SYSTEM SAFETY FOR AUTONOMOUS MINING

A White Paper to Increase Industry Knowledge and Enable Industry Collaboration on Applying a System Safety Approach to Autonomous Systems

GMG

About the Global Mining Guidelines Group

The Global Mining Guidelines Group (GMG) is a network of representatives from mining companies, original equipment manufacturers (OEMs), original technology manufacturers (OTMs), research organizations and academics, consultants, regulators, and industry associations around the world who collaborate to tackle challenges facing our industry. GMG aims to accelerate the improvement of mining performance, safety, and sustainability by enabling the mining industry to collaborate and share expertise and lessons learned that result in the creation of guidelines and related documents, such as white papers like this one, that address common industry challenges.

Interested in participating or have feedback to share? GMG is an open platform, and everyone with interest and expertise in the subject matter covered can participate. Participants from GMG member companies have the opportunity to assume leadership roles. Please contact GMG at info@gmggroup.org for more information about participating or to provide feedback on this white paper.

GMG was formed out of the Surface Mining Association for Research and Technology (SMART) group as part of the Canadian Institute of Mining, Metallurgy and Petroleum (CIM) and with the support of other Global Mineral Professionals Alliance (GMPA) members.

GMG is a legal entity of the Canadian Institute of Mining, Metallurgy and Petroleum.

Document Usage Notice

Recommended citation: System Safety for Autonomous Mining (White Paper). Global Mining Guidelines Group (2021).

Publication information
Publication Date: 2021-09-29

Contact information
Global Mining Guidelines Group
info@gmggroup.org
Gmggroup.org

About GMG White Papers

GMG white papers are educational documents that provide broad knowledge and identify further reading on a topic that is new to or not well-understood in the industry. This white paper is the product of industry-wide collaboration based on experience and lessons learned. White papers can lead to the development of GMG guidelines, which aim to help identify key considerations, good practices, and questions to ask on the topic covered.

White papers are reviewed throughout development and editing but do not undergo the working group review and voting process as guidelines do.

GMG white papers are for informational purposes only and are not intended to be used as direct guidance. The use and application of this white paper is the responsibility of the user. The information provided in this document does not replace or alter standards or any other national, state, or local governmental statutes, laws, regulations, ordinances, or appropriate technical expertise and other requirements. While the white paper was developed and reviewed by participants across the mining industry, GMG cannot guarantee that it is accurate or complete, and it does not necessarily represent the views of all of the participating organizations. See the disclaimer at the end of the document for further detail.

Credits

The following organizations and individuals were involved in the preparation of this white paper at various stages including content definition, content generation, and review. Please note that the white paper does not necessarily represent the views of the organizations listed below.

Project Group: System Safety for Autonomous Mining

Working Group: Autonomous Mining

Project Leader(s)
Chirag Sathe, BHP
Gareth Topham, Rio Tinto

Organizations Involved in the Preparation of this White Paper
ADRIA, Alcoa, AMOG Consulting, ASI Mining, Aurecon, Australian Droid + Robot, Beroe, BHP, British Columbia Ministry of Energy and Mines, Caterpillar, Chameleon Mettle Group, Edge Case Research, Enaex, Epiroc, Finning, GBM Limited, General Dynamics, Gold Fields, Government of Alberta, Greyhound, Hatch, Helios Consulting, Hitachi, IBM, Imdex Limited, Imperial, Impress Solutions, Ionic Engineering, Komatsu, Kroon Technology, MacLean Engineering, MEC Mining, Mining Plus, MineWare, MTGA, Newtrax, NIOSH, Norilsk Nickel, Nova Systems, PanAust, Peck Teck, Rio Tinto, Rockwell Automation, Roy Hill, Sandvik, Siemens, SMS Equipment, Strategy Focused Innovation, Symbiotic Innovations, Teck, Tellus Mining, Thales, Universal Field Robots, University of Queensland, Western Australia Department of Mines, Industry Regulation and Safety (DMIRS), Whitehaven Coal, Worley, Vale.

CONTENTS

1. INTRODUCTION AND BACKGROUND

Purpose

This white paper aims to provide a comprehensive view of the need for a system safety approach for those deploying and using autonomous systems in the mining industry. It also aims to increase awareness of system safety and its benefits in delivering and maintaining safe and efficient autonomous systems.

Scope

This white paper addresses the use of autonomous systems within the mining industry, both surface and underground. It applies to all autonomous machines and to the integration of autonomous and semi-autonomous machines with manually operated machines, as well as to complex integrated systems of systems across the mining industry. While this white paper was developed with a focus on autonomous systems, most of the information is general and is also relevant to manual operations.

Out of scope

This document does not provide a detailed procedure to manage system safety. Any procedural requirements associated with integration with fixed or processing plants are excluded.

Audience

The intended reader for this paper is any stakeholder within the mining industry looking to learn about system safety within the context of applying autonomous systems in mining.

1.1 Background

The need for a system safety approach arose in the mid-twentieth century as systems in industries such as nuclear power, civil aviation, defence, and space became increasingly large and complex. Because it is not always feasible to rely on testing and learning from experience, the lack of consideration given to the interactions between multiple subsystems being integrated into the custom systems increased risks for unexpected failures.

Further Reading

The Introduction to System Safety (Leveson, 2008) on the NASA website provides further background on system safety and its history.

System safety is a view of safety that extends beyond the machines to consider the complete system (i.e., machines, human factors, and environment, and the interfaces between these). The goal of system safety is to reduce risks associated with hazards to safety. It is a planned, disciplined, and systematic approach to identifying, analyzing, eliminating, and controlling hazards by analysis, design, and management procedures throughout a system's lifecycle. System safety activities start in the earliest concept development stages of a project and continue through design, development, testing, operational use, and disposal. For further consideration of the lifecycle, see Section 2.1.

Definition of system safety "System Safety is about applying systems engineering and systems management to the process of hazard, safety, and risk analysis to identify, assess and control associated hazards while designing or modifying systems, products, or services. The aim is to reduce or eliminate the potential for accidents before production, construction, or operation takes place." (IET System Safety Engineering Network, "Changing for the Future of Safety," 2018)

See the glossary at the end of this paper for the definitions of other terms as they are used in this document.

