Safe Integration of Autonomous Machines in Underground Mining Environments

Julieth Patricia Castellanos-Ardila, Hans Hansson and Sasikumar Punekkat
IDT, Mälardalen University, Västerås, Sweden
Email: (julieth.castellanos, hans.hansson, and sasikumar.punnekkat)@mdu.se

***Abstract*—Autonomous and Semi-Autonomous Machines (ASAMs) provide several benefits and have already emerged in mining environments. However, for cost-efficiency reasons and for ASAMs to reach their full potential, they should be capable of operating seamlessly with manually operated machines. Establishing the requirements for sufficient safety for such integration is a non-trivial task. This paper proposes a methodology for safely integrating ASAMs in underground mining environments. First, we describe the purpose of the integration and define the constituent components. Second, we identify the conditions that ASAMs will likely encounter using ODD-UM, an operational design domain specification for underground mining. Third, we derive high-level requirements for individual components based on ODD-UM attributes. Such requirements are allocated into the constituent components and considered as assumptions for the safety analysis. Fourth, we perform STPA (System-theoretic Process Analysis) to analyze safety-related control requirements for the integrated system. Our methodology could help the system integrator to systematically identify integration requirements to be enforced in constituent components and safety control systems.**

***Index Terms*—Underground Autonomous Mining, Integration Requirements, ODD-UM, STPA, Safety-guided Design.**

I. Introduction

Autonomous and semi-autonomous machines (ASAMs), integrated into underground mines, provide several benefits and have already started to emerge in those environments [1]–[3]. However, establishing the requirements for sufficient safety for such integration is a non-trivial task. For example, ASAMs have diverse backgrounds, i.e., different technologies from various vendors. Moreover, ASAMs should cope with specific site conditions that the vendors do not necessarily know. In addition, ASAMs may share the operational site with humans. If such factors are not adequately managed, they may result in vulnerabilities for unsafe interactions between system components, leading to people being injured or even killed.

Generally, the safety of complex system environments, such as ASAM systems, results from a joint effort between ASAM vendors and site integrators. In particular, vendors are compelled to provide safety-certified ASAMs, i.e., ASAMs that comply with regulatory frameworks regarding safety, e.g., the machine directive [4] for the European market. However, certified machines may not respond to specific site conditions. Thus, integrators should define requirements for the ASAMS considering their intended use in a specific operational environment, enforce those possible via contractual specifications, and work on additional protective measures, e.g., provision of additional safeguards [5], for remaining issues.

Operational conditions can be described using the ODD (Operational Design Domain) concept [6], which contains the aspects that autonomous driving systems should sort out, e.g., environmental, time-of-day, and traffic conditions. An ODD specification for road vehicles is provided in the Publicly Available Specification PAS 1883 [7]. We extended such specification in [8] for providing ODD-UM, a context-specific ODD for underground mining. However, ASAMs do not operate alone in a specified context. Thus, the site integrator needs to analyze the potential safety issues arising from the ASAMs control interactions with other system components.

A promising approach for safety analysis is the System-theoretic Process Analysis (STPA) [9], which is a safety analysis method that defines safety as a control problem. STPA has been considered in similar contexts. For example, Waymo, an American company developing automated driving technology, finds that STPA is a better-suited methodology than traditional hazard analysis methods to spot dangerous interactions between automated vehicles [10]. In the mining sector, STPA has also been suggested for the analysis of ASAMs integration in their operations [11]–[13]. STPA is part of an integrated process called safety-guided design [9], which helps guide the design of complex systems where only the system-level requirements are available.

In this paper, we propose a four-step methodology for the safe integration of autonomous machines in underground mining environments. First, we describe the ASAM system integration, including its general purpose and constituent systems. Second, we identify the operational characteristics of the site by using ODD-UM attributes. Third, we derive high-level requirements for components integrating the ASAM system based on the identified ODD-UM attributes and consider them as assumptions for the safety analysis. Finally, we define and analyze the control structure. For this analysis, we use the guidance provided by STPA. Our methodology, which is illustrated with a case study, could help the system integrator to systematically identify requirements to be enforced in specific system components and safety control systems.

This research has been supported by Vinnova via the project ESCAPE-CD (Efficient Safety for Complex Autonomous Production Environments - Concept Design) Reference: 2021-03662. We thank our industrial partner - Boliden Mineral AB- for the preliminary review of the proposed approach.

This paper is organized as follows. Section II presents essential background. Section III presents our methodology for identifying requirements for the integration of ASAMs in underground mines. Section IV presents a case study, where we illustrate our methodology. Section V discusses our findings. Section VI presents related work. Finally, Section VII presents conclusion and future remarks.

II. Background

A. Applicable Regulations and Standards for Mining

1) The Machine Directive [4]: is a regulation that provides requirements to ensure a high level of protection of the health and safety of persons in the context of machinery. This regulation primarily applies to machine manufacturers but also considers requirements for machinery designed to work together. For example, article 1.2.4.4 mentions general stop controls for machines and related equipment. The directive also confers a presumption of conformity for manufacturers complying with harmonized standards, i.e., standards developed by recognized European Standards Organisations.

2) ISO 17757:2019 [14]: is a harmonized standard type C, i.e., it provides requirements for compliance with standards in other categories but has precedence over them in case of contradiction. In particular, ISO 17757:2019 specifies safety criteria for Autonomous and Semi-Autonomous Machines (ASAMs) and their associated systems and functional environments. It prescribes the creation of an Autonomous Operating Zone (AOZ) (See Fig. 1), which is controlled by an access control system, where monitored non-autonomous machines and persons are able to perform activities together with the ASAMs. Such interactions should be controlled by a supervisor system that provides a control center for operation in autonomous mode. The standard also considers operational environments as a prerequisite for risk assessment.

