GUIDELINE FOR APPLYING FUNCTIONAL SAFETY TO AUTONOMOUS SYSTEMS IN MINING

SUBMITTED BY
Functional Safety for Autonomous Equipment Sub-committee

VERSION DATE
09 Jul 2020

APPROVED BY
Autonomous Mining Working Group
31 Jul 2020
and
GMG Executive Council
12 Aug 2020

PUBLISHED
18 Aug 2020

DATE DOCUMENT TO BE REVIEWED
18 Aug 2022

PREPARED BY THE FUNCTIONAL SAFETY FOR AUTONOMOUS EQUIPMENT SUB-COMMITTEE OF THE AUTONOMOUS MINING WORKING GROUP
DISCLAIMER

Although the Global Mining Guidelines Group (GMG) believes that the information on https://gmggroup.org, which includes guidelines, is reliable, GMG and the organizations involved in the preparation of the guidelines do not guarantee that it is accurate or complete. While the guidelines are developed by participants across the mining industry, they do not necessarily represent the views of all of the participating organizations. This information does not replace or alter requirements of any national, state, or local governmental statutes, laws, regulations, ordinances, or other requirements. Your use of GMG guidelines is entirely voluntary.

CREDITS

Organizations Involved in the Preparation of these Guidelines


Project Leaders
Chirag Sathe, Principal Equipment Automation, BHP
Gareth Topham, Principal Functional Safety, Rio Tinto

COPYRIGHT NOTICE

This document is copyright protected by the Global Mining Guidelines Group (GMG). Working or committee drafts can be reproduced and used by GMG participants during guideline development. GMG hereby grants permission for interested individuals/organizations to download one copy. Written permission from GMG is required to reproduce this document, in whole or in part, if used for commercial purposes.

To request permission, please contact:
Global Mining Guidelines Group
Heather Ednie, Managing Director
hednie@gmggroup.org
http://www.gmggroup.org

Reproduction for sales purposes may be subject to royalty payments or a licensing agreement. Violators may be prosecuted.
# TABLE OF CONTENTS

1. FOREWORD .............................................. 2
2. DEFINITIONS OF TERMS AND ABBREVIATIONS .......... 2
3. KEYWORDS .............................................. 2
4. SCOPE ...................................................... 2
5. INTRODUCTION .......................................... 3
6. CONTEXTUAL BACKGROUND ON IMPLEMENTING AUTONOMOUS AND SEMI-AUTONOMOUS SYSTEMS .......... 3
   6.1 Managing People and Change .............................. 3
   6.2 Operation .............................................. 3
   6.3 Original Product Supplier and Mine Operator Relationship .............. 4
   6.4 Risk Assessment and Emergency Management ................... 4
   6.5 Configuration .......................................... 4
7. RECOMMENDED REFERENCE MATERIAL .................. 4
8. FUNCTIONAL SAFETY LIFECYCLE .......................... 5
9. SOFTWARE DEVELOPMENT, VERIFICATION, AND VALIDATION .......... 12
   9.1 Architectural Considerations ............................ 12
   9.2 Lifecycle Considerations ................................ 12
   9.3 Developing Conventional System Elements .......... 13
10. COMPETENCY MANAGEMENT ............................... 14
11. CYBERSECURITY ........................................ 14
12. ASSURANCE DOCUMENTATION ............................ 14
13. NON-DETERMINISTIC SYSTEMS ............................ 15
14. FUTURE WORK ............................................ 15
15. RESOURCES AND REFERENCES ............................ 16

APPENDIX A: FUNCTIONAL SAFETY IN OVERALL SAFETY MANAGEMENT .......... 18

APPENDIX B: SUMMARY OF STANDARDS ................. 19
   B.1 Key Standards ...................................... 19
   B.2 Non-Core Standards ................................ 19

APPENDIX C: EXAMPLE FUNCTIONAL SAFETY MANAGEMENT PLAN .......... 21

APPENDIX D: POTENTIAL ACTIVITIES FOR SOFTWARE DEVELOPMENT .......... 22
1. FOREWORD

The Global Mining Guidelines Group (GMG) is a network of representatives from mining companies, equipment and technology suppliers, research organizations, academia, regulatory agencies, consultancies, and industry associations who collaborate to tackle the challenges facing our industry. GMG aims to accelerate the improvement of mining performance, safety, and sustainability and creates guidelines, such as this one, that address common industry challenges. GMG guidelines are peer-reviewed documents that offer best practices, advise on the implementation of new technologies, develop industry alignment, or educate broadly. They are developed through industry-wide collaboration to assist the global mining community in implementing practices to improve operations and/or implement new technologies. Please note that GMG guidelines are not industry standards. Draft documents are checked and approved by working group members prior to approval by the GMG Executive Council.

Please note: If some of the elements of this document are subject to patent rights, GMG and the Canadian Institute of Mining, Metallurgy and Petroleum (CIM, of which GMG is a legal entity) are not responsible for identifying such patent rights.

2. DEFINITIONS OF TERMS AND ABBREVIATIONS

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 system: 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.

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

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.

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 artificial intelligence route planning). It may not be possible to establish an integrity level/performance level rating (e.g., MPL/PL/SIL) when using these systems.

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 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 involved people or environment.

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. Functional safety is a part of system safety.