1.2 System Safety Within the Broader Context of Workplace Safety

System safety, when viewed from the broader context of workplace safety, includes several layers as shown in Figure 1. These layers are the outer regulatory layer that considers workplace safety management in operating environments, the middle layer that covers organizational safety management systems, and the inner system safety layer that provides an overall view that the right system has been built and it can be operated safely. These are described in more detail below, but they are not intended to be exhaustive.

The outer layer is a regulatory layer, which considers workplace safety management to enable a safe operating environment expressed through legislation and common law. Note that it is important to understand local legislative requirements for evaluating system safety.

The middle layer is the organizational layer, which covers managing and supporting the safe operation of the system. This layer includes:

- **Operational risk management:** to assess and manage operational risks to as low as reasonably practicable (ALARP).
- **Emergency management:** to confirm the understanding of potential consequences of an emergency event and be prepared to respond effectively to mitigate its effects and enable the subsequent recovery.

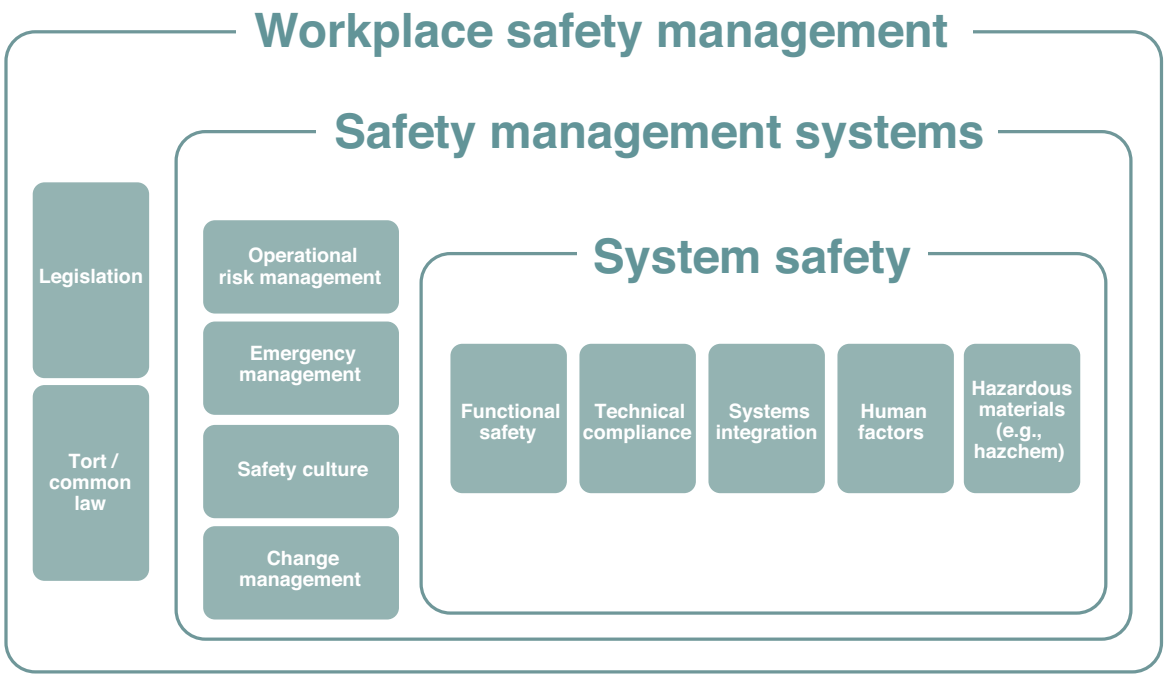

Figure 1. System Safety Viewed from the Broader Context of Workplace Safety, adapted from the *GMG Guideline for Applying Functional Safety to Autonomous Systems in Mining* (2020)

- **Safety culture:** to strive for an informed, flexible, and just safety culture within the organization that includes learning from mistakes and driving improvements in safety as part of routine performance.
- **Change management:** to confirm that every change implemented is assessed, approved, and communicated for the safe operation of the system.

The inner system safety layer provides an overall view that the right system has been built and it can continue to be operated safely. It includes the following aspects:

Functional safety is defined by the IEC (2021) as "part of the overall safety that depends on a system or equipment operating correctly in response to its inputs." Functional safety provides a systematic framework and outlines established practices that provide confidence in delivering and maintaining safety-related and safety-critical control measures. Functional safety is considered in the GMG *Guideline for Applying Functional Safety to Autonomous Systems in Mining* (2020). Functional safety, however, does not adequately cover systems that are non-deterministic, including those reliant on human behaviour or interacting with humans. As non-deterministic systems are likely to be used increasingly as technologies advance, a system safety approach will make sure the mining industry is developing a mechanism for the future that will support complex autonomous systems and intelligent mining solutions. For further consideration of non-deterministic systems, see Section 2.3.

Technical compliance refers to the need for a system to be compliant with existing regulations, codes of practice, and standards appropriate to its operating context. These sources provide evidence that good practices have been applied to eliminate or minimize risks so far as reasonably practicable.

Systems integration refers to the requirement for systems to be integrated safely, as the safety of the individual components of a system does not account for how these systems may (or may not, if required) interact. The system safety program should apply tools and techniques to confirm the safe integration of these systems as components in the larger system. Application of systems engineering as a design methodology, in particular safety systems engineering, addresses the "increased complexity, driven by increased use of software and automation, systems of systems, internet of things, closed loop control, and 'inexpert operators'" (INCOSE, 2021).

Human factors refer to the relationship between humans and the systems with which they interact, including performance, ergonomics, processes, and other environmental or physical factors. As a part of system safety, human factors need to be considered alongside the objectives of human-systems integration. Human-systems integration, the interdisciplinary technical and management process for integrating human considerations within and across all system elements is considered in more depth in Section 4 of this paper.

