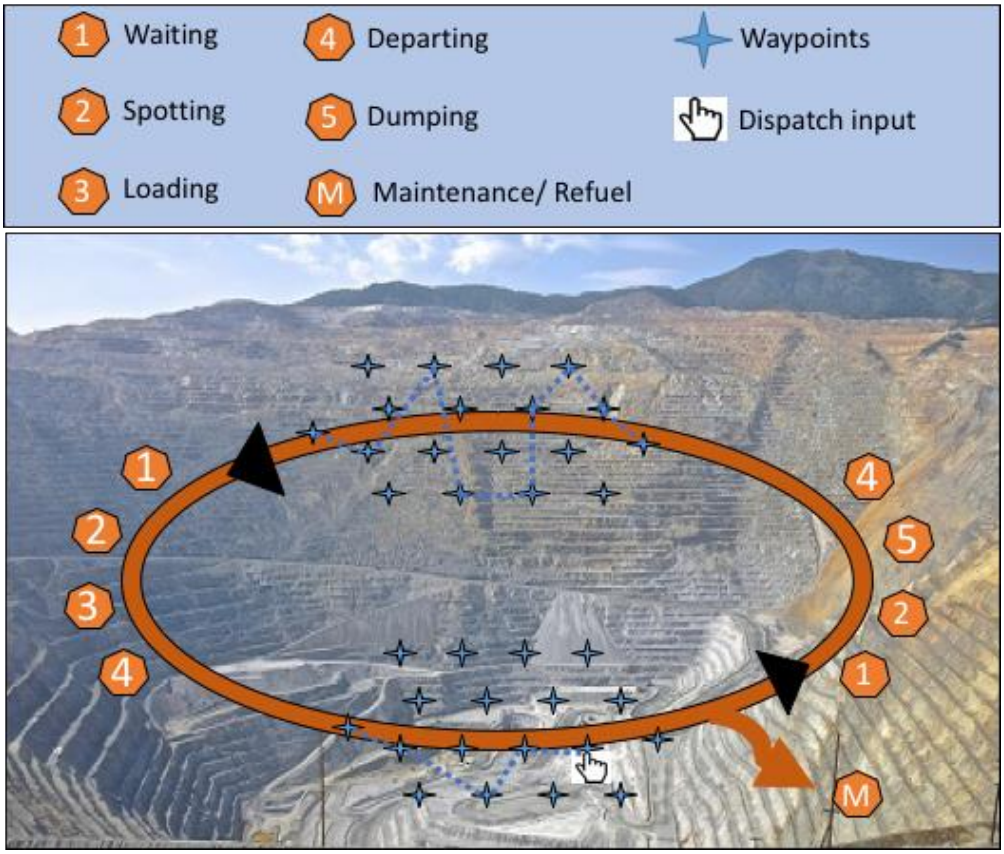

Figure 8 Hauling function ConOps (Image: Bingham Canyon copper mine, UT, USA)

The autonomous haul truck and its ConOps is as shown in Figure 8. The operation of hauling follows eight steps namely waiting, spotting, loading, departure, dumping, hauling, and maintenance/refueling. For autonomous haul trucks, all the operations listed above are performed autonomously with little or no instruction from the dispatch except under certain circumstances. The hauling sections between points four and one are either figured out by haul truck itself based on the most optimal path or it could be decided by the dispatch through "dispatch input" in the form of waypoints which the haul truck would then follow to the destination.

- Step one is called "waiting" where autonomous haul trucks wait until they are given a green light by the shovel or crusher for spotting. Shovels are mining vehicles with buckets used

for extracting material from the ground, and crusher is a processing equipment used for breaking down bigger chunks of material removed by the shovel.

- Step two is called “spotting” and it identifies the act of positioning the autonomous haul truck next to the shovel or crusher for optimal loading or dumping respectively. The OEMs offer new and innovative features such as Caterpillar’s Command Truck Spotting [25], which allow the haul truck to position itself at a particular point and in a certain orientation next to the shovel for optimal loading and process efficiency. Traditional way of spotting involves the shovel operator position the bucket above the region where he/she would like the haul truck to park and the haul truck operator would use the bucket as guide. Spotting for dumping usually takes the form of backing the haul truck perpendicular to the berm and stopping just short of the berm.
- Step three is called “loading” and involves the operation of loading the haul truck by the shovel with the material of interest. Loading objectives include optimizing the load distribution, avoiding over and under loading, and achieving optimal cycle times. The OEMs offer features that allow payload monitoring and sharing of loading trends [26].
- In the case of dumping material, the step after spotting is called “Dumping.” Given by step five in Figure 8, it involves controlled lifting of the haul truck bed to unload the material into the crusher.
- Next operation after loading is called “Departing,” given by step four in Figure 8. This is when the haul truck shifts transmission states from ‘park break applied’ to ‘forward’ or ‘reverse’ and starts to move away from shovel or crusher.
- Maintenance and refueling operation are an important step in hauling operation. One of the selling points for autonomous hauling is the ability to predict equipment wear, and hence gaining the ability to better plan machine maintenance.

3.4 Autonomous hauling vehicle system architecture

The literature on autonomous hauling vehicle system architecture is scarce, but there are elements in any autonomous system that are essential to meeting the goal of autonomy. Hence it will be safe to assume that the autonomous haul truck shares some of its autonomy architecture with the on-road autonomous vehicle prototypes. Additional information regarding required hardware and software components for the haul truck autonomy are derived from two sources. First are the mining OEM and supplier patents, and second from literature on the system

architecture for autonomous on-road vehicles. An inferred architecture of the autonomous haul truck is as shown in Figure 9.

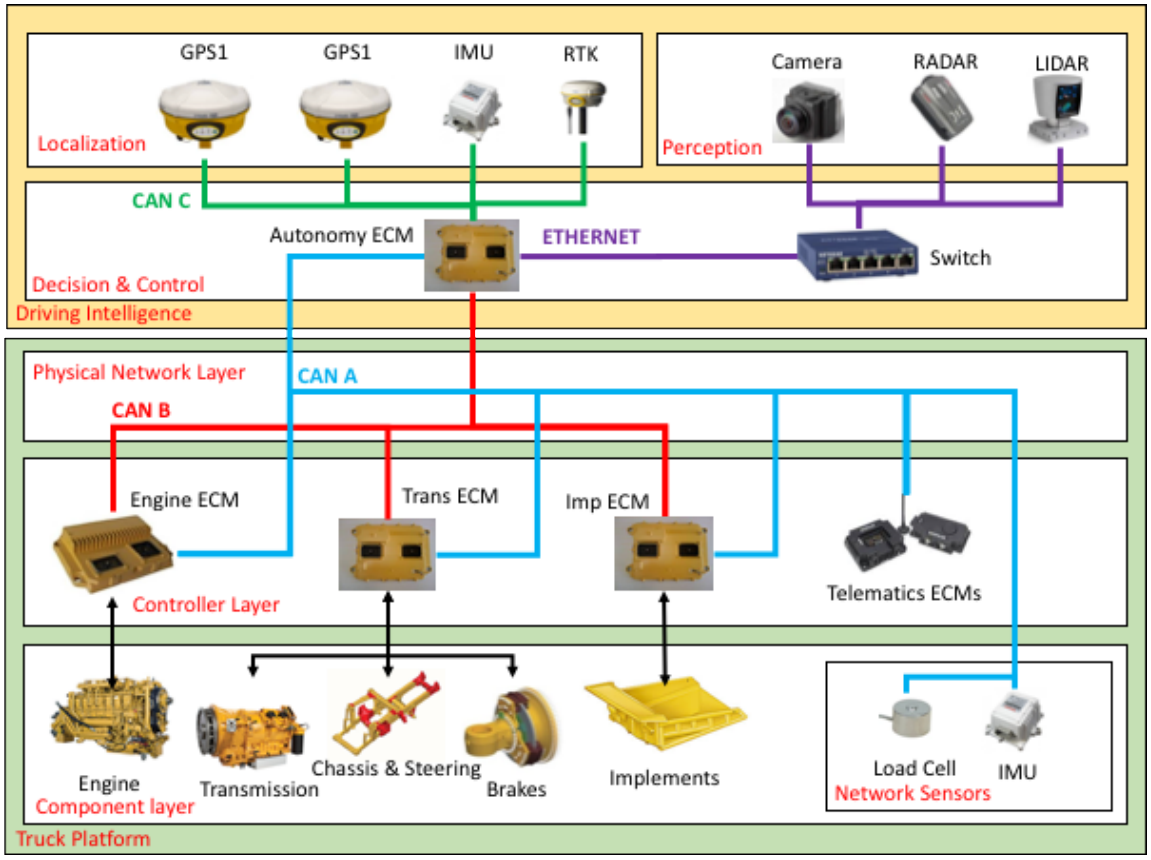

Figure 9 A system architecture for autonomous hauling

The Figure 9 is motivated by one possible system architecture for autonomous vehicle derived qualitatively by Bhere & Torngren [27]. This architecture stresses the use of clean division between vehicle platform and driving intelligence as a method for managing complexity. The electro-hydraulic haul truck platform has been in existence for some time now and does not need an in-depth explanation of its parts and their functionality. For the sake of completeness, a summary of the haul truck platform is being provided instead. The haul truck platform consists of the component layer, controller layer, and the physical network layer. The component layer includes subsystems such as the engine, transmission, chassis and steering, brakes, implements, and the network sensors. Implements in the case of a haul truck means the truck bed, which can be raised or lowered for dumping and loading respectively. The network sensors are physically mounded on components such as the chassis and the truck bed, and they transmit signals of interest over one or more networks. There are other sensors, not shown in Figure 9, that are mounted on

the components and are connect directly to the electronic control units (ECUs). The controller layer includes all the controllers used for controlling the components based on sensor input, world model, and control logic. The controller layer also includes telematics ECU that don't control a physical device, rather they allow storage and transfer of haul truck critical parameters to stakeholders through satellite or cellular channels. Physical network layer includes transmission medium running different communication protocols such as controller area network (CAN), automotive Ethernet, and local interconnect network (LIN) [28].

The driving-intelligence replaces the driver and the need for a human-machine interface (HMI) and a cab, by including components that fall under the category of localization, perception, and decision & control. The ability to perform localization gives haul truck the power to ascertain its location using the GPS receivers, inertial measurement units (IMUs), and real time kinematic (RTK) receivers. Raw or processed signals from these sensors and receivers is shared with controllers using one or more datalinks. Perception components include multiple cameras, RADARs, and LIDARS with different range capability. Due to the requirement for high update rate and greater volume of data transfer, raw or processed signals from these sensors could be shared with the controller using the Ethernet protocol. Controllers under decision and control perform four important tasks namely sensor fusion, localization, semantic understanding, and decision & control [27]. These tasks are further elaborated below:

- Sensor fusion is the process of using signals from multiple sources such as cameras, RADARs, and LIDARs to generate an image of the haul truck's environment. In addition, sensor fusion could also detect and track objects in the environment around the haul truck.
- Localization task uses the information from the GPS receivers, along with inertial navigation from the IMU, and corrections from the RTK to generate a set of highly accurate location, speed, and direction information.
- Semantic understanding task focuses on perception. It could include classifiers for detected objects, predict future behavior of detected objects, detect ground planes, drivable areas, and haul road geometries.
- Decision and control task include generation of a set of obstacle free trajectories, selection of optimal trajectory, generating propulsion, steering, and braking commands, diagnosis and fault management, reactive control, and addressing dispatch requests. Current mine

maps are also made available to the onboard autonomy controller by the dispatch for decision and control.

3.5 Summary

In this section we introduce the mining ConOps as the foundation for cybersecurity analysis to follow. The high-level mining system-of-systems was defined and we zoom-in two levels down to first look at the mine pit and then at the mining vehicle. The mine operator functional architecture was identified along with the changes that autonomous mining initiative brings to the chain of command. Autonomous hauling operation at the vehicle level was defined. One potential system architecture of the autonomous haul truck was shared, and various components identified, and tasks defined.

4. LITERATURE REVIEW

The safety and security of occupants and other road users is an important topic for automotive industry and regulators. Multiple frameworks, guidelines, standards, and best practices have been developed to ensure safety and security of both OT and IT in the automotive domain. In this chapter the focus will be on a popular automotive safety framework called ISO26262, a relatively new framework based on systems theory called STPA, and an automotive safety and security guideline called SAE J3061.

4.1 ISO26262 Road Vehicle Functional safety

The ISO26262 is a functional safety standard for electrical and/or electronic (E/E) systems used in road vehicles. It is derived from IEC61508, which is a functional safety standard for electronic, electronic, and programmable electronic safety systems applicable across various industries. ISO26262 introduces safety activities that influence all stages of E/E product, namely concept development, product development, and production and operation. The concept phase is arguably the most important phase since the foundation for the resulting system safety is set here through functional safety requirements. In addition, the concept phase is most comparable to other methods and frameworks under review in this section because the output form concept phase are functional requirements. There are four parts to the concept phase of E/E product development using ISO26262 [29]. The four parts to the concept phase are as shown in Figure 10.

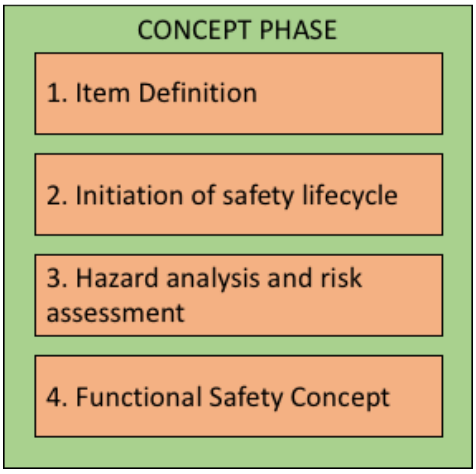

Figure 10 Concept phase of ISO26262

4.1.1 Item definition

The “item definition” part of concept phase involves item definition and description along with identifying its dependencies and finding interactions with environment and other systems.

The “item” is defined as the system or system-of-systems implementing a function at the vehicle level. For consistency and comparability with other methods and frameworks, the word “system” shall be used in place of “item” for rest of ISO26262 review.

4.1.2 Initiation of safety lifecycle

The “initiation of safety lifecycle” part of concept phase includes finding out if the item requesting development is a new item or an old item requesting modification or change of environment. If found to be a new item, next step will be to perform the hazard analysis and risk assessment. In the case of an older idem seeking modification or change of environment, the applicable lifecycle sub phases and activities are determined.

4.1.3 Hazard analysis and risk assessment (HARA)

HARA allows the identification and categorizations of hazards resulting from malfunctioning item and aids in deriving safety goals for prevention of hazardous events and avoid unreasonable risk [29]. Application of HARA involves implementing the following four steps:

- Situation analysis and hazard identification
- Classification of hazardous event
- Determination of ASIL and safety goals
- Verification

4.1.3.1 Situation analysis and hazard identification

The situation analysis part involves defining operational situations and operating modes in which system malfunction will result in a hazard. This includes both intended and unintended use of the vehicle. The standard recommends performing system level hazard identification using activities such as brainstorming, checklists, quality history, FMEA, and field studies. Some important requisites for hazard analysis include:

- Hazard definition needs to be in terms of condition or behavior that can be observed at the vehicle level
- Elements outside the system boundary are assumed to be functioning correctly
- Combination of operational events can result in a hazard
- Consequences of a hazard needs to be identified

4.1.3.2 Classification of hazardous event

Hazards are classified based on severity, exposure, and controllability. Severity is with respect to degree of potential harm to vehicle occupants and other people potentially at risk. There are 4 classes of severity given by:

- S0- no injuries
- S1- light and moderate injuries
- S2- severe and life-threatening injuries (survival probable)
- S3- life threatening injuries (survival uncertain)

Hazard exposure is identified through choice of a probability of exposure class. There are 5 classes for exposure given by:

- E0- incredible
- E1- very low probability
- E2- low probability
- E3- medium probability
- E4- high probability

Controllability captures the level of controllability of a hazard event by the driver or other people at risk. Classes of controllability are given by:

- C0- controllability in general
- C1- simply controllable
- C2- Normally controllable
- C3- difficult to control or uncontrollable

Each identified hazard is assigned a class from severity, exposure, and controllability.

4.1.3.3 Determination of ASIL and safety goals

ASIL stands for the automotive safety integrity level and is composed of 4 levels to specify the system or component level necessary requirements of ISO26262 and safety measures that need to be applied for avoiding unreasonable residual risk [29]. The four ASILs are defined as ASIL A, ASIL B, ASIL C, and ASIL D, where ASIL D is the highest safety integrity level and ASIL A is the lowest. With predetermined severity, exposure, and controllability class information for a given hazard, ISO26262 provides a mapping arrangement to ascertain the appropriate ASIL level.

Safety goal is determined for each hazard with an ASIL level. Safety goals are high level safety requirements which lead to function safety requirements in the next part of the concept phase.

4.1.3.4 Verification

Verification checks for completeness and correctness are performed on hazard analysis and risk assessment of the system.

4.1.4 Functional safety concepts

Functional safety concepts aim to use the safety goals and convert them to functional safety requirements and assign them to architectural elements of the system. A preliminary system architecture is desired in this step, which can come from dominant architectures in the industry or from existing vehicle architecture after accounting for additional architectural elements that could fulfill the new mission of the vehicle.

4.1.4.1 Functional safety requirements-

Functional safety requirements are derived from safety goals, while considering operating modes, fault tolerant time interval, safe states, emergency operation interval, and functional redundancies. The use of FMEA, FTA, and HAZOP is also recommended to generate a complete set of functional safety requirements.

4.1.4.2 Allocation of functional safety requirements

Functional safety requirements are assigned to the elements of the preliminary system architecture. Directions are also provided for dealing with special cases such as, multiple requirements for a single architectural element, reliance on elements of other technology outside the system boundary.

4.1.5 Literature on ISO26262

ISO26262 is by design a safety standard and hence lacks in its ability to address security concerns of a connected vehicle. Extensions to ISO26262 to account for this gap can be found in recent literature [30].

Macher et al. [31] address this issue by combining automotive HARA method with security domain STRIDE threat model to develop a new method called the security-aware hazard analysis and risk assessment (SAHARA). STRIDE is a threat modeling approach applied to software systems and developed at Microsoft Inc. [32]. Security threats are identified using the STRIDE approach. The authors propose a scoring system like ASIL, called security level (SecL). SecL

considers three factors, namely resources required to exert a threat, knowledge required to pose a threat, and threat criticality. Security threats identified to have impact on system safety are further analyzed using HARA. While the authors do not clearly specify what to do with security only threats, it is assumed here that security threats independent of safety could be addressed by determining associated security goals, functional security requirements, and their allocation to architectural elements.

Ward et al. [33] address this issue of limited scope of ISO26262 with respect to cybersecurity by proposing a new unified approach to vehicle security and cybersecurity. Elements from the e-safety vehicle intrusion protection application (EVITA), namely privacy, financial, operational, and safety impact of a cyber-attack are considered, and severity level is evaluated for each. Attack potential is evaluated based on expert judgement of the vehicle system and the effort required to launch an attack. Using combined severity score, attack probability, and controllability as inputs to the risk graph, a risk classification on the same lines as ASIL is obtained. The security risk level can then be used for developing appropriate cyber-security integrity and functional safety requirements.

4.2 Systems Theory Based Framework

Safety under system theory is considered an emergent property dependent on interactions between system components operating within an environment. As a result, safety can be managed when such interactions are controlled efficiently by enforcing safety constraints. Under systems approach to functional safety, accidents are attributed to interactions between system components that violate safety constraints. Safety is viewed as a control problem, where efficient control of safety constraint is essential to maintain system safety. Security needs are addressed by identifying associated security and safety constraints and designing control strategies for them. There are two parts to the systems theory-based framework for safety and security. First part helps with system modeling, while the second part of the analysis helps with hazard analysis and risk assessment.

4.2.1 System Modeling using STAMP

STAMP stands for the systems-theoretic accident model and process and is a top-down accident causality model based on the concepts of safety constraints, hierarchical control structures, and process models [34]. The basic control loop resulting from STAMP model is as shown in Figure 11.

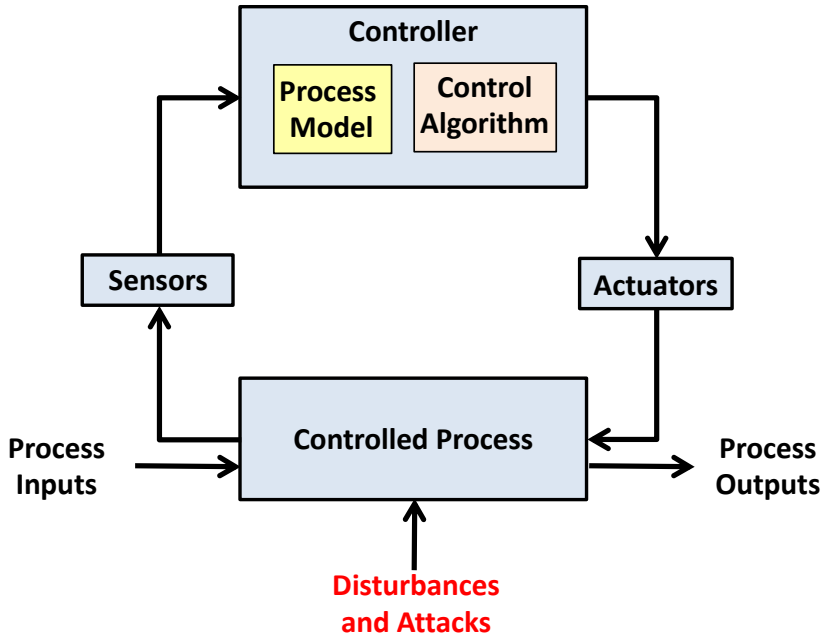

Figure 11 Basic control loop [39, 34]

Key attributes of the STAMP model and the basic control loop include:

- Safety constraints are system property that depend on design decisions. Lack of enforcement of safety constraint leads directly to events that result in losses.
- Hierarchical control structure involves representing the socio-technical system as a combination of hierarchical levels, where each level influences the activity of the level below it. This is shown in Figure 11 as controller and controlled process. Control processes are active between these levels and are tasked with implementing appropriate safety constraints on levels immediately or few rungs below. Implementation of safety constraints is accomplished through actuators.
- Process models are integral to all controllers trying to control for safety constraints in a hierarchical control system. A process model requires information on the relationship between system variables, current state of system variables, and the ways in which a process can change state. Based on the feedback from the level below and external inputs, a process model aids in determining the control actions that need to be taken such that the safety constrains could be maintained.

STAMP model was introduced in 2004 by Leveson in [35] [36], and was developed as an alternative to traditional hazard analysis techniques that focused on component failure alone and

were inept at addressing hazards originating from component interactions, and complexity added by human decisions and software. The STAMP model finds application as the foundation for two subsequent analysis called CAST and STPA. CAST stands for the causal analysis using system theory and is a look back analysis that aims to identify inadequate control that caused an accident. STPA is an acronym for the system-theoretic process analysis and is a system safety design analysis that aims to identify inadequate control that could cause an accident.

4.2.2 Hazard Analysis using STPA-Sec

STPA is a hazard analysis technique that identifies a comprehensive set of accident scenarios by focusing on the component design, interactions, human decision making, and social, organizational, and management factors [34]. STPA-Sec is an extension of STPA that supports security analysis in addition to the finding scenarios that could lead to loss of system safety [3] [37]. STPA is a four-step process, as shown in Figure 12.