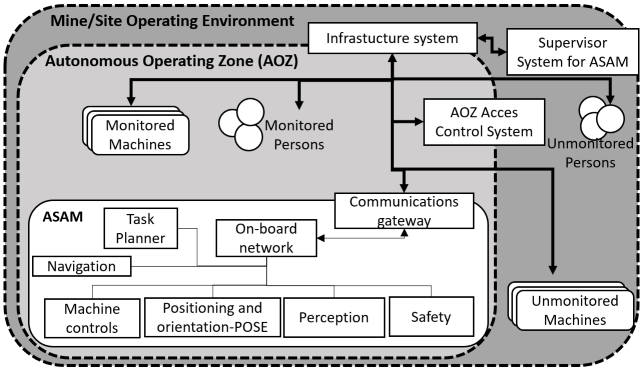
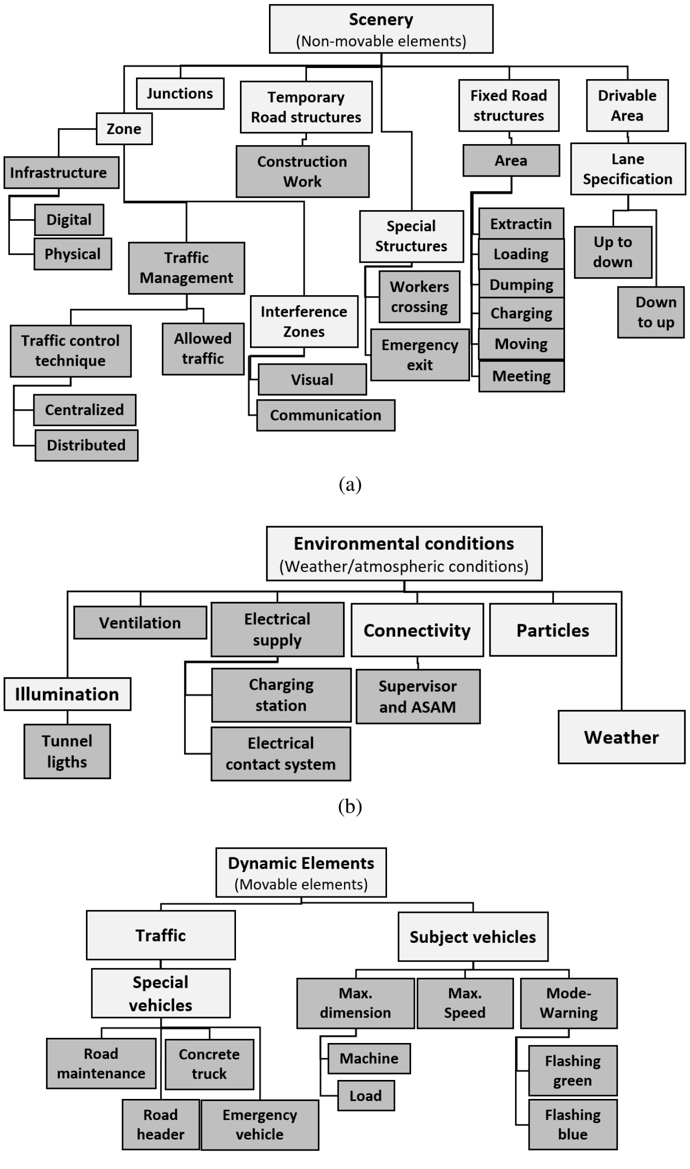


Fig. 1: Main Elements in the ASAM System

B. Operational Design Domain for Underground Mining

The Operation Design Domain for Underground Mining (ODD-UM) [8] is a specification based on the ODD taxonomy provided by the PAS 1883:2020 [7] and extended with the attributes provided by ISO 17757:2019 (See Section II-A). It contains three main attributes, i.e., scenery (Fig. 2a), environmental conditions (Fig. 2b), and dynamic elements (Fig. 2c).



(a)

(b)

(c)

Fig. 2: ODD-UM Attributes.

1) The Scenery: describes static elements. In particular, the infrastructure required for controlling AOZ access (see Fig 1) is *physical* (e.g., mechanical guards, physical chains, and signs) and *digital* (e.g., light curtains, laser beams, and geofences). The *traffic control techniques* can be *centralized* or *distributed*. *Allowed traffic* should consider monitored and unmonitored people and vehicles. *Interference areas* should include communication and visual interference areas. In our case, the drivable area has two possible travel directions, e.g., *up to down* and *down to up*. The attribute *fixed road structures* includes the working areas in underground mining, i.e., *extracting, load, charging, moving, and dumping areas*. It is common that mines only have one lane to go in both directions, so it is important to consider *meeting* zones as well. In addition, the sub-attributes *workers crossing* and *emergency exit* are considered for special structures, and *construction work* for temporary road structures.

2) Environmental conditions: describes the weather and atmospheric conditions. Inside a mine, the weather affects the mine entrance and produces weather-induced conditions, i.e., wet, muddy, and slippery roads. In addition, electrical supply is considered in the form of two sub-attributes: *charging areas* (for battery-based machines) and *electrical contact systems* (for trolley machines). *Supervisor system and ASAM*, which is considered under the connectivity attribute, is also essential to maintain control of the ASAMs other machines, and persons. Finally, there are artificially induced conditions in a mine such as *ventilation* and *tunnel lights*.