Hazardous materials refer to requirements for storing, handling, transporting, and managing materials that may lead to adverse health effects if personnel are exposed.

1.3 Mining-Specific Benefits and Considerations

Safety is one of the core values in the mining industry. In many cases, risk cannot be eliminated entirely, which is a key consideration when improving safety. A system is considered safe when the risks associated with it are reduced to an acceptable level, such as ALARP. Technological advances such as autonomous systems can make it possible to reduce certain risks by removing humans from dangerous situations. This possibility provides opportunities to make systems safer than the level accepted with manually operated systems.

When managing the transition to autonomous systems in mining, there are many aspects of safety to take into consideration beyond machine automation, these include:

- Dynamic operating conditions (e.g., dump locations, new mining areas)
- Single vendor or multi-vendor fleets
- Integration of manually operated and autonomous equipment environments
- Interoperability of autonomous systems
- Operating conditions that are new or less mature for autonomous systems in mining
- Considerations of local regulatory requirements

A system safety approach provides an overview of the overall effectiveness of the safety controls that extends beyond the machines and can be a useful qualitative tool for operations when assessing the overall safety of their systems. This type of systems approach is especially important as highly autonomous and highly integrated solutions evolve.

Some of the key benefits of using a system safety approach are that it:

- Provides a holistic safety approach for integrating autonomous systems into the mine site
- Reduces risk to the business
- Enables the identification of hazards caused by interfaces and interconnectivity

- Permits the assessment of non-deterministic and complex systems or those using newer technology (e.g., those based on artificial intelligence [AI], neural networks, or machine learning)
- Assists with enhancing a safety culture
- Assists with the engagement and acceptance of autonomous systems by all internal and external stakeholders, such as regulators and community groups
- Enables the adaptation of existing and the development of new maintenance practices and infrastructure
- Considers cybersecurity beyond data integrity to include cyberterrorism, cyberespionage, and cybersabotage from competitors or state actors

1.4 Navigation

The rest of this white paper is structured into four sections to provide context on some of the key aspects of adopting a system safety approach, though it does not intend to be comprehensive.

- Section 2 provides an overview of applying a system safety approach by describing an example of a lifecycle and offering further considerations about hazard identification and risk assessment and non-deterministic systems.
- Section 3 describes the purpose of a safety case in the context of autonomous systems in mining and some of the typical contents within one.
- Section 4 describes the significance of eliminating or controlling risks to humans and the environment over the course of a system's lifecycle.
- Section 5 provides context on some factors that influence the degree of risk reduction that can be considered for a software-based safety control in the development and operation of autonomous systems.

2. SYSTEM SAFETY MANAGEMENT

Safety management refers to managing the safety of changes that may affect the risk of harm. For autonomous systems in mining, safety management involves considering all relevant factors and making sure that the risks related to adopting automation are as low as they can be practicably made. While this process involves considering the system throughout the life of the change, it is mostly done before the change is made. This section begins by describing an example of an overall lifecycle approach from concept to operation (Section 2.1). Then, it expands on hazard identification and risk assessment as a key first step in system safety management (Section 2.2). It closes by considering non-deterministic systems, which are not as easily mapped to a traditional lifecycle (Section 2.3).

2.1 Lifecycle

System safety activities for the autonomous mine site are applied throughout the entire system lifecycle. Figure 2 outlines an example of what a system safety lifecycle could look like for an application of autonomous systems in mining, highlighting some key aspects of the system safety approach. The connections identified with arrows are not intended to be exhaustive. Continuous improvement connects the concept and operation stages of the lifecycle to indicate that a system safety approach is also iterative and does not stop when the autonomous system is in operation. Table 1 provides further context about the potential actions throughout the lifecycle stages.

Because applications of autonomous systems in mining will vary, so too will the approach to the system safety lifecycle. Some factors that may affect the application of the lifecycle include whether the system is a commercially available system or a new system development, the scale of the project, the operational environment, and operational maturity at the mine site.

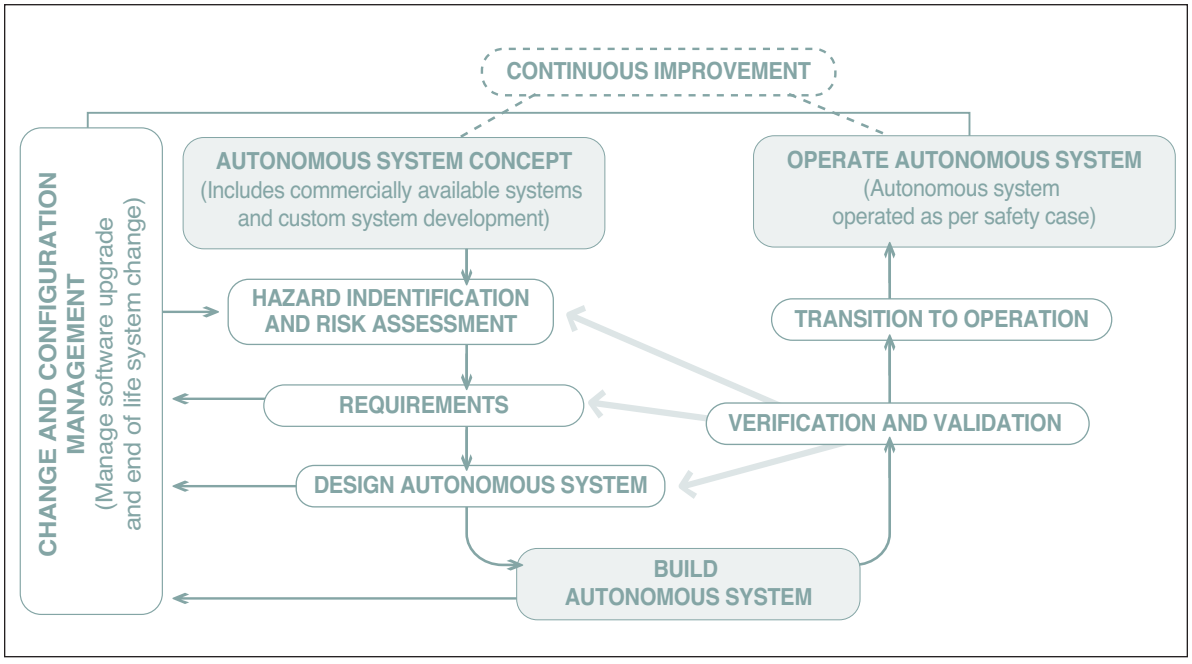

Figure 2. Example of System Safety Lifecycle for Applying Autonomous Systems in Mining