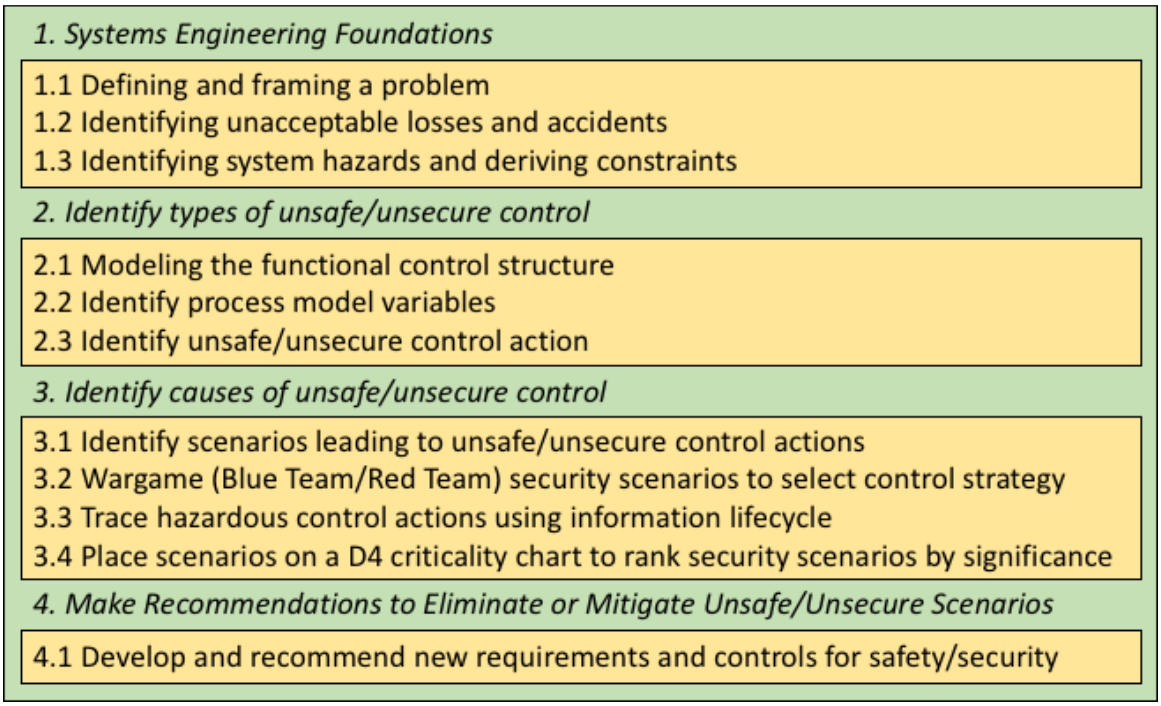

Figure 12 STPA-Sec process steps [38, 40]

4.2.2.1 System engineering foundations

First step involves defining the purpose and goal of the system, identifying unacceptable losses and accidents, and identifying system hazards and derive constraints. Three parts to the first step are further explained below:

4.2.2.1.1 Defining and framing the problem

Defining and framing the problem involves answering following questions:

- What is the intended purpose of the system?
- How does the system achieve that purpose?
- Why does the system do what it says it does?

4.2.2.1.2 Identifying unacceptable losses and accidents

Accidents in the traditional STPA setting included, for example, loss of human life or injury. STPA-Sec allows expanding the scope by including losses which do not result in any physical harm. For example, loss of intellectual property or loss of production are allowed under the new security framework.

4.2.2.1.3 Identifying system hazards and deriving constraints

Hazards occur when certain system states combine with a set of worst-case environmental conditions [38, 39], leading to losses and accidents. Hazards can be controlled either at the design stage or during operation, with preference given to the former. Safety and security constraints relate directly to the identified hazards. As identified earlier under STAMP, these constraints are enforced by the controllers to avoid the hazards.

4.2.2.2 Identify types of unsafe/unsecure control

This step involves modeling the functional control structure, identify process model states, and identifying unsafe/unsecure control actions.

4.2.2.2.1 Modeling the functional control structure

The functional control structure representation of a system, also called the hierarchical control structure representation, involves representing the system as layers of controllers and controlled process connected through control actions and feedbacks. Controlled process could further act as controller for process downstream.

4.2.2.2.2 Identify process model variables

The process model variables capture the information that is required by a controller to determine a control action that needs to be provided. The set of process model variables change based on the control action and the control loop under study, hence they are dependent on the functional control structure. The process model variables can have different operational states depending on the process.

4.2.2.2.3 Identify unsafe/unsecure control action

Each of the control actions identified in the functional control structure along with different combinations of process model variable states are evaluated against four conditions to find out control actions that could result in a hazardous situation and ultimately unacceptable loss and accident. These four conditions are given by:

- Not providing control action causes hazard
- Providing control action causes hazard
- Incorrect timing or order of control action causes hazard
- Control action stopped too soon or applied too long results in hazard

Within the resulting universal set of contextual control actions not all control actions are hazardous. Based on expert judgement, a smaller set of control actions called the unsafe/unsecure control actions (UCA) is created which are found to result in unsafe/unsecure situation.

4.2.2.3 Identify causes of unsafe/unsecure control

Third step in the application of STPA-Sec involves tracing UCAs by identifying scenarios leading to unsafe/unsecure control actions, wargaming security scenarios to select a control strategy, using the information lifecycle to trace hazardous control actions, and by ranking security scenarios based on severity.

4.2.2.3.1 Identify scenarios leading to unsafe/unsecure control actions

The scenario generation process divides the control loop into two parts. The first part tries to answer the question: why would unsafe control action occur? At the same time focusing on the sensors, controller, and any other element leading into the controller.

The second part tries to answer the question: why would control actions be improperly or not executed? This time the focus will be on the actuator, controlled process, and any other elements leading into the controlled process [6]. This division of the basic control loop is shown by the dashed line in Figure 13. Also shown in Figure 13 are the common modes of safety and security (in orange) failure that result in unsafe and unsecure control.

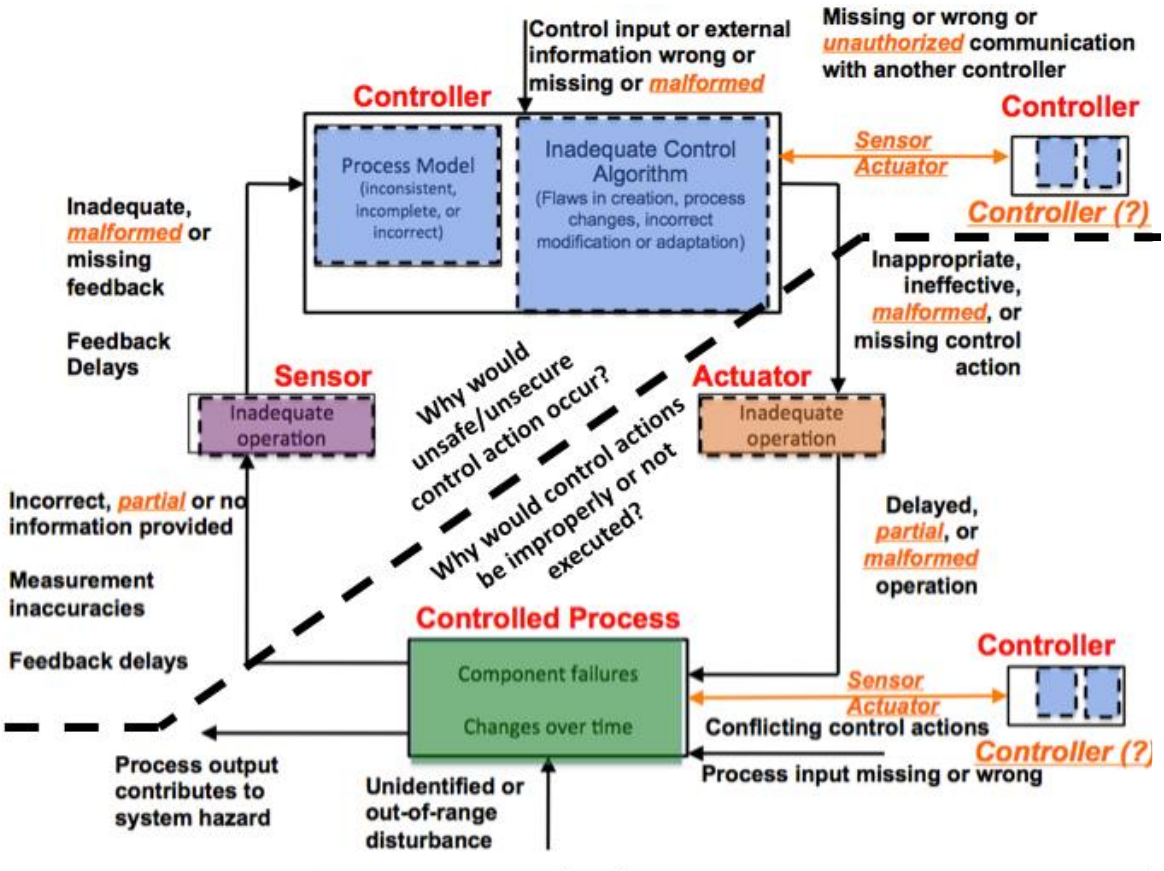

Figure 13 Control loop with safety and security scenario generation aid [40, 34] (from Young)

4.2.2.3.2 Wargame (Blue Team/Red Team) security scenarios to select control strategy

Wargaming is used as an aid in generating security related scenarios [40]. Blue team is tasked with designing enforcement strategy for security constraints identified earlier. Red team designs attacks to violate those constraints. Each hazard scenario is evaluated under three considerations:

- What strategy was designed to enforce the security constraint?
- What is the cost of implementing that strategy?
- How did the strategy fare against attacks?

4.2.2.3.3 Trace hazardous control actions using information lifecycle

Information lifecycle is a scenario refinement technique that focuses on information dependencies and how particular attacks could leverage them to disrupt mission performance [40]. The six stages of information lifecycle are given by- generation, processing, storage, communication, consumption, and destruction of information. Components involved in each of

the identified hazardous control action are evaluated for vulnerabilities especially when performing one or more stages of information lifecycle.

4.2.2.3.4 Place scenarios on a D4 criticality chart to rank security scenarios by significance

The D4 critically chart [41] is a framework for ranking security scenarios according to their extent and duration of impact on mission performance [40]. The chart is as shown in Figure 14.

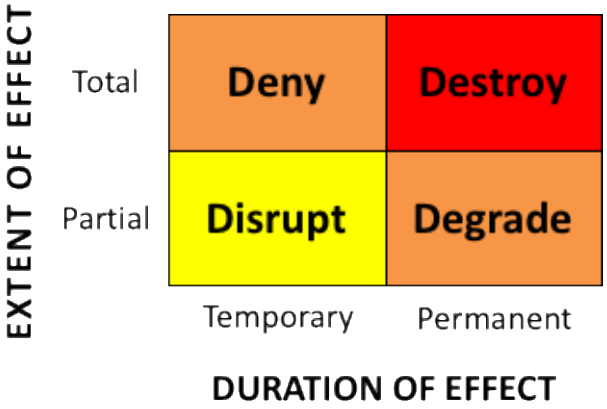

Figure 14 D4 criticality chart [41, 40] (from Young)

Ranking of STPA-Sec generated security scenarios according to D4 criticality allows the analyst to map system damage to mission failure. In addition, D4 filter can be employed to further rank scenarios on duration and extent of impact.

4.2.2.4 Make Recommendations to Eliminate or Mitigate Unsafe/Unsecure Scenarios

Preceding steps result in a ranked set of safety, and security scenarios. In this step of the process, recommendations are made to eliminate or mitigate unsafe/unsecure scenarios.

4.2.2.4.1 Develop and recommend new requirements and controls for safety/security

Based on the stage of the system architecture, whether it is conceptual or operational, recommendations for new requirements are made. These new requirements aim to alter and/or better control existing and new safety and security constraints.

4.2.3 Literature on systems theory-based framework

Since its introduction in 2013, STPA-Sec has been applied in various industries and its performance compared with other security frameworks. Recent literature on STPA-Sec and its application on complex systems is shared below:

Lee [42] compares STPA-Sec with Combined Harm Analysis of Safety and Security for Information Systems (CHASSIS). The CHASSIS framework for safety and security uses use-cases

and sequence diagrams to run safety and security assessment and generate mitigation measures. STPA-Sec is found to identify additional hazards and aid in generating better requirements. The author also recommends a hybrid method where CHASSIS is used for information lifecycle management and STPA-Sec is used for safety and security analysis.

Kriaa et al. [43] compare STPA-Sec and other methods for their strength and weakness in analyzing safety and security for industrial control systems. Methods were compared on their applicability in development vs. operational phase of a system and qualitative vs. quantitative results. STPA-Sec was found to be suitable for development phase of a system; resulting in macroscopic and qualitative results.

STPA-Sec was applied on the automotive battery management system by Schmittner et al. [44]. The authors suggest improvements to STPA-Sec by considering attacks on controller process model and control algorithm. In addition, factoring of specific attack vectors is recommended. Results from this study include support for STPA-Sec's suitability during development phase of a system, the need for complimentary methods to fill the gaps, and questions were raised regarding ease of applying STPA-Sec on large and complex systems.

Friedberg et al. [45] propose a new framework called STPA-SafeSec for integrated safety and security analysis. The STPA-SafeSec framework claims to address the shortcomings of STPA-Sec by implementing four improvements given by: allowing both safety and security analysis, inclusion of security losses that are independent of safety, extension of causal factors from safety to security domain, and a method to link the control structure to physical system design to integrate the results from traditional security analysis methods.

A hybrid model integrating the systems-theoretic and component-centric analysis was proposed by Temple et al. [46]. Combination of STPA-Sec and failure mode, vulnerabilities and effect analysis (FMVEA) is recommended such that the scenarios from systems-theoretic analysis (STPA-Sec) could be prioritized and managed using component-centric analysis (FMVEA).

4.3 SAE J3061 Cybersecurity Guidebook Methods

The SAE J3061 cybersecurity guidebook for cyber-physical systems is a recommended practice that establishes a set of high-level guiding principles for cybersecurity as it relates to cyber-physical vehicle systems [47]. The guidebook describes some techniques for threat analysis, risk assessment, threat modeling, and vulnerability analysis. These techniques are listed below:

- E-Safety Vehicle Intrusion Protection Application (EVITA)

- Threat and Operability Analysis (THROP)
- Threat, Vulnerabilities, and Implementation Risks Analysis (TVRA)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS)
- Attack trees

and further described in detail below.

4.3.1 E-Safety Vehicle Intrusion Protection Application (EVITA)

EVITA framework is a three-step process which starts with threat and risk identification through brainstorming attack trees with emphasis on operational, safety, privacy, and financial objectives, followed by identification of cybersecurity goals from threats and risks. The risk assessment method HARA is then used to prioritize threats according to risk level.

In EVITA the starting assumption is that the system is already defined in function and/or form and is available to the team applying the method. The EVITA objective and process flow is shown in Figure 15. There are four cybersecurity objectives, namely operational, safety, privacy, and financial. The operational objective aims to maintain the intended operational performance of all vehicle and its functions. The safety objective aims to ensure the functional safety of the vehicle occupants and other road users. The privacy objective aims to protect the privacy of vehicle drivers and IP of the vehicle manufacturers and their suppliers. The financial objective aims to prevent fraudulent commercial transactions and theft of vehicles.

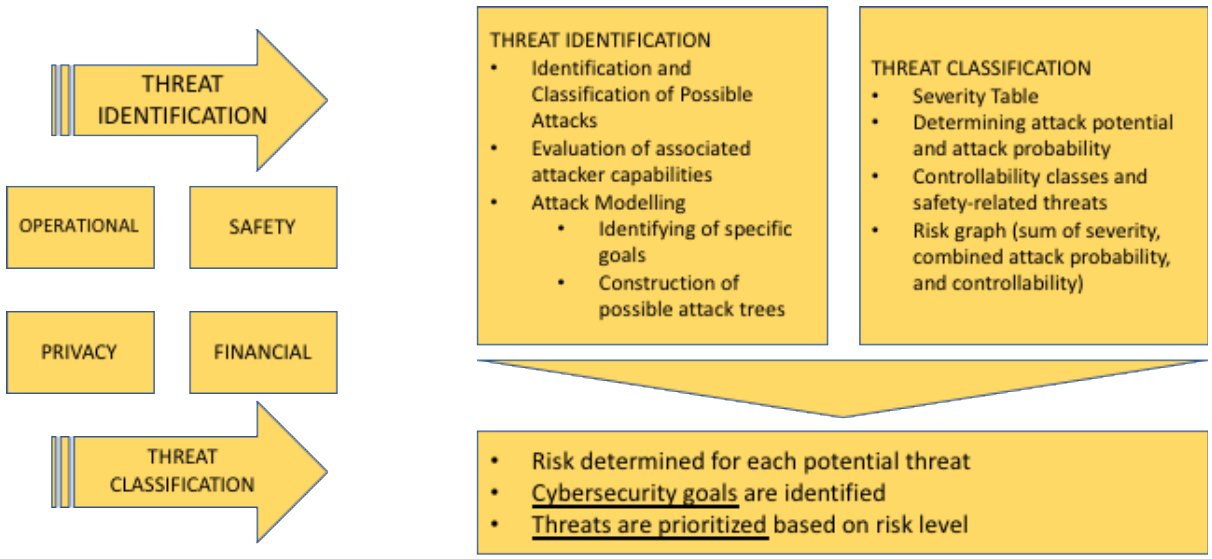

Figure 15 EVITA process flow

Threat identification uses dark-side scenarios and attack trees to identify generic threats and hence generic cybersecurity requirements. Threat classification develops recommendations for classifying threat risk-based severity of threat outcome and probability of successful attack based on ISO26262 HARA method. HARA allows the identification and categorization of hazardous events and the to specify safety goals and ASILs related to prevention or mitigation of the associated hazards to avoid unreasonable risk [29].

4.3.2 Threat and Operability Analysis (THROP)

THROP is an extension of EVITA and tries to delineate the process of brainstorming possible attacks. THROP process flow is shown in Figure 16.

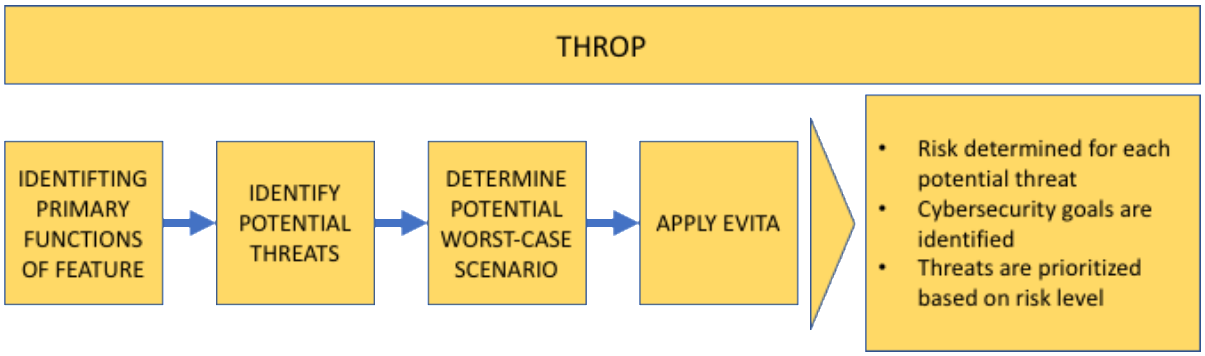

Figure 16 THROP process flow

4.3.3 Threat, Vulnerabilities, and Implementation Risks Analysis (TVRA)

The TVRA method requires defining functional safety requirements upfront followed by transforming them into detailed cybersecurity requirements by running threat and risk analysis. There are ten sequential steps to this process.

1. Identify the target system assets and specify the goal, purpose, and scope of analysis.
2. Identify the objectives and produce a high-level statement of cybersecurity to be resolved.
3. Identify the functional cybersecurity requirements.
4. Inventory assets and refine the descriptions from step 1 and add additional assets identified in steps two and three.
5. Identify threats, vulnerabilities that can be exploited, and the consequence of the exploitation.
6. Determine the occurrence, likelihood, and impact of the threats.
7. Determine the risks.
8. Identify cybersecurity controls to reduce risks.

9. Perform a cybersecurity control cost-benefit analysis to identify which cybersecurity controls should be implemented first.
10. Detailed requirements for implementing the cybersecurity services and capabilities identified in step 9.

4.3.4 Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

The OCTAVE method is the first that explicitly looks at organization along with technology. OCTAVE proposes series of workshops to define sociotechnical risks, protection strategy and mitigation plan. OCTAVE process flow is as shown in Figure 17.

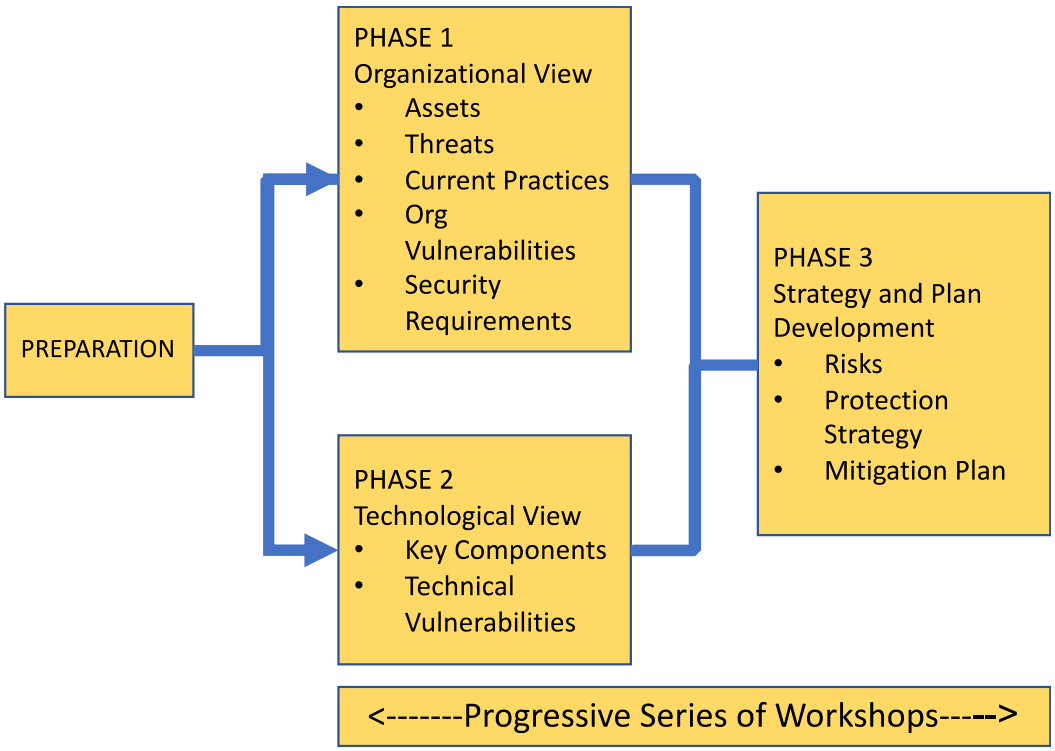

Figure 17 OCTAVE process flow

Developed by the Software Engineering Institute (SEI) and the Department of Defense's (DoD) Telemedicine and Advanced Technology Research Center (TATRC), OCTAVE brings together stakeholders with system experience, subject matter expertise, and security experience. Stakeholders participate in series of detailed workshops to develop a through organizational and technical view of the problem domain. This method is heavy on time and resource investment. It is used primarily for assessing risks in existing enterprise information systems and not for cyber-physical systems.

4.3.5 Healing Vulnerabilities to Enhance Software Security and Safety (HEAVENS)

The HEAVENS method focuses on methods, processes, and tools for threat analysis and risk assessment with respect to the vehicle electrical and/or electronic system. The method establishes a direct mapping between security attributes and threats during threat analysis. This facilitates visualizing and making early estimations of the technical impact of a threat on a particular asset. High level security requirements are calculated based on the asset, threat, security attribute, and the security level. The work flow for HEAVENS method is shown in Figure 18.