3) Dynamic Elements: considers movable elements, i.e., the machines, with *max. dimmension* for the machines and the load, *max. speed*, and *mode warning* (e.g. *flashing green* and *flashing blue*, which are currently indicated by the standard). We could consider the most common options in the special vehicles attribute, i.e., *road maintenance, road header, concrete truck, and shut down systems*.

C. Safety-guided Design

The safety-guided design [9] is an integrated process that helps guide the design and system development of complex systems where only the system-level requirements are available. This process uses the System-theoretic Process Analysis (STPA) proactively. The process starts by identifying system-level hazards and requirements, which can be traced back to individual systems components as the iterative design and analysis proceeds. If any of the hazards cannot be eliminated, the potential for their control should be identified at the system level. STPA is a hazard analysis technique aiming to accumulate information regarding behavioral system safety constraints to enforce them during the system lifecycle. STPA is based on the accident causality model called STAMP (Systems Theoretic Accident Model and Processes), which is grounded on systems and control theory. STPA comprises the following four steps:

1) Define the purpose of the analysis: During this step, the system of interest is defined, and potential accidents and hazards related to the application scenarios are identified.

2) Model the control structure: The system is modeled by considering the set of feedback control loops between their functional components.

3) Identify unsafe control actions (UCAs): We examine how control actions could become unsafe, leading to losses. A UCA has a defined structure, i.e., the source controller (C), control action type (CAT), control action (CA), and context (Ct). Ct corresponds to the conditions for the hazard to occur. CAT leads to the CA being unsafe in four ways. a) A CA required for safety *is not provided* or *not followed*. b) A UCA *is provided*. c) A potentially safe CA is provided *too early* or *too late* or *out of sequence*. d) A CA required for safety *is stopped too soon* or *applied too long*.

4) Identify loss scenarios: Two types of loss scenarios must be considered. a) Unsafe controller behavior, i.e., failures involving the controller (for physical controllers), inadequate control algorithm, unsafe control input, and inadequate process model. b) Inadequate feedback, i.e., feedback or information not received and inadequate feedback is received.

III. Integration Requirements for ASAMs

For correct integration in a specific context, e.g., an underground mine, ASAMs should be able to perform tasks done by humans, e.g., perception and control. However, investing in ASAMs may create expectations regarding productivity leading to unsafe site designs where workers spend more time than desirable inside autonomous zones. Therefore, ASAMs should be safely integrated by considering not only their individual capabilities but also their contribution to the complex System of Systems (SoS), where other elements are also present.

Safety-guided design (see Section II-C) is a methodology aimed at preventing safety challenges in SoS by considering accident prevention as a control problem with assumptions regarding the context of the whole operation. For our context, such assumptions can be formally identified by considering the ODD-UM (see Section II-B). With this information, suppliers are aware of the target site environment and can focus on optimizing individual machines as well as making them compliant with the machine directive (see Section II-A1). In particular, the ODD-UM specification can contribute to the definition of the limits of the machinery [5], which is an initial input required by suppliers for their risk assessment tasks. In turn, the site integrator can focus on guaranteeing the safety of the control structure that should oversee the whole operation, as required by the standard ISO 17757:2019 (see Section II-A2).

We propose a process for identifying integration requirements for underground sites using ASAMs. As Fig. 3 depicts, the first task is the *description of the integration.* In this step, we identify the purpose of the system and the expected constituent components. The second task is the *description of the ODD.* In this step, we describe the operational domain using

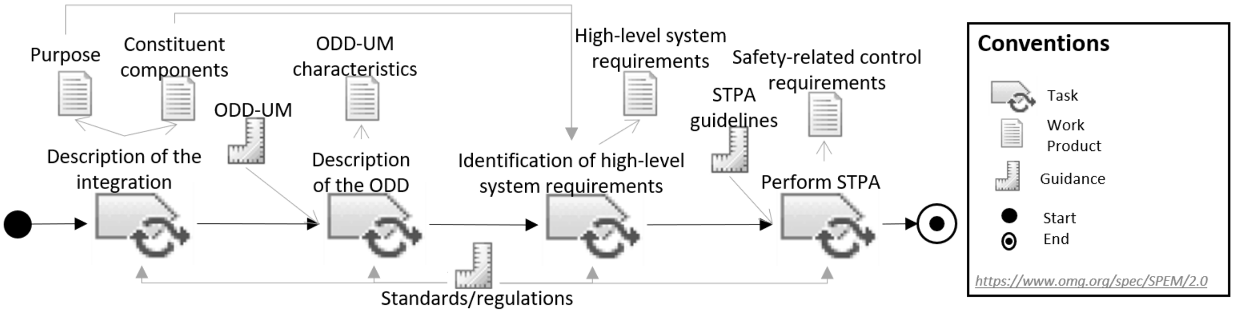

Purpose
Constituent components
ODD-UM characteristics
High-level system requirements
Safety-related control requirements
ODD-UM
STPA guidelines
Description of the integration
Description of the ODD
Identification of high-level system requirements
Perform STPA
Standards/regulations
Conventions
Task
Work Product
Guidance
Start
End
https://www.omg.org/spec/SPEM/2.0

Fig. 3: Integration Requirements Identification Process

the ODD-UM taxonomy. The third step is the *identification of high-level system requirements.* In this step, we map the individual ODD-UM attributes to specific system components and derive high-level requirements for the integration. Finally, we analyze the control structure by *performing STPA.* For this, we identify the system's responsibilities in terms of control based on the high-level requirements identified in the previous step. As the figure also shows, applicable standards and regulations are used to guide the previously mentioned steps. In Section IV, we present a case study to illustrate this methodology.