Table 1. Potential Actions Throughout the System Safety Lifecycle

Hazard Identification and Risk Assessment (See Section 2.2 for further detail)	• Safety planning • Identify hazards and risk controls • Identify all supporting systems and processes required to manage effectiveness of risk control • Identify human factor aspects that can influence safety • Identify any deterministic functional safety controls and follow relevant functional safety standards and guidance • Identify cybersecurity risks and conduct a separate risk analysis
Requirements	• Define risk control requirements to meet intention of claim in each hazard scenario • Derive functional, technical, and safety specifications from the concept of operations • Define human factor aspect requirements • Define requirements for supporting systems and processes to manage controls effectively • Define risk control monitoring requirements to maintain control effectiveness • Develop forward and backward traceability to link requirements throughout the validation process • Develop a verification and validation plan • *Optional:* Provide preliminary safety case (this will help with the final safety case but is not required)
Design Autonomous System	• Design risk controls according to requirements • Design human factor aspects according to requirements • Design supporting systems and processes according to requirements • Design monitoring tools according to requirements • *Optional:* Provide an interim safety case (this will help with the final safety case but is not required)
Verification and Validation	• Confirm that risk controls are verified and validated • Confirm that human factor aspects are verified and validated • Confirm that supporting systems and process are verified and validated • Confirm that monitoring tools are verified and validated • Confirm that all initial assumptions are valid • Confirm that all verification and validation activities link back to requirements and hazard and risk assessment • Perform user acceptance testing (some testing can be done in controlled circumstances)
Transition to Operation	• Complete the operational safety case and include all safety-related evidence and operational safety requirements • Confirm that the operation is ready to receive the autonomous system (training, supporting systems, management processes, monitoring tools) • Identify and control commissioning risks
Operate Autonomous System	• Confirm that the system is operated as per the safety case and that the safety requirements and objectives are being met while the system is operational • Manage risks associated with emerging issues and implement required changes • Maintain the system in line with the required processes • Confirm that the training and capability of resources is adequate • Monitor human-systems integration and human factors that may affect safety • Monitor risk controls for consistency with the requirement specifications
Change and Configuration Management	• Manage change and configuration of the autonomous system to enable optimal safety performance • Manage software upgrade and end of life system changes

2.2 Hazard Identification and Risk Assessment

Identifying the hazards associated with the change to autonomous systems and making sure that controls are in place against each hazard is an important first step. For minor risks, an alternative to this step would be to demonstrate that the risk arising from the hazard is neither severe nor probable.

The risks and controls for autonomous machines and systems in mining can be noted in original equipment manufacturer (OEM) documentation, in international standards, or in other industry guidance and research. For example:

- ISO 17757 provides safety requirements for autonomous and semi-autonomous machine systems in an earth-moving and mining environment (International Organization for Standardization [ISO], 2019a).
- UL4600 Chapter 6 "Risk Assessment" may be another useful source with content and scoping references, including details required of fault models, hazards, and risk assessment (Underwriters Laboratories, 2019). See also the considerations under hazard and risk assessment in the lifecycle example outlined in Section 2.
- ISO 12100 identifies basic principles and methodology for the risk assessment in achieving safety in the design of machinery (ISO, 2010).

In addition, it is critical to understand any project or site-specific risks and the potential controls.

Note

While the most recent versions of these standards at the time of publication are cited here, please refer to the relevant websites for the latest version.

As a minimum, the controls identified and implemented should satisfy the requirements that are set out in the local regulatory requirements. Applying industry-recognized standards and guidelines is a practical method to demonstrate that the risk is managed appropriately.

Before deciding that referring to standards is sufficient, confirm that:

- The equipment is being used as intended
- The standards enable the reduction of the risk to as low as reasonably practicable

When implementing a change to an autonomous system in mining, it is appropriate that the new system improves the safety of the overall system and reduces any risks identified, including the risks to humans in any changed operating environment.

2.3 Non-Deterministic System Elements and Machine Learning

Consideration of non-deterministic system elements

Autonomous systems can have non-deterministic elements, meaning that decisions are derived from complex sensor and processing algorithms and/or involve machine learning (e.g., emergency intervention systems, advanced driver assistance systems, and AI route planning). Traditional safety standards—and by extension traditional software development processes—may not apply to these situations. If the system includes non-deterministic software, it may be unlikely that it will be possible to assign it a significant risk reduction, thereby requiring risk to be reduced either by other deterministic software controls that are independent from the non-deterministic software or by other controls entirely (e.g., mechanical, administrative).

Machine learning

A growing number of complex capabilities are being developed using machine learning (e.g., image analysis and route planning). These capabilities learn from examples rather than by using conventional development, which can make them cost-effective. Using machine learning has an impact on lifecycles and on assurance, and this impact can cause challenges when employing machine learning during the implementation of some of the system software.

A machine learning lifecycle has a highly iterative development process; thus, mapping it to the normal safety lifecycle is not as simple as it would be for traditional systems. The input requirements could be considered comparable, but the rest of the machine learning lifecycle does not enable clear definition through to verification and validation. Tests of the deployed system in the real environment, however, may provide data that support both verification and validation. In practice, it is also likely that the distinction between the product and application will be more blurred with machine learning than with a conventional lifecycle. For example, obstacle avoidance is a core product function, but it needs to be particularized to the classes of objects and their locations in a specific operational setting.

