GLOBAL MINING GUIDELINES GROUP

GMG

GUIDELINE FOR APPLYING SYSTEM SAFETY IN MINING

PUBLISHED DECEMBER 2023

AUTONOMOUS MINING WORKING GROUP

Global Mining Guidelines Group (GMG)

ABOUT GMG

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, such as 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 guideline.

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 an independent, industry-led organization.

ABOUT GMG GUIDELINES

GMG guidelines are peer-reviewed documents that describe good practices, advise on the implementation and adoption of new technologies, and/or develop industry alignment. They are the product of industry-wide collaboration based on experience and lessons learned. The guidance aims to help readers identify key considerations, good practices, and questions to ask on the topic covered and enable operational improvements for safe, sustainable, and productive mines.

Once the guideline is reviewed and accepted by the project group steering committee, working group members peer review and GMG members within the working group vote to approve draft documents prior to their approval by the GMG Board of Directors.

GMG guidelines are intended to provide general guidance only, recognizing that every situation will be different. Use of these guidelines is entirely voluntary and how they are applied is the responsibility of the user. These guidelines do 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 guidelines are developed and reviewed by participants across the mining industry, they do not necessarily represent the views of all of the participating organizations and their accuracy and completeness are not guaranteed. See the disclaimer on p. ii for further detail.

RELATED GMG DOCUMENTS

While guidelines are the primary output of GMG Working Groups, GMG also produces documents that supplement guidelines. These include:

- White papers: Educational or foundational documents that provide broad knowledge and identify further reading on a topic that is new to or not well-understood in the industry. These documents are reviewed throughout development and editing but do not undergo the working group review and voting process as guidelines do. These projects can lead to guideline development.
- Reports: Outcomes of outreach, industry research, and events can be presented in reports and can inform the priorities for developing industry guidance.
- Landscapes: Reviews of ongoing related work by other organizations on a key topic. These aim to provide the industry with an idea of what exists and prevent duplication of effort.
- Case studies/other examples and tools: These documents aim to share knowledge and provide examples for the benefit of the broader industry and supplement GMG guidelines.

RELATIONSHIP TO STANDARDS

GMG guidelines are not standards and should not be treated as such. The guidelines can be used to assist the mining community with practices to improve their operations and/or implement new technologies. They aim to supplement, not replace, existing standards, regulations, and company policies. Guidelines can also be a first step in identifying common and successful practices and feed into standardization efforts. GMG does not develop standards but does participate in standardization efforts through partnerships.

CREDITS

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

Project Group

System Safety for Autonomous Mining Guideline

Working Group

Autonomous Mining Working Group

Project Leaders

Carlos Viquez, Rio Tinto

Chirag Sathe, BHP

Gareth Topham, CWG Project Services

Project Steering Committee

Andrew Scott, BHP

Carlos Viquezm, Rio Tinto

Chirag Sathe, BHP

Christian Quirion, Agnico Eagle

Gareth Topham, CWG Project Services

Rhys Scholefield, Rio Tinto

PARTICIPATING ORGANIZATIONS

3D-P • ABB • A&B Global Mining Pty Ltd • Accenture • Agnico Eagle • Agent Oriented Software • Aksum University • Alex Atkins & Associates • AM Economics • Amazon Web Services • Anglo American • Atlas Iron • Australian Android • Autonomous Solutions (ASI) • BBA • Blast Movement Technologies • Boliden • Bosch Rexroth AG • Canmic Consulting • Caterpillar • China Mining Products Safety Approval and Certification Center • CMIC-CCIM • Combitech • CWG Project Services • Doug Turnbull • EACON Mining Technology Pty Ltd • Enaex • Endress + Hauser Group • Flanders • FLSmidth A/S • Glencore • Hatch • Hitachi • Horiba • Ifosys • Imerys • Imvelo • Ivanhoe Electric Inc. • Jim Porter Mining Consulting • JPI Mine Equipment & Engineering • Komatsu • Liebherr • LKAB • Lundin Mining • MacLean Engineering • Mandela Mining Precinct • Marcus Punch Pty. • Michael Fitjer and Associates • Minera Centinela • Mineral Resources Ltd • MinProc Analysis • Model Mining • Motem Pty Ltd. • Newmont • NIOSH • NRCAN • OAK Automation • OFIL Systems Group • OLOI Technology Solutions • Orica • Partners in Performance • RCT • Rio Tinto • Sandvik • Scania CV AB • Schneider Electric • SkymineUAV • Stantec • Suncor • Teck • Tellus • Thiess • TKM Consulting Inc. • UC Berkeley • Universidad Mayor • University of Pretoria • University of Queensland • UQAT • Vale • Vermeer • VIST Group • Volvo • Wenco • Worley • Wuhan University of Science and Technology • Xing Mobility Inc. • XMPro

PUBLICATION INFORMATION

Guideline Number: GMG-AM-SS-v01
Published: 2024-02-02
Revision Cycle: 5 years

DOCUMENT USAGE NOTICE

CONTACT INFORMATION

Global Mining Guidelines Group
info@gmggroup.org
gmggroup.org

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 guidelines do not necessarily represent the views of GMG and the organizations involved in the preparation of these guidelines. Use of GMG guidelines 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 these guidelines 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 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. 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. 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 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 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.

EXECUTIVE SUMMARY

System safety is used to demonstrate that the introduction of new technologies into a larger integrated system (e.g. a mine) is adequate in terms of managing the risks to the system as a whole. The approach is based on the fact that a system is more than simply the sum of its parts. It relies on scientific, technical, and operational skills to identify, understand and control the hazards; and to ensure the risk is satisfactory to operate.

Guideline Purpose

This guideline is intended to assist with applying system safety practices to autonomous mobile equipment systems in mining, building from the existing GMG System Safety for Autonomous Mining White Paper. The purpose of the guideline is to understand that system safety is providing a process to evaluate safety rather than improving safety and health of people.

The "V" Lifecycle Model

The adapted "V" Lifecycle Model provides an overview of the safety related activities throughout a system lifecycle. The high-level summary of the phases is then broken down into separate tables highlighting their inputs and outputs. Continuous improvement is a crucial factor for the process and should be the linking factor across all 11 phases.

System Safety Management Activities

There are a number of safety management activities involved when using autonomous mobile equipment in mining including:

- Understanding in detail the hazards and associated risk
- Change management
- Management of systematic failures
- Configuration management
- Work design and competency management
- Deriving the right requirements and assuring they are met
- Training and communication management
- Maintenance plans
- Cybersecurity management
- System upgrade management

System Safety should include all the above considerations and should help make sure that the risks related to adopting automation are minimized as much as practicable. While this process involves considering the system throughout the life of the change, the key benefits are achieved before a system is in operation.

Product Upgrade Development

Following the implementation of the system, product upgrades are made for enhanced functionality or implementing new functionalities. The process in the guideline considers appropriate impact analysis procedures, planning and analysis, testing and evaluation, implementation and handover, and ends with monitoring to verify changes have addressed the performance requirements.

Safety Case Development

The safety case should inform mine operators of the ability for the system to satisfy the operational requirements of the system based on the site and application risk assessments and analysis of the hazards. The section includes a figure that highlights the similarities and differences for safety cases developed by the OPS vs the mine operator. The section also includes a table that includes content that is typically included in a safety case.

TABLE OF CONTENTS

1. INTRODUCTION

System safety refers to the risk management of an engineered system that enables the operation to balance safety and operability by providing a rationale for it.

The traditional approach focusing only on functional safety tends to impose a techno-centric focus that does not consider all the aspects of the system and its environment, only providing guidance on the implementation and management of risk controls using control systems.

On the other hand, a system safety approach provides an overview of the overall effectiveness of the safety controls and can be a useful tool for operations assessing the safety of their systems. This type of systems approach is especially relevant as fully autonomous, highly integrated solutions evolve.

1.1 BACKGROUND AND CONTEXT

The need for a system safety approach arose in the mid-twentieth century as systems in industries such as nuclear power, civil aviation, defense, and space grew and became more complex. As 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 system increased risks for unexpected failures. Although a direct application of the standards relevant to any of these sectors would not be practical in a mining context, the basic principles of system safety can be applied across all industries.

System safety is a view that extends beyond the equipment and 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 safety hazards. It is a planned, disciplined, and systematic approach to identifying, analyzing, eliminating, and applying practical hazard controls 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.

1.2 RELEVANT GMG PUBLICATIONS

Guideline for Applying Functional Safety to Autonomous Systems Mining

This guideline provides a common approach to applying functional safety to autonomous systems and references international standards within the context of the mining industry and its current maturity. It also describes clear expectations for the communication requirements to support change management and effective application.

Guideline for the Implementation of Autonomous Systems

This guideline provides stakeholders with the tools necessary to move forward with implementation of autonomous systems in mining and advance those projects. It should be used as a first step to assist companies implementing autonomous mining projects regardless of the size and scope of project.