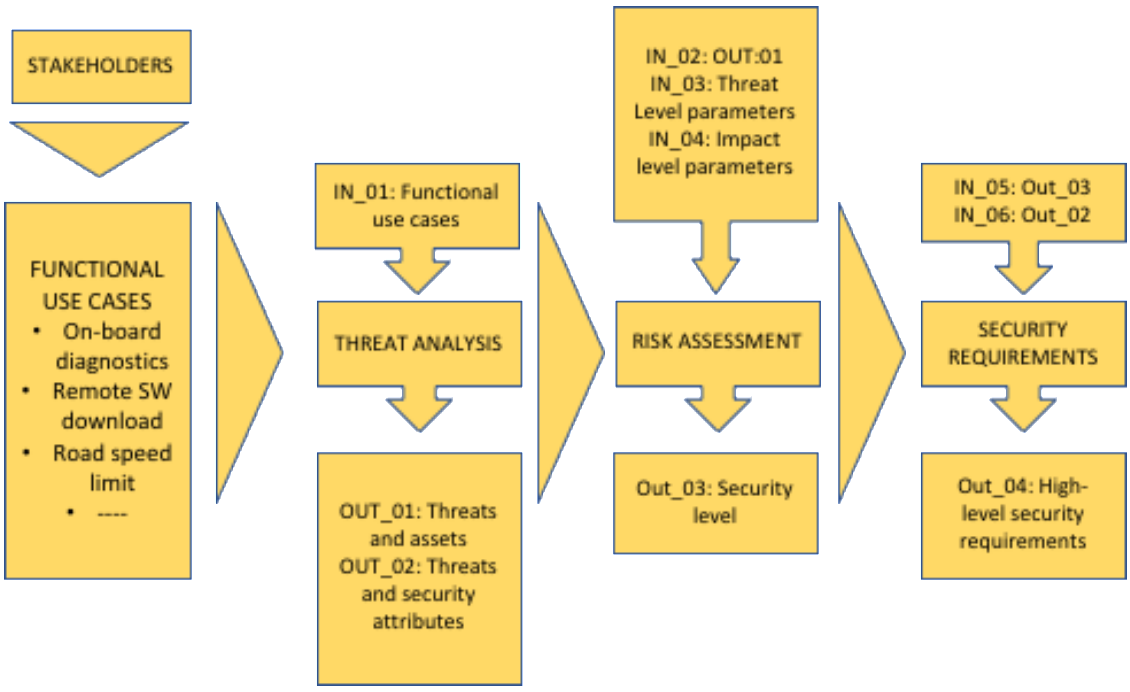

Figure 18 HEAVENS process flow

4.3.6 Attack trees

Inspired from fault trees, attack trees are a threat modeling technique where attacks against a system are represented in the form of a tree structure. This technique identifies top level cybersecurity attack goal followed by decomposing into sub-goals and attack steps to achieve those goals. Each element in the tree builds to the final attack goal. This results in multiple attack scenarios for a single attack goal. In this tree, the goal of attack is represented by the root node and different ways of achieving that goal as leaf nodes [48]. Cybersecurity requirements are then derived from the scenarios captured by the tree. Attack trees are a chain-of-events causality model and offer the following key advantages:

- Provide a structured approach to identifying threats.

- Allow analysis of a system at multiple level of abstraction. Analysts can work at high level with functional elements and if required move into low level with components and protocols.
- Promote exhaustiveness through consideration of every possible attack vector.

Classically some of the drawbacks of using attack trees include:

- High level of dependency on expert. Attack trees could easily differ depending on experience and mental model of the expert.
- As systems grow in size and complexity, scaling a tree becomes unwieldy.
- Creating attack trees is a time-consuming effort.

Recent research efforts related to attack trees are focused on mitigating some of the drawbacks listed above. For example, Falco et al. [49] have developed an artificial intelligence (AI) based automated attack tree generator that takes system model and attack rule set as inputs and provides an attack tree as output. The generated trees are claimed to show no expert dependency, have ability to handle complexity and scaling, and take very little time to generate, along with other benefits. The first two methods in J3061- EVITA and THROP, both use attack trees for generic threat identification. Example of an attack tree is as shown in Figure 19.

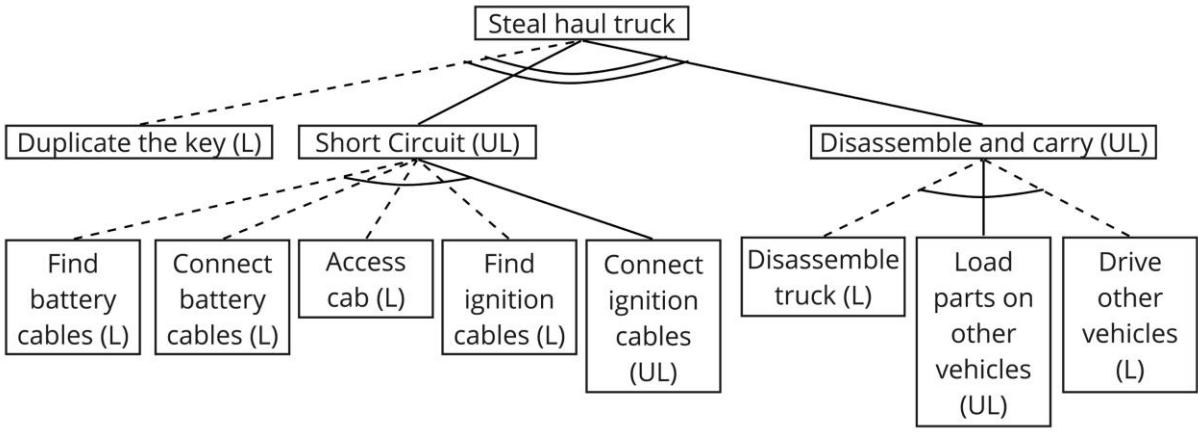

Figure 19 Attack tree

In the attack tree example of Figure 19, goal of the attack is to steal the haul truck and is represented as the root node. Three leaf nodes branch out from the root node given by duplicate the key, short circuit, and disassemble and carry. The double curves running across these three branches indicate the exitance of OR logic, meaning that the theft of haul truck can happen from any of the three modes. Duplication of the key is assumed to be enough for stealing the haul truck

and is therefore terminated at this point, i.e. no more leaf nodes spring out of key duplication. Consider the second leaf node from root node given by short circuit. The single curve cutting across multiple leaf nodes originating from short circuit represents AND logic, meaning that for short circuit to be successful requires the successful execution of all the following events: finding battery cables, connecting of battery cables, access cab, find ignition cables, and connect ignition cables. Attack trees can also capture additional details, for example, nodes can carry 'L' or 'UL' to represent the likelihood or the unlikelihood of that node based on expert judgement. In addition, connecting lines can be solid or dashed to depict connections that are likely to be successful. For example, in Figure 19 duplication of the key has high likelihood of leading to successful theft, therefore the link from "duplicate the key" to "steal haul truck" is dotted. Also, the link between "disassemble and carry" and "steal haul truck" is solid because for the leaf nodes originating from "disassemble and carry" are under the AND logic; all the leaf nodes need to be "likely" for the root node to be "likely".

4.3.7 Literature on SAE J3061

Schmitter et al. [50] apply parts of HEAVENS and EVITA models from SAE J3061 on an automotive electronic control unit (ECU) serving as a communications gateway. Starting with the basic architecture of the system, each asset is analyzed for threats and attack scenarios. Threats are ranked based on attack probability, which is estimated based on the perceived difficulty in executing an attack. Severity class is assigned based on EVTA severity classes. A combined risk score for each threat is then ascertained based on attack probability and severity class as inputs. Cybersecurity goals are then derived for high and medium severity risks.

4.4 Summary

Different solutions addressing the need for vehicle cybersecurity were analyzed. They all have their strengths and weaknesses. Comparison of these standards, guidelines, and frameworks is as shown in Table 1. Comparison criteria (columns) in the table are given by: the tool, analysis type, method for threat/hazard identification, method for risk assessment, name of threat/hazard ranking artifact, method of scenario generation, quantity of scenarios generated by a given method, and scope of the method. Under analysis type, FuSa and Sec stands for functional safety and security respectively. Threat/hazard identification captures various tools and techniques that are used for identifying threats and/or hazards. Risk assessment identifies various criteria that could be used for analyzing and ranking of the hazards. Threat/hazard ranking artifact lists the name of

any combinatorial concept that uses various risk assessment criteria for ranking of the hazard. Scenario generation captures the process of generating scenarios from identified hazards. Requirement mapping gives a measure of the number of requirements that can be generated from one hazard. Scope is indicative of the type of system that the tool can process for cybersecurity threats. Key observations for Table 1 are given below:

- Scenario generation in almost all the given tools maps from hazard through goals to scenarios. System theory-based tools, STPA and STPA-Sec, differ such that hazards lead to functional control structure, control action identification, context table generation, and finally to scenario generation.
- Requirement mapping is high for systems theory-based tools, where one hazard can lead to an order of magnitude more high-level requirements. Comparing with other tools, one hazard can lead from 1 to 5 high level requirements. At least one requirement per identified hazard is mandated by most non-system theory-based tools.
- The inclusion of risk assessment criteria such as financial, attacker capability, and privacy for example, makes most of the cyberthreat compatible tools socio-technical in nature compared to their safety only counterparts. Systems theory based tools expand this scope by including social hierarchy in safety and security analysis.

Table 1 Comparison of cybersecurity methods

Tool	**Analysis Type**	**Threat/Hazard Identification**	**Risk Assessment**	**Threat/Hazard Ranking Artifact**	**Scenario Generation**	**Requirement Mapping**	**Scope**
ISO26262	FuSa	Brainstorming, checklists, quality history, FMEA, and field studies	Severity, exposure, controllability	ASIL	From safety goals which are related to hazards	Low - Medium	Technical
ISO26262 with SAHARA	FuSa + Sec	STRIDE	Resources required to exert a threat, knowledge required to pose a threat, threat criticality	SecL	From security goals which are related to threats	Low - Medium	Socio-technical
ISO26262 with EVITA	FuSa + Sec	Attack trees, capability analysis, brainstorming	Privacy, financial, operational, safety	Combined attack probability	From security goals which are related to threats	Low - Medium	Socio-technical
STPA	FuSa	Safety accidents and functional architecture	Control action missing, present, incorrect timing or order, stopped too soon or applied too long	None	From functional control structure, control action identification, context table generation	High	Highly socio-technical
STPA-Sec	FuSa + Sec	Safety and security accident and	Control action missing, present,	D4 Chart, wargaming,	From functional control	High	Highly socio-technical

Tool	Analysis Type	Threat/Hazard Identification	Risk Assessment	Threat/Hazard Ranking Artifact	Scenario Generation	Requirement Mapping	Scope
		functional architecture	incorrect timing or order, stopped too soon or applied too long		structure, control action identification, context table generation		
EVITA	Sec	Attack trees, capability analysis, brainstorming	Privacy, financial, operational, safety	Combined attack probability	From security goals which are related to threats	Low - Medium	Socio-technical
THROP	Sec	Malicious behavior (unintended, incorrect, missing) with respect to critical functions	Privacy, financial, operational, safety	Combined attack probability	From security goals which are related to threats	Low - Medium	Socio-technical
OCTAVE	Sec	Brainstorming	Brainstorming	None	From security goals which are related to threats	Low - Medium	Socio-technical
HEAVENS	Sec	STRIDE	Expertise, knowledge, equipment, window of opportunity, safety, financial, operational,	Security level	From security goals which are related to threats	Medium - High	Socio-technical

Tool	**Analysis Type**	**Threat/Hazard Identification**	**Risk Assessment**	**Threat/Hazard Ranking Artifact**	**Scenario Generation**	**Requirement Mapping**	**Scope**
			privacy and legislation				
ATTACK TREES	FuSa + Sec	Brainstorming	None	None	From possible branches of the tree	Low	Socio - technical

5. STPA-Sec ON MINING CASE

5.1 Define and frame the problem

Autonomous haul trucks are performing full scope of operation in mine sites without operator in the cab. Successful autonomous hauling requires multiple human and mechatronic systems scattered across geography to coordinate and control critical processes. These autonomy supporting systems have high degree of connectivity compared to their predecessors and as such a higher exposure to cyber-attacks that could result in safety and security losses.

5.2 Specify unacceptable losses and accidents

The second task in the application of STPA-Sec on autonomous hauling application requires listing of unacceptable losses. These losses specify at a very high level all the undesirable conditions resulting from autonomous hauling.

Table 2 Unacceptable losses

Unacceptable Losses
L1: Loss of life or injury to people
L2: Collision between vehicles
L3: Collision with obstacles or mine terrain
L4: Loss of IP and critical information
L5: Loss of production

The first unacceptable loss (L1) is concerned with loss of life resulting directly from the operation of the autonomous haul truck. With staged infusion of autonomy in the mine site, autonomous haul trucks share the same space as other human operated machines, increasing the likelihood of an injury or fatal accident.

The next unacceptable loss (L2) is related to collisions between vehicles. Fatalities, injury, vehicle and production loss can result from collision between vehicles. Although not an autonomous haul truck collision, Figure 20 shows one recently reported collision between a manually operated haul truck and a stationary supervisor van. No vehicle-to-vehicle collision accident report related to AHS was found in the MSHA database.

Figure 20 Haul truck collision with supervisor van [62]

The third unacceptable loss (L3) is due to collision between vehicle and obstacle or mine terrain. Obstacles could include towers, fueling stations, hoppers, crushers, and mine terrain could include berm and bench face, and material stockpile. Some of the open pit mine terrain attributes are as shown in Figure 21, and include two profiles, namely active and final outline. The active profile is dynamic such that for the prescribed bench attributes of face angle and height, the number of roads and ramps keep adding up as the mine gets deeper.

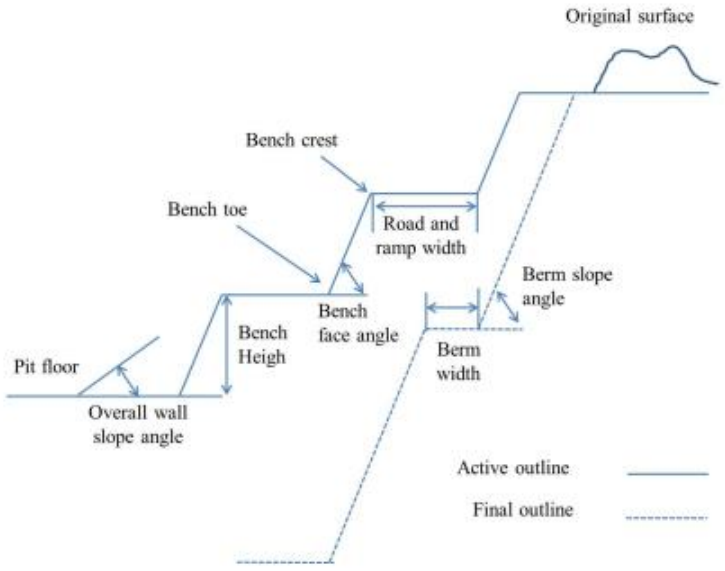

Figure 21 Open pit nomenclature [60] (from Arteaga et al.)

Dropping down into mine terrain can be catastrophic and result in death, injury, vehicle, and production loss. Figure 22 shows an overturned, manually operated, haul truck that fell into mine terrain while end dumping over an edge. End dumping is a term used in hauling operation and is associated with the process of tilting the haul truck's bed to unload material. No vehicle-to-mine terrain collision accident report related to AHS was found in MSHA database.

Figure 22 Haul truck overturned on dumpsite [61]

Loss of IP and critical information (L4) is the fourth unacceptable loss because IP loss can threaten the company's future [51]. This type of loss can have additional ramifications because IP and critical information loss can go undetected for some period, thus exacerbating the financial and operational issues including physical mine safety.

Loss of production (L5) is the final unacceptable loss identified for this analysis. Mine operators closely monitor production at the mine site as a metric to gauge efficiency and productivity. Loss of production can result in financial losses and can be indicative of organizational and technical issues.

Losses L4 and L5 are new to the STPA framework and are part of the change mandated by STPA-Sec for conducting security analysis. In the next section, we map these losses to system hazards of interest. Since we are interested in the operation of autonomous haul truck, the system hazards pertaining to an autonomous haul truck are envisioned.

5.3 Identify system hazards and derive constraints

Keeping the hauling ConOps and unacceptable losses in mind, we develop the mission hazard and loss table as shown below:

Table 3 Mission hazard and loss

System Hazard		Unacceptable Loss
H1	Haul trucks violate minimum separation standards with other vehicles	L1, L2, L5
H2	Haul trucks violate minimum separation standards with obstacles or terrain	L3, L5
H3	Haul truck network security is compromised	L1, L2, L3, L4, L5
H4	Hauling system rate of handling material falls below minimum standard	L5

Haul truck violating minimum separation standards with other vehicles results in the hazard H1. H1 refers to the hazard condition where the autonomous haul truck is unable to maintain safe distance between itself and other vehicles around it. Multiple scenarios can lead to this hazard condition. For example, consider a scenario with the haul truck speed impacted by controller latency and sensor delays, hence reducing the reaction window of an autonomous haul truck and resulting in loss of minimum separation with other vehicles, and increasing the odds of a collision (L2). If the other vehicle is also carrying passengers or driver, then H1 can also lead to loss of life (L1). In the case of either L1 or L2 resulting from H1, there is bound to be loss of production (L5) due to accident investigation and loss of capacity. Therefore in Table 1, for the system hazard H1 the unacceptable losses are given by L1, L2, and L5.

Haul trucks violating minimum separation standards with obstacles or terrain (H2) is a hazard condition where the autonomous haul truck is unable to maintain safe distance between mine obstacles or terrain and itself. Again, different scenarios could result in this hazard condition. For example, discrepancies between autonomy controller topographical map and actual map, coupled with sensor limitations can result in haul truck losing the minimum required separation with obstacles and terrain, and increase the risk of running into these obstacles and terrain features (L3). Investigation of collision, recovery and fixing of haul truck will take time, hence impacting production (L5).

Haul truck network security compromised (H3) is a hazard condition in which the vehicle network security gets compromised. This type of hazard results in loss of IP and/or critical information (L4) related to internal and external environmental parameters, localization, path selection, and collision avoidance [52]. Attacks on vehicle network availability, authentication, and confidentiality can also result in loss of minimum separation between vehicles, obstacles, and terrain (L2 & L3). If critical controllers are found to be vulnerable and get hacked, then autonomous haul trucks can be used as weapons against other manually operated vehicles, resulting in fatality (L1). Any accident or realization of a compromised network security is bound to shut down production (L5).

The hauling system's rate of handling material falling below minimum standard is a hazard condition (H4) where the rate of material handling by autonomous haul trucks and hence hauling system falls below the minimum required. The minimum required production per unit time could be driven by production goals and other process dependencies.

System level constraints are system conditions that need to be satisfied in-order to prevent hazard conditions and resulting losses. Derived directly from system hazards, system safety/security constraints are given in Table 4. The safety and security constraints (SCs) given by SC1 through SC4 maps directly to hazards H1 through H4.

Table 4 System safety/security constraints

System Safety Constraint		System Hazard
SC-1	Haul trucks must satisfy minimum separation standards from other vehicles	H1
SC-2	Haul trucks must satisfy minimum separation standards with obstacles and terrain	H2
SC-3	Haul truck network security must be maintained under worst-case conditions	H3
SC-4	Hauling system rate of handling material must not fall below minimum standard	H4

The next step in STPA analysis involves drawing the functional control structure, identifying process control variables that most accurately capture process state, and identifying the most relevant feedback control loop and control action to study.

5.4 Functional control structure and process model state space

The hierarchical functional control structure draws its motivations from systems theory, which is based on two main ideas-

- Emergence and hierarchy
- Communication and control [34].

Cybersecurity and safety are emergent properties of the AHS since they can only be evaluated when considered in the context of the whole system. Hierarchy is inherent to AHS operations and the system is divided into different levels with each level imposing constraints or lack thereof on the functioning of the level below it. Communication and control channels are paramount to ensure the desired behavior of the system. These channels include goals, constraints, commands being imposed by the higher level on the lower level, and feedbacks in the form of reports and requests from the lower level to the higher level.

The high level sociotechnical operational control structure is as shown in Figure 23. For details regarding blocks, control, and feedback flows in Figure 23, the reader is advised to refer the mine operator organizational structure of Figure 6 under Chapter 3. STPA-Sec requires selecting a control loop from the functional control structure to zoom into for running subsequent experiments. The term control loop is used for a loop created between one controller and one controlled process connected through actuators and sensors. Multiple STPA-Sec iterations were performed with different control loops at various hierarchy level involving the mining company, OEM and suppliers, unions, mining associations, and the government. The criteria for selecting the loop was also refined during this process with the two major considerations for selecting a control loop given by:

- The loop shall capture systems directly impacted by autonomous hauling.
- The loop shall include sociotechnical aspect of the system involving human and machine controllers and controlled processes.

The red box was drawn around the given sociotechnical elements because they satisfied the above-mentioned criteria.

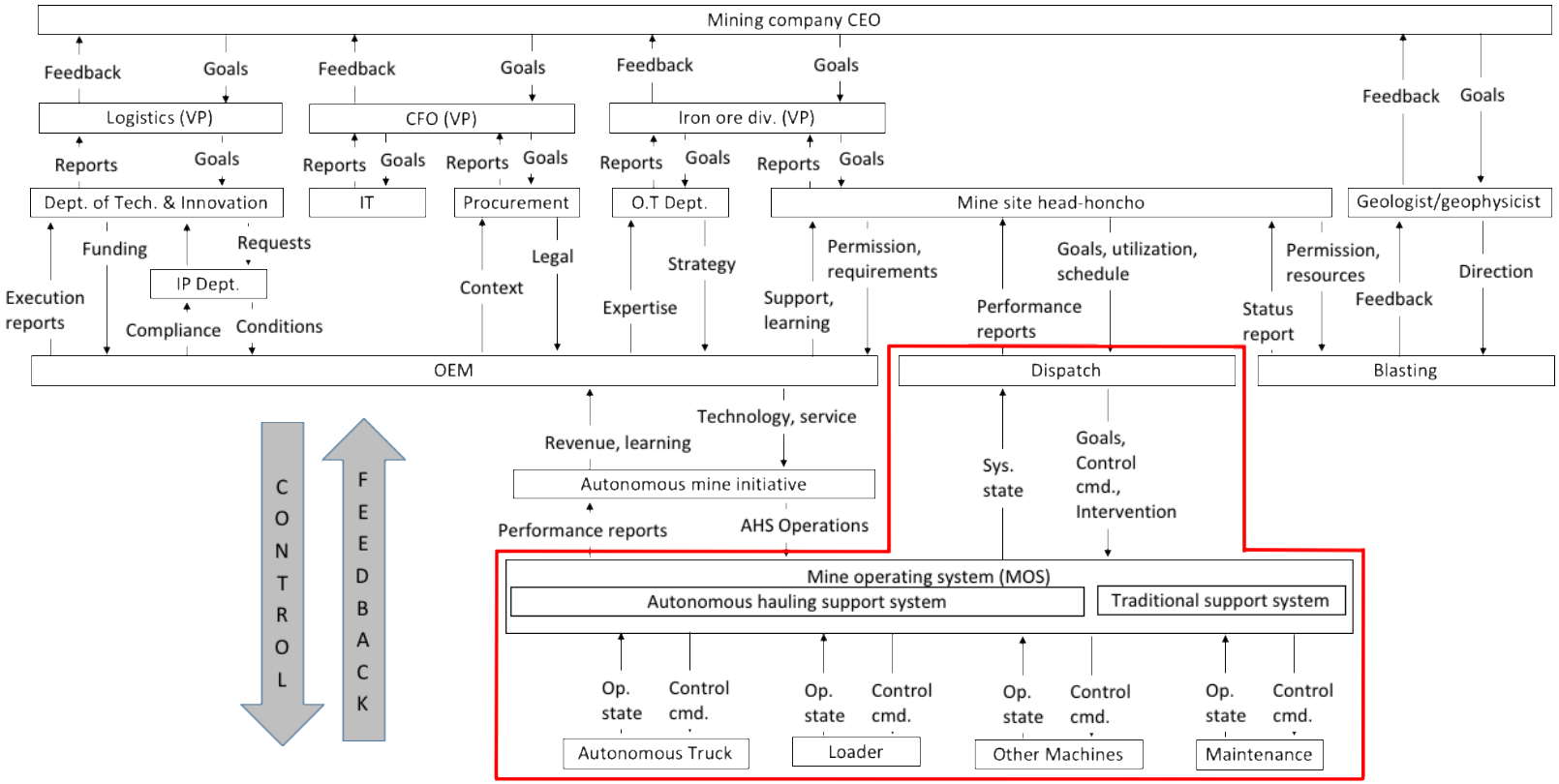

Figure 23 AHS operational control structure

At the vehicle level, vehicular systems have seen big change in terms of components and architecture. At one level above, the MOS has assumed autonomy driven additional responsibilities in the value chain. Level above MOS consists of dispatch, which controls the MOS. Dispatch has also assumed additional operational responsibilities that come with autonomy. For example, managing autonomous operating zone (AOZ) access, updating terrain map available to haul truck autonomy controller, autonomous asset control and coordination, are some additional responsibilities that the dispatch has fulfilled. Also, other mining systems sharing the same environment as the autonomous haul truck have had to adapt to this change of adding autonomy.