IV. Case Study

A. Description of the Integration

1) Purpose: The use case consists of a tunnel connecting the underground with the surface storage. The purpose is to integrate a set of ASAMs with manned machines in a dedicated AOZ to maximize transportation efficiency while providing the necessary stop controls that ensure a high level of protection for the health and safety of the workers, as required by the machine directive (see Section II-A1). In the case study, we assume that human access to the tunnel during operation is restricted to the drivers inside manned machines.

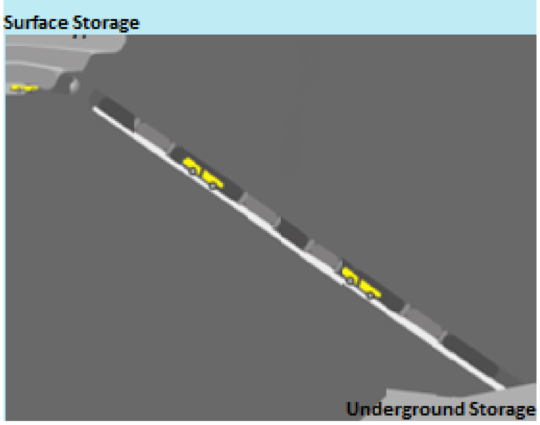


Fig. 4: Tunnel under Investigation

2) Constituent Components: Fig. 5 depicts in light gray the initial set of constituent components required for the integration. In particular, the mechanisms provided by the vendors are included, i.e., the traffic management system (TMS) and both types of machines equipped with their respective safety control systems. In addition, components included in the mine infrastructure could help the TMS to schedule the transit of the machines (further details in Section IV-B).

B. Description of the ODD

The tunnel has one lane (see Table I), which is 5 kilometers long and 6 meters wide. It also has a loose surface and serves both directions. The lane does not have line markers or shoulders; the only barrier is the surrounding rock. There are two areas in the fixed road structures, i.e., moving and meeting. The initial design considers that the efficiency of the operation could be maximized if the moving area is divided into zones. Such zones should contain a meeting area to facilitate the transit of machines in both directions. For this, sensors in the infrastructures shall be installed to detect the status of the moving, and the meeting areas (occupied or empty). The initial design considers laser gates and parking sensors for such a purpose. In addition, the TMS should be centralized and able to monitor the position of the machines.

The mine's humidity varies between 60% to 95%. Its temperature varies during the year, i.e., between -40 and +30 degrees Celsius outside the tunnel and between -5 and +20 degrees Celsius inside the tunnel. The particles that may impede the vision are dust, smoke, and pollution. Regarding the subject vehicles, their maximum dimension is 3 meters in width and 11 meters in length. Finally, the max speed of the ASAMs shall be 30 kilometers per hour.

TABLE I: ODD-UM Checklist

Attribute	**Sub-Attributes**		**Selection**
Scenery-Drivable Area			
Lane Specification	Number of lanes		1
	Distance		5 Km
	Dimension		6 m
	Direction of travel	Up to Down	✓
		Down to up	✓
	Surface	Loose ✓	mud/gravel
Edge	Line markers		
	Shoulder		
	Solid Barriers	Grating	
		Rails	
		Cones	
		Rock	✓
Scenery-Fixed Road Structures			
Area	Extracting		
	Loading		
	Dumping		
	Charging		
	Moving		✓
	Meeting		✓
Scenery-Zone			
Infrastructure	Digital	Geo-fence	
		Light curtains	
		Laser gates	✓
		Video imaging	
		Parking sensors	✓
	Physical	Mechanical guards	
		Physical chains	
		Signs	
Traffic Management	Traffic control technique	Centralized	✓
		Distributed	
	Allowed traffic	Monitored machines	✓
		Monitored Persons	
Environmental Conditions-Weather			
Temperature		Outside tunnel	-40/+30°C
		Inside tunnel	-5/+20°C
Humidity		60% to 95%	
Environmental Conditions-Particles			
Non-precipitating water			✓
Sand			
Dust			✓
Smoke			✓
Pollution			✓
Dynamic Elements-Subject Vehicle			
Max. Dimension- Machine		Width	3 m.
		length	11 m.
Max. Speed- Machine			30 km/h.

C. *Identification of High-level Requirements*

The ODD characteristics presented in Section IV-B can be described as high-level system requirements that can be transferred to machine and systems providers and considered as general assumptions of the integration. For example, the sensors and actuators included in the machines should detect conditions regarding the surface, particles, temperature, and humidity. A strategic mine planning decision aimed at maximizing production efficiency will also require a proper fleet selection that supports requirements related to the machine type (given the allowed dimensions and speed). In addition, such machines shall also be provided with anti-collision systems that prevent collisions with the tunnel surroundings, road structures, and other machines. Finally, the TMS shall plan the transportation schedule in the one-lane tunnel, divided into zones by the selected digital infrastructure. The TMS shall also consider that each zone contains moving and meeting areas.

D. *Perform STPA*

1) Purpose of the analysis: We start the analysis by considering the participation of humans in the integration and the potential loss that involves them. In particular, humans, which access to the tunnel during operation is restricted to the drivers inside the manned machines, could lose their lives or suffer injuries if their machines collide. Three general assumptions exists in this case. First, drivers are not allowed to be outside the machines. Second, operators outside machines are restricted to guarded areas. Third, drivers receive enough training regarding operation rules, e.g., allowed machine speed and distance from other machines. However, there is still the possibility of accidents involving ASAMs. In particular, we should consider the risk involving ASAMs in the proximity of manned machines. Thus, the system level hazard is that manned machines are in zones where ASAMs operate in autonomous mode. The corresponding safety requirement is derived from this hazard (see Table II).