System Safety for Autonomous Mining White Paper

The purpose of this white paper is 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 aims to increase awareness of system safety and its benefits in delivering and maintaining safe and efficient autonomous systems.

1.3 PURPOSE

This guideline provides guidance on applying system safety practices to autonomous systems in mining, building off GMG's System Safety for Autonomous Mining White Paper and associated Layers of Safety Figure (see Figure 1) published in 2021. This guideline will act as both an informative document on system safety and a reference for reviewing end-user internal processes against industry best practices.

The implementation of autonomous equipment is expected to improve productivity and profitability, enable mining in environments that are prohibitive to humans, and reduce the overall health and safety risks for mining operations. The current core principle for autonomous development is to assess whether the autonomy application is better able to improve health and safety outcomes compared to the existing processes (e.g., mixed fleet operation) that are being replaced. This guideline is intended to assist with this evaluation.

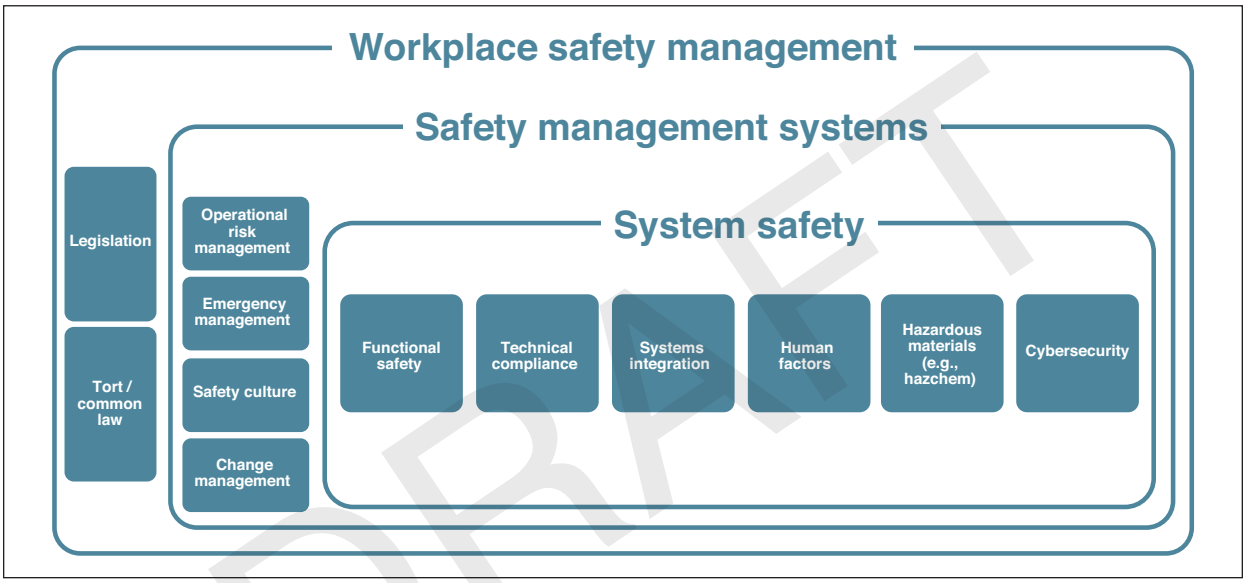

Figure 1. System Safety Viewed from the Broader Context of Workplace Safety, adapted from the GMG Guideline for Applying Functional Safety to Autonomous Systems in Mining (2020).

1.4 SCOPE

This guidelines target audience includes:

- Mine planners
- Mining operator technology, operations, maintenance and health, safety and environment (HSE) teams
- Operations delivery and integration teams
- Procurement (Supply chain)
- Regulators
- Those who design and supply autonomous systems

The following table includes details on what the guideline will and will not cover.

In Scope	Out of Scope
• Best practice for applying system safety principles, including an overview of a system safety lifecycle and guidance for safety management and safety case development. • Considerations for software safety management (e.g., training, software release management, access management, and recovery procedures). • Considerations related to cyber-risks and protection against cyber-attacks as they relate to safely applying autonomous systems in mining. • Considerations for patch and upgrade management. • Autonomous machines: 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 guideline, it refers specifically to mining machines.	• System safety principles specific to other industries. • Detailed step-by-step process for managing system safety. • Specifics to underground, surface, or a particular scenario. • Considerations for machine learning and advanced analytics (AI).* • Non-deterministic system elements from autonomous systems (I.e., decisions derived from sensors and processing algorithms) (See CMEIG-EMESRT-ICMM).*

*More information on this principle and its applicability to non-deterministic systems can be found in the **CMEIG-EMESRT-ICMM White Paper**.

2. SYSTEM SAFETY LIFECYCLE

The system safety lifecycle shows where and how safety fits into the entire existence of an autonomous mining system, from development and testing to integration and operation. This section goes into detail on the "V" Lifecycle Model (Figure 2) which outlines each of the phases and the connections amongst them. It includes detail on the inputs and outputs from each phase along with best practices for the operations philosophy, management plan, hazard and risk assessment, requirement specifications, verification and validation, and the transition to operations.

2.1 "V" MODEL INTRODUCTION

The "V" Model serves as a structure for organizing and guiding the safety related activities throughout the system lifecycle. It establishes a clear sequence of phases, making sure that safety aspects are considered early on and continuously reviewed throughout the system's design and operation.

It is important to acknowledge that other lifecycle models exist and that an agile process might not always conform with the "V" Model. Either agile or waterfall process can be used in autonomous mining system development. Careful consideration should be given to make sure there is strict traceability, change management, and minimization of systematic errors are maintained. The "V" Model attempts to establish a logical and structured approach that aligns the phases of the system lifecycle with verification and validation activities. Such models can assist in applying a system safety approach to identified operational risks.

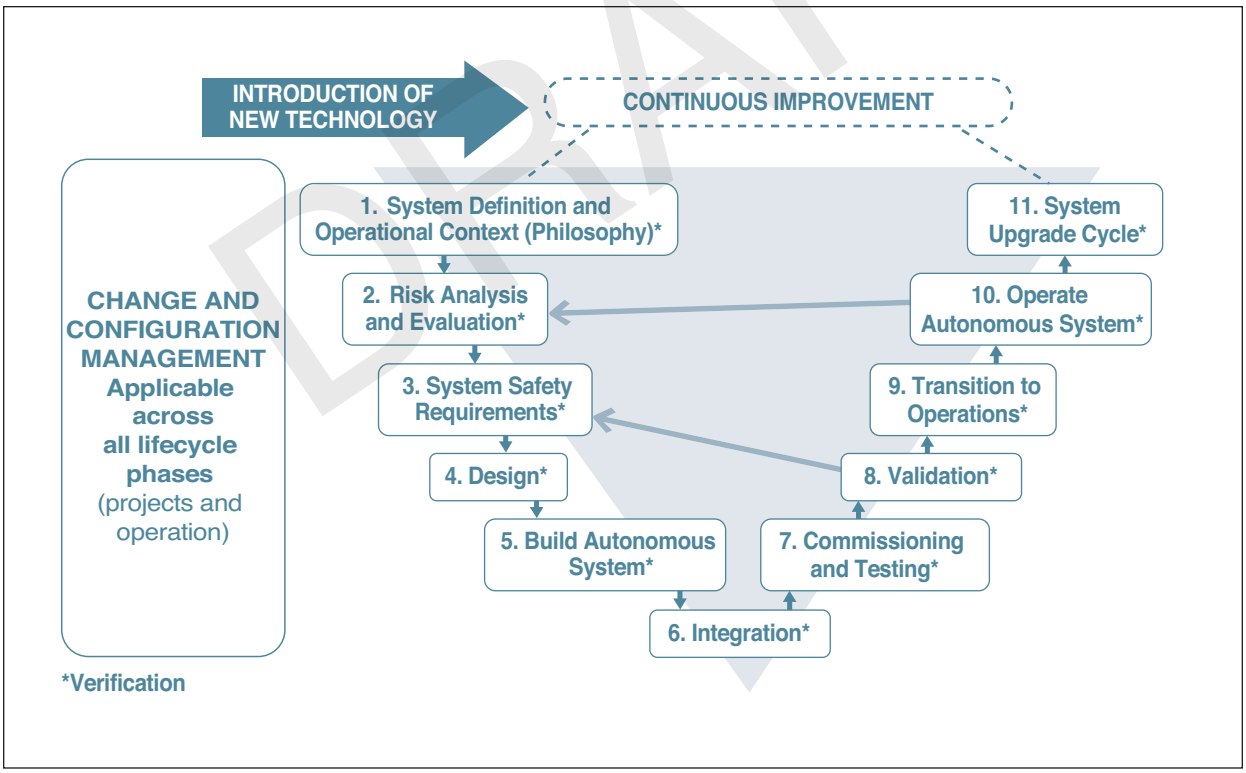

Figure 2. The "V" Model's phases of safety related activities throughout the system lifecycle.