Assessing the safety of systems using machine learning is currently not well addressed in standards. While some work is ongoing on standards and guidelines in mining and quarrying and in related disciplines such as autonomous road vehicles, it may take some time before widely accepted standards emerge. In the interim, a risk-based approach may be the most appropriate way to manage overall system safety. Such an approach will likely require consideration of other controls (e.g., deterministic software, mechanical, administrative) to reduce residual risk to a tolerable level.

Further Reading

Some considerations for machine learning and AI techniques are covered in Section 8.5 of UL 4600 (Underwriters Laboratories, 2019).

3. SAFETY CASE

The purpose of a safety case for the deployment of an autonomous system is to communicate a clear and comprehensive argument that a system is acceptably safe to operate in a particular context, thereby providing confidence that the appropriate work has been completed. The development of the safety case involves engaging with several internal and/or external stakeholders including:

- Regulators
- Mine operators
- OEMs and suppliers
- Technology integrators

A maintained safety case supports future modifications to a system, changes to the way a system is operated, or changes to its application.

The system safety case should provide evidence that:

The system or product has been accurately defined and, particularly, the autonomous systems. This should include the limits of concern, standards to be addressed, and the relationship to other systems and where supporting safety arguments are made elsewhere.

An effective program of safety activities has been performed.

Safety requirements have been set for the system or product that are consistent with safety objectives and targets.

Human factors have been satisfactorily considered for interacting with the autonomous systems in both normal and degraded modes.

Any conditions on the application of the system have been accepted by people who are able to confirm that the system complies with these conditions.

The system or product was designed, built, and installed within **defined quality arrangements** in compliance with relevant standards.

The safety objectives and targets for the system or product have been established.

The risk associated with the system or product has been estimated and shown to be acceptable.

Hazards associated with the system or product have been comprehensively identified.

Any assumptions made during the analysis have been confirmed.

The safety requirements have been met.

The system or product and its documentation are under **effective configuration management**.

The risk associated with any unresolved issues (e.g., hazards that are not closed, unresolved assumptions that have not been confirmed, and safety requirements that have not been complied with) has been controlled and arrangements are in place to resolve these issues.

The software has been developed to deliver the safety requirements using an appropriate process (e.g., ISO 19014-4, ISO, 2020).

It is **practical to maintain the system in a safe state** and to maintain and operate it safely going forward.

A good practice when approaching a safety case is "seamless development" by the production and presentation of the safety case at several stages of a project. Identifying safety objectives early allows the autonomous system design and/or application to be influenced as the system development progresses to establish a more compelling safety case. Note that the development of the safety case can differ depending on whether the autonomous system is a custom system or a commercially available one.

Potential approach

It may also be appropriate and beneficial to use a modelling notation approach, such as Goal Structuring Notation (2018) as a graphical way to represent the argument.

Three versions of the safety case are suggested at different stages of the autonomous system development lifecycle. Please note that while these are progressive and help to develop the final safety case, not all are required.

1. **Preliminary safety case:** After definition and review of the system requirements specification (see "requirements" in Figure 2)
2. **Interim safety case:** After initial system design and preliminary validation activities (see "design autonomous system" in Figure 2)
3. **Operational safety case:** Just prior to in-service use, including complete evidence of satisfaction of system requirements (see "transition into operation" in Figure 2)

In other industries, it is common to use a compilation of subsystem safety cases that can be used to support an overall application or system and its own safety case. This practice offers advantages by clarifying the ownership of the safety argument between the different parties who are involved and can reduce potential rework.

Useful references and further information

Systematic Approach to Safety Case Management (Kelly, 2004): This article outlines safety case development using the Goal Structured Notation technique.

UL 4600 Standard for Safety for the Evaluation of Autonomous Products (Underwriters Laboratories, 2019). This standard covers safety case construction, the chapters on Safety Case and Arguments (Chapter 5) and Risk Assessment (Chapter 6) are especially relevant.

The Assuring Autonomy International Programme (AAIP) Body of Knowledge: This is an online body of knowledge that aims to provide guidance about the safe development of autonomous systems (University of York, n.d.).

4. HUMAN-SYSTEMS INTEGRATION

System safety engineering applies a comprehensive approach to identifying and eliminating or controlling risks to humans and the environment over the course of a system's lifecycle. Understanding the roles people play within systems is essential for system safety to be achieved (Walden et al., 2015). Human-systems integration is the interdisciplinary technical and management process for integrating human considerations within and across all system elements. In mining operations introducing autonomous systems, the following six domains are considered relevant to human-systems integration, as identified in Burgess-Limerick (2020):

Staffing
Decisions regarding the number, and characteristics, of the roles that will be required to operate and maintain the joint human-automation system.

Personnel
Characteristics of the people such as operators and managers filling the staffing roles.

Training
The extent and methods for preparing and assessing personnel to obtain and maintain competencies required for safe operation and maintenance of the joint human-automation system. ISO 17757 includes some content on training (ISO, 2019a).

Human Factors Engineering
The consideration of human capabilities and limitations in system design, development, evaluation, and operations.

Safety
Involves traditional risk analysis and evaluation techniques such as hazard and operability studies, layers of protection analysis, failure modes and effects analysis, as well as systems focused risk analysis techniques (e.g., Systems-Theoretic Process Analysis).

Occupational Health
Promotes and maintains physical, mental, and social well-being of personnel through prevention, mitigation, and adaptation of risky working conditions.

History

Human-systems integration processes were formalized by the US defence industry, first addressed in the Manpower and Personnel Integration (MANPRINT) program in 1986 (Booher, 2003) to make sure that human-related issues are adequately considered during system planning, design, development, and evaluation (Folds, 2015). They have since been widely adopted in other industries, particularly aviation, space, rail, and health (NASA, 2019; Melnik et al., 2018). Human-systems integration has been found to be key in system performance across these industries that, like autonomous mining, require remote network operations (Nneji, 2019).

Human-systems integration includes consideration of interactions and potential trade-offs between decisions made in different areas. For example, decisions regarding the autonomous system and interface complexity may influence personnel characteristics and training requirements, as well as the anticipated number of people required for system operation and maintenance.