TABLE II: Purpose of the Analysis

Loss	Drivers are injured or lose their lives when operating machines in the tunnel
Hazard	Manned machines are in zones where ASAMs operate in autonomous mode.
Safety Constraint	Manned machines shall not be in zones where ASAMs operate in autonomous mode.

2) Model control structure: The control structure (see Fig. 5) includes the constituent components described in Section IV-A2, which interact with a safety controller (depicted in dark gray in the middle of the figure), the mine environment (shown with a dotted line at the bottom of the figure), and human operators. The safety controller (SC), which oversees the operation in autonomous mode (as required by the standard ISO 17757:2019 - see Section II-A2), is envisaged to have central and remote parts to be installed on the safety controller included in the individual machines.

The main task of the SC is to ensure the safety constraint described in Table II. For this, the SC should automatically issue an emergency stop command when it detects manned machines operating in dangerous zones, i.e., operating in autonomous zones or entering a non-autonomous zone where an ASAM is operating in autonomous mode. The issued command shall stop all the ASAMs within the dedicated AOZ and notify drivers in manned machines that they should stop.

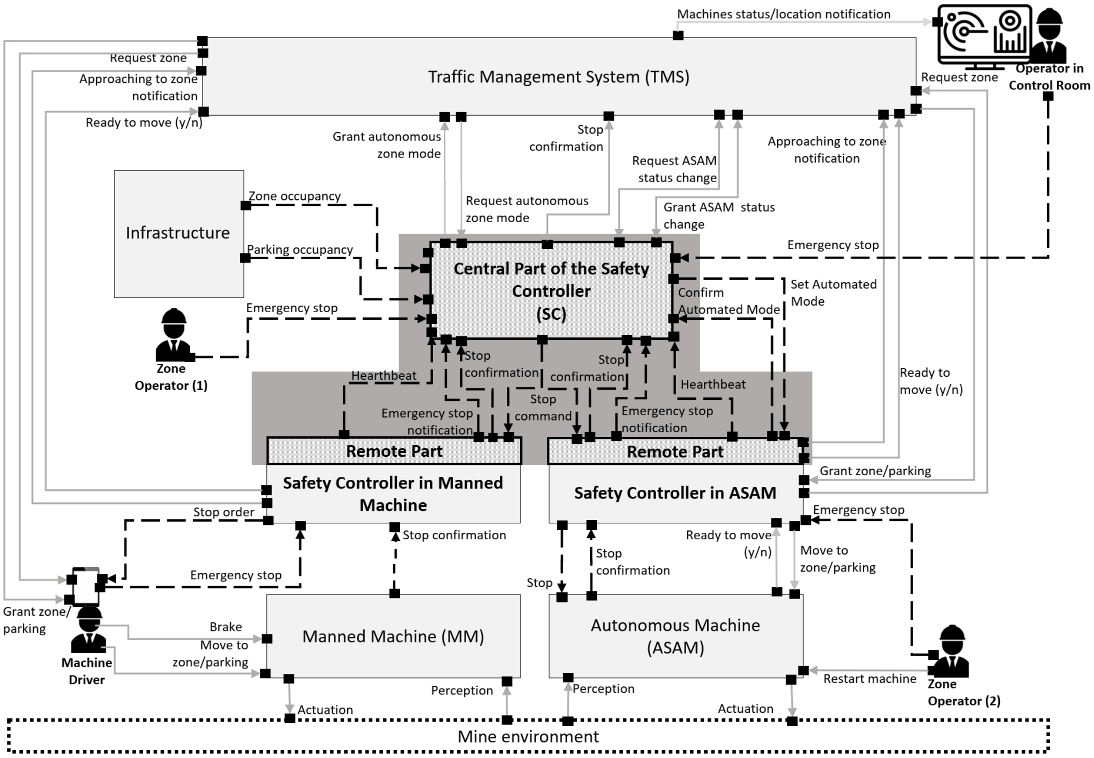


Fig. 5: Control Structure for the Safety System

This automated solution is complemented with emergency stop buttons, allowing human operators to manually stop the operation in a dedicated AOZ. The SC shall also propagate the stop button commands. Stop buttons are localized in different places of the AOZ, i.e., the control room, the machines, and the tunnel's walls. The current way the safety control acts is by continuously sending a signal (a heartbeat) that indicates a safe operation. Thus, the emergency stop command is, in reality, the disappearance (complete interruption) of such a signal. In this way, a physical failure of the SC is also covered.

The process model of the SC contains the list of zones and ASAMs and their statuses (i.e., autonomous or non-autonomous). During operation, the TMS operator can request changes to the zone status, which have to be granted and set up by the SC. The TMS operator can also request a change in the ASAM status, which the safety controller shall grant, set up in the ASAM (which should notify the change to the SC), and notify the TMS. The process model also contains the state machine model that groups all possible system occurrences that lead to the emergency stop. For example, the SC shall always issue an emergency stop if the manned machine enters an autonomous zone or if an ASAM, in autonomous mode, occupies a zone regardless of the zone status.