* The formal IEC International Standard IEC 61508 definition of functional safety is: “The part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system that depends on the correct functioning of the E/E/PE (Electrical/Electronic/Programmable Electronic) safety-related systems and other risk reduction measures.”

3. KEYWORDS

Autonomous mining, autonomous systems, functional safety, lifecycle, mobile autonomous machines, risk management, safety

4. SCOPE

This document provides guidance on the application of functional safety to new deployments of autonomous systems in mining in surface and underground operations. It is intended as a starting point to help readers who are implementing autonomous systems navigate communication with other key stakeholders, but is not an exact process to follow and does not serve as a standard or set of rules. It covers in situ material—the mining and related support activities that contribute to material extraction such as drilling, blasting, loading, haulage, dumping.
Non-deterministic systems are outside of the scope of this guideline. However, some high-level information on non-deterministic systems is provided in Section 13.

While functional safety exists within the larger scope of system safety, guidance on overall system safety is outside the scope of this guideline. However, Section 6 outlines some contextual background on implementing autonomous systems and overall safety, and Appendix A describes how functional safety fits into overall safety management. A separate GMG document on overall autonomous system safety is currently in development.

The four key audiences for this guideline are:
- Those who design and supply autonomous systems (i.e., OPS)
- The operations delivery and integration teams
- Mining company technology, operations, and maintenance teams
- Regulators

These groups have different perspectives and needs, so the scope has been kept broad enough to cover all.

5. INTRODUCTION
The global mining industry is embracing automation. However, requirements for managing functional safety are unclear. There are several reasons for this lack of clarity:
- The use of autonomous systems is accelerating, but adoption is uneven across the industry.
- Current OPSs are at different stages of maturity in terms of managing functional safety.
- Several international and national functional safety standards exist or are in development, but there is a lack of clarity regarding what applies to autonomous systems in 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. This guideline also describes clear expectations for the communication requirements to support change management and effective application. To this end, this guideline:
- Identifies important reference materials and lists standards that are relevant to applying functional safety to various aspects of autonomous systems (Section 7)
- Outlines an example of a functional safety lifecycle for applying autonomous systems in mining and identifies some key expectations and responsibilities for providing information, documentation, and support at each stage (Section 8)
- Offers high-level guidance on software development, verification, and validation (Section 9); competency management (Section 10); cybersecurity (Section 11); and assurance documentation (Section 12)

6. CONTEXTUAL BACKGROUND ON IMPLEMENTING AUTONOMOUS AND SEMI-AUTONOMOUS SYSTEMS
A focus on functional safety is important for autonomous systems due to their reliance on technology (i.e., hardware and software) to manage safety functions. A strong focus on the administrative controls that are critical to system safety is also important.

6.1 Managing People and Change
Change management should be comprehensive because, for example, software changes can affect the system operates, and system operator actions can affect safety. There should also be appropriate communication to all relevant stakeholders, and all necessary updates should be made to the user documentation—such as guidelines and training manuals—to confirm that the operations personnel are ready to adapt to the change.

Training for all personnel who will interact with autonomous systems is imperative for safe automation. Everyone working at the operation should understand the risks of automation for the mine site to be safe.

6.2 Operation
Conflicts between the procedures for manned operation and those for autonomous operation need to be addressed.

Operational procedures need to be well defined. Autonomous systems require standard operating procedures in code that is executable because a machine cannot understand the intent of the standard operating procedures like a human can.

Different levels of autonomous maturity require different safety practices. For example, a current practice is to designate an autonomous operating zone that restricts unauthorized access. However, as mobile autonomous machines evolve, this practice will not always be the most cost-effective option. In order to address varying levels of maturity, safety standards will need to be developed or updated.

Metrics about autonomous systems need to be much more precise with respect to functional safety.
- Infrastructure / system status metrics should be accurate. For example, if a GPS device moves half a metre, it can significantly affect how the autonomous system functions.
- Autonomous mining system health metrics are critical in validating the performance that forms the assumptions in the risk assessments.
6.3 Original Product Supplier and Mine Operator Relationship

Operational intent defines the concept of operations and the assumptions about how the system will operate. Operational intent is a partnership between the mine operator and OPS when using autonomous systems, while it is within the control of the mine operator when using manned systems.

Effective channels of communication are required between the OPS and mine operator to address aspects such as residual risk and operations and maintenance requirements. More interaction may be required due to the complexity of such systems. For further information, see the Western Australia Code of Practice for Safe Autonomous Mining (Government of Western Australia Department of Mines, Industry Regulation and Safety, 2015).

6.4 Risk Assessment and Emergency Management

Risk assessments require:

- A broader scope because autonomous systems are typically more complex than manned systems.
- A strong focus on the administrative controls on which the autonomous system is reliant. They should also consider how human behaviour changes as aspects of manned operation are replaced by the autonomous systems.
- More focus on edge case scenarios, which are the scenarios that test the system design in unexpected and often untested ways. While the system operator can adapt to uncertainty and change when using a manned system, an autonomous system works within its design limits.