Human-systems integration incorporates human-centred analysis, design, and evaluation within the broader systems engineering process. Human-systems integration is a continuous process that should begin during the development of the concept of operations for any automation project, and continue throughout system design, testing, and evaluation to iteratively verify that safety goals are being achieved.

Human-systems integration for introducing autonomous systems in mining encompasses:

- Concept of operations and scenario development
- Task analyses
- Function and role allocation and definition between humans and autonomous systems, including training and competency assessment needs analysis
- Iterative conceptual design and prototyping
- Empirical testing (e.g., human-in-the-loop simulation)
- Monitoring of human-system performance during operation

The increase in available data produced by autonomous systems could be leveraged to help monitor human-system performance and identify associated issues that more traditional approaches might not uncover.

Relationship between Human Factors and Human-Systems Integration

When considering the objectives of introducing autonomous systems and of human-systems integration in system safety, human factors issues that are related to human-systems integration also need to be considered. These issues include job design, workplace layout, workload, communication means, decision rights, training, and technology and system components such as displays, alarms, and alerts. Without sufficient emphasis on human factors and human-systems integration during the risk assessment phase, there is a risk that the project will not meet its initial objective of improving productivity and safety and deliver the benefits of the overall investment.

Human factor assessments can also reveal stressors introduced due to human-systems integration that may not reveal themselves as a health risk in the short term. These health factors should be considered in human-systems integration risk assessments but are often overlooked because they occur over a long-term time frame and may have multiple contributing factors. The risks of overlooking these issues include:

- Decreased productivity
- Shortcuts in using the systems as designed
- Workarounds in processes (particularly where key performance indicators are involved)
- Workforce attrition
- Absenteeism
- Decrease in employee satisfaction negatively affecting the workplace culture
- Overlooking critical alerts
- Reduced understanding of how the issues can be resolved

There are several key human-systems integration issues to consider when implementing autonomous systems in mining, described in Table 2.

Table 2. Key Human-Systems Integration Considerations for Autonomous Systems in Mining

Operator Span of Control	• The decisions regarding the number of roles included in the joint human-automation system (staffing) and the selection of people for these roles (personnel). • The interactions with the design of interfaces by which people supervise autonomous systems (human factors engineering). • The design of training and competency assessment methods to confirm that the ratio of people to automated components enables the maintenance of situation awareness and an optimal workload. • The cognitive capacity of the operator and any potential issues around it. • Maintaining engagement and the attention of the operator.
Role of Existing Personnel	• The decisions regarding the changes in roles and responsibilities of existing personnel to take advantage of existing knowledge and experience. • Recognition of the need for ongoing training and competency assessment.
Confidence and Complacency	Paying careful attention to the design of interfaces, safety analyses, and training. • Providing personnel with the ability and understanding that allows them to recognize and react to a failure in the technology or situations when the technology not responding as expected. Personnel need to be confident they understand the technology so well that they know when and how they can override it or revert to a manual process, if they ever need to do so. • Making sure that people in the system are neither complacent nor lack confidence in the design of the automation technology and confirming that they understand the capabilities and limitations of the technology. This confirmation also requires that the technology be designed and tested in a trustworthy manner.
Critical Alarm Management	• Designing effective ways to display alarms to make sure that operators can identify critical alerts and understand how the issues can be resolved. • The development of alarm management processes and alarm management key performance indicators for effective alarm response. An alarm philosophy is typically used to document the alarm management strategy.
Existing Systems and Processes	• Understanding existing processes and systems and how they integrate with each other and with the introduced technology. • Human-systems integration considerations should not be considered in isolation to one system or process but with every integration point within the span of control of any system personnel.

5. SOFTWARE SAFETY MANAGEMENT

Autonomous systems are typically software intensive and the software is increasingly used to carry out safety-critical functions such as object detection and avoidance. However, there are several factors that influence the degree of risk reduction that can be considered for a software-based safety control, for example:

- The software development lifecycle
- The languages and operating environment of the software
- The testing methodology and completeness of the documentation
- The competencies of those involved in the development and maintenance of the software

5.1 Developing the Autonomous System

Software safety standards generally cover the following aspects to secure a particular level of risk reduction:

- How the requirements for the software component have been specified and assessed
- The languages used to implement the software component and the operating system the component runs on
- Whether the component has non-deterministic aspects
- The verification and validation procedures that have been applied to the component, including consideration of the extent of the tests' completeness and appropriateness
- The review of the component and the degree of the reviewers' independence
- The independence of the software component itself from other safety software controls

Delivering software that provides a safety risk reduction typically involves reference to recognized standards such as ISO 13849 or ISO 19014-4 (ISO 2015, ISO 2020). These standards are used for base machine system development, but the overall process may be used for autonomous system development. ISO 21448 provides an example of a risk-based approach using the safety of the intended function (SOTIF) for developing a software function (ISO 2019b).

Note

While the most recent versions of these standards at the time of publication are cited here, please refer to the relevant websites for the latest version.

5.2 Operating the Autonomous System

Operating autonomous systems requires the development and implementation of a software safety management plan. Some of the key processes to consider are:

- An effective training environment for implementing an autonomous system so that there is sufficient context and domain knowledge among operators and maintainers onsite
- Effective communication to relevant stakeholders to manage operation of the autonomous system
- Conducting required verification tests following any software upgrade and updating the relevant documents with the outcome of verification tests
- Access management that limits access to authorized personnel

- Change management that tracks all aspects of changes to the configuration of the system, documenting the details of the change, updating operating procedure, verification procedure, and rollback procedure
- Recovery procedures, including a failure analysis to determine the vulnerabilities if there is an unforeseen event such as a lightning strike or hardware failure, disaster recovery procedures, and backup options, such as redundancies or spares

5.3 Other Considerations

Other key considerations around software safety management for autonomous systems in mining include:

Iterative and continuous software lifecycle: The software lifecycle steps, which are similar to the steps outlined in Figure 2, will typically require an iterative and responsive process with continual updates to manage gaps, dependability, change, and redundancies. UL 4600 Chapter 9 on "Software and System Engineering Processes" is a useful reference on this topic.