The system boundary of interest set by the red box in Figure 23 includes dispatch, MOS, equipment, and maintenance. Zooming into this subsystem, a high-level interaction between the dispatch, shovel, and an autonomous haul truck is shown in Figure 24. Dispatch human controller could control a mine pit or a site with multiple autonomous haul trucks and shovels. Human controllers have dispatch or shovel automation assisting them. Dispatch, shovel, and haul truck are connected through control actions, feedbacks, and information flows. Interactions between the shovel and the autonomous haul truck is made possible only once the haul truck is within a virtual circle around the shovel.

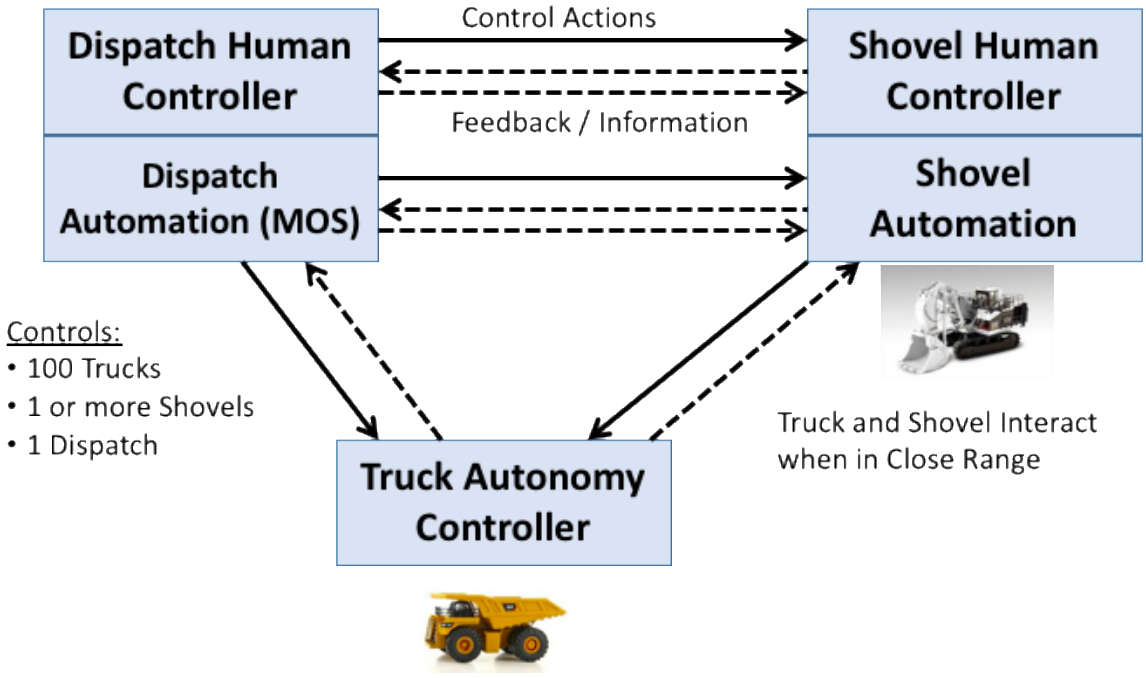

Figure 24 Shovel-truck-dispatch interaction

Detail view of the dispatch-shovel-autonomous haul truck interaction is as shown in Figure 25. Dispatch is made up of people with four key designations [53]:

- Shift lead
- Command technician
- Command builder
- Command operator

Everyone in dispatch have access to relevant and timely information made available to them through the MOS. Responsibilities of the dispatch are given below.

5.4.1 Shift lead

Shift lead oversees all activities in the shift, with tasks designed to meet daily mine production and operations goals. Shift lead tasks are listed include:

- Staff scheduling
- Setting productivity targets
- Equipment management and assignment

5.4.2 Command operator

Command operator's duties are associated with configuring the MOS to meet mine productivity goals. Command operator tasks include:

- Pre-shift and shift change functions
- Observation and management of load
- Dump and mine site activities
- Monitor and manage autonomous operating zone access
- Coordinate site wide activities for equipment operators, water trucks, graders, maintenance equipment

5.4.3 Command builder

Command builder is responsible for the following two activities:

- Creation and maintenance of the site survey and surfaces for autonomous haul truck operations in load, dump, and haul road areas.
- Integrating planning activity with the overall mine plan to meet short and long-term planning and productivity goals.

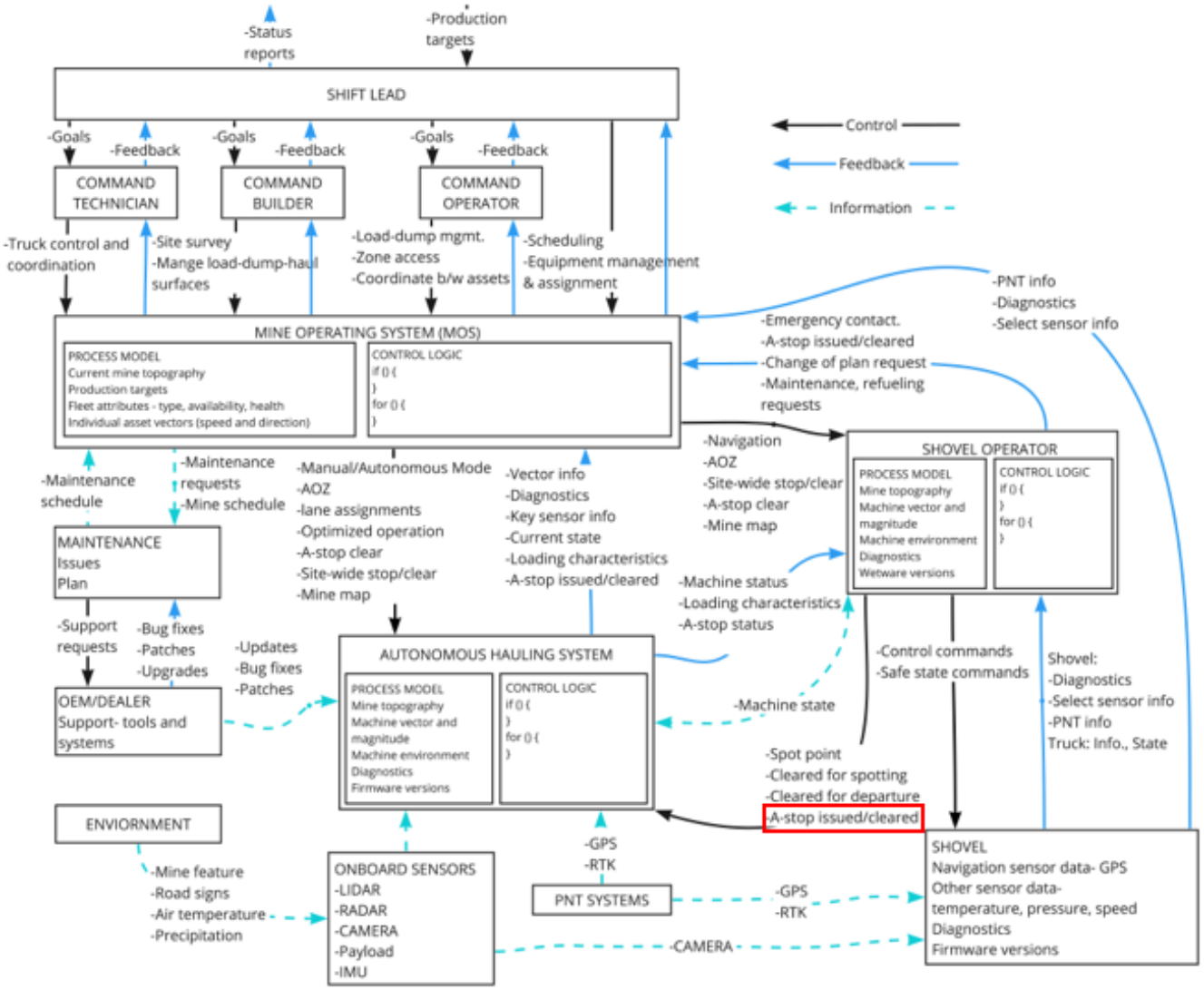

Figure 25 Detailed control structure

5.4.4 Command technician

Command technician's work involves direct interaction with the autonomous haul trucks, including:

- Pre-start, starting and coordinating haul truck movement in the AOZ.
- Working with command operator and command builder to meet mine planning and operations goals.

5.4.5 MOS and dispatch interaction

The MOS receives mission critical information from AHS, shovel operator, shovel, and maintenance. There are different ways to model dispatch-MOS interaction. Five basic models of this interaction are as shown in Figure 26.

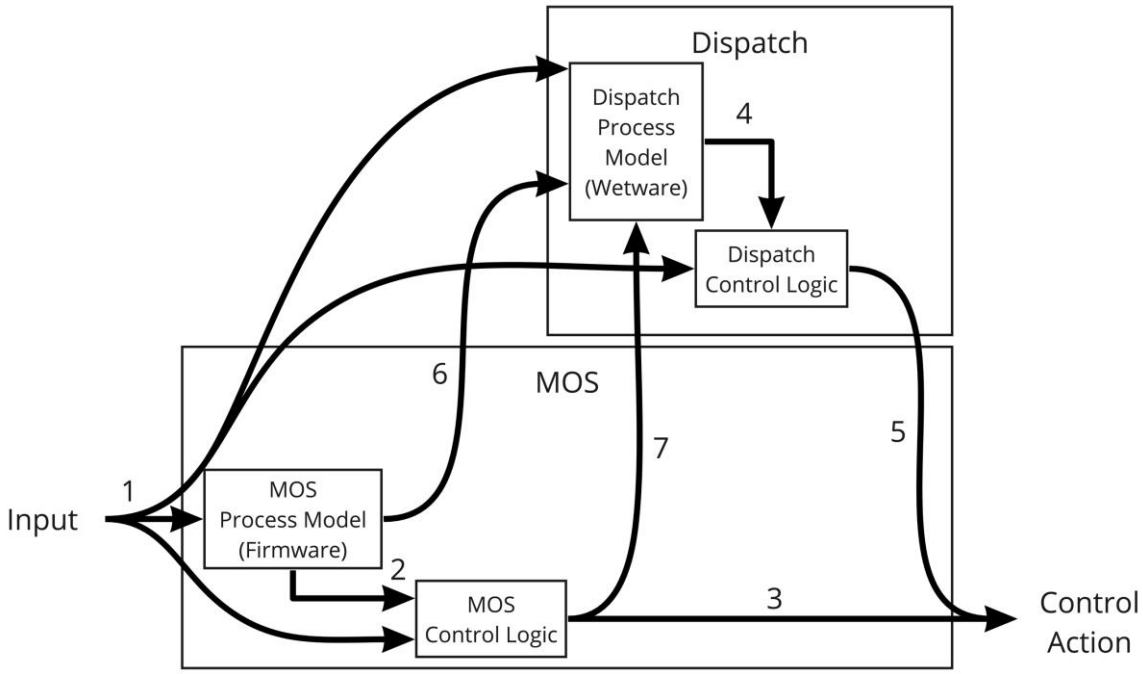

Figure 26 MOS-dispatch controller logic

The first model involves running the input parameters, given by input (1), though MOS process model (firmware), and comparing the expected (2) with actual state of the system (1). The gap between expected and actual could then be used by the MOS for issuing appropriate control action (3).

The second model could involve sharing raw input (1) with the dispatch though the human-machine interface (HMI) as an input to dispatch process model. Output from the mental model of the dispatch (4) could then be compared with the actual state of the system (1) to find the gap

between the actual and perceived. This gap is then used for issuing appropriate control actions (5) by the dispatch, which are transmitted through the MOS. For capturing MOS-dispatch controller logic, physical elements such as the HMI are not shown in Figure 26. Also, it is assumed that the dispatch mental model and control logic is valid.

The third model could be to run the input (1) through MOS process model and then share the output of the process model as an input to dispatch process model (6). This new input from MOS could act as an aid to dispatch's mental model. Final decision on the control action is taken by the dispatch and transmitted through MOS (5).

The fourth model could involve sharing output from MOS control logic (7) with dispatch process model for approval from the dispatch. Based on evaluation from the dispatch, the control action (3) could be denied, approved, or approved with edits.

The fifth model could involve sharing output from MOS control logic block (7) with dispatch process model while the control action from the MOS (3) is also issued to the appropriate system downstream without the need for dispatch approval.

Actual implementation of MOS-dispatch functional architecture could involve the use of all five of these models depending on the criticality of the decision.

5.4.6 A-stop

Before introducing other interactions from the detailed control structure of Figure 25, it is important to introduce the A-stop functionality. A-stop is short for autonomous-stop product offered by Caterpillar Inc [54] [55]. Designed as a safety device to be carried by every human operator working in the AOZ, the A-stop device offers the capability of stopping all autonomous haul trucks operating within 300 meter radius of the transmitter. From safety and security context, A-stop is an interesting subject because of the complexity and multiple controller interdependencies inherent to the A-stop safety feature. In our shovel-truck-dispatch subsystem the option to issue the A-stop command is available to the shovel operator in case departure from acceptable haul truck behavior is observed. The resulting high-level sequence of events after an A-stop is issued by the shovel operator are listed below:

- All autonomous vehicles in a fixed region of influence around the shovel operator stop operation and transition to a safe state.
- Dispatch is informed through the MOS about A-stop being issued by a particular shovel operator.

- Autonomous machines impacted by the A-stop could also share their state with the MOS if a second layer of oversight from the MOS/dispatch is desired.
- Shovel operator clears A-stop once the perceived risk subsides.
- Dispatch is informed through the MOS about the A-stop being cleared by a particular shovel operator.
- Dispatch issues A-stop cleared command and confirms or reassigns mission if all conditions are met.
- All autonomous vehicles resume operation.

To avoid accidental clearing of A-stop command by the shovel operator and to ensure proper escalation of the issue resulting in the command being issued in the first place, MOS needs to clear A-stop command for the autonomous haul truck to function. MOS can also choose to issue additional site-wide stop commands incase the issue resulting in A-stop application in the first place is not fixed and poses a risk to continued operation.

5.4.7 MOS-AHS interaction

The MOS controls the AHS in both manual and autonomous mode. In manual mode, the MOS controls the haul truck's motion and bed movement by providing direct commands. In autonomous mode, the haul truck is free to operate within constraints if the mission goals are met. MOS also relays updated AOZ information, mine maps, and lane assignments to the AHS. The AOZ and map information is critical for safe operations at the mine site. Site wide stop/clear commands are also issued by the MOS and directed towards every machine both autonomous and manual, including the AHS. When an A-stop command is issued and later cleared by an operator inside the AOZ on the mine site, the MOS is required to issue an A-stop clear command to the autonomous machines impacted by the initial A-stop command, thus acting as a backup system against accidental A-stop clear issued by the operator.

The feedback from the AHS to the MOS includes sharing of location, heading, diagnostic, key sensor, and current system state information. In addition, AHS could share loading profiles, load carried per run, and information regarding issuance or clearing of an A-stop command.

5.4.8 MOS-shovel interaction

Shovel shares its position and heading, diagnostics, and select sensor information with the MOS.

5.4.9 MOS-shovel operator interaction

The shovel operator receives navigation information in case it is requested by the shovel operator or required by the MOS. The MOS also shares the current AOZ and any changes in it. Any site wide stop/clear along with A-stop clear commands are also issued by the MOS for shovel operator.

Shovel operator contacts MOS in case of emergency, change of plan, maintenance, and refueling requests. When A-stop is issued or cleared by the shovel operator, messages are also sent to the MOS to make MOS aware of the event.

While most of the interactions listed here will take place through the communication systems housed on the shovel, but for the sake of simplicity these communications and message transfers are shown to be originating and terminating from the shovel operator block in the detailed controls structure of Figure 25.

5.4.10 MOS-maintenance interaction

The MOS shares mine schedule including equipment assignment along with any maintenance requests with the maintenance department. Maintenance shares its set of planned maintenance activities around the mine site with the MOS.

5.4.11 OEM/Dealership

The dealership works with the mine maintenance to provide software and hardware upgrades. Mine maintenance provides dealership with support requests for hardware and software issues. For new technology implementations such as the AHS, the OEM may get directly involved with supporting hardware and software upgrades on the AHS.

5.4.12 AHS and shovel operator interaction

The shovel operator clears autonomous haul trucks for spotting, sets the spot point for efficient spotting process, clears the haul truck for departure once loaded, and issues/clears the A-stop command. In addition, the shovel may also share shovel states, for example digging, idle, etc., with the AHS. The AHS also shares its system status, loading profile, and potentially A-stop state active/inactive status with the shovel operator.

5.4.13 Shovel operator and shovel

Shovel operator controls the shovel through electro-hydraulic controls. Shovel operator receives position and navigation information, diagnostics, and other critical information through

the control panel in the cab. In addition, AHS information pertaining to one or more trucks would also be made available through communication systems housed on the shovel.

5.4.14 Other systems

PNT systems include GPS and RTK systems that enable precision mining along with autonomous hauling operation. The GPS and RTK services are available to both the autonomous haul truck and the shovel.

Onboard sensor stack includes LIDAR, RADAR, camera, loadcells, IMU, and more. All or most of the sensors listed above can be used by AHS for autonomy. Some of the sensors such as the IMU and camera are used by the shovel.

5.4.15 Control loop

The shovel operator, autonomous haul truck, MOS, onboard sensors, and PNT represented in a control loop fashion is as shown in Figure 27. A control loop [34] [4] [56] [37] consists of a controller, a controlled process, actuators, sensors, and additional elements leading into and out of the controller and controlled process if deemed important for the analysis. Moving in the clockwise direction, shovel operator as a controller issues commands such as spotting point setting, clearing haul truck for spotting, clearing haul truck for departure post loading, and issuance or clearing of A-stop. Actuators include individual or combination of hardware, software, network elements that enable the commands to reach the autonomous haul truck controller. Consider as an example a scenario where the autonomous haul truck is spotting and the sensors on the shovel are tracking the haul truck to facilitate correct parking of the haul truck next to the shovel. Sensors on the shovel could detect the haul truck and transmit the message to haul truck detection module [57] on the shovel. The haul truck detection module, using sensor and additional information, could decide if the haul truck is in the correct position. Haul truck detection module would then send appropriate message to communicate correct position through its CAN network addressed to telematics ECU, which then sends it to the radio transmitter. Radio transmitter broadcasts this message. Haul truck's receiver decodes the data and its telematics ECU transmits the message addressed to autonomy controller through the haul truck's CAN network. Haul truck's autonomy controller receives and authenticates the message and sends messages to transmission ECU to stop motion.

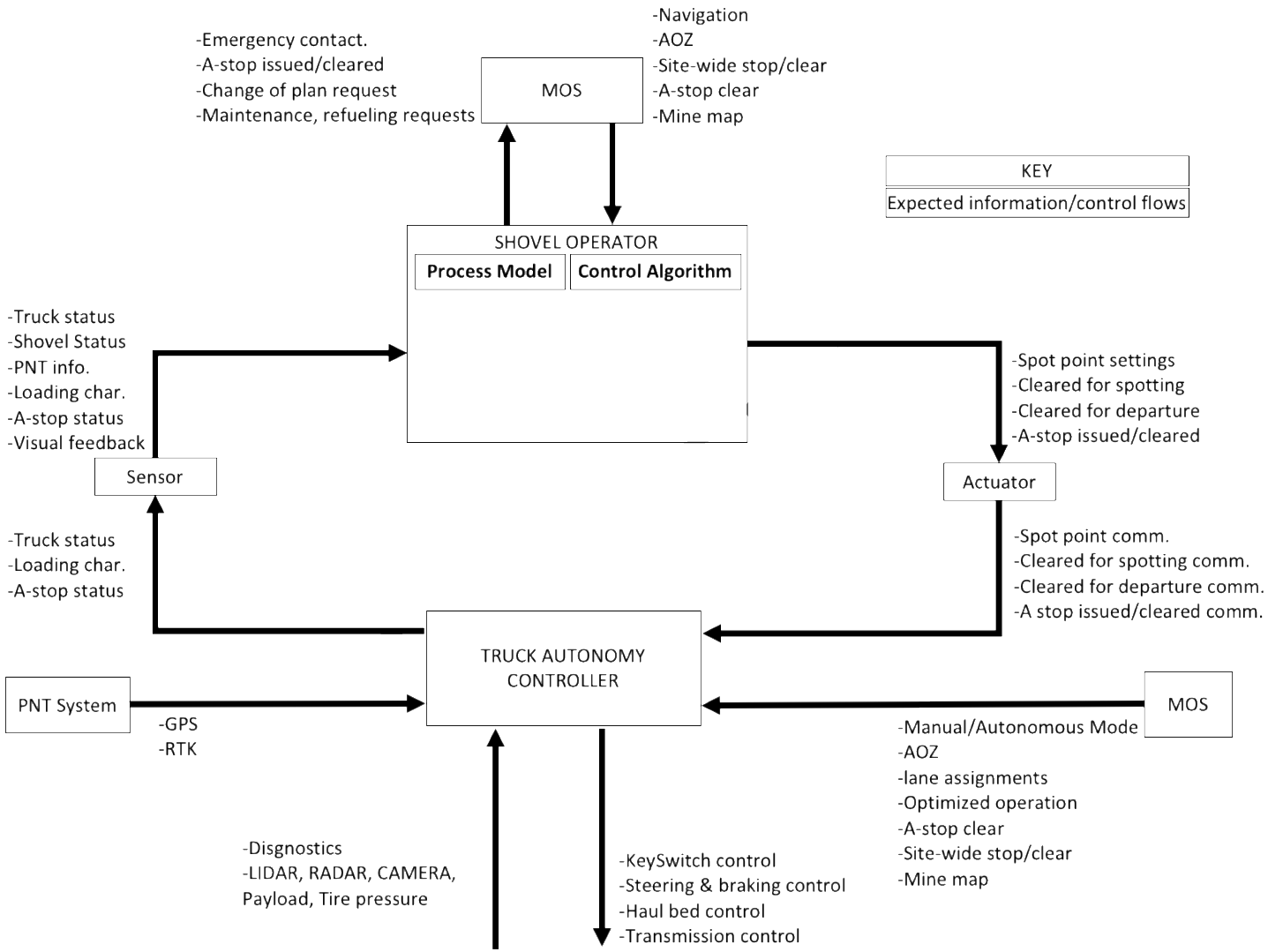

Figure 27 Control Loop

Transmission ECU then takes control action through electro hydraulic (EH) systems to shift the transmission into neutral, apply brakes, and activate park brake. In this example, starting from shovel's haul truck detection module and ending with haul truck's autonomy controller, everything in between constitutes the actuator.