The control algorithm of the SC relies on the process model to provide control actions. In addition, the control algorithm requires inputs from the infrastructure, i.e., the occupancy status of the moving and meeting zones (occupied or empty), which is provided by the laser gates and parking sensors, respectively. Moreover, the control algorithm shall have information regarding the regular operation of the machines (a heartbeat) and the stop buttons command. In particular, the absence of the heartbeat from a machine or the presence of the stop command from a stop button are sufficient conditions for stopping the AOZ operation. As feedback, the SC requires a stop confirmation from the ASAMs and the drivers of the manned machines and a confirmation of the automated mode set to ASAMs. When the operation in the AOZ is normalized, human operators can manually restart ASAMs.

3) Identify unsafe control actions: As depicted in Fig. 5 there are two arrows leaving the SC, representing the control actions provided by the SC.

- **CA1:** The SC provides a stop command whenever:
  - Manned machines operate in zones that are in autonomous mode (Ct1).
  - Manned machines operate in non-autonomous zone where there is an ASAM operating in autonomous mode (Ct2).
  - A human operator triggers an emergency stop button (Ct3).
  - The heartbeat from the machines does not arrive within t milliseconds (Ct4), where t is a required freshness parameter derived from the dynamic behaviour of the system.
- **CA2:** The SC sets the mode to the corresponding ASAM to autonomous whenever:
  - the autonomous mode is granted (Ct5)

CAs could be unsafe as presented in Table III.

TABLE III: Identification of UCAs

CA	**CAT**			
	CA is not provided or followed	**Unsafe CA is provided**	**CA is provided too early/late/out of sequence**	**CA is stopped too soon or applied too long**
CA1	UCA1-1 UCA1-2	UCA1-3	UCA1-4	UCA1-5
CA2	UCA2-1	UCA2-2	UCA2-3	UCA2-4

Table III results in a list of 9 UCAs. Some of these UCAs (written in gray) may lead to a loss unrelated to the hazard we are treating in this analysis. For example, UCA1-2 reads as *the SC provides the stop command when S1 or S2 or S3 or S4 are not occurring*. In this case, the control action will lead to unnecessary operation stops, which may cause a significant loss in productivity. We focus on the UCAs that lead to the hazard under consideration (see Table II) and derive system safety requirements for their mitigation (see Table IV).

TABLE IV: UCAs and System Safety Requirements

UCA	**System Safety Requirement**
UCA1-1: The SC does not provide the stop command whenever Ct1 or Ct2 or Ct3 or Ct4	**SR1:** The SC shall provide the stop command withing t milliseconds after Ct1 or Ct2 or Ct3 or Ct4 are detected.
UCA1-4: The SC provides the stop command too late whenever Ct1 or Ct2 or Ct3 or Ct4.	
UCA1-2: The SC provides the stop command whenever Ct1 or Ct2 or Ct3 or Ct4 but it is not followed.	**SR2:** ASAMs shall follow the stop command when it is issued.
	SR3: Drivers shall follow the stop notification when issued.
UCA1-5: The stop command is interrupted too soon when Ct1 or Ct2 or Ct3 or Ct4 are still ongoing.	**SR4:** The AOZ operation shall not be restarted until all the ASAMs have notified their stop status.
	SR5: The SC shall notify operators when machines can be restarted.
	SR6: Every restarted ASAM shall notify their moving status.
UCA2-2: The SC sets the automated mode to a non-corresponding ASAM whenever Ct5.	**SR7:** The SC shall always set the automated mode to the corresponding ASAM whenever Ct5.
UCA2-3: The SC sets the automated mode in a non-autonomous zone (or vice-versa) to the corresponding ASAM whenever Ct5.	**SR8:** The SC shall set the automated mode to the corresponding ASAM in the designated zone within t milliseconds after Ct5.
UCA2-4: The SC sets the autonomous mode to the corresponding ASAM too long after Ct5, and the ASAM is already in a non-autonomous zone.	**SR9:** The safety controller shall inactivate the automated mode when an ASAM enters a non-autonomous zone.

4) Identify loss scenarios: We further analyze the causes of violations for the safety requirements identified in Table IV. As an illustration, we present the analysis related to SR1. In particular, the control algorithm requires a correct process model to issue the emergency stop. The designed process model considers the states of the zone and the occupancy of such zones and the meeting areas (see Table V).

TABLE V: Unsafe Scenarios in Moving Areas

Id	**Zone State**	**Zone Occupancy**	**Meeting Area Occupancy**	**Safe?**
S1	Autonomous	-	-	Unsafe
S2	Non-autonomous	Empty	Empty	Safe
S3	Non-autonomous	Empty	Occupied	Undetermined
S4	Non-autonomous	Occupied	-	Unsafe

However, the information in the process model is not enough in one case, i.e., S3. The reason is that ASAMs could move towards an empty moving zone that is a non-autonomous state when a manned machine is in transit. This case could happen if the SC believes that the zone changes status. To avoid such kind of situation, requirements S10 and S11 are specified (see Table VI). The control algorithm also relies on inputs from the infrastructure and feedback from ASAMs, which should receive information within a certain period (see SR12-SR14). In addition, an analysis regarding the stop buttons should be done, as their operation is safety-critical. Thus, such buttons should always work (see SR15).

TABLE VI: Additional System Safety Requirements

ID	Additional System Safety Requirement
SR10	ASAMs speed in a meeting zone shall be 0 Km/h when the moving zone is in autonomous mode.
SR11	ASAMs speed shall be provided when ASAMs are in operation.
SR12	Parking sensors information shall be provided continuously.
SR13	Laser gates shall provide the signal within t milliseconds after the ASAM has passed the zone.
SR14	ASAM shall send the stop notification to the SC within t milliseconds after the emergency stops is issued.
SR15	The emergency stop function shall be available and operational at all times.