Emergency procedures need to be reviewed to include autonomous operations. The following questions should be considered when reviewing and updating existing procedures and as part of ongoing change management:

- How to stop an autonomous operation
- How to approach the autonomous operating zone
- How to remove the autonomous machine if it is broken down
- Training requirements for emergency responders

6.5 Configuration

A configuration management approach should be implemented to establish and maintain optimal performance for the autonomous system. This process needs to capture all hardware and software elements that could impact safety (e.g., the configuration definition should include vehicle mechanical items used in manned operation as well as the sensing, computing, and tuning implemented in software). This process also needs to capture delivery, integration, and maintenance aspects that could affect safety.

For further guidance refer to ISO 10007, Quality management - Guidelines for configuration management (2017c). Updates may occur frequently because of the rapid pace of innovation.

7. RECOMMENDED REFERENCE MATERIAL

Consideration should be given to the following documents during the design and implementation process:

- Local and international standards
- Industry guidelines
- Jurisdictional regulations and legislation
- Corporate standards
- OPS and vendor product information

Table 1 lists standards that are relevant to applying functional safety to various aspects of autonomous systems. A summary of each of these standards, as well as other standards that are non-core but still useful references, can be found in Appendix B. Subsequent references to these standards are by standard number. Full references, including individual published parts, can be found in Section 15.

<table>
<thead>
<tr>
<th>Table 1. Key Standards (in numerical order)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard</strong></td>
</tr>
<tr>
<td>ISO 13849 Safety of machinery – Safety-related parts of control systems</td>
</tr>
<tr>
<td>ISO 17757 Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety</td>
</tr>
<tr>
<td>ISO 19014 Earth-moving machinery – Functional safety (Parts 1 and 3 are published, Parts 2, 4, and 5 are currently in development)</td>
</tr>
<tr>
<td>ISO 31000 Risk management</td>
</tr>
</tbody>
</table>
8. FUNCTIONAL SAFETY LIFECYCLE

The functional safety lifecycle is a process for managing functional safety over the life of a product. This section is an example of a functional safety lifecycle for autonomous system applications that describes the relationship between the OPS’s product lifecycle and the mine operator’s application lifecycle. It also summarizes some recommendations for information to be communicated between the key participants. OPSs may vary in how they manage the approach to their product lifecycles, so these recommendations may also vary depending on the approach. This lifecycle example also considers both new and existing systems and how the process may be adapted for each.

This lifecycle example covers an overall site-specific autonomous system environment with several layers of automation. These layers comprise several types of product lifecycles that need to be integrated into the application lifecycle (Figure 1).

Figure 2 summarizes this lifecycle example. Tables 2–12 describe the expectations and the relevant information, documentation, or support that the mine operator and OPS may be responsible for providing at each related stage. Figure 2 and Tables 2–12 outline the key stages of both the product and application lifecycles from concept and scope to operation and maintenance as well as some key aspects (other risk controls, operational readiness, and change management) that should be considered as part of functional safety lifecycle management. In Figure 2, dotted arrows indicate where these other aspects fit within the overall lifecycle example. The arrows between the two lifecycles represent some key communications.

While the stages of product and application lifecycles can be similar, they do not have a one-to-one relationship, and they do not necessarily happen concurrently. If the OPS and mine operator are developing a custom solution, they may be on similar timelines. However, the product is often developed first, and then some stages of the product lifecycle may be revisited based on the application. For example, if the mine operator communicates information from any stage of the application lifecycle back to the OPS, then an earlier stage of the product lifecycle may need to be repeated or revisited. If design modifications are identified during the application, the hazard identification and risk assessment may need to be revisited for the product. Further, the sequence of activities outlined in Figure 2 is one of many examples of what the process can look like. This is especially true for the product lifecycle, as some of the stages may occur in a different order or may not apply in every situation depending on the product development approach.

The OPS is accountable for functional safety while developing a product. The OPS provides the mine operator with all the necessary information to demonstrate that the application specification is met and that the autonomous system can be operated and maintained at the required safety performance. Once the product is deployed in an operation, the mine operator is accountable for the overall safety of the autonomous system. However, the OPS is still accountable for changes that they make to their product during the product upgrade cycle (i.e., software upgrade). If a third party performs the integration, then the system integrator would be responsible for the development and analysis of the safety functions within the autonomous system while the mine operator would still be accountable for the overall safety of it.

Communication and transparency between the mine operator applying the autonomous system and the OPS providing it is essential. The OPS will typically develop the autonomous system for an intended use; over time, there may be modifications to both the system and the use cases in the field. If such modifications are made, then it is critical that mine operators apply change and configuration management principles. The mine operator needs to determine their user requirements and the resulting system and safety requirements for their application. They then need to communicate with the OPS to confirm that the product meets those requirements.
Table 2. Concept and Scope

At this stage, the concept and scope are examined within well-defined operational, regulatory, and risk environments. The potential requirements and safety controls for managing functional safety are also identified.