2.1.1 "V" Model Phases

Phase 1: System Definition and Operational Context (Philosophy)	
Purpose: Define the functionality and environmental and operational paradigm of the system.	
Inputs	Outputs
• Legislation and regulator guidance (Codes of Practice, etc.). • Company policy/safety management system/ company standards (end user). • Operational and maintenance requirements (end user). • Autonomous mobile equipment specifications (from the original product supplier (OPS)) including functional description of the product. • Infrastructure/utility condition.	• Concept of Operations (ConOps). • Preliminary safety management plan.

Phase 2: Risk Analysis and Evaluation	
Purpose: Understand and document hazards, define risk criteria, and evaluate risks (consequence and frequency).	
Inputs	Outputs
Outputs from Phase 1 and: • Company risk criteria (end-user). • Relevant standards. • Product design information (from OPS).	• Hazard log. • System Safety management plan. • Determine level of safety rigor required.

Phase 3: System Safety Requirements	
Purpose: To derive safety requirements from the risk analysis, standards, and regulations.	
Inputs	Outputs
Outputs from Phase 2 and: • Site procedures.	• Safety requirements specification. • System architecture, layer of protection analysis (LOPA), etc. • Safety definition.

Phase 4: Design	
Purpose: Develop the system to the requirements.	
Inputs	Outputs
Outputs from Phase 3 and: • Work design. • Human-system interactions.	• Verification report of design to requirements. • Test plan and impact/integration analysis. • Design acceptance criteria.

Phase 5: Build Autonomous System	
Purpose: Build the system from the design and build confidence in safety systems are rigorously implemented with appropriate assurance.	
Inputs	Outputs
Outputs from Phase 4 and: • Quality Management Plan. • Inspection plan.	• As built diagrams. • Quality assessment (QA) report.

Phase 6: Integration	
Purpose: Optimize system use with allied site systems.	
Inputs	Outputs
Outputs from Phase 5 and: • System requirements specifications. • Interface (e.g., application programming interface (API)) required and available.	• Verification of effective integration. • Configuration management plan and governance model.

Phase 7: Commissioning and Testing	
Purpose: Verify the requirements have been delivered.	
Inputs	Outputs
Outputs from Phase 6 and: • Functional and operational test plan. • Test Specification.	• Test report. • Commissioning documentation.

Phase 8: Validation	
Purpose: Demonstrate the overall system meets the requirements and expected performance.	
Inputs	Outputs
Outputs from Phase 7 and: • Validation plan including acceptance criteria.	• Validation report.

Phase 9: Transition to Operations	
Purpose: Prepare the operations team to use the system.	
Inputs	Outputs
Outputs from Phase 8 and: • Work design. • Training requirements. • Competency requirements. • Workforce planning. • Change management. • Regulatory engagement or approvals. • Historical record and lessons learned. • Handover to operational team to use system.	• Safety case. • Acceptance into service. • Operational and maintenance procedures. • Training needs assessment and procedures. • Competencies assessments (including profiles for recruitment and resourcing).

Phase 10: Operate Autonomous System	
Purpose: Build confidence in the effective operation of the system and monitor its performance.	
Inputs	Outputs
Outputs from Phase 9 and: • Operations and maintenance processes.	• Change requests and management.

Phase 11: System Upgrade Cycle	
Purpose: Conduct change and obsolescence management, performance reviews/incident response, and additional functionality implementation.	
Inputs	Outputs
Outputs from Phase 10 and: • Details of any change. • Details of functionality – scope and limitations. • Competency requirements. • Training requirements. • Operations change requirements.	• Updated operations, maintenance, and training materials and systems. • Updated risk assessment and controls.

Note: Where end-user or OPS is mentioned throughout the tables listed in 2.1.1, it should be their responsibility, while if it is not noted, it can be relevant to both

2.1.2 Continuous Improvement

As shown in Figure 2, continuous improvement is the linking factor between phase 1 and 11, and refers to an iterative process of enhancing the development, functionalities, verification and validation methods, and overall safety and productivity of the autonomous system. In addition, it involves systematically identifying areas for improvement and implementing measures to refine/improve system performance, address safety concerns, and meet evolving requirements throughout the system lifecycle.

Continuous improvement addresses the opportunities and challenges associated with implementing, operating, and adopting new technologies. Continuous improvement can be triggered by incidents, industry learnings, and/or product upgrades.

2.1.3 Challenges and Opportunities When Entering the Lifecycle at Different Phases

How products and systems are sold can vary significantly depending on the product type. A small scale "off-the-shelf" system might be handled more like the selling of basic equipment. On the other end of the spectrum are the large-scale systems affecting the mine's entire work processes and might require a significant adoption project. There is no one process or solution to validate safety. Each implementation is often unique and thus requires customized analysis. However, integration of a new autonomous technology into mine operations should follow the same lifecycle model.

Although all systems should go through the whole lifecycle, some products might already have been through the early phases before they get to an application at a site. Earlier phases should be reviewed for a system entering application later in the lifecycle to make sure that the outputs are all valid or to determine if updates are needed in order to avoid challenges including:

- Mining operators might approach integrating new technologies in different ways based on their previous experiences and their maturity to manage the change. Fast-moving technology and lack of standardization, and global guidelines could lead to an impact of the product or system integration that is not well understood.
- OPS could have limited understanding of the mining operator environment or mining environment in general. These limitations might lead to the assumption that technologies which seem to work in other environments can automatically work in mining and in a mining operator's specific environment.
- Mining operators might focus too much on the product or system individually. Mine-specific environment and potential change to the work processes and work culture might therefore not be adequately considered. Although the OPS should follow a structured safety process resulting in a safe and reliable product, it does not automatically mean all the hazards have been identified in the system operator's environment; therefore, systems should be locally analyzed.

In some cases, following the full lifecycle model might not always be possible (e.g., in a limited automation deployment of a standard product). It is important not to only identify the critical steps for each new technology deployment, but to

also make sure that the content of each step can be scaled and adjusted based on the actual technology to be integrated. Potential benefits of following the full lifecycle model include:

- Improved understanding of the local environments and requirements.
- Improved understanding of system maturity, limits, and capabilities (e.g., correct information to the workers and correct level of trust towards the system).
- Consideration of human factors in design.
- Improved understanding of different roles and associated strengths and competencies:
  - OPS and Integrator: Exposure to different mining customers and environments.
  - Mining operators: Specific mining expertise and understanding of their local environment.
- Opportunity to provide a platform or tool for the overall change management (if adjusted correctly for different cases).
- Opportunity to improve information sharing and visibility between mining operators and OPS (if both stakeholders are actively participating).

In addition to the above, there can be differences between autonomous systems and determining when a process should be followed more or less strictly as a function of required safety levels and associated risks, for example:

- Higher risk: autonomous systems or products where poor implementation of the associated safety system can contribute to significant adverse outcomes. These can require a stricter and more systematic approach to safety management.
- Lower risk: autonomous systems or products, typically with lower complexity, where ineffective implementation of the associated safety system is unlikely to lead to significant adverse outcomes. A more agile strategy can be acceptable in such cases.

Regardless of strictness and complexity of a system, risk assessment and appropriate governance and management should be employed.

2.2 OPERATIONS PHILOSOPHY

Due to novelty and complexity of autonomous mining systems (e.g., obstacle detection systems, proximity awareness), existing functional safety standards are not suited to address design considerations. System safety, as a part of the overall systems engineering, helps to assess a system in a particular environment and application.

The operations philosophy of a mine refers to the overall approach and strategies used to safely manage and operate the mine. It is used to define the functions and environmental and operational paradigm of the system, which can help improve autonomous systems management (the safety considerations of an autonomous mining operation will be different to a conventional mining operation).

A scenario-based operations philosophy describes different mine operations and associated requirements. This approach includes mapping the different operating scenarios within the mine and identifying potential safety requirements and risks followed by developing plans and procedures to define the requirements and mitigate the risks.

When developing an operations philosophy model, there can be several factors that vary in importance (high level or minimum level items); however, some notable factors include:

- Mine operation and maintenance.
- Degraded modes.
- Mine design: defining haulage routes for conventional, tele-remote operated, tele-supervised, autonomous equipment, use of material movement techniques based on the type and style of mining methods.
- Restricted access to automated areas, or appropriately managing the risk.
- Mine rescue maps.
- Mixed fleet operations.

2.2.1 Integration of multiple systems

Where an entity (i.e. the integrator) is integrating two or more systems together to create an integrated solution set, careful consideration is required by the integrator to prevent hazardous situations, undesirable behaviour or financial loss in both the original two or more systems, and the integrated system. The integrator should have understanding of how each system works, and how each system can fail to integrate properly. As the number of different integration points increases along with the number of systems integrated, additional effort might be required to make sure complex systems operate together correctly, safely, and reliably.