Through the sensor arm of the control loop, the haul truck autonomy controller relays to the shovel operator its state, indicating whether it is waiting, spotting, loading, departing, or hauling. In addition, current load profile could also be shared to avoid over and/or uneven loading.

Shovel operator receives information from the shovel HMI. This information could contain shovel diagnostics, shovel parameters, position and heading information of vehicles in the vicinity, autonomous haul truck information, and autonomous haul truck state. Shovel HMI is considered part of the sensor block leading into the shovel operator. Additional sensor elements include shovel operator's human senses of sight, hearing, smell, and touch.

PNT systems collectively represent the civil GPS satellites, vehicle mounted receivers, elements of augmentation systems including receiver stations, transmitting towers, and vehicle mounted receivers. PNT systems are connected to both the shovel operator and haul truck autonomy controller.

MOS plays the role of secondary controller for the autonomous haul truck and primary controller for the shovel operator.

Using the control loop of Figure 27, the A-stop command issued by the shovel operator will be further analyzed for safety and cybersecurity in the following sections.

5.5 Identify process model variables

The process model variables capture the system information that is required by a controller to determine the control action that needs to be provided. The set of process model variables change based on the control action and the controller under study. The A-stop command is not used by the operator under normal conditions and is only issued when abnormal operation is detected. Few conditions contributing to the issuance of A-stop command by the shovel operator, and which could help in the selection of the process model variables, are listed below:

- High approach speeds: high approach speeds of the haul truck while spotting can result in overshoot and hence a smaller window for error correction.
- Movement outside acceptable region: movement of haul truck outside the limits of acceptable region can result in collision with the shovel or mine feature.

- Potential crash with other vehicles/personnel: movement of the haul truck that could potentially result in a collision with service vehicle or support vehicles such as dozers and motor graders operating in the area around the shovel.
- Unexpected motion: unexpected motion of the haul truck, for example, when shovel is not ready to begin loading operation and the haul truck initiates spotting.
- Departure from proper operation: depending on the severity of the deviation, A-stop could be issued when the haul truck departs from optimal operation.

These contributing conditions for activation of A-stop can be traced to different parts of the system. While some can be attributed to component failure, others will result from incorrect design, and process model flaws. From these conditions, we can derive the process model variables along with their states, as shown in Table 5.

Table 5 Process model variables with states

Process model variable	States
Haul truck	waiting, spotting, loading, departing, hauling
Shovel	waiting-idle, waiting-spotting, loading, waiting-departing
Onboard sensor	adequate, inadequate
PNT	adequate, inadequate
MOS	adequate, inadequate

For the process model variable “shovel”, the state “waiting-idle” means that the shovel is waiting while the haul truck is idle. Since A-stop command has high impact on shovel-haul truck interaction, the states of process model variable “shovel” are also indicative of this interaction. Inadequate process model variable means missing, incorrect, or misleading signals coming from that node. For example, inadequate onboard sensor would mean that the data from LIDAR, RADAR, camera, and/or payload sensors is missing, incorrect, or misleading. If the aim of the study is extended to analyze individual onboard sensor for safety and cybersecurity requirements, in that case the onboard sensors must be further de-lumped into individual sensors with respective states for analysis. For our objective, all onboard sensors lumped together as a single unit should be enough.

5.6 Identify unsafe/unsecure control actions and safety/security constraints

5.6.1 Unsafe/unsecure control actions

A context table is developed using the process model variables defined earlier along with the A-stop control action under study. Combining different process model states results in 160 unique system states, as given by the entries in Table 7 under Appendix A. As an example, one of the system states could be identified as shown in the Table 6 below:

Table 6 Example of a valid system state derived from process model variables

Process model variable	State	Validity Remark
Haul truck	Waiting	Both haul truck and shovel operator are waiting while incorrect, delayed, or missing commands from MOS are received.
Shovel	Waiting-idle	
Onboard sensor	Adequate	
PNT	Adequate	
MOS	Inadequate	

Haul truck is waiting in a staging area, shovel operator is waiting, onboard sensors and PNT systems are performing adequately, but MOS is inadequate. Inadequacy from MOS could manifest itself in the form of incorrect, delayed, or missing communication.

From all the system states identified in Table 7, majority of them are dropped based on three filtering criteria.

- Everything good does not provide any insight and can be dropped. These are tagged as “all good” under validity remark column in Table 7.
- Double faults are not considered for the first run. However, it is recommended to consider these states for second round of analysis. These are tagged as “double failure.”
- Some system states are invalid based on the assumption that process state difference of two or higher is invalid. For example, given that the process states for the haul truck are waiting, spotting, loading, departing, and hauling, if the haul truck is in loading, the shovel can only be in waiting-spotting, loading, or waiting-departing, and any other state combination is assumed to be invalid. This assumption may work well with matured systems, but for new systems such combination of states may occur and depending on their propensity for resulting in a hazard, requirements need to be written to avoid such system states. In the interest of further filtering the data, this condition is enforced. These system states are tagged as “unlikely.”

Discounting double faults should not be considered as permanent filtering criteria. Scenarios resulting from multiple fault conditions are inherently complex, but designers and analysts should strongly consider addressing them. Cyber-attack on Ukrainian power grid in 2015 serves as a recent example of coordinated effort resulting in double faults occurring at the same time [58]. Scenarios capturing multiple faults are essential to generating stronger defenses. Applying these three filters result in 43 possible unsafe control actions (UCA). System state represented by the 43 UCAs are further evaluated by asking four questions [56], given by:

- Is the control action itself hazardous?
- Is the control action hazardous if too late?
- Is the control action hazardous if too early?
- Is not providing control action hazardous?

Answering these questions allows the mapping of the UCA to the system hazards identified earlier. Twenty more UCAs get added to the exiting 43 by considering the time component of too early and too late. The updated UCA table with 63 unacceptable system states are listed in Table 8 under Appendix B.

5.6.2 Safety/security constraints

Safety/security constraints (SC) are enforced by the shovel operator (controller) on the AHS (controlled process). These can be derived directly from the UCAs and are listed in Table 9 under Appendix C.

5.7 Summary

This chapter focuses on STPA-Sec framework applied to the mining case with mine operator's perspective. As a first step in STPA-Sec framework, the problem of cybersecurity and safety in the mining system was defined and framed. Next, unacceptable losses and accidents were identified. These losses and accidents included financial and operational losses, in addition to safety losses, effectively increasing the scope of STPA from safety only to safety and security analysis.

System level hazards were derived by combining innate knowledge of the system with unacceptable losses. Hazards were identified as factors that can be controlled by safety and security artifacts designed into the system. SCs were derived from hazards. These constraints are system conditions that need to be satisfied so that no hazards and losses could occur.

A high-level functional control structure depicting control, feedback, and hierarchy in mine operator organization was adopted from the ConOps. Based on the objective of analyzing cybersecurity and safety in a sociotechnical subsystem, the functional control structure was further zoomed into. Interactions between the shovel operator, MOS, and autonomous haul truck were selected for further analysis and represented in the form of detailed control structure. This higher magnified control structure brings to light many more elements and interactions that were previously hidden in the functional control structure. The A-stop command issued by the shovel operator and directed at the autonomous haul truck was selected for safety and security analysis. A control loop based on STPA guidelines was developed for further analysis of A-stop control action.

From the control loop, process model variables were selected. Process model variables are used by the shovel operator to decide on whether to issue A-stop. Context table was created by considering valid combinations of process model variables along with analysis of the A-stop control action against a set of evaluation questions recommended by STPA. A UCA table was created from the context table, and SCs were identified from the UCAs.

6. SCENARIO IDENTIFICATION

The SCs developed in the previous section can be violated in two ways, given by:

- Shovel operator issues unsafe and unsecure control actions.
- Lack of proper execution of safe and secure control actions.

The shovel operator issuing unsafe and unsecure control actions can be attributed to elements depicted in the zone one of the control loop, as shown in Figure 28. Elements in the zone one includes the following:

- Sensors
- Shovel operator process model
- Shovel operator control algorithm
- Control/informational inputs from MOS

The lack of proper execution of safe and secure control actions can be mapped to elements in zone two of the control loop. Elements in zone two include the following:

- Actuators
- Control and informational inputs from MOS
- Haul truck autonomy controller

- PNT systems
- Feedback from the haul truck

Based on the characteristics of control and information flows and their failure modes under safety and security, Figure 28 also captures potential safety and security issues [40] [56] in the boxes next to their respective connective links. In addition, the control loop in Figure 28 also shows the expected control and information flows next to the connecting links.

The UCAs and SCs identified in the previous section connect with the concept of dividing the control structure into two zones. Incorrect control action result from issues originating in zone 1, while correct control action not being implemented can be attributed to issues from zone 2.

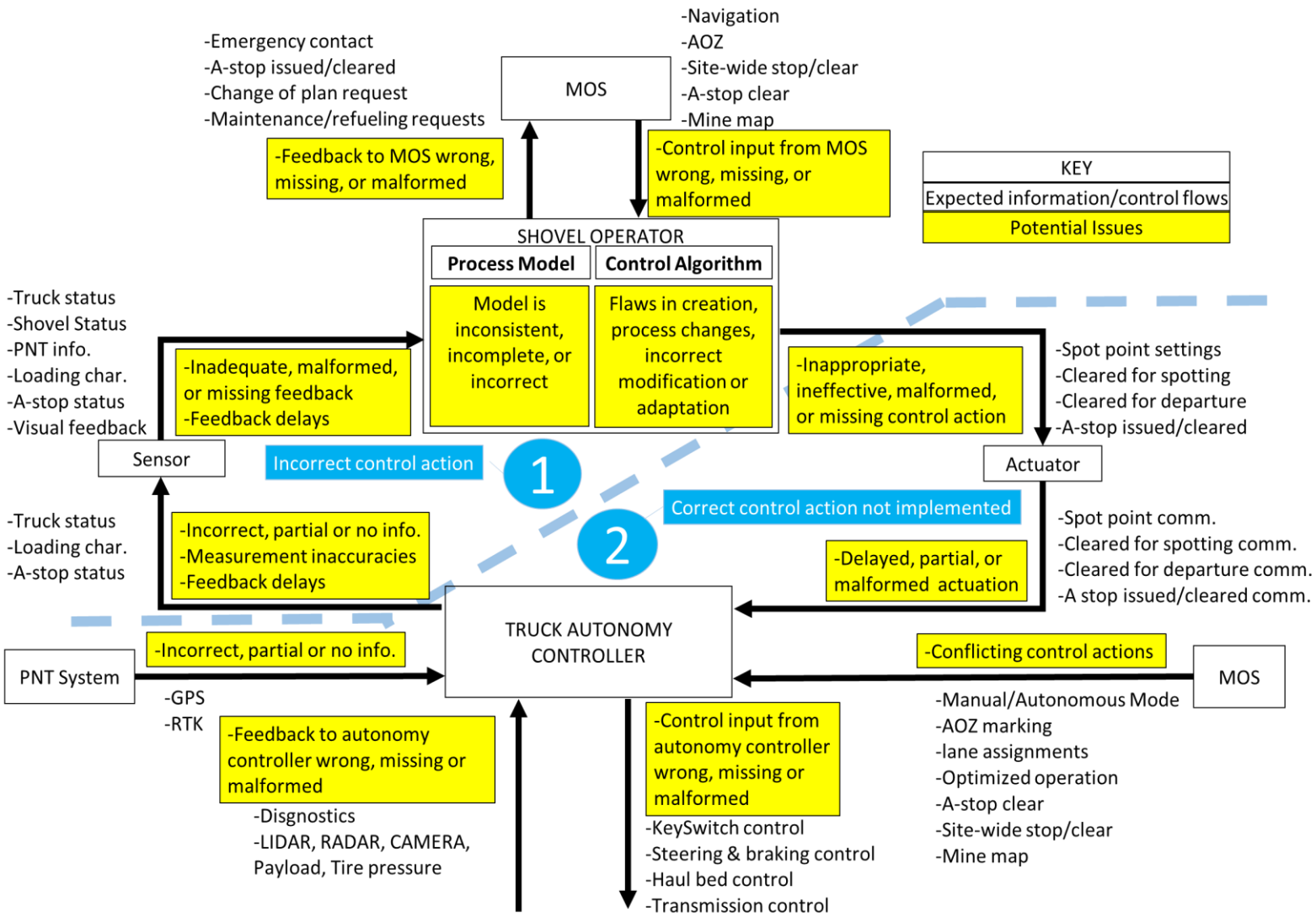

Figure 28 Control loop to causal factors

In the next few sections, five UCAs and SCs from Table 9 under Appendix C are considered with the objective for generating safety and security requirements. Selection of these UCAs and SCs is based on the perceived severity of damage that could result from them.

6.1 Process for generating scenarios using attack trees

Attack tress are used as an aid in the development of scenarios. The new five step process for generating scenarios from UCAs and SCs using attack trees is given by:

> STEP 1: Generate an attack goal statement from the UCA and make this the root node of the attack tree.
> STEP 2: Consult control loop zone one to think of the elements and their interactions that could result in the occurrence of the system state represented by root node of the attack tree.
> STEP 3: Add any identified possible element and/or interactions contributing in part or whole to the root node as the leaf nodes of the attack tree.
> STEP 4: If no further cause leading up to these new leaf nodes is found, then terminate the branch of the attack tree.
> STEP 5: Generate scenarios using branches likely to result in the achievement of attack goal.

Attack tree conventions to represent logic, likelihood, and other attributes of an attack are expected to be adhered to when following the above process.

6.2 UCA 9:

UCA 9 is given by:

> A-stop not provided when shovel operator expects waiting while the haul truck starts spotting and all systems are GO [H1, H3, H4].

The UCA 9 arises due to missing A-stop command that should have been issued by the shovel operator when the haul truck starts spotting since the truck should have stayed in the waiting area. At this time, all other essential support systems are assumed to be working as expected. Figure 29 depicts the UCA 9 scenario where the truck has moved out of autonomous haul truck waiting zone.

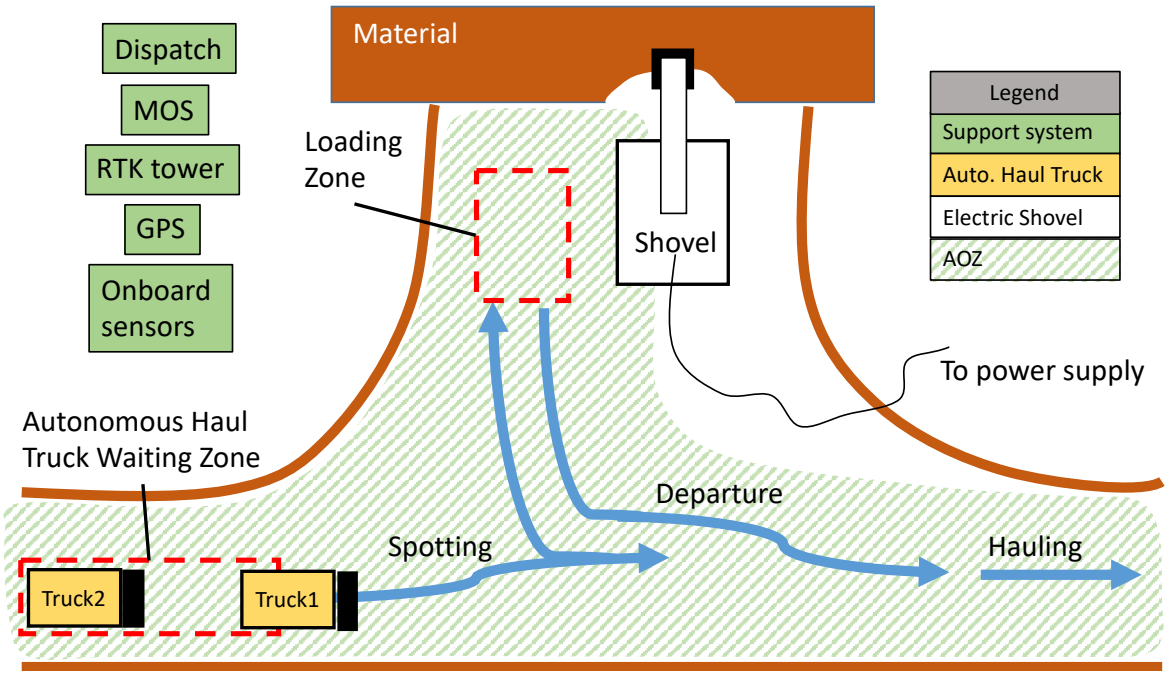

Figure 29 UCA & SC 9: autonomous truck starts spotting unexpectedly

6.2.1 UCA 9- Cause:

This is the condition when the shovel operator has not given a go ahead for spotting, but the haul truck starts spotting. The haul truck continues to spot, and the shovel operator never issues A-stop. Scenarios leading to UCA 9 are developed using attack tree shown in Figure 30. The goal of the attack, represented in the root node of the tree, is to make sure A-stop is not provided and the haul truck continues to spot. Different ways of achieving this goal are captured by the leaf nodes. In the attack tree of Figure 30, the AND logic between the branches is given by the presence of an arc connecting the branches, and OR logic is represented by the missing arc. In addition, the combined likelihood of two or more terminating leaf nodes resulting in a successful attack is represented by the single arc for AND logic along with letter L for ‘likely’ in the middle.

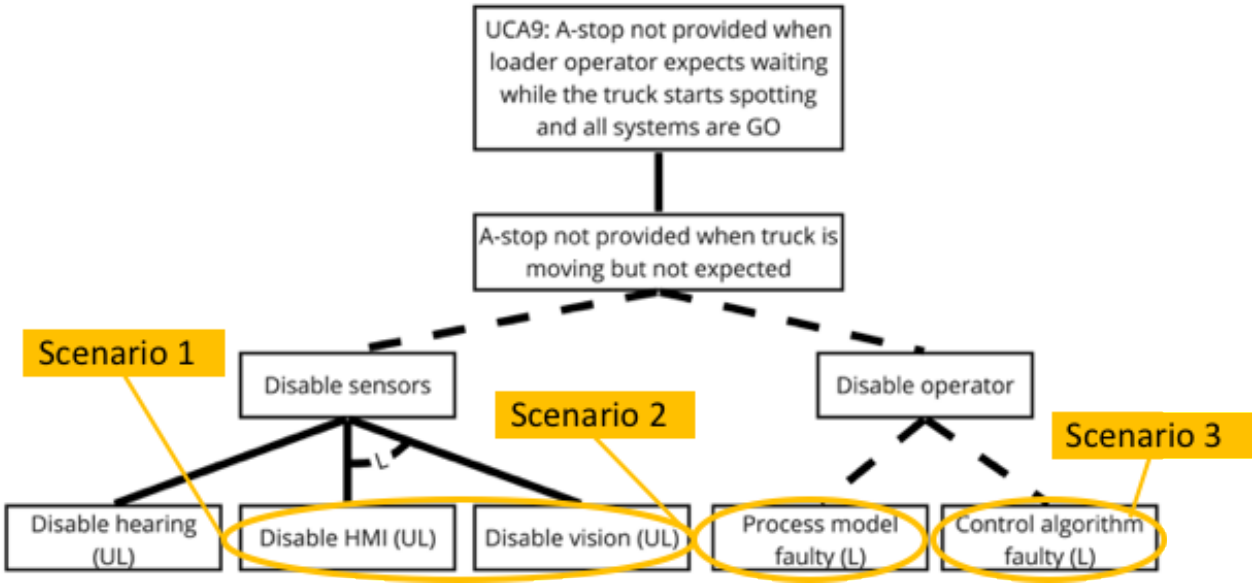

Figure 30 UCA 9: A-stop not provided when the truck is moving unexpectedly

Based on the control structure, lack of a correct control action can be attributed to the sensors, the MOS, and the shovel operator. Considering all the sensors available to the shovel operator along with standard operating procedure of the shovel before and during spotting, further leaf nodes are selected. These include human sensory inputs of hearing, and vision, which are relied heavily on by the operator even amid high technology. In addition, the operator receives a lot of information about his/her environment, including shovel, haul truck, and auxiliary equipment, through the HMI in the cab. Hence the three sensor elements that form the leaf nodes for "disable sensor" node include:

- Disable hearing
- Disable HMI
- Disable vision

Second leaf node for the root node is to disable the operator. Based on the control loop from Figure 28, shovel operator as a controller has two mission critical parts that could be faulty:

- Process model fault
- Control algorithm fault

It is assumed that MOS will not provide oversight or perform checks to ensure equipment operating in the AHS is performing as per functional design. Hence, MOS is not part of the attack tree in Figure 30.

Subsequent attack scenarios are generated using the identified elements from the attack tree along with expert judgement.

6.2.2 UCA 9 Scenario 1: HMI and operator vision are disabled

This is the condition when the operator is operating in low visibility, the HMI is disabled, and the haul truck start spotting for some reason. The operator is not aware that a situation requiring an A-stop has developed. This scenario is less likely because of the need for double conditions, however it is possible to have degraded HMIs due to out-synced firmware version where the device is either not asking for the required variables or other controllers don't have the support to provide variables requested by the HMI. This will result in the shovel operator being unaware of the haul truck movement and subsequent motion by the shovel could result in the shovel running into the haul truck.

6.2.2.1 UCA 9 Potential Mitigation for Scenario 1

The MOS scope could be increased to monitor and intervene by recommending A-stop to shovel operator. This step could be followed by attempts to contact the shovel operator over radio. Further, audible warnings could be added in the cab to indicate shovel-haul truck state mismatch or more simply indicate an approaching vehicle. Operational changes could also be suggested for the shovel driver to identify degraded HMIs. The shovel operator could be required to make sure no diagnostics are present on the HMI resulting from missing or incomplete expected information from other controllers and sensors on the shovel.

6.2.2.2 UCA 9 Requirements for Scenario 1:

R1. The MOS shall monitor machine interactions and intervene by recommending issuance of the A-stop to the shovel operator incase departure from expected behavior is observed [UCA9.S1].a

R2. The dispatch or the MOS shall contact shovel operator to identify reasons behind the lapse [UCA9.S1].

R3. The shovel HMI shall be equipped with audible warning beeps to indicate an approaching vehicle [UCA9.S1].

R4. The shovel operator shall identify and report all diagnostic codes and failure mode indicators (FMI) at the beginning of the shift [UCA9.S1].

6.2.3 UCA 9 Scenario 2: Operator does not know if anything is wrong

The second scenario concerns operator's faulty process model. Which essentially means that all the correct info is getting to the operator, but his/her process model output is inconsistent with the widely accepted process model.

6.2.3.1 UCA 9 Potential Mitigation for scenario 2:

Gaps between the shovel operator's process model and accepted process model needs to be identified and filled in through training. First time and recurring training should include scenarios where the A-stop is required to be issued. On a larger scope, shovel operator process model should be corrected and reinforced with the correct standard operating procedure at regular intervals.

6.2.3.2 UCA 9 Requirements for Scenario 2:

R5. The shovel operator shall be exposed to scenarios where the A-stop command should be issued [UCA9.S2].