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify the relevant legislation, regulations, standards, and codes of practice</td>
<td>• Identify the relevant legislation, regulations, standards, and codes of practice</td>
</tr>
<tr>
<td>• Identify the equipment under control and its intended use and limits of operation</td>
<td>• Clearly define the concept of operations</td>
</tr>
<tr>
<td>• Identify the potential operating environments</td>
<td>• Clearly define the operational parameters</td>
</tr>
<tr>
<td>• Identify the communication requirements</td>
<td>• Identify the actual operating environment</td>
</tr>
<tr>
<td>• Identify the OPS-specific risk criteria</td>
<td>• Identify the existing or planned communications infrastructure</td>
</tr>
<tr>
<td></td>
<td>• Engage with the relevant regulators</td>
</tr>
<tr>
<td></td>
<td>• Identify the operation-specific risk criteria</td>
</tr>
</tbody>
</table>

Provided from OPS to mine operator:
• All product expectations (as outlined in the product column above)

Provided from mine operator to OPS:
• All application expectations (as outlined in the application column above)
### Table 3. Planning

This stage involves developing the process for managing functional safety and assigning the responsibilities for implementing it. See Appendix C for an example outline for a functional safety management plan.

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Document the process for how functional safety should be managed</td>
<td>• Set up the functional safety management plan based on the appropriate functional safety standard(s) where applicable and adapted to the specific application</td>
</tr>
<tr>
<td>• Set up the process for managing functional safety based on the appropriate functional safety standard(s) where applicable and adapted to the specific product</td>
<td>• Determine clear roles and responsibilities for all parties throughout the application lifecycle</td>
</tr>
<tr>
<td>• Put certified quality management in place (e.g., certified to ISO quality management systems standard, ISO 9001; 2015a)</td>
<td></td>
</tr>
</tbody>
</table>

Provided from OPS to mine operator:
- Documentation of the rationale for the selection and use of the methodology for managing functional safety

Provided from mine operator to OPS:
- The expected use conditions for the equipment

### Table 4. Hazard Identification and Risk Assessment

Robust hazard identification and risk assessment activities are completed at this stage so that the available controls can be identified, and effective decisions can be made about how to apply functional safety. During design, the OPS will typically complete the hazard identification and risk assessment for their product based on industry-wide standards. The mine operator applying the product will then complete their risk assessment with support from the OPS to clarify what risks are mitigated and to identify where they may need to put additional measures in place.

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify all of the hazards associated with operating the product in its intended use cases, including foreseeable misuse</td>
<td>• Use a facilitator and group of stakeholders with the appropriate expertise</td>
</tr>
<tr>
<td>• Assess the risks associated with the hazards (use external sources such as ISO 17757 for a list of hazards to consider and a list of risk identification tools)</td>
<td>• Identify all hazards associated with operating the product(s) in the context of the operational scenario, including foreseeable misuse</td>
</tr>
<tr>
<td>• Identify the existing controls</td>
<td>• Assess the risks associated with the hazards (use external sources such as ISO 17757 for a list of hazards to consider and a list of risk identification tools)</td>
</tr>
<tr>
<td>• Use an appropriate methodology and the appropriate tools (e.g., ISO 12100 or IEC 31010) to suit the equipment and related systems</td>
<td>• Identify the existing and proposed controls</td>
</tr>
<tr>
<td>• Use an appropriate methodology and the appropriate tools (e.g., ISO 12100 or IEC 31010) to suit the equipment and related systems</td>
<td>• Use an appropriate methodology and the appropriate tools (e.g., ISO 12100 or IEC 31010) to suit the equipment and related systems</td>
</tr>
</tbody>
</table>

Provided from OPS to mine operator:
- A list of hazards considered
- Participation in risk assessment:
  - Communication of outcomes from OPS design risk assessment
  - Participation in the mine operator risk assessment
- A description of the product functionality / use cases and the primary risk controls of the equipment / safety manual

Provided from mine operator to OPS:
- A list of the hazards from the operation to consider
Table 5. Other Risk Controls

Other risk controls—safety-related controls that need to be handled outside of, but in parallel with, the functional safety lifecycle—also need to be considered. For example, these controls may include physical changes such as road width, access control, and signage that are needed to safely accommodate autonomous machines.

<table>
<thead>
<tr>
<th>Action</th>
<th>Related lifecycle stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identified</td>
<td>Hazard identification and risk assessment (Table 4)</td>
</tr>
<tr>
<td>Specified</td>
<td>Control identification, specification, and requirements (Table 6)</td>
</tr>
<tr>
<td>Managed (in parallel)</td>
<td>Design and possible design modifications (Table 7)</td>
</tr>
<tr>
<td>Validated</td>
<td>Validation (Table 8)</td>
</tr>
</tbody>
</table>

Table 6. Control Identification, Specification, and Requirements

At this stage, the functional safety performance requirements and controls are defined and specified so that safety can be embedded in the design or in any design modifications.

**Product**
- Define the safety function and the required safe state
- Evaluate the performance and risk reduction requirements
- Specify the safety requirements at the product level

**Application**
- For existing (i.e., off-the-shelf) systems:
  - Conduct workshops with the OPS to understand the outcomes of the risk assessment and functional safety analysis to use as an input for the mine operator’s risk assessment and procedures to enable safe operation of the system
- For systems being modified extensively or a custom system that is being developed:
  - Conduct workshop(s) to define safety function performance and risk reduction requirements with input from product domain experts
  - Define the application-specific functional safety requirements, as identified in the layer of protection analysis (LOPA) or equivalent evaluation
- Specify the safety requirements at the application level
- Verify that the product performance meets the application targets

Provided from OPS to mine operator:
- Documented safety functions, including any safety-critical information, safety-related parts, and risk reduction requirements. These may be defined as integrity levels / performance levels if applicable.