NOTE: Normal operation can be simpler to understand than exceptions, new failure modes or error handling, which can lead to a false level of confidence. Appropriate risk mitigation strategies and system integration rigor are required to address these.

NOTE: Integrators might need to consider any designer and manufacturer responsibilities and liabilities associated with integrating systems that were not intended by the original designer to work together. New responsibilities to consider in the system safety case can include:

- Compliance testing and certification that needs to be re-evaluated or re-performed by the integrator.
- Lifecycle management including version management, validation and verification tests impacted.
- Change management.
- Providing and maintaining operation, maintenance, and service literature for the integrated system.

2.3 SYSTEM SAFETY MANAGEMENT PLAN

Once a system has been identified to go through the phases discussed in Figure 2, plans should be prepared for safety and management activities as soon as there is sufficient information to do so. Figure 3 shows what the plans should include:

Figure 3. System Safety Management Plan Considerations.

2.4 HAZARD ANALYSIS AND RISK ASSESSMENT

The role of hazard analysis and risk assessment is to help operations proactively manage risks to make sure the system operates safely. Risk assessments are an ongoing process that requires continuous evaluation to support the safety and reliability of autonomous systems, while considering different factors and changes to the system. See Appendix C for a table on various Risk Assessment Tools. Figure 4 shows some of the different steps in risk management.

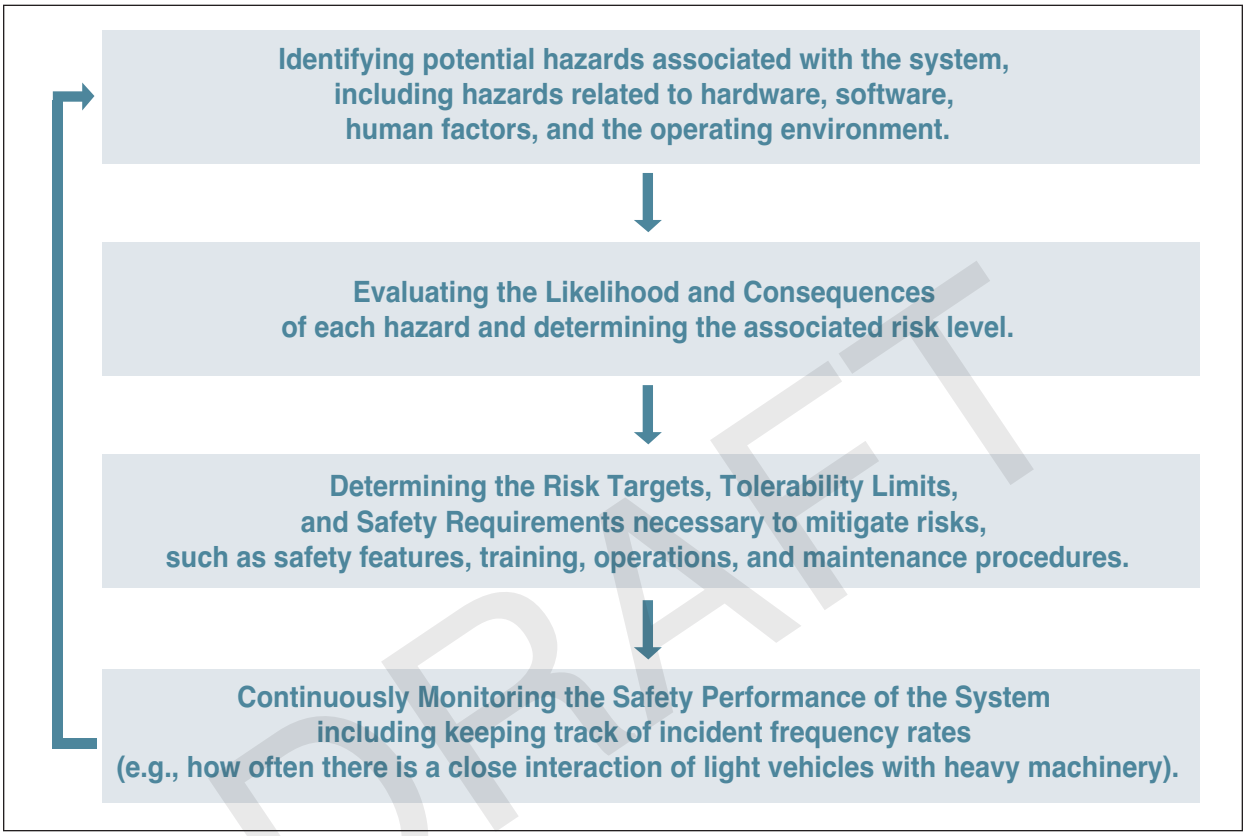

Figure 4. Consideration for developing a risk assessment plan.

2.5 SAFETY REQUIREMENT SPECIFICATIONS

Requirement specifications are descriptions of the safety related functions that a system should meet to make sure of safe operations. The specification for a safety function should describe the function and the expected level of risk reduction. Additionally, these safety functions are typically specific to the system being used and the operating environment.

Requirement Specifications	Safety Function Examples
• Established during the hazards and risk analysis phase. • Apportioned between subsystems and traceable to prove that top-level safety requirements have been met. • Specific, measurable, achievable, relevant, and testable. Requirements, by the time they are validated, should be written in a way that there is no ambiguity in them.	• Obstruction detection. • Collision avoidance. • Isolation requirements (lock out, tag out, access control). • Loss of communications (i.e., when the system loses contact with the control center).

2.5.1 Other Risk Measures

In addition to requirement specifications, considering other risk measures is also necessary for making sure the system is safe and identified risks have been addressed.

2.5.2 Verification and Validation

Verification is typically methodical testing against system requirements, preferably testing one requirement at a time, while validation is exposing the system to more complex use cases in (or very close to) the operational environment. Verification and validation should be occurring sequentially, with verification providing confidence for the validation phase. During verification and testing evaluation of the system, design and implementation should be done to make sure the system meets the specified safety requirements while validation should demonstrate that the system objectives have been delivered and that the overall system meets the definition and performance requirements.

A test management plan should be developed to outline the approach taken for verifying and validating the system. To do this, it is recommended to map out the requirements for the test plans show in Section 2.5.

Further considerations for testing:

- Testing should be an ongoing process that is continuous throughout the lifecycle (including design) of the system. Even after initial testing is completed, there should be continued monitoring and testing of the system to verify that it continues to operate safely.
- Where systems changes are driven by an OPS, the OPS should be involved in the testing process and mining operators should understand the OPS prescribed test outcomes.
- Testing should be conducted in a controlled and safe environment, such as at a test site, local calibration area, software environment, controlled mine environment, or mock station.
- Regulators can provide awareness and guidance related to specific risks and should be included where it is appropriate to do so. Mining operators should understand the regulatory requirements and make sure the system is compliant with them.
- Aspects from standards such as IEEE 1012: Standard for System, Software, and Hardware Verification and Validation and ISO 19014 Earthmoving Machinery - Functional Safety (series) can be helpful.

2.6 TRANSITION TO OPERATIONS (OPERATIONAL READINESS)

The transition to operations involves transferring the system's responsibility from the project development team to the operations team. The OPS responsibility is also normally handed over to the mine operator during this phase, following the responsibility transition flow in the contract. Best practices for this transfer of responsibilities are to have an integrated team specific to the project and operations.

During this transition, the operations team should have:

- All negotiated or necessary documentation, including handover certificates, test plan records, items that could not be tested due to limitations of the test environment, and the action management system (including procedural controls/administrative controls).
- Clear communication and training on the new technologies and changes to the system.
- A governance and assurance process that oversees the transition, and to whom mining operators should turn to for guidance.
- Risk lists with confirmation that all risks evaluated as unacceptable in the analysis have been mitigated.

3. SYSTEM SAFETY MANAGEMENT ACTIVITIES (SYSTEM SAFETY OPERATIONAL ACTIVITIES)

This section describes the different safety management activities involved when using an autonomous system. 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 practically attainable.

While this process involves considering the system throughout the lifecycle, it is mostly done prior to any changes being made.

3.1 CHANGE MANAGEMENT

Change management should be considered throughout the system safety lifecycle. Mining operators should be aware of the different phases of the system safety lifecycle and what role change management will play in each phase.

Most mining operators will already have established change management processes and can leverage existing processes when making modifications.

As part of the change management process, companies should:

1. Identify the stakeholders impacted by the change and determine who needs to approve the change.
2. Develop a technology adoption plan and implementation to support the acceptance of workforce.
3. Develop a proper communications strategy to make sure mining operators are aware of the changes and how they will be affected. This could also include a review of existing, or the development of new, training packages.
4. Conduct an impact analysis.
5. Confirm there is operational and technical support for the operations team.
6. Approved changes are implemented and tracked to closure.