6.2.4 UCA 9 Scenario 3: Operator does not know what A-stop is

Third scenario concerns operator's faulty control algorithm. This is the case when the operator correctly identifies a discrepancy between the output of his/her process model and the real world. Operator desires to address this gap but does not know how to do it.

6.2.4.1 UCA 9- Potential Mitigation for scenario 3:

The shovel operator training should focus on all the possible alternatives available incase deviation from acceptable haul truck behavior is observed.

6.2.4.2 UCA 9 Requirements for Scenario 3:

R6. The shovel operator shall be trained to perform all possible actions, including A-stop, when deviation in haul truck behavior is observed [UCA9.S3].

6.3 SC 9:

SC 9 is given by:

A-stop must be provided when shovel operator expects waiting while the haul truck starts spotting and all systems are GO.

The SC 9 arises due to incorrect implementation of an A-stop command that had been correctly issued by the shovel operator when the haul truck starts spotting while it should have stayed in the waiting area. At this time all other essential support systems are assumed to be working as expected. Figure 29 also depicts the SC 9 scenario where the truck has moved out of autonomous haul truck waiting zone.

6.3.1 SC 9 Cause:

This is the case when the shovel operator correctly identifies unexpected motion from the haul truck and issues an A-stop, but no impact of the command is observed on the haul truck. The elements that make the functional architecture and sequence of events involved from commanding of A-stop to its implementation at the autonomous haul truck level are as shown in Figure 31.

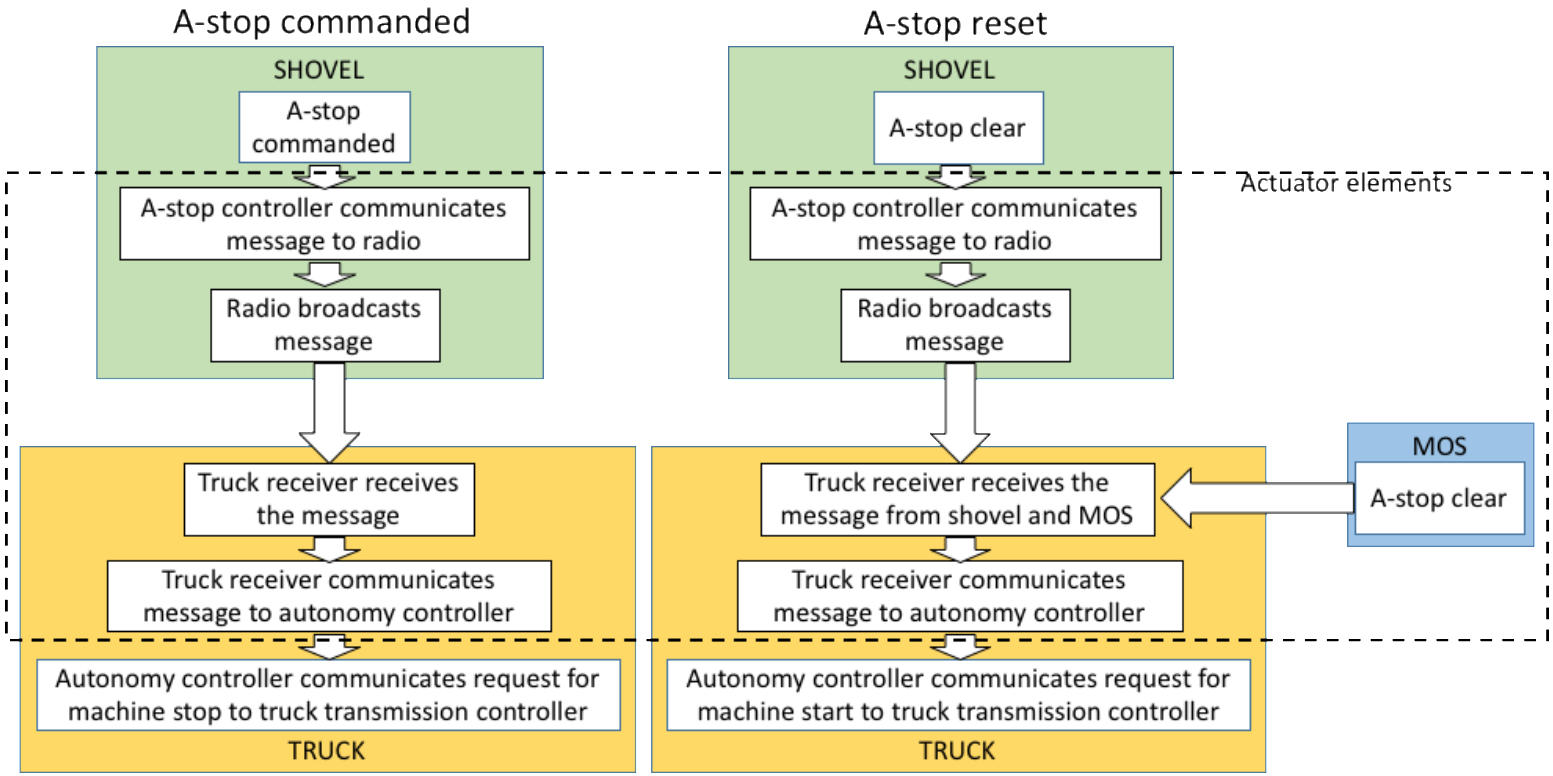

Figure 31 A-stop functional architecture

Once the A-stop command is issued by the shovel operator, it is processed by the A-stop controller. The controller then communicates the message to the radio transmitter. The radio broadcasts A-stop message for some duration and range. The haul truck radio receiver receives this message and transmits it to the autonomy controller, which then issues appropriate commands to transmission and other downstream controllers for bring the haul truck to a stop.

In the A-stop reset scenario, most of the functional elements and processes remain the same except for three changes. First change relates to the A-stop clear command as this functionality would require depressing a separate button by the operator. Second change relates to the commands issued by the haul truck autonomy controller. In the A-stop reset case, haul truck autonomy controller issues commands to low-level controllers so that the haul truck starts its motion again. Third and most important change comes from the MOS. To reset an active A-stop, in addition to reset command from the shovel operator, the haul truck requires a request for reset from the MOS. Only once A-stop reset request from shovel operator followed by similar request from MOS is received within a certain time window, does the haul truck autonomy controller process an A-stop reset. While any of the actuator elements could be attacked based on the attacker capability, as a first run at safety and security analysis, it is assumed that the attacker does not have access to the internal elements of shovel, haul truck, or MOS. Therefore, only radio communication is available for attack by an adversary.

The scenarios resulting in SC9 are developed using the attack tree in Figure 32 .The goal of the attack is to make sure that the A-stop command issued by the shovel operator does not get implemented by the autonomous haul truck. One of the ways to achieve this goal is given by disabling of the actuator. Based on the control loop of Figure 28, there are other elements of the system in zone two that can be leveraged for an attack. Considering the mechanics involved in the implementation of A-stop, it can be said that the A-stop command has no interaction with the MOS, PNT systems, or feedback from the haul truck, these elements are hence not accounted for in the attack tree.

Disabling of actuator can be achieved through either jamming or spoofing. These are represented as the two leaf nodes originating from “disable actuators” node in the attack tree of Figure 32.

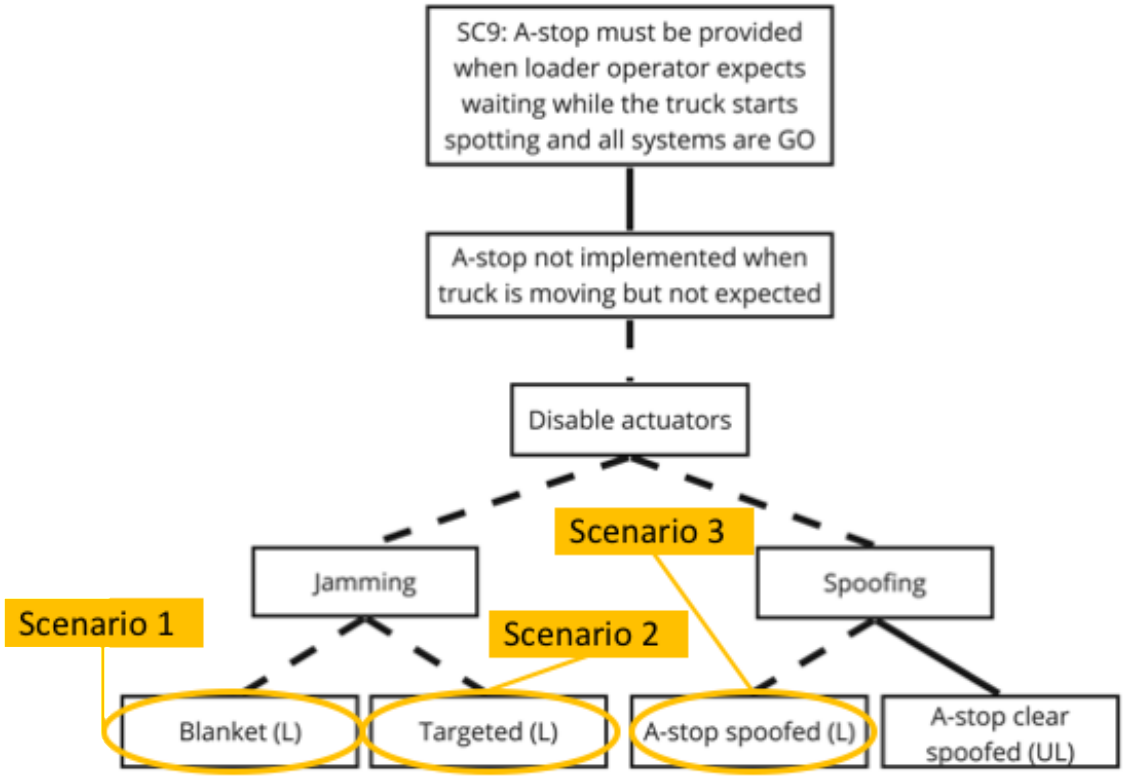

Figure 32 SC9: A-stop not implemented when truck is moving but not expected

Jamming represents a denial-of-service (DoS) attack where the attacker sniffs out the carrier frequencies being transmitted/broadcasted and then causes intentional interference to result in blanket or targeted jamming. Blanket and targeted jamming are the two leaf nodes originating from “jamming” node. Spoofing attack is defined as a situation where the attacker pretends to be a legitimate node in the system and communicates with other nodes with the objective to cause interference. Spoofing node has two leaf nodes, namely “A-stop spoofed” and “A-stop clear spoofed.” The node “A-stop spoofed” represents the attack event where the adversary can target the haul truck autonomy controller by issuing A-stop messages. “A-stop clear spoofed” is a bit more complex and sophisticated attack where the attacker can trick the haul truck autonomy controller by sending fabricated A-stop clear messages by pretending to be shovel operator and/or the MOS.

6.3.2 SC 9 Scenario 1: Blanket jamming of radio communication

The A-stop is initiated by the operator, but the message does not reach the haul truck autonomy controller due to jamming of all possible frequencies. It is assumed that the adversary would monitor and be aware of all active radio frequencies used near a shovel.

6.3.2.1 SC 9 Potential mitigation for scenario 1

It is hard to ensure that there is always no frequency sniffing taking place around mining equipment. A viable approach to mitigation could involve adding additional markers that could indicate the health of radio network between vehicles. One defensive degrade approach could be to support transmission and reception of heartbeat messages between the shovel and the autonomous haul truck. Loss of these health messages could be used for transitioning the haul truck into safe state, hence degraded but safe functionality. Other measures could include defensive evasion approach, offered for example, by channel hopping. As soon as jamming is detected, the transmitter could jump to a different channel to evade the effects of jamming and hence maintain functionality.

6.3.2.2 SC 9 Requirements for scenario 1

R7. The shovel and the haul truck shall implement methods to detect jamming with minimal loss of functionality [SC9.S1].

R8. The shovel and the haul truck shall have in place countermeasures to evade jamming without deterioration of functionality [SC9.S1].

R9. The haul truck shall transition into an extended safe state if countermeasures are found to be unsuccessful after finite time [SC9.S1].

6.3.3 SC 9 Scenario 2: Targeted jamming of A-stop communication

Instead of blanket jamming, which impacts all wireless communication between the shovel and the haul truck, the attacker could employ targeted jamming so that only A-stop communication is impacted. It is assumed that the attacker is aware of some attributes of the A-stop communication by observing, recording, and investigating instances of A-stop being commanded. This scenario has the potential of defeating some of the mitigation solutions suggested under scenario 1. For example, jamming of A-stop communication would in theory still allow other wireless communication between the shovel and the haul truck. Incase this ‘other' communication is used to detect jamming, then A-stop jamming shall go undetected, resulting in a potential safety hazard.

6.3.3.1 SC 9 Potential mitigation for scenario 2

A-stop command and channel health monitoring will need to be coupled such that jamming of A-stop signals alone should be enough to raise a flag in jamming detection process.

6.3.3.2 SC 9 Requirements for scenario 2

R10. Signal transmission health monitoring strategy shall account for individual channel jamming [SC9.S2].

6.3.4 SC9 Scenario 3: Spoofing of A-stop commands to cause disruption

The adversary in this scenario fabricates A-top commands and issues them pretending to be the shovel operator. These fabricated commands have some desired error in the implementation of protocol with the intention of expecting error response from the haul truck autonomy controller. The aim from adversary’s perspective is to inundate the autonomy controller with incorrect messages so that any valid A-stop message from the shovel operator gets buried in the traffic.

6.3.4.1 SC 9 Potential mitigation for scenario 3

Mitigation approach could start by classifying a message received by the autonomy controller according to safety and security priority. In addition, timers and counters could be added in the controller code to track the number and rate of incorrect messages received by the autonomy controller of the haul truck. High priority and repeatedly incorrect messages could be used as sufficient reason to transition the haul truck into safe state. Low priority and repeatedly incorrect messages could be used as a trigger for disabling respective functionality and issuing diagnostic codes, hence freeing up precious bandwidth and providing ample information for troubleshooting.

6.3.4.2 SC 9 Requirements for scenario 3

R11. Repeatedly incorrect A-stop commands within some time window shall result in the haul truck transitioning into safe state [SC9.S3].

6.4 UCA 16:

UCA 16 is given by:

A-stop not provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4].

The UCA 16 arises due to missing A-stop command that should have been issued by the shovel operator when the haul truck is spotting and the PNT systems are incorrect, delayed, or missing. Figure 33 depicts the UCA 16 scenario where the truck is spotting while RTK and GPS are inadequate.

6.4.1 UCA 16 Cause:

Since most of the elements and mechanisms involved are the same as UCA 9 and are not discussed in detail here. New information concerning UCA 16 is explained in detail.

Valid PNT information is critical to the shovel and haul truck operation. Referencing control loop from Figure 28, bad PNT entails incorrect, partial, or no information from PNT systems. The UCA 16 references the situation where the shovel operator does not command A-stop while PNT system is bad. The goal for this attack is derived from the UCA statement and is given by “A-stop not provided when haul truck is moving and PNT systems are bad.” The attack tree for UCA 16 is given in Figure 34.

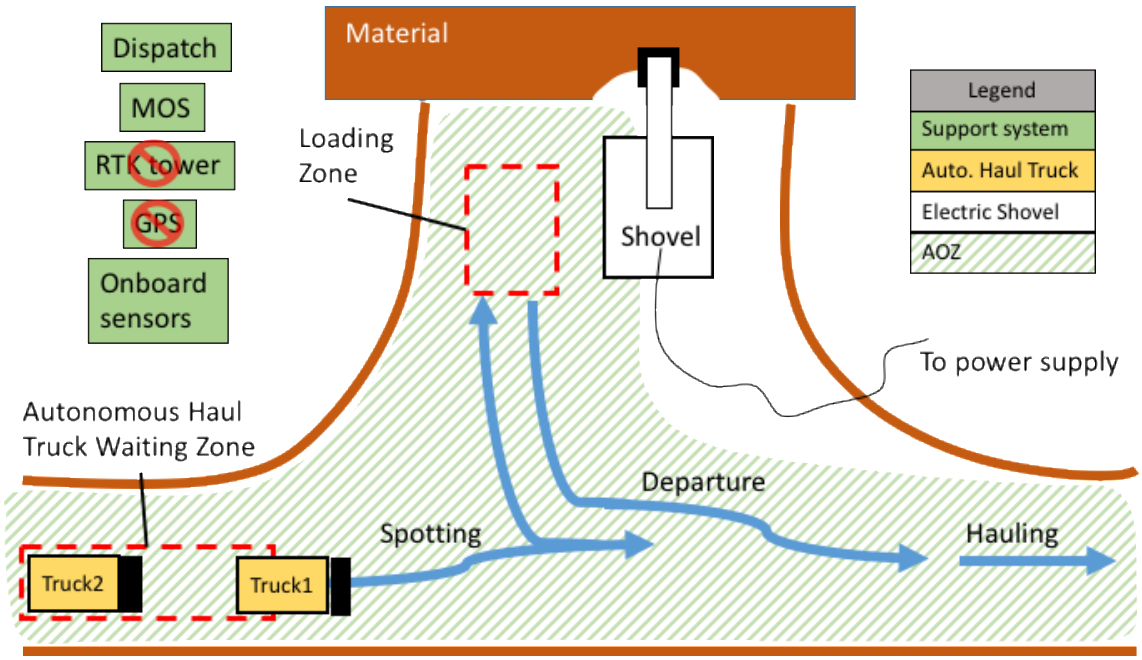

Figure 33 UCA & SC 16: autonomous truck is spotting and PNT systems fail

The root node given by the goal is connected to two leaf nodes namely "disabling sensors" and "disabling operator." Sensor inputs relevant to the PNT include the HMI and operator vision. Through HMI the shovel operator receives position and navigation information of the shovel and haul truck. Operator vision can also aid the operator in making a crude determination of haul truck's position when in line of sight. The two leaf nodes originating from "disable sensors" includes "disable HMI" and "disable vision." Both leaf nodes are unlikely because disabling an HMI requires access to haul truck physical network along with high degree of familiarity with propriety technology. While it is unlikely that a targeted attack on operator vision is possible, operations during periods of low visibility does lower operator's capability to visually detect haul trucks about to veer off-course.

The "disable operator" root node has two leaf nodes, namely "process model faulty" and "control algorithm faulty." It is assumed that the operator is presented with all the information that could allow him/her to decide about issuing A-stop due to incorrect, partial, or missing PNT information.

Faulty process model captures the event where the shovel operator is unable to identify any issues with the PNT systems, while the PNT systems are bad.

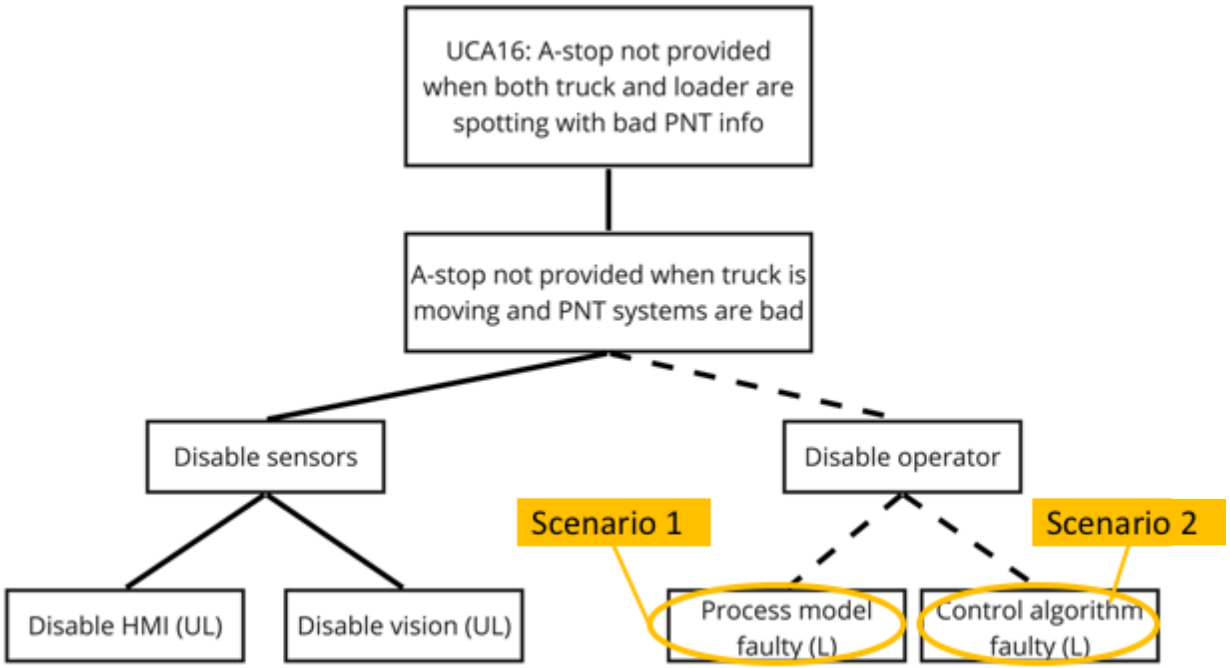

Figure 34 UCA16 A-stop not provided when truck is moving and PNT systems are bad

Faulty control algorithm captures the event where the shovel operator correctly identifies issues with the PNT systems but is unaware of the appropriate action that needs to follow and/or how to implement that action.

6.4.2 UCA16 Scenario 1: Operator unable to identify bad PNT systems

This scenario concerns the mental model of shovel operator. Based on all the information available to the operator, he/she is unable to identify anything amiss with the PNT system.

6.4.2.1 UCA16 Potential mitigation for scenario 1

This issue can be addressed by imparting training that focuses on identifying required information, processing of this information, and updating the process model. Information could be in the form of PNT health monitoring system recommendations, visual clues, etc.

Orthogonal requirements could be developed to satisfy the assumption that the operator has means to identify bad PNT. It should be required that PNT health monitoring systems be developed to identify bad PNT information at the asset level. For example, one implementation of such system could be in the form of oversight by the MOS. In this system, asset could share their vector information with the MOS, which then compares it with the latest topography information along with reference markers to find the asset's actual location. Actual and reported vector information could be compared to ascertain bad PNT.

6.4.2.2 UCA16 Requirements for scenario 1

R12. Shovel operator shall be trained to identify bad PNT information [UCA16.S1].

R13. Systems shall be put in place that could identify bad PNT information for every asset [UCA16.S1].

6.4.3 UCA16 Scenario 2: Operator does not know what to do with bad PNT systems

The shovel operator can identify bad PNT systems based on accurate process model, but he/she does not know what needs to be done next.

6.4.3.1 UCA16 Potential mitigation for scenario 2

The shovel operator should be provided with training that focuses on handling exceptions such as bad PNT information.

6.4.3.2 UCA16 Requirements for scenario 2

R14. Shovel operator shall be trained to decide and act on the PNT related issues identified by the operator's mental model [UCA16.S2].

R15. Shovel operator shall issue A-stop commands if PNT related gaps are above a threshold [UCA16.S2].

6.5 SC 16:

SC16 is given by:

A-stop must be provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing GPS and/or RTK info.

The SC 16 arises due to incorrect implementation of an A-stop command that had been correctly issued by the shovel operator when the PNT systems are inadequate while the haul truck is spotting. Figure 33 also depicts the SC 16 scenario where the truck is spotting while RTK and GPS are inadequate. For the given adversary capability, non-implementation of a valid A-stop with bad PNT will result in similar analysis and requirements as shown in SC 9.