Provided from mine operator to OPS:
- A revised safety requirements specification if modifications are made or the design is done in collaboration with the OPS
Table 7. Design / Possible Design Modifications

At this stage, the product is designed to meet the performance and risk reduction requirements and the functional safety requirements specification. Those applying the solution should verify the product and identify any possible design modifications.

<table>
<thead>
<tr>
<th>Product (design)</th>
<th>Application (possible design modifications)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Design the product in accordance with the performance and risk-reduction requirements identified in the control identification, specification, and requirements stage (Table 6)</td>
<td>• Verify that the product performance meets the performance requirements identified in the control identification, specification, and requirements stage (Table 6)</td>
</tr>
<tr>
<td>• Verify the design for safety</td>
<td>• If required, apply any additional controls</td>
</tr>
<tr>
<td>• If the required application safety requirements specification performance target cannot be met, then provide the documentation to demonstrate that all reasonably practicable steps have been taken, any limitations are clearly identified, and the actual performance that can be achieved</td>
<td>• Design the other risk controls identified in risk assessments in previous stages (e.g., road layout, access control)</td>
</tr>
</tbody>
</table>

Provided from OPS to mine operator:
• A listing of the safety functions of the autonomous system and what is required to maintain their integrity over the lifecycle of the machine / system

Provided from mine operator to OPS:
• A revised functional safety requirements specification

Table 8. Installation and Commissioning

This stage involves preparing the autonomous system to be put into service safely, including implementing installation and test plans.

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Develop clear instructions for on-site installation and commissioning</td>
<td>• Implement the installation plan for the overall system where applicable</td>
</tr>
<tr>
<td>• Generate the installation and configuration records</td>
<td>• Generate the installation and configuration records</td>
</tr>
<tr>
<td>• Implement the installation and test plan for safety functions</td>
<td>• Test the overall system, including the integration of sub-systems and ensuring a record is captured</td>
</tr>
<tr>
<td>• Run acceptance testing*</td>
<td></td>
</tr>
</tbody>
</table>

Provided from OPS to mine operator:
• Installation and site acceptance test plan* for review
• Configuration checklist
• As-built and commissioning records

Provided from mine operator to OPS:
• Feedback on any deviations from installation and test plan or failures
• Configuration records where appropriate (e.g., communications network performance meets specified requirements)

*Types of acceptance tests: Factoy acceptance test: An evaluation of the equipment completed by the vendor before installation to identify whether or not it is operating as specified. It is the final step of the manufacturing process. Site acceptance test: A joint activity between the vendor, integrator, and mine operator to identify whether or not the equipment is operating as specified and if the site is prepared for installation and commissioning. It is signed off by the integrator. User acceptance test: The testing completed by the mine operator to identify whether or not the system works for them and meets the business intent.
### Table 9. Validation

At this stage, procedures are completed to validate that the autonomous system has undergone all relevant assessments and meets all requirements. The product validation and application validation will not happen at the same time unless the OPS and mine operator are developing a custom solution.

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Clearly demonstrate that the product safety requirements have been fulfilled as defined in the product safety requirements specification</td>
<td>• Confirm that the overall integrated system application validation is carried out at the mine site, working in conjunction with the OPS</td>
</tr>
<tr>
<td>• Confirm that all verifications and functional safety assessments have been completed as required</td>
<td>• Clearly demonstrate that the application safety requirements have been met as defined in the application safety requirements specification</td>
</tr>
<tr>
<td>• Document the residual risks after verification</td>
<td>• Confirm that all additional controls required to meet risk reduction factors have been implemented</td>
</tr>
<tr>
<td></td>
<td>• Confirm that the scope of validation covers the fully integrated system</td>
</tr>
<tr>
<td></td>
<td>• Confirm that all required verifications and functional safety assessments have been completed</td>
</tr>
</tbody>
</table>

**Provided from OPS to mine operator:**
- Evidence that the product safety requirements have been met

**Provided from mine operator to OPS:**
- If the OPS agrees to validate a third-party modification or interface, then any required information that the OPS needs to evaluate the impact of the modification

### Table 10. Operational Readiness

Assessing operational readiness is essential before the autonomous system can be safely operated. It is primarily an application process, but it uses input from product development (see also ISO 17757:2019).

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide the relevant support documentation and input (see list below of what the OPS provides to the mine operator)</td>
<td>• Confirm that configuration management processes related to functional safety are in place</td>
</tr>
<tr>
<td></td>
<td>• Identify and procure the safety-critical spares</td>
</tr>
<tr>
<td></td>
<td>• Confirm that preventive maintenance plans and strategies are in place (e.g., proof testing, inspections, end of life replacement)</td>
</tr>
<tr>
<td></td>
<td>• Develop a strategy such as bypassing or overriding to manage impaired safety functions</td>
</tr>
<tr>
<td></td>
<td>• Develop strategies for performance monitoring diagnostics</td>
</tr>
<tr>
<td></td>
<td>• Recruit and train staff and assess their competencies</td>
</tr>
<tr>
<td></td>
<td>• Develop and modify the standard operating procedures</td>
</tr>
</tbody>
</table>

**Provided from OPS to mine operator:**
- Test procedures
- Safety manuals, operating procedures, maintenance instructions, and other information required for operating and maintaining safety functions
- Performance monitoring diagnostics and training

**Provided from mine operator to OPS:**
- Confirmation that the functional safety-related requirements and specifications from the OPS have been met and are ready to go live
Table 11. Operation and Maintenance

Continuous functional safety management and maintenance are essential once the autonomous system is in operation; it is part of applying the solution, but it also requires support from the product side.