3.2 MANAGEMENT OF SYSTEMATIC FAILURES

Systematic failures are caused by problems in a process, system, organization or product, indicating fundamental or structural issues, which could compromise the expected safety controls. Systematic failures are often discovered by the system operator; however, they can often occur after an upgrade.

To manage systematic failures effectively, mining operators should:

- Have protocol to detect possible systemic failures before an incident (use of simulation).
- Have a well-defined immediate response plan triggered upon encountering an incident that includes consideration of systemic failures.
- Engage the OPS for technical support.
- Establish the right processes and allocate the necessary resources to provide the OPS with detailed technical knowledge and data (this enables the OPS to understand the mining operator's description and to re-enact the failure in a controlled environment, facilitating accurate problem diagnosis and resolution).
- Confirm that a rollback procedure is in place.

3.2.1 Recovery Process

The recovery process of system safety management activities can be categorized by three groups:

General Recovery: *Overarching recovery process.*

A failure analysis should be performed at the site to determine the vulnerabilities if there is an unforeseen event or abnormal system behaviour.

Disaster Recovery: *How to recover from catastrophic failures?*

A disaster recovery analysis should be performed before the system is deployed to understand how to recover from a significant failure. A disaster recovery plan should be developed and documented. The disaster recovery plan should be reviewed at least once per year and updated as needed.

Back-up Strategies: *These are typically things that can be used as part of diagnosis of issues.*

Back-up and recovery procedures should be established within an organization as a defensive measure against failures. An impact analysis should be performed to determine how to recover as components of the system fail. Where there is significant risk of downtime, redundancy in the system should be used. When redundancy is not used, spare parts should be available to expedite recovery. The spare parts should never be used when new systems are set up and there is a delay in ordering new components.

3.3 CONFIGURATION MANAGEMENT

Configuration management refers to the process of identifying, organizing, and controlling changes made to a system throughout its lifecycle. Configuration management can help confirm the integrity, traceability, and consistency of the system's components, software, and hardware configurations. It involves maintaining accurate documentation of the system's configuration, tracking changes, and implementing change management procedures.

Configuration management plays a key role in the verification and validation process. To validate the reliability of a configuration management process, considering the following:

- A configuration audit as part of a readiness review.
- Configuration management in test environments.
- Configuration management tool to facilitate the management process.
- Software Identifiers: Such as version numbering, build date, and verifier name.
- Hardware Identifiers: Such as manufacturer, model, and part Number.
- Management of security and authorization of personnel to make changes.
- OPS engage miner of possible outage
- Record that any changes implemented have been validated.

3.4 SAFETY ASSURANCE

Safety assurance is about making sure that the system is designed, implemented, and operated as expected and in a safe manner. Part of safety assurance is conducting audits on the system operation to help make sure safety processes are functioning correctly. These audits can include a wide range of models depending on what the objective is for those conducting the audit. Some considerations include:

- Different types of auditing models can be used depending on the specific requirements of the system and the scope of the audit, and the mining operator.
- On-site auditing of the mining operators can help make sure that the safety management systems, operational processes, maintenance practices, testing requirements, refresher training, and performance monitoring are effective in managing risks and supporting safe operations.
- Depending on the safety performance requirements, independent assessments can be carried out to evaluate the effectiveness of the safety assurance process.

A governance framework can help with safety assurance by:

- Overseeing the safety assurance process and making sure that safety requirements are being met.
- Making sure that the safety lifecycle is being followed.
- Defining the roles and responsibilities of the stakeholders involved in the safety assurance process.

3.4.1 Review of Hazard Analysis and Risk Assessment and Actions

When a new system or technology is introduced, it is important to keep a live record of the associated hazards and risks the technology introduces or influences. This is usually developed early in the lifecycle (see Section 2.4) during the hazard analysis and risk assessment phase.

The hazard analysis and risk assessment should be handed over from the project phase to the operational owners in the form of a hazard log as the technology is implemented and becomes operational. The hazard log provides a linkage between the risks of the technology (including causes, barriers, and frequencies), the assumptions made, and the associated safety requirements that should be met and maintained.

A live hazard log allows operations to have a structured review of assumptions, technology hazards, and risks through a planned review cycle. Hazard log reviews should be a scheduled and defined activity within the management plan and could include:

- Review of incidents/accidents/events involving the technology.
- Review of demand and utilization of safety systems.
- Review of safety performance indicators.
- Re-validation or removal of assumptions (based on operational data).
- Addition of any new hazards identified through operation.
- Removal of any redundant hazards removed through operation.
- Consideration of system upgrades and the impacts on hazards and controls.
- Re-validation and quantification of safety requirements (if required).

The hazard log review should have a documented action management process that provides a structured way of managing actions and verifying information that comes out of the review. Where possible, assumptions should be monitored and verified throughout operations as part of the technology safety performance indicators.

3.4.2 Monitoring Safety Controls (Safety Performance Indicators)

Safety performance indicators are measures used to evaluate the effectiveness of safety controls and identify potential safety risks and hazards. Indicators should be developed and tailored to feed into the hazard log review, and they can be used to verify any assumptions made. If certain assumptions are made in the hazard log early in the lifecycle, there should be a process to later verify those assumptions through data gained from the performance indicators.

Consider the following when monitoring safety controls:

- Metrics should be defined to provide a relevant risk profile. These metrics should be specific and measurable to be able to assess the safety performance of the system.
- Assign a person who will be responsible for monitoring the safety controls. Part of the safety assurance process is to allocate that responsibility. Without personnel responsible for monitoring, the indicators can compromise usefulness to operations.
- Define the appropriate time intervals for measuring the safety controls. Regular monitoring can identify and mitigate issues and allow for quicker corrective action.
- Whenever possible, indicators should be automatically generated and provided by the system rather than relying on a person to notice them and then record it (i.e., demands should be automatically tracked as opposed to a person needing to raise an incident to be tracked).

3.4.3 Reporting Incidents

Mining operators should communicate critical incidents to the system providers promptly. There should be a timely response as the expectation from the mining operator is for the provider to be proactive and engaging with a plan for how to address the incident and mitigate potential future incidents. Maintaining traceability and transparency within the management framework is essential.

The definition of a reportable incident can be guided by established frameworks of each mining operator. Local regulation requirements for incident reporting should be identified and followed where the findings collected should be fed back into the continuous improvement process. There should also be a list of items from the incident report which should be prioritized for the safety case and hazard log.

Incident guidance (often called 'playbooks') should be part of an incident or emergency management procedure specific within a company. These forms of guidance typically should include the required reporting for an incident, along with the required safety/government authorities (i.e., have a plan for recovery when an incident occurs and confirm that the right people are informed).

3.5 WORK DESIGN AND COMPETENCY MANAGEMENT

Work design refers to the operational procedures performed as well as interactions with the system from a human perspective. In the process of designing work, operations should identify the work that is needed and how it should be conducted while considering human-system interactions.

Operating an autonomous system requires specific skills and competence. To help make sure that operators have proper competencies and skills prior to performing operations. Other considerations for competency include:

- Machine design and the supporting tools and processes should complement the required competency.
- If personnel possess low-level competency or if there are semi-frequent tasks performed requiring interaction, then visual and auditory indicators should be put in place to indicate hazards rather than relying on training and competency.

There should be as much indication as possible on when it's safe to interact with the autonomous machine. However, care should be taken into the design to make sure that alarms/indicators are not overwhelming to the operator.

Human-Systems Integration for Mining Automation

During the preparation for new autonomous technology, there should be a human-system integration program plan that details the human system integration work that will be performed and how it will be completed and by whom. See Table 1 for human factor considerations.

Table 1. Human factors to consider

Alarms
Consistency in operator experience (e.g., mixed fleet/multiple types of autonomous equipment, all mode lights/sirens/procedures are as consistent as possible)
Ergonomics
Facility design
Interface design – remote mining operators, maintainers
Maintenance
Position of screens and impact on other tasks (e.g., mining operators of manual vehicles in a pit)
Situational awareness

3.6 TRAINING AND COMMUNICATION MANAGEMENT

There are two management plans that should be incorporated with system safety for an autonomous system: training management plan and the communication management plan. By including these plans in the operation, it can validate safety through competent personnel and improved communications throughout the operation.

Training Management Plan

A training management plan builds confidence that personnel are competent in the operation and maintenance of the system. Training is ideally conducted outside the production environment such that any errors made in the training environment do not create a safety issue.

After an upgrade or system change, operations should decide how much re-training is needed and when it should be completed. Examples of scenarios that can trigger re-training include:

- **Introduction of a new system:** Involves training the whole workforce on a new technology.
- **Gap training for a system upgrade:** Involves any new features or changes to the system that should be communicated to the mining operators.
- **Periodic refresher:** Involves regular testing of personnel's competencies.
- **Ad-hoc re-training:** Involves retraining one person or multiple people because of incidents.