6.6 Summary

Scenario generation is a process of guided brainstorming using the feedback control loop representation, attack trees, and expert knowledge. Attack goals were identified from the UCAs and SCs. The feedback control loop was divided into two zones, with one zone representing elements that could result in incorrect A-stop being issued by the shovel operator, and the other zone with elements that could result in non-implementation of a correct A-stop from the shovel operator.

Guided by common failure modes of the mining systems, events were identified that could lead to the achievement of the attack goal. The process of scenario identification was enhanced using attack trees with each branch representing unique attack vector. Attack scenarios were generated from valid attack tree branches. Each scenario was then used to generate one or more system safety and security requirements. Orthogonal requirements were also generated for systems and processes that stem out of assumptions used while generating scenarios. Requirements were generated for UCA 9, SC 9, and UCA 16 as an example of the STPA-Sec with attack tree scenario generation process.

7. CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

The goal of a mining operation invested in automation is to run a safe, sustainable, and profitable business by efficiently removing minerals from the earth using autonomous mining systems. Safety and security of a cyber-physical system such as the autonomous mining system is important to meeting that goal. Ensuring complete safety and security of the autonomous mining system such as the AHS is a difficult problem to tackle. The difficulty arises due to AHS inherent complexity and evolving adversary capabilities. However, high levels of system reliability can be ensured by considering safety and security factors during the product design phase.

Popular methods in use for functional safety and security analysis were explored. Security extensions to ISO26262 in the form of SAHARA and EVITA were analyzed. Methods proposed in SAE J3036 aimed primarily at cybersecurity of connected vehicles were also examined. Systems theory based STPA-Sec was considered for safety and security analysis of the AHS. Most of the ISO26262 and J3061 based methods were found to be good priming agents by setting the right approach to analyzing cybersecurity and resulting safety scenarios. However, the jump from priming to scenario identification was found to be rather large and almost always relying rather heavily on the expert judgement through brainstorming, and other chain-of-event failure models. As a result, the quality and quantity of scenarios directly depended on the expert. In addition, the reliance on expert experience could lead to side effects such as missing information due to assumptions and industry accepted dogmas.

The STPA-Sec framework also relies on expert judgement, but not to the same degree as its counterparts. By representing subsystems of interest in the form of a control loop and further dividing the loop into incorrect perception and incorrect implementation, a framework is set in place that aids the analyst in generating a rich set of scenarios to identify causal factors. The issues related to expert judgement are also observed with STPA-Sec. Scenario generation from UCA and SC rely on expert's experience and innate knowledge of the system and its failure modes. The implicit knowledge and missing causal links are captured very well by the attack trees, one of the methods recommended by J3036. A combined STPA-Sec with attack trees variant of the STPA analysis is applied on the A-stop command, one of the many critical commands issued in the shovel-truck-dispatch subsystem. The various capability assumptions, functional elements, and logical combinations involved in an attack become clear from the resulting attack trees. Enhanced scenario identification with attack trees was run on two UCA and SCs as a proof of concept. The

resulting requirements were found to be easy to trace to the originating UCA and SCs. This additional step of drawing the attack trees in the STPA analysis enables the analyst to go back and review the elements, sequence, and logic of events involved in an attack. The attack tree provides a method to make expert knowledge more tangible by presenting it on paper.

Some interesting high level insights emerged from the application of the STPA-Sec framework on the mining cybersecurity case. The shovel operator was found to operate blind during instrument failure and low visibility, resulting in high collision risk between the autonomous truck and the shovel. Addressing one possible cyberattack does not guarantee coverage against all other losses; stopping of the autonomous truck operation during jamming attack as a safety response still results in loss of production due to asset inoperability. There were no checks for incorrect navigation information, so if the intruder was able to transmit malicious PNT signals, he could take control of the autonomous truck and the shovel.

The STPA-Sec framework relies heavily on the stakeholders for defining the purpose of the analysis by identifying losses, system-level hazards, and safety constraints. A new and hybrid approach to defining the purpose of the STPA-Sec analysis could involve the use of system analysis techniques such as stakeholder analysis, needs analysis, and stakeholder mapping, to supplement the process of asking stakeholders for losses, hazards, and constraints. The resulting system goal from the application of the hybrid approach results in logical and seamless flow from the needs of the stakeholders to potential losses and system-level hazards.

One of the challenges related to the application of STPA is the problem of scaling. Based on the number of process model variables and their states, the system state table grows exponentially on adding commands and operational stages. With each entry in the system state table resulting in one or more scenarios, and each scenario resulting in multiple requirements, the number of scenarios and requirements can grow very quickly. Methods and procedures to track and analyze resulting requirements are still missing and need to be developed.

The high level of detail and thoroughness offered by STPA-Sec analysis can be leveraged by the popular standards such as the ISO26262 to develop a hybrid approach. Under the HARA stage of ISO26262, STPA-Sec could be used for analysis and hazard identification. The resulting artifacts from the application of STPA could be the scenarios generated from UCAs and SCs. Further, each scenario could be classified based on severity, exposure, and controllability. A sorted

list of scenarios based on ASIL and SecL levels could then be derived. Multiple safety and security goals with ASIL and SecL ratings could then be generated from each scenario.

BIBLIOGRAPHY

[1] Frost & Sullivan, "Digital Transformation in the Australian Mining Industry, Forecast to 2021".

[2] D. Walden, G. Roedler, K. Forsberg, D. Hamelin and T. Shortell, Systems engineering handbook : a guide for system life cycle processes and activities, Hoboken, New Jersey: Wiley, 2015.

[3] W. Young and N. Leveson, "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, 2014.

[4] N. Leveson and J. Thomas, "An STPA Primer," 1 08 2013. [Online]. Available: http://sunnyday.mit.edu/STPA-Primer-v0.pdf. [Accessed 1 6 2017].

[5] W. Young and N. Leveson, "Systems thinking for safety and security," in *Proceedings of the 29th Annual Computer Security Applications Conference*, 2013.

[6] N. Leveson and J. Thomas, "STPA Handbook," Cambridge, MA, 2018.

[7] W. Young, "A System-Theoretic Security Analysis Methodology for Assuring Complex Operations Against Cyber Disruptions," MIT Ph.D. dissertation, 2017.

[8] B. Cameron, D. Selva and E. Crawley, System Architecture: Strategy and Product Development for Complex Systems, Hoboken, NJ: Pearson Higher Education, 2016, pp. 210-211.

[9] edX, *The Business of Mining*, 2018.

[10] D. Fites, "Make your dealers your partners," *Harvard Business Review*, 1996.

[11] Caterpillar Inc., "Caterpillar Form 10-K," Unites States Securities and Exchange Commission, 2017.

[12] National Mining Association, "Mission and Objectives," 2018. [Online]. Available: https://nma.org/about-nma/mission-objectives/.

[13] United Mine Workers of America, "UMWA- who we represent," 2018. [Online]. Available: http://umwa.org/about/who-we-represent/.

[14] Society of Automotive Engineers, *J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, 2014.

[15] United States Environmental Protection Agency, "Regulatory Information By Sector-Mining," 2018. [Online]. Available: https://www.epa.gov/regulatory-information-sector/mining-except-oil-and-gas-sector-naics-212.

[16] Mine Safety and Health Administration, "Mission," 20 01 2018. [Online]. Available: https://www.msha.gov/about/mission.

[17] National Highway Traffic Safety Administration, "Cybersecurity Best Practices for Modern Vehicles," 2018. [Online]. Available: https://www.nhtsa.gov/.

[18] D. Dori, Object-process methodology: A holistic systems paradigm, Springer Science & Business Media, 2011.

[19] D. Dori, C. Linchevski and R. Manor, "OPCAT–An Object-Process CASE Tool for OPM-Based Conceptual Modelling," in *1st International Conference on Modelling and Management of Engineering Processes*, 2010.

[20] National Aeronautics and Space Administration, "NASA Systems Engineering Handbook," 2017. [Online]. Available: https://www.nasa.gov/connect/ebooks/nasa-systems-engineering-handbook.

[21] B. Hofmann-Wellenhof, H. Lichtenegger and J. Collins, Global positioning system: theory and practice, Springer Science & Business Media, 2001.

[22] GPS.gov, "GPS Accuracy," 5 Dec 2017. [Online]. Available: https://www.gps.gov/systems/gps/performance/accuracy/.

[23] Garmin Inc., "What is GPS?," 2017. [Online]. Available: https://www8.garmin.com/aboutGPS/.

[24] Caterpillar Inc., "Command for dozing to the rescue.," October 2015. [Online]. Available: https://www.caterpillar.com/en/news/caterpillarNews/innovation/command-for-dozing-to-the-rescue.html.

[25] Caterpillar Inc., "CAT Command Truck Spotting," [Online]. Available: https://www.cat.com/en_US/by-industry/mining/articles/truckspottingsystem.html.

[26] Caterpillar Inc., "Cat payload with production measurement," Caterpillar Inc., 2018. [Online]. Available: https://www.cat.com/en_US/products/new/technology/payload/payload/1000030237.html.

[27] S. Behere and M. Torngren, "A functional architecture for autonomous driving," in *First International Workshop on Automotive Software Architecture (WASA)*, Montreal, 2015.

[28] K. Matheus and T. Königseder, Automotive Ethernet, Cambridge University Press, 2017.

[29] International Organization for Standardization, "ISO26262: Road vehicles- functional safety," ISO, 2011.

[30] S. Grubmüller, J. Plihal and P. Nedoma, "Automated Driving from the View of Technical Standards," in *Automated driving*, Springer, 2017, pp. 29-40.

[31] G. Macher, H. Sporer, R. Berlach, E. Armengaud and C. Kreiner, "SAHARA: A Security-Aware Hazard and Risk Analysis Method," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, 2015.

[32] S. Hernan, S. Lambert, T. Ostwald and A. Shostack, "Uncover Security Design Flaws Using the STRIDE Approach," MSDN, 2006.

[33] D. Ward, I. Ibarra and A. Ruddle, "Threat Analysis and Risk Assessment in Automotive Cyber Security," *SAE Int. J. Passeng. Cars*, 2013.

[34] N. Leveson, Engineering a safer world: Systems thinking applied to safety, Cambridge, MA: MIT press, 2011.

[35] N. Leveson, "A new accident model for engineering safer systems," *Safety science*, 2004.

[36] N. Leveson, "A systems-theoretic approach to safety in software-intensive systems.," *IEEE Transactions on Dependable and Secure computing*, 2004.

[37] W. Young and N. Leveson, "Systems thinking for safety and security," in *29th Annual Computer Security Applications Conference*, 2013.

[38] W. Young and R. Porada, "System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA," in *STAMP Conference*, Boston, 2017.

[39] J. Thomas, "Systems Theoretic Process Analysis (STPA) Tutorial," Cambridge, 2013.

[40] W. Young, "Systems-theoretic security engineering analysis," MIT Thesis.

[41] P. A. Yannakogeorgos and A. B. Lowther, Conflict and Cooperation in Cyberspace: The Challenge to National Security, CRC Press, 2013.

[42] C. W. Lee, "A system theoretic approach to cybersecurity risks analysis of passenger autonomous vehicles," MIT Thesis, Cambridge, 2018.

[43] S. Kriaa, L. Pietre-Cambacedes, M. Bouissou and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety,* 2015.

[44] C. Schmittner, Z. Ma and P. Puschner, "Limitation and improvement of STPA-Sec for safety and security co-analysis," in *International Conference on Computer Safety, Reliability, and Security*, 2016.

[45] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty and S. Sezer, "STPA-SafeSec: safety and security analysis for cyber-physical systems," *Journal of Information Security and Applications,* 2017.

[46] W. G. Temple, Y. Wu, B. Chen and Z. Kalbarczyk, "Reconciling Systems-Theoretic and Component-Centric Methods for Safety and Security Co-analysis," in *International Conference on Computer Safety, Reliability, and Security*, 2017.

[47] Society of Automotive Engineers, J3061: Surface Vehicle Recommended Practice - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, Troy: SAE International, 2016.

[48] B. Schneier, "Attack trees," 2018. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html. [Accessed July 2018].

[49] G. Falco, A. Viswanathan, C. Caldera and H. Shrobe, "A Master Attack Methodology for an AI-Based Automated Attack Planner for Smart Cities," *IEEE Access,* 2018.

[50] C. Schmittner, Z. Ma, C. Reyes, O. Dillinger and P. Puschner, "Using SAE J3061 for Automotive Security Requirement Engineering," in *International Conference on Computer Safety, Reliability, and Security*, 2016.

[51] Deloitte Review, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," 25 7 2016. [Online]. Available: https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html.

[52] A. Paul, N. Chilamkurti, A. Daniel and S. Rho, Intelligent Vehicular Networks and Communications: Fundamentals, Architectures and Solutions, Elsevier Science and Technology Books, Inc., 2017.

[53] Caterpillar Inc., "Command for hauling," [Online]. Available: http://s7d2.scene7.com/is/content/Caterpillar/C10338825.

[54] FCC ID.io, "Autonomous stop (A-stop) system for autonomous hauling," 18 January 2012. [Online]. Available: https://fccid.io/PQMASTOP2/User-Manual/User-Manual-1664966.

[55] Caterpillar Inc., "Miners get an inside look at technology," [Online]. Available: https://www.cat.com/en_US/articles/customer-stories/mining/miners-get-look-at-technology.html.

[56] J. Thomas, "Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis," Massachusetts Institute of Technology, Cambridge, 2013.

[57] P. Friend, "Truck spotting system using position detection and perception". United States of America Patent US20160035149A1, 2014.

[58] Electricity- Information Sharing and Analysis Center and SANS- Industrial Control Systems, "Analysis of the cyber attack on the Ukrainian power grid," 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

[59] K. Grover, L. Alvin and Y. Qing, "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey," *International Journal of Ad Hoc and Ubiquitous Computing*, 2014.

[60] F. Arteaga, Nehring, Knights and J. Camus, "Schemes of Exploitation in Open Pit Mining," in *Mine Planning and Equipment Selection Conference*, 2014.

[61] Mine Safety and Health Administration, "Fatality Alert - Fatality #22 - November 25, 2014," 2014. [Online]. Available: https://www.msha.gov/data-reports/fatality-reports/2014/fatality-22-november-25-2014/fatality-alert.

[62] Mine Safety and Health Administration, "MNM Serious Accident Alert Surface - Haul Truck," 2017. [Online]. Available: https://www.msha.gov/news-media/alerts-hazards/mnm-serious-accident-alert-surface-haul-truck.

[63] newatlas.com, "University of Texas team takes control of a yacht by spoofing its GPS," 11 08 2013. [Online]. Available: https://newatlas.com/gps-spoofing-yacht-control/28644/.

[64] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity v1.1," NIST, 05 12 2017. [Online]. Available: https://www.nist.gov/.

[65] Mining Industry Human Resources Council, "Mine dispatcher career profile," [Online]. Available: https://www.mihr.ca/pdf/careers/39_mine-dispatcher-english_002.pdf.

[66] Mining Industry Human Resources Council, "Heavy equipment operator career profile," [Online]. Available: https://www.mihr.ca/pdf/careers/25_heavy-equipment-operator-career-profile-english_final-govt.pdf.

Appendix A: Context Table for A-stop Control Action

The context table is generated using different combinations of the process model variable states. Each entry in the context table represents a potential state of the mining system under study. The column "validity remark" carries more information regarding the importance of the particular system state.

Table 7 Context table for the shovel operator issuing A-Stop control action

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
1	waiting	waiting- idle	adequate	adequate	adequate	All good
2	waiting	waiting- idle	adequate	adequate	inadequate	Both haul truck and shovel operator are waiting while Incorrect, delayed, or missing commands from MOS
3	waiting	waiting- idle	adequate	inadequate	adequate	Both haul truck and shovel operator are waiting while Incorrect, delayed, or missing GPS and/or RTK info
4	waiting	waiting- idle	adequate	inadequate	inadequate	Double failure
5	waiting	waiting- idle	inadequate	adequate	adequate	Both haul truck and shovel operator are waiting while Incorrect, delayed, or missing info from onboard sensors

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
6	waiting	waiting- idle	inadequate	adequate	inadequate	Double failure
7	waiting	waiting- idle	inadequate	inadequate	adequate	Double failure
8	waiting	waiting- idle	inadequate	inadequate	inadequate	Double failure
9	waiting	waiting-spotting	adequate	adequate	adequate	Shovel operator expects spotting while the haul truck is still waiting, and all systems are GO
10	waiting	waiting-spotting	adequate	adequate	inadequate	Shovel operator expects spotting while the haul truck is still waiting and Incorrect, delayed, or missing commands from MOS
11	waiting	waiting-spotting	adequate	inadequate	adequate	Shovel operator expects spotting while the haul truck is still waiting and Incorrect, delayed, or missing GPS and/or RTK info

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
12	waiting	waiting-spotting	adequate	inadequate	inadequate	Double failure
13	waiting	waiting-spotting	inadequate	adequate	adequate	Shovel operator expects spotting while the haul truck is still waiting and Incorrect, delayed, or missing info from onboard sensors
14	waiting	waiting-spotting	inadequate	adequate	inadequate	Double failure
15	waiting	waiting-spotting	inadequate	inadequate	adequate	Double failure
16	waiting	waiting-spotting	inadequate	inadequate	inadequate	Double failure
17	waiting	loading	adequate	adequate	adequate	Unlikely
18	waiting	loading	adequate	adequate	inadequate	Unlikely

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
19	waiting	loading	adequate	inadequate	adequate	Unlikely
20	waiting	loading	adequate	inadequate	inadequate	Double failure
21	waiting	loading	inadequate	adequate	adequate	Unlikely
22	waiting	loading	inadequate	adequate	inadequate	Double failure
23	waiting	loading	inadequate	inadequate	adequate	Double failure
24	waiting	loading	inadequate	inadequate	inadequate	Double failure
25	waiting	waiting-departing	adequate	adequate	adequate	Unlikely

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
26	waiting	waiting-departing	adequate	adequate	inadequate	Unlikely
27	waiting	waiting-departing	adequate	inadequate	adequate	Unlikely
28	waiting	waiting-departing	adequate	inadequate	inadequate	Double failure
29	waiting	waiting-departing	inadequate	adequate	adequate	Unlikely
30	waiting	waiting-departing	inadequate	adequate	inadequate	Double failure
31	waiting	waiting-departing	inadequate	inadequate	adequate	Double failure
32	waiting	waiting-departing	inadequate	inadequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
33	spotting	waiting- idle	adequate	adequate	adequate	Shovel operator expects waiting while the haul truck starts spotting and all systems are GO
34	spotting	waiting- idle	adequate	adequate	inadequate	Shovel operator expects waiting while the haul truck starts spotting and Incorrect, delayed, or missing commands from MOS
35	spotting	waiting- idle	adequate	inadequate	adequate	Shovel operator expects waiting while the haul truck starts spotting and Incorrect, delayed, or missing GPS and/or RTK info
36	spotting	waiting- idle	adequate	inadequate	inadequate	Double failure
37	spotting	waiting- idle	inadequate	adequate	adequate	Shovel operator expects waiting while the haul truck starts spotting and Incorrect, delayed, or missing info from onboard sensors
38	spotting	waiting- idle	inadequate	adequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
39	spotting	waiting- idle	inadequate	inadequate	adequate	Double failure
40	spotting	waiting- idle	inadequate	inadequate	inadequate	Double failure
41	spotting	waiting-spotting	adequate	adequate	adequate	All good
42	spotting	waiting-spotting	adequate	adequate	inadequate	Both haul truck and shovel operator are spotting and Incorrect, delayed, or missing commands from MOS
43	spotting	waiting-spotting	adequate	inadequate	adequate	Both haul truck and shovel operator are spotting and Incorrect, delayed, or missing GPS and/or RTK info
44	spotting	waiting-spotting	adequate	inadequate	inadequate	Double failure
45	spotting	waiting-spotting	inadequate	adequate	adequate	Both haul truck and shovel operator are spotting and Incorrect, delayed, or missing info from onboard sensors

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
46	spotting	waiting-spotting	inadequate	adequate	inadequate	Double failure
47	spotting	waiting-spotting	inadequate	inadequate	adequate	Double failure
48	spotting	waiting-spotting	inadequate	inadequate	inadequate	Double failure
49	spotting	loading	adequate	adequate	adequate	Shovel operator starts loading while the haul truck is still spotting, and all systems are GO
50	spotting	loading	adequate	adequate	inadequate	Shovel operator starts loading while the haul truck is still spotting and Incorrect, delayed, or missing commands from MOS
51	spotting	loading	adequate	inadequate	adequate	Shovel operator starts loading while the haul truck is still spotting and Incorrect, delayed, or missing GPS and/or RTK info

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
52	spotting	loading	adequate	inadequate	inadequate	Double failure
53	spotting	loading	inadequate	adequate	adequate	Shovel operator starts loading while the haul truck is still spotting and Incorrect, delayed, or missing info from onboard sensors
54	spotting	loading	inadequate	adequate	inadequate	Double failure
55	spotting	loading	inadequate	inadequate	adequate	Double failure
56	spotting	loading	inadequate	inadequate	inadequate	Double failure
57	spotting	waiting-departing	adequate	adequate	adequate	Unlikely
58	spotting	waiting-departing	adequate	adequate	inadequate	Unlikely

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
59	spotting	waiting-departing	adequate	inadequate	adequate	Unlikely
60	spotting	waiting-departing	adequate	inadequate	inadequate	Double failure
61	spotting	waiting-departing	inadequate	adequate	adequate	Unlikely
62	spotting	waiting-departing	inadequate	adequate	inadequate	Double failure
63	spotting	waiting-departing	inadequate	inadequate	adequate	Double failure
64	spotting	waiting-departing	inadequate	inadequate	inadequate	Double failure
65	loading	waiting- idle	adequate	adequate	adequate	Unlikely

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
66	loading	waiting- idle	adequate	adequate	inadequate	Unlikely
67	loading	waiting- idle	adequate	inadequate	adequate	Unlikely
68	loading	waiting- idle	adequate	inadequate	inadequate	Double failure
69	loading	waiting- idle	inadequate	adequate	adequate	Unlikely
70	loading	waiting- idle	inadequate	adequate	inadequate	Double failure
71	loading	waiting- idle	inadequate	inadequate	adequate	Double failure
72	loading	waiting- idle	inadequate	inadequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
73	loading	waiting-spotting	adequate	adequate	adequate	Shovel operator is spotting while the haul truck is in loading mode and all systems are GO
74	loading	waiting-spotting	adequate	adequate	inadequate	Shovel operator is spotting while the haul truck is in loading mode and Incorrect, delayed, or missing commands from MOS
75	loading	waiting-spotting	adequate	inadequate	adequate	Shovel operator is spotting while the haul truck is in loading mode and Incorrect, delayed, or missing GPS and/or RTK info
76	loading	waiting-spotting	adequate	inadequate	inadequate	Double failure
77	loading	waiting-spotting	inadequate	adequate	adequate	Shovel operator is spotting while the haul truck is in loading mode and Incorrect, delayed, or missing info from onboard sensors
78	loading	waiting-spotting	inadequate	adequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
79	loading	waiting-spotting	inadequate	inadequate	adequate	Double failure
80	loading	waiting-spotting	inadequate	inadequate	inadequate	Double failure
81	loading	loading	adequate	adequate	adequate	All good
82	loading	loading	adequate	adequate	inadequate	Shovel operator is loading, and haul truck is in loading mode and Incorrect, delayed, or missing commands from MOS
83	loading	loading	adequate	inadequate	adequate	Shovel operator is loading, and haul truck is in loading mode and Incorrect, delayed, or missing GPS and/or RTK info
84	loading	loading	adequate	inadequate	inadequate	Double failure
85	loading	loading	inadequate	adequate	adequate	Shovel operator is loading, and haul truck is in loading mode and Incorrect, delayed, or missing info from onboard sensors