<table>
<thead>
<tr>
<th>Product (support)</th>
<th>Application (operation and maintenance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Manage obsolescence</td>
<td>• Manage safety-critical spares</td>
</tr>
<tr>
<td>• Provide fault investigation support and support continuous improvement (see change management, Table 12)</td>
<td>• Implement a strategy such as bypassing or overriding to manage impaired safety functions</td>
</tr>
<tr>
<td>• Manage incident alerts and advice</td>
<td>• Maintain a configuration management system for functional safety</td>
</tr>
<tr>
<td>• Provide training updates</td>
<td>• Confirm that there is ongoing use of performance monitoring diagnostics</td>
</tr>
<tr>
<td></td>
<td>• Maintain staff competencies</td>
</tr>
<tr>
<td></td>
<td>• Verify all controls, including procedures and other risk reduction measures, on an ongoing basis</td>
</tr>
<tr>
<td></td>
<td>• Revalidate the operational risk assessments periodically</td>
</tr>
<tr>
<td></td>
<td>• Confirm that there is an appropriate investigation methodology (e.g., incident cause analysis method) in place with competent independent facilitators</td>
</tr>
<tr>
<td>Provided from OPS to mine operator:</td>
<td>Provided from mine operator to OPS:</td>
</tr>
<tr>
<td>• The documentation relevant to the support items listed under the product column</td>
<td>• Feedback on performance, incidents, and failures</td>
</tr>
</tbody>
</table>

Table 12. Change Management

Change management is a key consideration throughout the lifecycle to make sure that every change that is made allows for the same level of functional safety. Every time changes are made to a product or application, the stages from planning onward may need to be revisited to consider the adjustments. If the mine operator is modifying or developing a system independently from the OPS, some of the expectations under the product column may need to be met on the application side.

<table>
<thead>
<tr>
<th>Product</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Confirm that the change management process* covers the evaluation of functional safety, including impact analysis</td>
<td>• Confirm that the change management process covers the evaluation of functional safety, including impact analysis</td>
</tr>
<tr>
<td>• Confirm that any changes made to the product that affect safety functions are communicated to all product owners, and the communications are documented</td>
<td>• Establish a mechanism to communicate product changes to the OPS and engage with them</td>
</tr>
<tr>
<td>• Reasonably support product owner in the change management process</td>
<td>• Apply functional safety change management processes to anything that affects the risk profile (e.g., a new use case, environmental changes, new initiating events, or changes to existing events)</td>
</tr>
<tr>
<td></td>
<td>• Confirm that the change management process defines the appropriate review and approval authorities</td>
</tr>
</tbody>
</table>

Provided from OPS to mine operator:

• An explanation of any changes that are made to the product that affect its safety functions

Provided from mine operator to OPS:

• The identification of opportunities for improvement with details for assessment

* Further detail on change management can be found in the GMG (2019) Guideline for the Implementation of Autonomous Systems in Mining.
9. SOFTWARE DEVELOPMENT, VERIFICATION, AND VALIDATION

Autonomous system software often carries out safety functions. This section describes general considerations around software development within the context of the functional safety lifecycle outlined in Section 8. It focuses on conventional software development methods and deterministic systems.

9.1 Architectural Considerations

The requirements for autonomous system software architectures will vary depending on the relationship between the control and protection elements.

While system architectures designed with separate control and protection elements allow functional safety requirements to focus on the protection system, it is not always possible or practical in mobile machine applications. This clear separation of control and protection elements is possible if those designing the safety protection function can specify and implement it without having any information about the workings of the control function (see Example A). This approach to functional safety is typical of stationary machines in factory automation settings.

If knowing the state of the control function or what it is doing is necessary to maintain safety, it is much harder to produce a simple, independent protection function (see Example B). In such situations, it is recommended to place a greater reliance on the integrity of the control function, however, for autonomous systems, there is still a notable reliance on other administrative and non-control system mitigation measures.

9.2 Lifecycle Considerations

The software development lifecycle is contained within a small portion of the functional safety lifecycle identified in Section 8 and Figure 2, particularly the product lifecycle. The software lifecycle primarily fits into the design / possible design modifications (Table 7) and the control identification, specification, and requirements (Table 6) stages. Some elements of the software requirements validation are part of the validation stage (Table 9).

Figure 3 shows how the functional safety lifecycle fits into a basic software development V-model diagram. Functional safety standards use similar V-models to describe the software development lifecycle (e.g., ISO 13849-1:2015, Figure 6 and IEC 61508-3:2010, Figure 6). This lifecycle corresponds well with the functional safety lifecycle outlined in Section 8, and the relationship between the two lifecycles is as follows:

- The “software safety requirements specification” is part of the “control identification, specification, and requirements” stage in Table 6.
- The “validation and acceptance testing” is part of the “validation” stage in Table 9.
- The remaining steps in Figure 3 are encompassed within the “design / possible design modifications” stage in Table 7.