More safety requirements can be derived by identifying the loss scenarios of the remaining UCAs. In addition, iterations with the evolving control structure (new versions of Fig. 5 that incorporate the identified requirements) may also result in additional safety requirements. Thus, the methodology, even though not explicitly depicted in Fig. 3, is iterative, i.e., we can come back from one step to any of the previous ones to do further analysis. For space reasons, we do not consider such interactions in this paper.

V. Discussion

Our methodology is the result of discussions between academic and industrial actors participating in the mining industry's transition towards mixed traffic (i.e., autonomous and manned machines) to safely improve efficiency in transporting materials and workers. We departed from available knowledge about mining and ASAMs operations. We also consider methodologies that aim at solving safety dilemmas, such as STPA, ODD concepts, and regulatory frameworks.

Our methodology requires an initial description of the system, which should set the integration's goal and the initial set of components for reaching that goal. This step requires knowledge about technology capabilities and stakeholders brainstorming. However, different stakeholders may have different goals in terms of productivity that sometimes conflict with safety. For resolving conflicts of this nature, the use of domain-specific standards targeting safety is crucial so that productivity goals do not overpass safety constraints.

Knowing the ASAMs' technological background is not enough for autonomy. A description of the environment in which the ASAMs will operate is essential. Such a description should be as faithful as possible, so real operational environments are determined and mapped with the technological offers of the market. Conditions for the operational environments not covered by current technology need deeper analysis or new developments. In the worst case, they will be the reason to stop the integration while we wait for matching technology.

In this work, we used ODD-UM, a taxonomy that provides essential information on the environmental conditions that ASAMs are likely to encounter in underground mines. This taxonomy provides a baseline for communication with machines, components, and system vendors since it permits defining high-level requirements that can be enforced on constituent components. It also permits defining initial assumptions for the safety analysis. However, considering the ODD-UM taxonomy as a base for creating contractual obligations will require the definition of additional levels of detail that include technical aspects. Thus, the impact of such extended ODD taxonomy, covering technical attributes for autonomous underground mining, is worth further research.

We limited the case study to the interactions between ASAMs and manned machines. However, an operator on foot may also be part of the interaction. We believe that our method could also cover such cases since operators can be considered system components. In addition, we have only considered the machine directive and the standard ISO 17757:2019. However, safety-related parts of control structures in machinery are also subject to the standard EN ISO 13849-1:2015 [15], which prescribes the definition of performance levels (PL), i.e., a value used to define the ability of safety-related parts of control systems to perform a safety function. We believe that our methodology could provide inputs for PL definitions, which will provide more safety measures for the control structure, i.e., redundancy means and validation and verification methods. Similarly, the UCAs found in Section IV-D3 could be a consequence of a security attack since the system is completely connected. Thus, such UCAs could also be an initial input to the cybersecurity analysis, which will require the guidance provided by cybersecurity standards targeting autonomous cars, e.g., ISO/SAE 21434:2021 [16]. Finally, we only considered the safety analysis within the specific operational design domain (ODD-UM). Further work will need to include the behaviors of the safety controller in Out-of-UM-ODD situations, i.e., what control actions are required when the safety controller recognizes that ASAMs are outside the ODD-UM.

VI. Related Work

STPA has been widely used in the analysis of safety for autonomous applications. For example, Adrianensen et al. [17] present a case study where STPA is used in the context of a collaborative robot application. Axelsson et al. [18] have also utilized STPA to create a risk analysis method for a system of systems. Yoo et al. [19] present the application of STPA in the definition of systems requirements for the design of a rotary-wing aircraft. The previous applications of STPA do not consider the ODD as we are doing in this work.

There are also works where the ODD is used as a base for design requirements in autonomy. For example, Heikkilä et al. [20] provides an approach for the qualification of an autonomous vessel prototype. Montewka et al. [21] proposes a safety qualification process for autonomous decision-making in the maritime sector, which includes the identification of new technologies, risk identification/assessment, safety goals specification, and qualification plan. Montewkaet al.' approach is considered by Tiusanen et. [12] as appropriate in the safety qualification of autonomous mobile machinery. However, Tiusanen et al.'s work does not show their specific application. In these cases, STPA is not part of the analysis. The ODD is also used as a starting point for the STPA analysis in the work of Khastgir et al. [22], but their ODD definition is vague. Instead, we propose a more detailed ODD description for the specific context under study. In addition, we map the ODD attributes to the constituent components to get a set of high-level requirements that facilitate the modeling of the control structure, which is an essential input for the STPA analysis.

There are other examples of hazard analysis in mining. For instance, in [23], the authors focus on hazard identification and mitigation for an electric quarry site by using hazard and operability (HAZOP) and fault tree analysis (FTA). Baumgart et al. [11] provide an STPA analysis for a quarry site. Finally, Sidhu [13] presents the use of STPA for the analysis of security. In our work, we propose a four steps approach where the safety analysis is not done in isolation. Instead, it considers the ODD that autonomous machines are likely to encounter in underground mines, which is not considered in the previous works targeting the mining context.

VII. Conclusions and Future Work

This paper proposes a four-step methodology for integrating autonomous machines with manned machines in underground mining environments. Our methodology is based on ODD-UM, an Operational Design Domain taxonomy designed for underground mining. The methodology is also based on STPA (System-theoretic Process Analysis), which is a safety analysis method that defines safety as a control problem. We also illustrate the proposed methodology by a case study from the mining sector. In this case study, we analyze the provision of emergency stops for the machine operations, as this is a crucial requirement prescribed by the machine directive. As a result, we derive a set of safety requirements, which can be enforced in specific system components and safety control systems.