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
86	loading	loading	inadequate	adequate	inadequate	Double failure
87	loading	loading	inadequate	inadequate	adequate	Double failure
88	loading	loading	inadequate	inadequate	inadequate	Double failure
89	loading	waiting-departing	adequate	adequate	adequate	Shovel operator expects the haul truck to depart while the haul truck expects loading and all system are GO
90	loading	waiting-departing	adequate	adequate	inadequate	Shovel operator expects the haul truck to depart while the haul truck expects loading and Incorrect, delayed, or missing commands from MOS
91	loading	waiting-departing	adequate	inadequate	adequate	Shovel operator expects the haul truck to depart while the haul truck expects loading and Incorrect, delayed, or missing GPS and/or RTK info

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
92	loading	waiting-departing	adequate	inadequate	inadequate	Double failure
93	loading	waiting-departing	inadequate	adequate	adequate	Shovel operator expects the haul truck to depart while the haul truck expects loading and Incorrect, delayed, or missing info from onboard sensors
94	loading	waiting-departing	inadequate	adequate	inadequate	Double failure
95	loading	waiting-departing	inadequate	inadequate	adequate	Double failure
96	loading	waiting-departing	inadequate	inadequate	inadequate	Double failure
97	departing	waiting- idle	adequate	adequate	adequate	Shovel operator think the haul truck has finished departing while the haul truck is still departing, and all systems are GO

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
98	departing	waiting- idle	adequate	adequate	inadequate	Shovel operator think the haul truck has finished departing while the haul truck is still departing and Incorrect, delayed, or missing commands from MOS
99	departing	waiting- idle	adequate	inadequate	adequate	Shovel operator think the haul truck has finished departing while the haul truck is still departing and Incorrect, delayed, or missing GPS and/or RTK info
100	departing	waiting- idle	adequate	inadequate	inadequate	Double failure
101	departing	waiting- idle	inadequate	adequate	adequate	Shovel operator think the haul truck has finished departing while the haul truck is still departing and Incorrect, delayed, or missing info from onboard sensors
102	departing	waiting- idle	inadequate	adequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
103	departing	waiting- idle	inadequate	inadequate	adequate	Double failure
104	departing	waiting- idle	inadequate	inadequate	inadequate	Double failure
105	departing	waiting-spotting	adequate	adequate	adequate	Unlikely
106	departing	waiting-spotting	adequate	adequate	inadequate	Unlikely
107	departing	waiting-spotting	adequate	inadequate	adequate	Unlikely
108	departing	waiting-spotting	adequate	inadequate	inadequate	Double failure
109	departing	waiting-spotting	inadequate	adequate	adequate	Unlikely

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
110	departing	waiting-spotting	inadequate	adequate	inadequate	Double failure
111	departing	waiting-spotting	inadequate	inadequate	adequate	Double failure
112	departing	waiting-spotting	inadequate	inadequate	inadequate	Double failure
113	departing	loading	adequate	adequate	adequate	Shovel operator is loading while the haul truck starts departing and all systems are GO
114	departing	loading	adequate	adequate	inadequate	Shovel operator is loading while the haul truck starts departing and Incorrect, delayed, or missing commands from MOS
115	departing	loading	adequate	inadequate	adequate	Shovel operator is loading while the haul truck starts departing and Incorrect, delayed, or missing GPS and/or RTK info

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
116	departing	loading	adequate	inadequate	inadequate	Double failure
117	departing	loading	inadequate	adequate	adequate	Shovel operator is loading while the haul truck starts departing and Incorrect, delayed, or missing info from onboard sensors
118	departing	loading	inadequate	adequate	inadequate	Double failure
119	departing	loading	inadequate	inadequate	adequate	Double failure
120	departing	loading	inadequate	inadequate	inadequate	Double failure
121	departing	waiting-departing	adequate	adequate	adequate	All good
122	departing	waiting-departing	adequate	adequate	inadequate	Shovel operator is waiting as the haul truck is departing and Incorrect, delayed, or missing commands from MOS

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
123	departing	waiting-departing	adequate	inadequate	adequate	Shovel operator is waiting as the haul truck is departing and Incorrect, delayed, or missing GPS and/or RTK info
124	departing	waiting-departing	adequate	inadequate	inadequate	Double failure
125	departing	waiting-departing	inadequate	adequate	adequate	Shovel operator is waiting as the haul truck is departing and Incorrect, delayed, or missing info from onboard sensors
126	departing	waiting-departing	inadequate	adequate	inadequate	Double failure
127	departing	waiting-departing	inadequate	inadequate	adequate	Double failure
128	departing	waiting-departing	inadequate	inadequate	inadequate	Double failure
129	hauling	waiting- idle	adequate	adequate	adequate	All good

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
130	hauling	waiting- idle	adequate	adequate	inadequate	Shovel operator is idle and getting ready for the next haul truck and Incorrect, delayed, or missing commands from MOS
131	hauling	waiting- idle	adequate	inadequate	adequate	Shovel operator is idle and getting ready for the next haul truck and Incorrect, delayed, or missing GPS and/or RTK info
132	hauling	waiting- idle	adequate	inadequate	inadequate	Double failure
133	hauling	waiting- idle	inadequate	adequate	adequate	Shovel operator is idle and getting ready for the next haul truck and Incorrect, delayed, or missing info from onboard sensors
134	hauling	waiting- idle	inadequate	adequate	inadequate	Double failure
135	hauling	waiting- idle	inadequate	inadequate	adequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
136	hauling	waiting- idle	inadequate	inadequate	inadequate	Double failure
137	hauling	waiting-spotting	adequate	adequate	adequate	Unlikely
138	hauling	waiting-spotting	adequate	adequate	inadequate	Unlikely
139	hauling	waiting-spotting	adequate	inadequate	adequate	Unlikely
140	hauling	waiting-spotting	adequate	inadequate	inadequate	Double failure
141	hauling	waiting-spotting	inadequate	adequate	adequate	Unlikely
142	hauling	waiting-spotting	inadequate	adequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
143	hauling	waiting-spotting	inadequate	inadequate	adequate	Double failure
144	hauling	waiting-spotting	inadequate	inadequate	inadequate	Double failure
145	hauling	loading	adequate	adequate	adequate	Unlikely
146	hauling	loading	adequate	adequate	inadequate	Unlikely
147	hauling	loading	adequate	inadequate	adequate	Unlikely
148	hauling	loading	adequate	inadequate	inadequate	Double failure
149	hauling	loading	inadequate	adequate	adequate	Unlikely

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
150	hauling	loading	inadequate	adequate	inadequate	Double failure
151	hauling	loading	inadequate	inadequate	adequate	Double failure
152	hauling	loading	inadequate	inadequate	inadequate	Double failure
153	hauling	waiting-departing	adequate	adequate	adequate	Unlikely
154	hauling	waiting-departing	adequate	adequate	inadequate	Unlikely
155	hauling	waiting-departing	adequate	inadequate	adequate	Unlikely
156	hauling	waiting-departing	adequate	inadequate	inadequate	Double failure

Sr. No.	AT	Shovel Operator	Onboard Sensor	PNT	MOS	Validity Remark
157	hauling	waiting-departing	inadequate	adequate	adequate	Unlikely
158	hauling	waiting-departing	inadequate	adequate	inadequate	Double failure
159	hauling	waiting-departing	inadequate	inadequate	adequate	Double failure
160	hauling	waiting-departing	inadequate	inadequate	inadequate	Double failure

Appendix B: Refined Context Table for A-stop Control Action

The context table in appendix A is refined by removing invalid, good, and double fault system states, with the remaining 63 system states represented in the table below. Each system state from the table is mapped to the identified system hazards by answering four questions given by:

1. Does not providing the control action causes a hazard?
2. Does providing the control action causes a hazard?
3. Does providing the control action too early, too late, out of order cause a hazard?
4. Does control action stopped too soon or applied too long cause a hazard?

In the table below, columns with names 1-4 are indicative of the question number. Entries under these columns capture the associated hazard code.

Table 8 Updated context table for the shovel operator issuing A-Stop control action

Sr. No.	Control Action	Autonomous Truck	Shovel Operator	Onboard Sensor	PNT	MOS	1	2	3	4
1	A-stop	waiting	waiting-idle	adequate	adequate	inadequate	H4	No	No	H3
2		waiting	waiting-idle	adequate	inadequate	adequate	H4	No	No	H3
3		waiting	waiting-idle	inadequate	adequate	adequate	H4	No	No	H3
4		waiting	waiting-spotting	adequate	adequate	adequate	H4	No	No	H3
5		waiting	waiting-spotting	adequate	adequate	adequate	H4	No	H4	H3

Sr. No.	Control Action	Autonomous Truck	Shovel Operator	Onboard Sensor	PNT	MOS	1	2	3	4
6		waiting	waiting-spotting	adequate	adequate	inadequate	H4	No	No	H3
7	A-stop	waiting	waiting-spotting	adequate	inadequate	adequate	H4	No	No	H3
8		waiting	waiting-spotting	inadequate	adequate	adequate	H4	No	No	H3
9		spotting	waiting-idle	adequate	adequate	adequate	H4	No	No	H1, H3
10		spotting	waiting-idle	adequate	adequate	adequate	H4	H1	No	H1, H3
11		spotting	waiting-idle	adequate	adequate	inadequate	H4	No	No	H1, H2, H3
12		spotting	waiting-idle	adequate	inadequate	adequate	H4	No	No	H1, H2, H3
13		spotting	waiting-idle	inadequate	adequate	adequate	H4	No	No	H1, H2, H3
14		spotting	waiting-spotting	adequate	adequate	inadequate	H4	No	No	H1, H2, H3
15		spotting	waiting-spotting	adequate	adequate	inadequate	H4	H1, H2	No	H1, H2, H3
16		spotting	waiting-spotting	adequate	inadequate	adequate	H4	No	No	H1, H2, H3
17		spotting	waiting-spotting	adequate	inadequate	adequate	H4	H1, H2	No	H1, H2, H3

Sr. No.	Control Action	Autonomous Truck	Shovel Operator	Onboard Sensor	PNT	MOS	1	2	3	4
18		spotting	waiting-spotting	inadequate	adequate	adequate	H4	No	No	H1, H2, H3
19	A-stop	spotting	waiting-spotting	inadequate	adequate	adequate	H4	H1, H2	No	H1, H2, H3
20		spotting	loading	adequate	adequate	adequate	H4	No	No	H1
21		spotting	loading	adequate	adequate	adequate	H4	H1	No	H1
22		spotting	loading	adequate	adequate	inadequate	H4	No	No	H1, H2
23		spotting	loading	adequate	adequate	inadequate	H4	H1, H2	No	H1, H2
24		spotting	loading	adequate	inadequate	adequate	H4	No	No	H1
25		spotting	loading	adequate	inadequate	adequate	H4	H1, H2	No	H1
26		spotting	loading	inadequate	adequate	adequate	H4	No	No	H1, H2, H3
27		spotting	loading	inadequate	adequate	adequate	H4	H1, H2	No	H1, H2, H3
28		loading	waiting-spotting	adequate	adequate	adequate	H4	No	No	H3
29		loading	waiting-spotting	adequate	adequate	adequate	H4	No	H4	H3

Sr. No.	Control Action	Autonomous Truck	Shovel Operator	Onboard Sensor	PNT	MOS	1	2	3	4
30		loading	waiting-spotting	adequate	adequate	inadequate	H4	No	No	H3
31	A-stop	loading	waiting-spotting	adequate	adequate	inadequate	H4	No	H4	H3
32		loading	waiting-spotting	adequate	inadequate	adequate	H4	No	No	H3
33		loading	waiting-spotting	adequate	inadequate	adequate	H4	No	H4	H3
34		loading	waiting-spotting	inadequate	adequate	adequate	H4	No	No	H3
35		loading	waiting-spotting	inadequate	adequate	adequate	H4	No	H4	H3
36		loading	loading	adequate	adequate	inadequate	H4	No	No	H3
37		loading	loading	adequate	adequate	inadequate	H4	No	H4	H3
38		loading	loading	adequate	inadequate	adequate	H4	No	No	H3
39		loading	loading	adequate	inadequate	adequate	H4	No	H4	H3
40		loading	loading	inadequate	adequate	adequate	H4	No	No	H3
41		loading	loading	inadequate	adequate	adequate	H4	No	H4	H3

Sr. No.	Control Action	Autonomous Truck	Shovel Operator	Onboard Sensor	PNT	MOS	1	2	3	4
42		loading	waiting-departing	adequate	adequate	adequate	No	No	No	H4, H3
43	A-stop	loading	waiting-departing	adequate	adequate	adequate	No	No	H4	H4, H3
44		loading	waiting-departing	adequate	adequate	inadequate	No	No	No	H4, H3
45		loading	waiting-departing	adequate	adequate	inadequate	No	No	H4	H4, H3
46		loading	waiting-departing	adequate	inadequate	adequate	No	No	No	H4, H3
47		loading	waiting-departing	adequate	inadequate	adequate	No	No	H4	H4, H3
48		loading	waiting-departing	inadequate	adequate	adequate	No	No	No	H4, H3
49		loading	waiting-departing	inadequate	adequate	adequate	No	No	H4	H4, H3
50		departing	loading	adequate	adequate	adequate	H4	No	No	H1
51		departing	loading	adequate	adequate	adequate	H4	H1	No	H1
52		departing	loading	adequate	adequate	inadequate	H4	No	No	H1, H2, H3
53		departing	loading	adequate	adequate	inadequate	H4	H1, H2	No	H1, H2, H3

Sr. No.	Control Action	Autonomous Truck	Shovel Operator	Onboard Sensor	PNT	MOS	1	2	3	4
54		departing	loading	adequate	inadequate	adequate	H4	No	No	H1, H2, H3
55	A-stop	departing	loading	adequate	inadequate	adequate	H4	H1, H2	No	H1, H2, H3
56		departing	loading	inadequate	adequate	adequate	H4	No	No	H1, H2, H3
57		departing	loading	inadequate	adequate	adequate	H4	H1, H2	No	H1, H2, H3
58		departing	waiting-departing	adequate	adequate	inadequate	H4	No	No	H1, H2, H3
59		departing	waiting-departing	adequate	adequate	inadequate	H4	H1, H2	No	H1, H2, H3
60		departing	waiting-departing	adequate	inadequate	adequate	H4	No	No	H1, H2, H3
61		departing	waiting-departing	adequate	inadequate	adequate	H4	H1, H2	No	H1, H2, H3
62		departing	waiting-departing	inadequate	adequate	adequate	H4	No	No	H1, H2, H3
63		departing	waiting-departing	inadequate	adequate	adequate	H4	H1, H2	No	H1, H2, H3

Appendix C: Unsafe/Unsecure Control Actions and Safety Constraints

The UCAs are developed from the system state table in appendix B by representing the tabular information in the form of statements. The SCs are developed from the UCAs. The combined UCAs and SCs for the 63 system states are listed below.

Table 9 Unsafe/unsecure control actions and safety constraints

Sr. No.	UCA	SC
1	A-stop not provided when both haul truck and shovel operator are waiting while incorrect, delayed, or missing commands from MOS [H4, H3]	A-stop must be provided when both haul truck and shovel operator are waiting while incorrect, delayed, or missing commands from MOS
2	A-stop not provided when both haul truck and shovel operator are waiting while incorrect, delayed, or missing GPS and/or RTK info [H4, H3]	A-stop must be provided when both haul truck and shovel operator are waiting while incorrect, delayed, or missing GPS and/or RTK info
3	A-stop not provided when both haul truck and shovel operator are waiting while incorrect, delayed, or missing info from onboard sensors [H4, H3]	A-stop must be provided when both haul truck and shovel operator are waiting while incorrect, delayed, or missing info from onboard sensors
4	A-stop not provided when shovel operator expects spotting while the haul truck is still waiting, and all systems are GO [H4, H3]	A-stop must be provided when shovel operator expects spotting while the haul truck is still waiting, and all systems are GO
5	A-stop provided too early when shovel operator expects spotting while the haul truck is still waiting, and all systems are GO [H4, H3]	A-stop must not be provided too early when shovel operator expects spotting while the haul truck is still waiting, and all systems are GO
6	A-stop not provided when shovel operator expects spotting while the haul truck is still waiting and incorrect, delayed, or missing commands from MOS [H4, H3]	A-stop must be provided when shovel operator expects spotting while the haul truck is still waiting and incorrect, delayed, or missing commands from MOS
7	A-stop not provided when shovel operator expects spotting while the haul truck is still waiting and incorrect, delayed, or missing GPS and/or RTK info [H4, H3]	A-stop must be provided when shovel operator expects spotting while the haul truck is still waiting and incorrect, delayed, or missing GPS and/or RTK info
8	A-stop not provided when shovel operator expects spotting while the haul truck is still waiting and incorrect, delayed, or missing info from onboard sensors [H4, H3]	A-stop must be provided when shovel operator expects spotting while the haul truck is still waiting and incorrect, delayed, or missing info from onboard sensors

Sr. No.	UCA	SC
9	A-stop not provided when shovel operator expects waiting while the haul truck starts spotting and all systems are GO [H1, H3, H4]	A-stop must be provided when shovel operator expects waiting while the haul truck starts spotting and all systems are GO
10	A-stop provided too late when shovel operator expects waiting while the haul truck starts spotting and all systems are GO [H1, H3, H4]	A-stop must not be provided too late when shovel operator expects waiting while the haul truck starts spotting and all systems are GO
11	A-stop not provided when shovel operator expects waiting while the haul truck starts spotting and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must be provided when shovel operator expects waiting while the haul truck starts spotting and incorrect, delayed, or missing commands from MOS
12	A-stop not provided when shovel operator expects waiting while the haul truck starts spotting and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must be provided when shovel operator expects waiting while the haul truck starts spotting and incorrect, delayed, or missing GPS and/or RTK info
13	A-stop not provided when shovel operator expects waiting while the haul truck starts spotting and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must be provided when shovel operator expects waiting while the haul truck starts spotting and incorrect, delayed, or missing info from onboard sensors
14	A-stop not provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must be provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing commands from MOS
15	A-stop provided too late when both haul truck and shovel operator are spotting and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must not be provided too late when both haul truck and shovel operator are spotting and incorrect, delayed, or missing commands from MOS
16	A-stop not provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must be provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing GPS and/or RTK info
17	A-stop provided too late when both haul truck and shovel operator are spotting and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must not be provided too late when both haul truck and shovel operator are spotting and incorrect, delayed, or missing GPS and/or RTK info
18	A-stop not provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must be provided when both haul truck and shovel operator are spotting and incorrect, delayed, or missing info from onboard sensors

Sr. No.	UCA	SC
19	A-stop provided too late when both haul truck and shovel operator are spotting and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must not be provided too late when both haul truck and shovel operator are spotting and incorrect, delayed, or missing info from onboard sensors
20	A-stop not provided when shovel operator is loading while the haul truck starts spotting again and all systems are GO [H1, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts spotting again and all systems are GO
21	A-stop provided too late when shovel operator is loading while the haul truck starts spotting again and all systems are GO [H1, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts spotting again and all systems are GO
22	A-stop not provided when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing commands from MOS [H1, H2, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing commands from MOS
23	A-stop provided too late when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing commands from MOS [H1, H2, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing commands from MOS
24	A-stop not provided when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing GPS and/or RTK info [H1, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing GPS and/or RTK info
25	A-stop provided too late when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing GPS and/or RTK info
26	A-stop not provided when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing info from onboard sensors
27	A-stop provided too late when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts spotting again and incorrect, delayed, or missing info from onboard sensors
28	A-stop not provided when shovel operator is spotting while the haul truck is in loading mode and all systems are GO [H3, H4]	A-stop must be provided when shovel operator is spotting while the haul truck is in loading mode and all systems are GO

Sr. No.	UCA	SC
29	A-stop provided too early when shovel operator is spotting while the haul truck is in loading mode and all systems are GO [H3, H4]	A-stop must not be provided to early when shovel operator is spotting while the haul truck is in loading mode and all systems are GO
30	A-stop not provided when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing commands from MOS [H3, H4]	A-stop must be provided when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing commands from MOS
31	A-stop provided too early when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing commands from MOS [H3, H4]	A-stop must not be provided too early when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing commands from MOS
32	A-stop not provided when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info [H3, H4]	A-stop must be provided when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info
33	A-stop provided too early when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info [H3, H4]	A-stop must not be provided too early when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info
34	A-stop not provided when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors [H3, H4]	A-stop must be provided when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors
35	A-stop provided too early when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors [H3, H4]	A-stop must not be provided too early when shovel operator is spotting while the haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors
36	A-stop not provided when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing commands from MOS [H3, H4]	A-stop must be provided when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing commands from MOS
37	A-stop provided too early when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing commands from MOS [H3, H4]	A-stop must not be provided too early when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing commands from MOS
38	A-stop not provided when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info [H3, H4]	A-stop must be provided when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info

Sr. No.	UCA	SC
39	A-stop provided too early when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info [H3, H4]	A-stop must not be provided too early when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing GPS and/or RTK info
40	A-stop not provided when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors [H3, H4]	A-stop must be provided when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors
41	A-stop provided too early when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors [H3, H4]	A-stop must not be provided too early when shovel operator is loading, and haul truck is in loading mode and incorrect, delayed, or missing info from onboard sensors
42	A-stop not provided when shovel operator expects the haul truck to depart while the haul truck expects loading and all system are GO [H3, H4]	A-stop must be provided when shovel operator expects the haul truck to depart while the haul truck expects loading and all system are GO
43	A-stop provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and all system are GO [H3, H4]	A-stop must not be provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and all system are GO
44	A-stop not provided when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing commands from MOS [H3, H4]	A-stop must be provided when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing commands from MOS
45	A-stop provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing commands from MOS [H3, H4]	A-stop must not be provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing commands from MOS
46	A-stop not provided when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing GPS and/or RTK info [H3, H4]	A-stop must be provided when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing GPS and/or RTK info
47	A-stop provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing GPS and/or RTK info [H3, H4]	A-stop must not be provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing GPS and/or RTK info

Sr. No.	UCA	SC
48	A-stop not provided when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing info from onboard sensors [H3, H4]	A-stop must be provided when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing info from onboard sensors
49	A-stop provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing info from onboard sensors [H3, H4]	A-stop must not be provided too early when shovel operator expects the haul truck to depart while the haul truck expects loading and incorrect, delayed, or missing info from onboard sensors
50	A-stop not provided when shovel operator is loading while the haul truck starts departing and all systems are GO [H1, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts departing and all systems are GO
51	A-stop provided too late when shovel operator is loading while the haul truck starts departing and all systems are GO [H1, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts departing and all systems are GO
52	A-stop not provided when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing commands from MOS
53	A-stop provided too late when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing commands from MOS
54	A-stop not provided when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing GPS and/or RTK info
55	A-stop provided too late when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing GPS and/or RTK info
56	A-stop not provided when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must be provided when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing info from onboard sensors

Sr. No.	UCA	SC
57	A-stop provided too late when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is loading while the haul truck starts departing and incorrect, delayed, or missing info from onboard sensors
58	A-stop not provided when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must be provided when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing commands from MOS
59	A-stop provided too late when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing commands from MOS [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing commands from MOS
60	A-stop not provided when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must be provided when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing GPS and/or RTK info
61	A-stop provided too late when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing GPS and/or RTK info [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing GPS and/or RTK info
62	A-stop not provided when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must be provided when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing info from onboard sensors
63	A-stop provided too late when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing info from onboard sensors [H1, H2, H3, H4]	A-stop must not be provided too late when shovel operator is waiting expecting departure as the haul truck is departing and incorrect, delayed, or missing info from onboard sensors