Example A: Situation where protection and control elements can be separate

An underground load, haul, dump automation system (i.e., the control element) is separated from human interaction by a barrier control system (i.e., the protection element). If the barrier system is breached, the machine goes to a safe state, which requires a specific process to be followed to reinitiate autonomous operations. This works because people, machines, and vehicles can be segregated from the autonomous machine.

Example B: Situation where knowing the state of the control function is necessary

When machine control systems (e.g., steering, braking, propulsion) are used as part of an autonomous machine system around other machines and vehicles with people in them, the autonomous system needs to know what the machine is doing, where it should be going, and where other things are so that it can act accordingly. The inputs into these systems can come from both deterministic and non-deterministic aspects. Safety is dependent on the correct operation of the autonomous and machine systems and other risk mitigation measures. Further information on non-deterministic aspects can be found in the CMEiG, EMESRT, and ICMM White Paper and Guiding Principles for Functional Safety for Earthmoving Machinery (2020).
9.3 Developing Conventional System Elements

It is recommended to develop the software based on the safety function performance requirements for a particular control and with consideration given to relevant standards (e.g., ISO 13849, IEC 61508, ISO 19014). When it is published, ISO/DIS 19014-4, Earth Moving Machinery — Functional safety — Part 4: Design and evaluation of software and data transmission for safety-related parts of the control system, will likely be the most relevant standard (https://www.iso.org/standard/70718.html). The safety performance requirements are often identified by the risk reduction required in the Control Identification, Specification, and Requirements stage of the functional safety lifecycle (Table 6).

For example, ISO 13849-1:2015 includes an analysis of the degree of reliance on safety functions, defining the performance requirements by designating performance levels (PLs). PLs are labelled a–e, with e representing the highest reliance on the function in terms of safety. See Appendix D for an example of the potential activities for software development for allocated PLs based on ISO 13849-12015. Some system developers may employ techniques / methods like these.

Errors made in software development can be reduced by constraining the use of the programming language. One option is the use of limited variability languages (LVLs). For example, function block diagrams are used to construct programs by linking pre-defined function blocks, thereby reducing the scope for error. When more general programming languages are used, it is common to use a language subset, which means only using some of the aspects of a language or using them in a particular way. For example, the Motor Industry Software Reliability Association (MISRA) has developed guidelines for commonly used languages:

- MISRA C, Guidelines for the Use of C Language in Critical Systems (2013), which has now been updated to address security concerns (2016)

These subsets are now widely used and supported by tools. While subsets are not defined for all languages and there are other variants of those that are defined, using a tool-enforced subset is good practice.

Note: Section 9 was developed with assistance from John McDermid, Director of the Assuring Autonomy International Programme, University of York
10. COMPETENCY MANAGEMENT

Those managing functional safety are expected to be suitably competent in their knowledge, skills, experience, and behaviours. This section provides guidance for mining operations on assessing competency. Potential competency requirements include the following:

- Identifying the relevant safety lifecycle phases
- Identifying the tasks to be carried out in those phases
- Defining a competency criterion for each task
- Mapping the tasks to roles
- Allocating the roles to departments or individuals
- Developing and executing a plan for assessment
- Planning for and proactively managing gaps
- Carrying out periodical assessments to confirm that competencies remain valid
- Managing competencies of new starters
- Periodically revisiting the tasks and criteria to confirm they remain relevant

Guidance for successfully implementing a competency management plan in an operation includes these steps:

- Develop the competency criteria to include requirements that demonstrate knowledge, skills, experience, and behaviours. This demonstration should go beyond training courses and certifications, which are not always comprehensive.
- Use clear language within the competency criteria.
- Match the level of detail and rigour within the competency criteria to the level of safety performance required by the product or application and its potential to cause harm.
- Consider how to evaluate domain knowledge within the competency criteria. For example, while it may be good to have a functional safety expert on board, their expertise needs to be complemented by knowledge of mining operations and autonomous systems.
- Integrate the competency criteria into existing systems. Some companies have a competency framework or system in place (e.g., managing health and safety risks by working in a restricted space).
- Collaborate with OPSs for assistance with formal training, simulated training, joint on-the-job assessments, and handover if there is not sufficient competency within the operation.
- Allow the criteria development process to expose competency gaps. Competency gaps can then be managed through strategies such as collaboration between team members who collectively meet the competency requirements for a given task.

Recommend literature that discusses functional safety competency management in detail includes:

- Institute of Engineering and Technology (2016), Competence Criteria for Safety-related System Practitioners
- The UK Health and Safety Executive (2006, 2007), Managing competence for safety-related systems

11. CYBERSECURITY

Cybersecurity is an emerging issue that has the potential to significantly affect the safety functions of autonomous systems; it should therefore be considered throughout the lifecycle. Because autonomous systems rely heavily on software, threats that affect sensor operation, software design, system interoperation, and human-machine interaction all have the potential to affect functional safety. Cybersecurity threats also exist that specifically target safety systems.

Cybersecurity measures should preserve the safety functionality of the autonomous system. The system should be designed to act to preserve safety as the highest priority if it is sent messages that could result in unsafe operation. Security for control interfaces should be considered and managed as part of the functional safety risk management process and should address the requirements for compliance, certification, and risk mitigation following a “so far as reasonably practicable” methodology. A risk assessment carried out on cybersecurity threats using information from the MM-ISAC autonomous systems threat model is recommended (http://www.mmisac.org/).