Adaptable software development, verification, and validation process: Software for autonomous systems will likely operate in a wide variety of environments, and it is impossible to exhaustively test all possible environmental conditions prior to deployment. Software verification and validation processes should be designed to accommodate this variability. For example, testing should be conducted for each deployment whenever there is a significant change to the software to confirm the software still operates correctly in the environment associated with that specific deployment.

Audit trail: Software should provide robust record keeping and audit abilities, especially for safety-critical functions, which support the ability to properly execute incident investigations and analysis. This is an essential step in any continuous improvement cycle and is equally important in the context of software lifecycle management and continuous safety improvement.

6. SUMMARY AND NEXT STEPS

By introducing some system safety concepts to consider when introducing autonomous systems in mining and addressing topics that GMG participants consider important in achieving the goals of safe implementation, this white paper provides a general overview that highlights some of the challenges for the industry and attempts to provide some high-level approaches to them.

However, as only an introduction to the topic, future work is required to provide more complete guidance on applying system safety to autonomous systems in mining. This paper aims to be used to inform the industry on the topic and assist with achieving the industry consensus and knowledge required to enable the development of this guidance. The GMG Autonomous Mining Working Group will collaborate to determine the direction and approach to this topic going forward.

GLOSSARY

This glossary contains several terms defined as they are used throughout this white paper. It is not intended to be exhaustive.

As low as reasonably practicable (ALARP): A principle used in assessing and managing operational risks so that residual risk is reduced to as far as reasonably practicable.

Autonomous machine: Refers to autonomous and semi-autonomous machines (ASAMs) as they are defined in ISO 17757 (2019a, 3.1.3.1 and 3.1.3.2). In this white paper, it refers specifically to mining machines.

Autonomous system: Refers to autonomous and semi-autonomous machine systems (ASAMSs) as they are defined in ISO 17757 (2019a, 3.1.2). In this white paper, it refers specifically systems in mining.

Deterministic system: A system where outcomes are determined based on known and understood modes and conditions.

Functional safety: "Part of the overall safety that depends on a system or equipment operating correctly in response to its inputs" (IEC, 2021).

Human factors: The relationship between humans and the systems with which they interact, including performance, ergonomics, processes, and other environmental or physical factors.

Human-systems integration: The interdisciplinary technical and management process for integrating human considerations within and across all system elements (see Section 4).

Non-deterministic system: A system or aspects of a system where decisions are derived from complex sensor and processing algorithms and/or involve machine learning (e.g., emergency intervention systems, advanced driver assistance systems, and AI route planning).

Safety case: A document produced that communicates a clear and comprehensive argument that a system is acceptably safe to operate in a particular context, thus providing confidence that the appropriate work has been completed.

Safety management: The management of the safety of changes that may affect the risk of harm.

System safety: "System Safety is about applying systems engineering and systems management to the process of hazard, safety, and risk analysis to identify, assess and control associated hazards while designing or modifying systems, products, or services. The aim is to reduce or eliminate the potential for accidents before production, construction, or operation takes place." (IET System Safety Engineering Network, "Changing for the Future of Safety," 2018).

Risk: Within the context of safety management, risk refers to the likelihood that an accident will happen and the harm that could arise.

REFERENCES AND FURTHER READING

A note on references to standards: The standards cited in this white paper refer to the most recent version at the time of publication. If a standard has since been updated, please refer to the more recent version.

References Cited in the Text

Booher, H. (2003). *Handbook of Human Systems Integration*. Wiley. https://doi.org/10.1002/0471721174

Burgess-Limerick, R. (2020). Human-systems integration for the safe implementation of automation. *Mining, Metallurgy & Exploration.* 37, =1799–1806. https://doi.org/10.1007/s42461-020-00248-z

Folds, D. J. (2015). Systems engineering perspective on human systems integration. In D. A. Boehm-Davis, F. T. Durso, & J. D. Lee (Eds.), *APA handbook of human systems integration.* (pp. 21–35). American Psychological Association. https://doi.org/10.1037/14528-002

Global Mining Guidelines Group. (2020). *Guideline for Applying Functional Safety to Autonomous Systems in Mining* (Guideline No. GMG-AM-FS-v01-r01). https://gmggroup.org/wp-content/uploads/2020/08/20200709_Guideline_for_Applying_Functional_Safety_to_Autonomous_Mining_Systems-GMG-AM-FS-v01-r01.pdf

INCOSE. (2021). *System Safety Mission & Objectives.* https://www.incose.org/incose-member-resources/working-groups/analytic/system-safety

International Electrotechnical Commission. (2013, November). Functional Safety. Electropedia. http://www.electropedia.org/iev/iev.nsf/display?openform&ievref=351-57-06

The Institute of Engineering and Technology System Safety Engineering Network. (2018, October 30). Changing for the Future of Safety. *IET System Safety Engineering Network Blog*. https://communities.theiet.org/groups/blogpost/view/47/203/6180

International Organization for Standardization. (2015). *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design* (Standard No. ISO 13849-1:2015). https://www.iso.org/standard/69883.html

International Organization for Standardization. (2019). *Earth-moving machinery and mining — Autonomous and semi-autonomous machine system safety* (Standard No. ISO 17757:2019). https://www.iso.org/standard/76126.html

International Organization for Standardization. (2019). *Road vehicles — Safety of the intended functionality.* (ISO Standard No. 21448:2019). https://www.iso.org/standard/70939.html

International Organization for Standardization. (2020). *Earth-moving machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system* (ISO Standard No. 19014-4:2020). https://www.iso.org/standard/70718.html

Kelly, T. (2004). A Systematic Approach to Safety Case Management. (SAE Technical Paper No. 2004-01-1779). SAE International https://doi.org/10.4271/2004-01-1779

Leveson, N. (2008, June 1). An Introduction to System Safety. *ASK Magazine* 31, 20-24. https://appel.nasa.gov/2008/06/01/an-introduction-to-system-safety/