Communication Management Plan

Communications management includes both internal and external communications. Companies should have processes to manage communications between the different groups and how the information impacts operations. This can include a communication plan that includes:

- Who needs to inform whom.
- When they should be informed.
- What they need to be informed on (including level of communications).

Upgrades to the system should follow a more formal communications methodology for communications between mining operators and OPS.

3.7 MAINTENANCE PLAN (FOR SAFETY CRITICAL SYSTEMS)

A maintenance plan is necessary to make sure safety critical systems are reliable. Developing a maintenance plan involves:

1. Defining the safety critical maintenance and proof testing within the computerized maintenance management system (CMMS) based on the safety requirements and safety functions.
2. Tracking overdue maintenance. A process should be in place to make sure follow-up actions are taken when maintenance is overdue.
3. Tracking follow-up maintenance. A process should be in place for following up on any faults identified during regular maintenance of a safety critical component or function.

The basis for critical maintenance should refer to the OPS manuals and recommendations regarding maintenance intervals.

In cases where maintenance tests fail (e.g., during proof testing/periodic maintenance inspection), a process should be in place to address them. This process can include conducting risk assessments, sign-offs by authorized and competent persons, interim controls, and determining the appropriate actions to return the system to service, including checklists for verification activities.

3.8 CYBERSECURITY AND SYSTEM ACCESS MANAGEMENT

Cybersecurity should always be in place when the system is selected and implemented. The mining industry is prone to cyber-attacks and risks and, although it is nearly impossible to fully prevent the attacks from happening, resilience and preparation is critical.

These attacks can influence how the autonomous equipment operates and depending on the attacker's intention, can put people's lives in danger or compromise their safety.

The communications infrastructure should be selected and designed with security in mind to mitigate hacking attempts. Although having reliable communication infrastructure is needed to build confidence in productivity of the operation, the primary intention of the equipment should be to confirm the safety of those in and around the mine site.

In addition to selecting infrastructure with security in mind, the technology and practices associated with the technology should be regularly updated in terms of configuration and security management.

Procedures and systems are required to only allow authorized and authenticated personal access to systems, with access limited based on the role or function required to perform the task. This access also requires alignment with successful completion of any required training, and the ongoing maintenance of appropriate training records.

ISO 27001: System Security Management System, ISA-99, or IEC 62443, are some of many standards that can provide further information on what to consider around system safety and cybersecurity.

3.9 SYSTEM UPDATE MANAGEMENT

A system update can be thought of as a sub-step of change management because any updates to the system can trigger the change management process.

Consider the reasons why the system is being updated, for example it could be because of:

- Incidents.
- New firmware changes to software or bug fixing.
- Obsolete hardware replacement.
- Continuous improvement.
- Malfunctions identified by OPS or mining operators.
- Security updates/system vulnerability management.

Effective system update management involves several steps, including:

- Identifying the need for an update.
- Evaluating the impact of the update.
- Planning for the update and then implementing the update, which could also involve:
  - Reviewing existing test plans and deciding if they should be expanded or amended because of the update.
  - Incorporating new test use cases into the test plan.
  - Developing a verification plan including how validation activities will be conducted.
- Monitoring the performance of the updated system. Monitoring can be through tracking performance indicators, gathering feedback from operations, and conducting audits and inspections.
- Defining a roll-back setup, including backup recovery.

4. PRODUCT UPGRADE DEVELOPMENT

Once the autonomous system has been implemented, there should be on-going upgrading of the system due to augmented functionality, new functionality, or rectification of the existing system. This section focuses on the upgrade process and assumes the system has already been deployed and is in use. Figure 5 provides high level process map for managing a product upgrade.

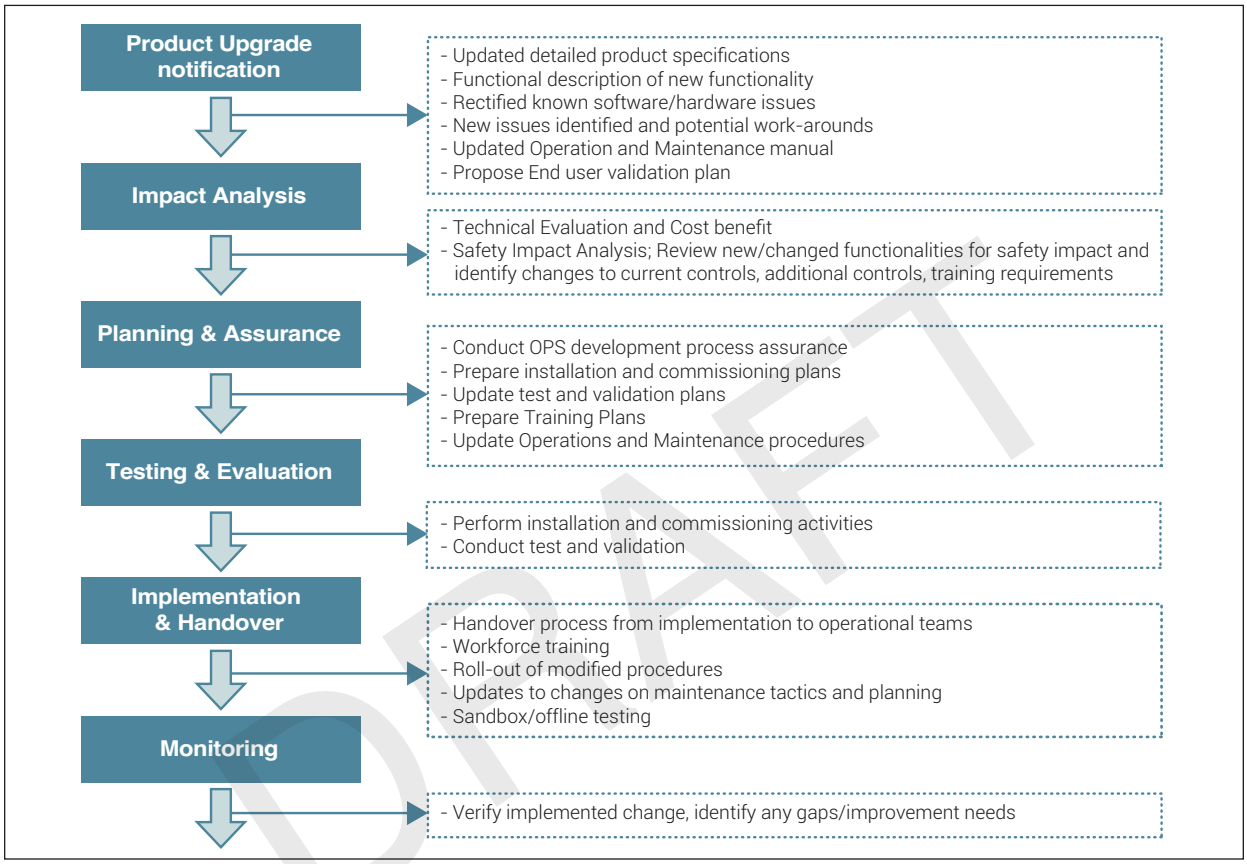

Figure 5. High level process map for managing product upgrades.

4.1 ORIGINAL PRODUCT SUPPLIER (OPS), MINING OPERATOR, AND INTEGRATORS COMMUNICATIONS METHODOLOGY

Effective communication between OPS, mining operators, and integrators is critical during the product upgrade process.

Some best practices around information sharing include:

- OPS should provide a minimum set of information to mining operators regarding safety requirements, system capabilities, and how the upgrade will impact their system.
- Communication channels should be established to share updates and changes with mining operators, preferably before the actual release of the product upgrade. This promotes transparency and allows mining operators to prepare for any impacts or modifications.
- In some cases, a third-party can be involved to help facilitate information sharing and make sure there is a common understanding between OPS, mining operators, and integrators.

Note: In most jurisdictions, it is the mining operator's responsibility to confirm that all the potential hazards are identified, and risks are mitigated to as low as reasonably practicable. However, OPS can also have obligations surrounding

the exercise of due diligence (upstream obligation holders), before releasing the product for installation, during use, and at disposal/decommissioning (under safety and health regulation). It is important to consider and obtain legal advice specific to jurisdiction.

4.2 UPGRADE INFORMATION, TECHNICAL EVALUATIONS, AND IMPACT ANALYSIS

Product upgrade development requires upgrade information, technical evaluations, and impact analysis before having an understanding of the system safety requirements of an autonomous system. The technical evaluation is needed to understand the technology and cost benefit aspects, and the impact analysis is only considering safety.

4.2.1 Upgrade Release Notes

The release notes are technical documents that the OPS should provide to the mining operators and integrators. They typically describe any new features, known issues, fixes to previous issues, workarounds for mining operators to implement, suggested test protocols, and/or detailed specifications of the product. Any software upgrade should be accompanied by a verification checklist to be confirmed before release of the upgraded system to operations.