Future work includes the validation of our methodology by considering more case studies and experts' opinions. Moreover, we plan to use the standard EN ISO 13849-1 for deriving performance levels (PLs) for the safety controller and its components. Finally, we plan to use the requirements identified in this work to create scenarios that can be used in testing activities and cybersecurity analysis.

References

[1] Volvo Construction Equipment. (2018) Testing begins at world's first ”emission-free” quarry. [Online]. Available: https://www.volvoce.com/global/en/news-and-events/press-releases/2018/testing-begins-at-worlds-first-emission-free-quarry/

[2] Ferreexpo. (2020) Yeristovo Mining. [Online]. Available: https://www.ferrexpo.com/what-we-do/operations/yeristovo/

[3] Boliden. (2021) Autonomous Hauling System for increased productivity in Boliden Aitik. [Online]. Available: https://news.cision.com/boliden/r/autonomous-hauling-system-for-increased-productivity-in-boliden-aitik,c3437805

[4] The Council of the Europen Parliament, *Machinery - Directive 2006/42/EC*, Std., 2006. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32006L0042

[5] ISO/TC 199, *ISO 12100:2010. Safety of machinery – General Principles for design – Risk Assessment and Risk Reduction*, Std., 2010. [Online]. Available: https://www.iso.org/standard/51528.html

[6] SAE International, *SAE J3016:2021. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*, Std., 2021. [Online]. Available: https://www.sae.org/standards/content/j3016_202104

[7] British Standards Institution, *PAS 1883:2020. Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification*, Std., 2020. [Online]. Available: https://www.bsigroup.com/en-GB/CAV/pas-1883/

[8] J. P. Castellanos-Ardila, S. Punnekkat, A. Fattouh, and H. Hansson, "A Context-specific Operational Design Domain for Underground Mining (ODD-UM)," in *Systems, Software and Services Process Improvement*. Springer International Publishing, 2022, pp. 161—-176.

[9] N. G. Leveson, *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

[10] N. Webb, D. Smith, C. Ludwick, T. Victor, Q. Hommes, F. Favaro, G. Ivanov, and T. Daniel, "Waymo's safety methodologies and safety readiness determinations," *arXiv preprint arXiv:2011.00054*, 2020.

[11] S. Baumgart, J. Froberg, and S. Punnekkat, "Can stpa be used for a system-of-systems? experiences from an automated quarry site," in *2018 IEEE International Systems Engineering Symposium (ISSE)*. IEEE, 2018, pp. 1–8.

[12] R. Tiusanen, E. Heikkilä, and T. Malm, "System safety engineering approach for autonomous mobile machinery," in *World Congress on Engineering Asset Management*. Springer, 2019, pp. 239–251.

[13] A. S. Sidhu, "Application of stpa-sec for analyzing cybersecurity of autonomous mining systems," Ph.D. dissertation, Massachusetts Institute of Technology, 2018.

[14] ISO/TC 127/SC 2, *ISO 17757:2019. Earth-moving machinery and mining — Autonomous and semi-autonomous machine system safety*, Std., 2019. [Online]. Available: https://www.iso.org/standard/76126.html

[15] ISO/TC 199, *EN ISO 13849-1:2015. Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*, Std., 2015. [Online]. Available: https://www.iso.org/standard/69883.html

[16] ISO/TC 22/SC 32, *ISO-SAE 21434:2021. Road vehicles — Cybersecurity engineering* , Std., 2021. [Online]. Available: https://www.iso.org/standard/70918.html

[17] A. Adriaensen, L. Pintelon, F. Costantino, G. Di Gravio, and R. Patriarca, "An stpa safety analysis case study of a collaborative robot application," *IFAC-PapersOnLine*, vol. 54, no. 1, pp. 534–539, 2021.

[18] J. Axelsson and A. Kobetski, "Towards a risk analysis method for systems-of-systems based on systems thinking," in *2018 Annual IEEE International Systems Conference (SysCon)*. IEEE, 2018, pp. 1–8.

[19] S. M. Yoo, A. N. Kopeikin, D. J. Gregorian, A. T. Munekata, J. P. Thomas, and N. G. Leveson, "System-theoretic requirements definition for human interactions on future rotary-wing aircraft," in *97th International Symposium on Aviation Psychology*, 2021, p. 334.

[20] E. Heikkilä, R. Tuominen, R. Tiusanen, J. Montewka, and P. Kujala, "Safety qualification process for an autonomous ship prototype–a goal-based safety case approach," in *Marine Navigation*. CRC Press, 2017, pp. 365–370.

[21] J. Montewka, K. Wróbel, E. Heikkilä, O. Valdez Banda, F. Goerlandt, and S. Haugen, "Challenges, solution proposals and research directions in safety and risk assessment of autonomous shipping," *Probabilistic Safety Assessment and Management PSAM*, vol. 14, pp. 16–21, 2018.

[22] S. Khastgir, S. Brewerton, J. Thomas, and P. Jennings, "Systems approach to creating test scenarios for automated driving systems," *Reliability Engineering & System Safety*, vol. 215, p. 107610, 2021.

[23] F. U. Muram, M. A. Javed, and S. Punnekkat, "System of systems hazard analysis using hazop and fta for advanced quarry production," in *2019 4th International Conference on System Reliability and Safety (ICSRS)*. IEEE, 2019, pp. 394–401.