Melnik, G., Roth, E., Multer, J., Safar, H., & Isaacs, M. (2018). *An Acquisition Approach to Adopting Human Systems Integration in the Railroad Industry* (Report No. DOT/FRA/ORD-18/05). US Department of Transportation Federal Railroad Administration. http://dx.doi.org/10.13140/RG.2.2.16041.65120

National Aeronautics and Space Administration. (2019). *NASA spaceflight human-system standard. Volume 2: Human factors, habitability, and environmental health*. (Standard No. NASA-STD-3001 VOL 2). https://standards.nasa.gov/standard/nasa/nasa-std-3001-vol-2

Nneji, V. C. (2019). *A Workload Model for Designing & Staffing Future Transportation Network Operations* (Doctoral dissertation, Duke University). Duke Dissertations. https://dukespace.lib.duke.edu/dspace/handle/10161/18694

Safety Critical Systems Club. (2018). Goal Structuring Notation. https://www.goalstructuringnotation.info/

Underwriters Laboratories. (2019). *Standard for Safety for the Evaluation of Autonomous Products* (Standard No. ANSI/UL 4600). https://www.shopulstandards.com/ProductDetail.aspx?productid=UL4600

University of York. (n.d). Body of Knowledge. Assuring autonomy international programme. https://www.york.ac.uk/assuring-autonomy/body-of-knowledge/

Walden, D., Roedler, G.J., Forsberg, K.J., Hamelin, R.D. & Shortell, T.M. (Eds.). (2015). *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities* (4th ed). https://www.incose.org/products-and-publications/se-handbook

Other Further Reading

The following references include other publications on safety and autonomous systems in mining, further reading on system safety, including documentation from other industries.

Aptiv. (2019). *Safety First for Automated Driving.* https://www.aptiv.com/docs/default-source/white-papers/safety-first-for-automated-driving-aptiv-white-paper.pdf?sfvrsn=534e2c3e_2

CMEIG EMESRT, and ICMM. (2020). *White Paper and Guiding Principles for Functional Safety for Earthmoving Machinery.* https://www.cmeig.com.au/working-groups/engineering/

Department of Defense. (2012). *Department of Defense Standard Practice: System Safety* (Standard No. MIL-STD 882E). http://everyspec.com/MIL-STD/MIL-STD-0800-0899/MIL-STD-882E_41682/

Federal Aviation Administration. (2000). *System Safety Handbook. Federal Aviation Administration: United States Department of Transportation.*
https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/ss_handbook/

Federal Railroad Administration. (2018). *An Acquisition Approach to Adopting Human Systems Integration in the Railroad Industry* (Report No. DOT/FRA/ORD-18/05). Federal Railroad Administration.
https://railroads.dot.gov/elibrary/acquisition-approach-adopting-human-systems-integration-railroad-industry

Government of Western Australia Department of Mines and Petroleum. (2015). *Safe mobile autonomous mining in Western Australia - Code of practice.*
https://www.dmp.wa.gov.au/Documents/Safety/MSH_COP_SafeMobileAutonomousMiningWA.pdf

International Electrotechnical Commission. (2015). *Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems* (Standard No. IEC 62279:2015).
https://webstore.iec.ch/publication/22781

IEEE Standards Association. (2020). *IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being* (Standard No. IEEE 7010-2020)https://standards.ieee.org/standard/7010-2020.html

International Organization for Standardization. (2010). *Safety of machinery — General principles for design — Risk assessment and risk reduction* (Standard No. ISO 12100:2010) https://www.iso.org/standard/51528.html

International Organization for Standardization. (2015). *Systems and software engineering — System life cycle processes* (Standard No. ISO 15288:2015). https://www.iso.org/standard/63711.html

The International Rail Industry's Engineering Safety Management Handbook. (2017). *The International Rail Industry's Engineering Safety Management Handbook.* https://www.intesm.org/download.html

Disclaimer

This publication contains general guidance only and does not replace or alter requirements of any national, state, or local governmental statutes, laws, regulations, ordinances, or appropriate technical expertise and other requirements. Although reasonable precautions have been taken to verify the information contained in this publication as of the date of publication, it is being distributed without warranty of any kind, either express or implied. This document has been prepared with the input of various Global Mining Guidelines Group (GMG) members and other participants from the industry, but the publications do not necessarily represent the views of GMG and the organizations involved in the preparation of this document. Use of GMG publications is entirely voluntary. The responsibility for the interpretation and use of this publication lies with the user (who should not assume that it is error-free or that it will be suitable for the user's purpose). GMG and the organizations involved in the preparation of this publication assume no responsibility whatsoever for errors or omissions in this publication or in other source materials that are referenced by this publication, and expressly disclaim the same. GMG expressly disclaims any responsibility related to determination or implementation of any management practice. In no event shall CIM or GMG (including its members, partners, staff, contributors, reviewers, or editors to this publication) be liable for damages or losses of any kind, however arising, from the use of or reliance on this document, or implementation of any plan, policy, guidance, or decision, or the like, based on this general guidance. CIM and GMG (including its members, partners, staff, contributors, reviewers, or editors to this publication) also disclaims any liability of any nature whatsoever, whether under equity, common law, tort, contract, estoppel, negligence, strict liability, or any other theory, for any direct, incidental, special, punitive, consequential, or indirect damages arising from or related to the use of or reliance on this document. CIM and GMG (including its members, partners, staff, contributors, reviewers, or editors to this publication) are not responsible for, and make no representation(s) about, the content or reliability of linked websites, and linking should not be taken as endorsement of any kind. We have no control over the availability of linked pages and accept no responsibility for them. The mention of specific entities, individuals, source materials, trade names, or commercial processes in this publication does not constitute endorsement by CIM and GMG (including its members, partners, staff, contributors, reviewers, or editors to this publication). In addition, the designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of CIM and GMG (including its members, partners, staff, contributors, reviewers, or editors to this publication) on the legal status of any country, territory, city or area or of its authorities, or concerning delimitation of any frontiers or boundaries. This disclaimer should be construed in accordance with the laws of Canada.


GLOBAL MINING GUIDELINES GROUP
GMG
Innovation through Collaboration