4.2.2 Technical Evaluations

The purpose of technical evaluation is to evaluate potential impacts to existing system interfaces (e.g., APIs).

Some examples of technical evaluation questions include:

- What is the impact on the process?
- What is the impact on infrastructure requirements?
- What are the system requirements?
- Is a new server upgrade required?
- Are site infrastructure hardware upgrades needed (e.g., antennas, base station)?

4.2.3 Impact Analysis

Before a change or upgrade occurs, an Impact analysis (see Table 2 for consideration) should be performed and should document the affected systems. OPS should design for potential rollback if issues arise from the upgrade.

Table 2. Impact analysis considerations

Impact Analysis	• **Quantitative:** Data based on parameters such as performance and operational optimization. • **Qualitative:** Quality of the system based on functionality, effectiveness rate, and efficiency.
How the Change Affects Safety of the System	• How is this system improving operational effectiveness? • How is it increasing productivity? • How profitable is business when engaging a system safety approach?
Aspects to consider during impact analysis and hazard log review	• Safety impact to existing control measures and risk scenarios. • Introduction of new hazards. • Interaction with humans and manual vehicles, human system interfaces, and change management processes. • Mode change process. • Degraded operations. • Response time considerations. • Cybersecurity. • Hardware obsolescence and availability. • Integration with other systems/configuration management.

4.3 ORIGINAL PRODUCT SUPPLIER (OPS) DEVELOPMENT PROCESS ASSURANCE

The need for safety audits should be evaluated for every update at regular intervals to review what safety assurance processes have been followed. However, the level of auditing required could be based on the significance of the upgrade. There are several ways to conduct an assurance audit, for example:

a) Mining operators or OPS can conduct a safety assessment of processes for competencies, quality assurance, safety analysis, and adherence to standards. It will largely depend on the contractual agreement between mining operator and OPS for such a safety assessment.
b) Mining operators and OPS could work together to develop an audit protocol for mining operators. This will allow for clarity on what is required to be audited, what is possible to audit, and what information sharing is required.
c) OPS can have their own "proving grounds", where initial testing of a new version is conducted by OPS and where appropriate, witnessed by mining operator before the release of the new version.

4.4 INSTALLATION AND COMMISSIONING PLAN

The installation and commissioning plan should clearly communicate which aspects of the system are safety-critical, outline the responsibilities of individuals involved, and reference relevant procedures.

An installation and commissioning plan should:

- Consider the sequencing of the installation to make sure there is a logical order of the initial setup (e.g., the initial installation and commissioning, then the component level, function level, system level, then integration).
- Establish criteria for evaluating results (i.e., what is a successful installation? When is it fully commissioned?) and resolving any incomplete tests.
- Develop and follow a schedule for installation.
- Address training needs and requirements and establish operating procedures.
- Have all supporting systems/machinery in place (e.g., IT infrastructure and checklists to confirm readiness)
- Include approval and sign-off procedures to facilitate the transition from commissioning to operations.
- Verification and validation test of fully integrated system.

4.5 TESTING AND VALIDATION

After completing commissioning, final testing and validation activities are carried out. The main intent of the validation is to confirm that the system has been successfully deployed satisfying functional and performance requirements. The tests developed to conduct validation should address the requirements.

Depending on the type of requirements, validation can also involve site/equipment inspections, analysis, or document/procedure reviews.

For the validation plan, mining operators should use information provided by OPS. The OPS should also provide relevant set of test cases to the mining operators, enabling them to effectively test and validate the system. The mining operator can also identify test cases, which should be combined with the OPS recommended test cases. This will make sure that appropriate testing is conducted taking into account the OPS recommendations.

While on-site tests are important, sometimes they alone cannot fully validate the system. The OPS should share known system limitations, risks and where required, recommended tests to assess safety. The information from acceptance testing (e.g., test records, system backups, non-conformances) should be retained and accessible.

5. SAFETY CASE DEVELOPMENT

The purpose of a safety case is to inform the mine operator of the ability of the system to satisfy the operational requirements of the system, based on a site and application specific risk assessment.

The safety case is something that should continuously be reviewed and updated in a live format as system safety processes, outlined in Figure 2, are completed. These updates are fundamental to the concept of operations and being able to sell the concept but also as each stage progresses, validating to minimize risk and updating to manage risks accordingly.

This section outlines the differences and similarities between the safety cases prepared by the mining operator and OPS. It also provides resources on how to develop a safety case.

5.1 MINING OPERATOR AND ORIGINAL PRODUCT SUPPLIER (OPS) SAFETY CASES

With autonomous mining, mining operators using the technology and OPS of the technology should both prepare and provide their own safety cases.

An OPS should develop a safety case to provide assurance that the products provided are safe to use based on the constraints of their use. By providing that safety case, the OPS can justify that the system is safe to use in generic applications (e.g., underground mines). The mine operator should work with the OPS to prepare a safety case so that the system can be used safely in its specific environment (i.e., mine site).

Where an OPS safety case is aimed at getting the system to the transition to operation phase, the mine operator's safety case should exist to take the system through that transition and through upgrade cycles to end-of-life and decommissioning.

All parts in the operator safety case is relying on information provided from the OPS, the part that is not overlapping in Figure 6.

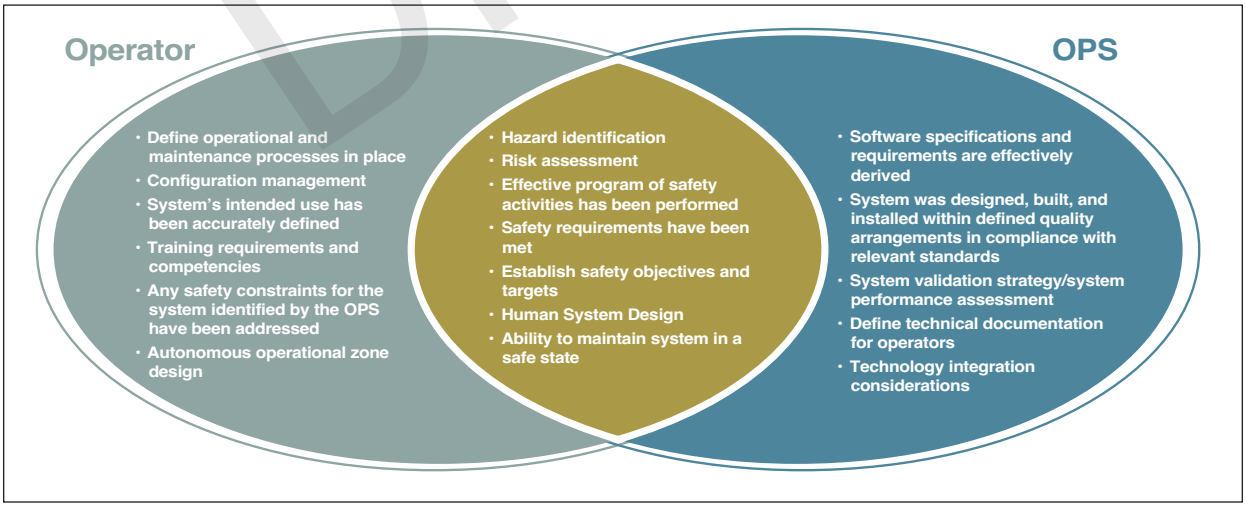

Figure 6. The Types of Safety Cases: Operator and OPS

5.2 UNDERSTANDING REGULATIONS/LOCAL JURISDICTION WHEN DEVELOPING A SAFETY CASE

Local regulations and local jurisdictions should be considered when developing a safety case because of they often vary with location (e.g., Australia regulations vs Canada). To make sure regulations are regularly followed, it can be beneficial to consult with local authorities to make sure there is alignment with existing submission processes.

Recommended Resources for Safety Cases	
Reference	Description
UL4600*	Standard for the Safety for the Evaluation of Autonomous Products
ISO 17757	Can be used to help build a safety case for OPS, but does not describe exactly how to build a safety case
	Western Australia Code of Practice for Autonomous Mining
	The Assuring Autonomous International Programme (AAIP) Body of Knowledge (University of York)
CENELEC EN 50129**	European Committee for Electrotechnical Standardization Railway applications - Communication, signaling and processing systems - Safety related electronic systems for signaling
SCSC-159	Safety Critical Systems Club
EN50126**	Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMs Process and Part 2: Systems Approach to Safety
EN/ISO 19014	Functional Safety for Earth Moving Machinery – Safety Case

* For automotive applications
** For Railway applications

5.3 COMMON SAFETY CASE INFORMATION

This section shares some common safety case information along with a description of content that is typically included.

Table 3. Typical Headings and Expected Safety Case Content

Heading	Content Description
System Description	• High-level (preliminary) overview of the system. • Key functions. • Outline of physical elements.
System Hazards	• Results of preliminary hazard analysis. • Key credible hazards (these can change for later submissions of the safety case). • Hazard Log status – have the hazards been adequately addressed.
Safety Requirements	• Description of top-level safety requirements (emerging from study of standards and the preliminary hazard analysis). • E.g., Failure rate in particular failure modes, tracking system on all autonomous, semi-autonomous, remote controlled, and conventional assets. • Verification and Validation that the requirements have been met.
Risk Assessment	• Result of risk estimation exercise, accident sequences, hazard resilience index (HRI) used and the resulting risk classes for all identified hazards. • As with the system hazards, the assigned risk classes can change for later submissions of the safety case.
Hazard Control / Risk Reduction Measures	• How the project plans to tackle each identified risk (e.g., design measures, protection systems, redundancy, etc.).

Table 3. Typical Headings and Expected Safety Case Content (continued)

Heading	Content Description
Safety Analysis / Test	• How the project intends to provide evidence of successful deployment of risk reduction measures, meeting failure rate targets, demonstrating correctness, etc. • Many industrial safety componentries aren't ruggedized to a level where they can withstand the dynamic mining environments. This should be satisfied (typically trialing the system for x hours in active operations) to validate its reliability. • Effects of faults with the aim of failing to a safe state.
Safety Management System	• Reference to contents of safety plan for roles, responsibilities, and procedures (this will be fairly stable for later safety cases). • Management of Safety constraints or conditions. • Safety objectives have been met
Development Process Justification	• An outline of the development procedures, design methodologies to be used, coding standards, change control procedures, etc., and how these will be shown to meet integrity level or development assurance level requirements.
Conclusion	• Key reasons why the project believes that the system can be implemented to an appropriate level of safety. • What will be concluded from analysis and test evidence.

Note: Where not noted, the safety cases can be applicable to either OPS or mining operator.

CONCLUSION

System safety for autonomous mining is not a concept that should be viewed from a competitive aspect or viewed in operational silos but should always be viewed collaboratively, by mining operators and OPS across all lifecycle phases noted in Figure 2.

The concept of the phases is to expand on each phase in the lifecycle, rather than viewing the inputs and outputs individually. The major message for the guideline is to consider system safety from a continuous improvement point of view when introducing new technologies to an operation. There is no "end-phase" to the lifecycle as the goal is to always build off the system, making sure that safety is always a top priority in terms of keeping those away from harm and risk.

REFERENCES

[1] Walden, D., Roedler, G.J., Forsberg, K.J., Hamelin, R.D. & Shortell, T.M. (2015) *INCOSE Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities*, John Wiley & Sons.

[2] Booher, H. (2003). *Handbook of human systems integration.* New York: Wiley. https://doi.org/10.1177/106480460401200309

[3] Endsley, M. R. (2015). *Human systems integration requirements analysis.* In D. A. Boehm-Davis, F. T. Durso, & J. D. Lee (Eds.), APA handbook of human systems integration (pp. 63–80). American Psychological Association. https://doi.org/10.1037/14528-005.

[4] Department of Defence (2008) *Instructions 5000.02.* ***https://www.acqnotes.com/Attachments/DoD%20Instruction%205000.2.pdf***

[5] NASA (2015). *Space flight human-system standard. Volume 2: Human factors, habitability, and environmental health.* NASA-STD-3001, Volume 2, revision A. https://www.nasa.gov/wp-content/uploads/2020/10/2022-04-08_nasa-std-3001_vol_2_rev_c_final.pdf

[6] Melnik, G., Roth, E., Multer, J., Safar, H., & Isaacs, M. (2018). *An Acquisition Approach to Adopting Human Systems Integration in the Railroad Industry*. US DOT. DOT/FRA/ORD-18/05. https://rosap.ntl.bts.gov/view/dot/34745/dot_34745_DS1.pdf

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

APPENDIX A: GLOSSARY AND ABBREVIATIONS

Term	Definition
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 guideline, it refers specifically to mining machines.
Autonomous Systems	Refers to autonomous and semi-autonomous systems (ASAMS) as they are defined in ISO 17757 (2019a, 3.1.2). In this guideline, it refers specifically to mining systems.
Competency	Having people with the necessary knowledge, skill, and experience to apply functional safety to autonomous systems.
Functional Safety	Refers to "the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs." It is defined as "the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the consequence of the hazardous event" (Source: www.iec.ch).*
Functional Safety Lifecycle	The process of managing functional safety over the life of a product.
Independent	In a review or investigation setting, refers to a separation of responsibilities to maintain objectivity.
Integrity Level/Performance Level	Identification of the risk reduction required to be provided by each safety function. Examples include machine performance level (MPL), performance level (PL), and safety integrity level (SIL).
Mine Operator	The mining operation applying functional safety to autonomous systems in mining who is responsible for the functional safety lifecycle of the application.
Requirement Specifications	Descriptions of the safety-related functions that a system should meet in order to confirm safe operations.
Original Product Supplier (OPS)	The equipment manufacturer or integrator who is responsible for part or all of the functional safety lifecycle of the product.
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 Function	The machine functions that are required to achieve or maintain a safe state and of which failure or malfunction could increase the risk of injury or harm to the people or environment involved.
Safety Management	The management of the safety of changes that can affect the risk of harm.
Systematic Failures	Something done in accordance to a system or method. E.g., If there is no change management process in place, it can lead to failures in the upgrade or product.
Systemic Failure	The impact on an entire system. E.g., no management change process in place.
System Operator	The person with control over a system.
System Safety	Measures that are taken to confirm that the overall design of a system is safe to operate. "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).

CMMS	Computerized Maintenance Management System
ESM	Engineering Safety Management (ESM)
FTA	Fault Tree Analysis
OPS	Original Product Supplier
STPA	System Theoretic Process Analysis

APPENDIX B: HUMAN-SYSTEM INTEGRATION PROGRAM CONSIDERATIONS

A human-systems integration program should include:

- **Human-systems integration activities:** The specific human-systems integration activities that will be performed by the OPS, in collaboration with the operator, to address each of the six core domains of human-systems integration (staffing, personnel, training, human factors engineering, safety, and occupational health) during system analysis, design, and evaluation. Identification of who will undertake these activities.
- **Human-systems integration schedule:** A milestone chart identifying each human-systems integration activity, including key decision points and their relationship to the program milestones.
- **Overview information:** An overview of the proposed system; preliminary concept of operations, associated human roles, and operational environment; and experiences with predecessor systems.
- **Organizational information:** Summary of the job descriptions and the qualifications of key human-systems integration practitioners within the OPS organization.
- **Program risks:** A discussion of how human-systems integration risks will be identified and addressed.

APPENDIX C: RISK ASSESSMENT TOOLS

Risk Assessment Tools		
Tool	Benefits	Limitations
System Theoretic Process Analysis (STPA)	• Systems view • Can include human interactions in hazard analysis • Useful for complex software systems • Captures more than just component failures – captures unsafe interactions (between hardware/software, software/software, human/hardware, human software, human/human, etc.)	• Lengthy process • No qualitative assignment of risk
Fault Tree Analysis (FTA)	• Top-down analysis, useful for identifying single point of failure and combinations of failures required for an unsafe event to occur	• Can become large and difficult to understand, especially for those who didn't create it
Functional Hazard Analysis	• Identifies failure modes of each system function and mitigations • Identifies safety critical functions • Can be applied at any level of design, depending on design maturity	• Only considers the functional safety aspect, there is a need to look at system safety
Failure Mode and Effects Analysis (FMEA)	• Systematic	• Combinations of failures and dependencies are difficult to find
Bowtie	• Visual	• Qualitative
Operability and Maintainability Analysis Technique (OMAT)	• Systematic	• Needs a good cross-functional team
Risk Analysis	• Quantifies risks • Determine the critical scenarios	• Site specific • Quality dependent on having experienced people involved • Where does the line get drawn between foreseeable use/misuse
Earth Moving Equipment Safety Round Table (EMESRT) Control Framework	• Defined process • Industry wide	
Simulation	• Allows for cost effective testing across a wide range of variables	• Depends on the quality of the simulation inputs
Hazard Log / Hazard Tracking System	• Record of hazard identified during any hazard analysis technique, can record current risk statuses and target risk goals	• Requires continuous updates and maintenance
Requirements Management Tools	• Can be used to enter and track requirements and multiple levels of integration • Safety requirements resulting from hazard analysis can be added or tagged	• Requires continuous updates and maintenance

Risk Assessment Tools (continued)		
Tool	Benefits	Limitations
Safety Case	• Overarching story of why the system is adequately safe to test and/or deploy	• Can be a large amount of supporting data • Format and organization is often not standardized
Layer of Protection Analysis (LOPA)	• Provides level of integrity required for the safety systems	• Critical scenarios need to be determined in another risk assessment