Recommended literature on cybersecurity includes:

- ISA TR 84.00.09_2017 Cybersecurity Related to the Functional Safety Lifecycle (International Society of Automation, 2017)

More detailed cybersecurity guidance will be developed through the GMG System Safety for Autonomous Mining project and the GMG-MMISAC Cybersecurity Working Group.

12. ASSURANCE DOCUMENTATION

The mine operator and OPS should collaborate on what assurance documentation and analysis are appropriate for the system. Options to consider include:

- References to or conformance with relevant international standards, including functional safety standards where applicable
Outcomes of the hazard and risk analysis
A list of the safety functions, a description of their functionality and safe states of operation
System limitations or safety goals necessary for the site to operate the system safely
Validation report that all safety functions are working during commissioning onsite (where practicable)
If safety functions are unable to be tested onsite, evidence of validation of those safety functions
Outcomes of causal analyses, for example failure modes and effects analysis (FMEA), fault tree analysis (FTA), and systems theoretic process analysis (STPA)
An overview of the software development process that may use methods such as those in ISO 19014, ISO 13849 or IEC 61508

Note that some documentation may not be shareable due to intellectual property protection requirements for the OPS. In such situations, the OPS and mine operator will need to agree on an appropriate mechanism for providing adequate assurance of the safety of the product to the mine operator.

It may also be helpful for the OPS to provide a high-level overview of the OPS product lifecycle management to the mine operator.

13. NON-DETERMINISTIC SYSTEMS
In its current state, the mining industry is accustomed to systems that are predominantly deterministic, meaning that they respond to known and understood states, failure modes, and conditions. Based on the current trends in the evolution of mining and other industries, it is likely that non-deterministic systems and aspects of systems will be prevalent. A non-deterministic system is one where decisions are derived from complex sensor and processing algorithms and / or involve machine learning. Examples of non-deterministic systems include:
- Perception systems (including collision avoidance systems)
- GPS technology (including geofences)
- Route planning systems based on artificial intelligence

The existing standards include the assignment of performance or integrity levels and can be applied more directly to deterministic systems. Because non-deterministic systems respond to conditions based on probability, these responses cannot be quantified using these methods. The CMEIG, EMESRT, and ICMM White Paper and Guiding Principles for Functional Safety for Earthmoving Machinery (2020) offers some high-level guidance on the direction for the mining industry in terms of non-deterministic systems. They describe:

- An interim approach until new standards are available: A risk-based evaluation that combines traditional and evolving risk management techniques, a robust development process, an extensive system testing and validation framework, and strong engagement and collaboration among relevant stakeholders ("Proposed Approach for the Evaluation of Systems with Non-Deterministic Aspects," CMEIG, EMESRT, and ICMM, 2020).
- The approach in the automotive industry: ISO/PAS 21448:2019 Road vehicles — Safety of the intended functionality is intended to be applied to evaluating non-deterministic aspects of safety-related systems through "extensive validation over a series of use/mis-use cases" ("Other Industries Approach," CMEIG, EMESRT, and ICMM, 2020).
- Relevant standardization work for earth-moving machinery: ISO/TC 127 Earth-moving machinery committee has some work ongoing to address the current lack of standardization in this area, including an adaptation of the automotive safety of the intended functionality approach for earth-moving vehicles (ISO/TC 127/SC2 WG 24; https://www.iso.org/committee/52180.html).

14. FUTURE WORK
Because functional safety for autonomous systems in mining is a rapidly evolving topic, this guideline is also expected to evolve and add any appropriate detail over time to align with new and updated standards and consider emerging concepts and technological advances. A separate GMG project on system safety is also ongoing and will complement this guideline by addressing adjacent topics such as safety case and risk management, human factors, integration, and verification and validation.
15. RESOURCES AND REFERENCES


Global Mining Guidelines Group (GMG)


APPENDIX A: FUNCTIONAL SAFETY IN OVERALL SAFETY MANAGEMENT

Overall safety relies on components of a safety system being designed and operated safely. Functional safety is a part of the broader context of overall safety, which consists of the following layers:

- Societal expectations of safety. What is considered to be safe is decided by socially defined descriptions of what risks are deemed tolerable with respect to the benefits with operating a system. These societal expectations are expressed through legislation and common law.

- Safety management systems are put in place to confirm that a system is operated safely. These include risk, emergency, and change management and establishing a safety culture.

- System safety confirms that the overall design of a system is safe. Functional safety is a part of this layer and refers to “a system or equipment operating correctly in response to its inputs” (source: www.iec.ch). Figure A1 illustrates some examples of what may be in each layer.

Figure A1. Layers of Overall Safety (Provided by a GMG Contributor)
APPENDIX B: SUMMARY OF STANDARDS

The following descriptions summarize the content and scope of key and non-core standards relevant to functional safety. The key standards are relevant to various aspects of the application of functional safety to autonomous systems in mining. The non-core standards are not specific to functional safety for autonomous systems in mining but are relevant to the processes and activities surrounding it or provide guidance for other industries that could be adapted to mining. They are arranged numerically.

Full references to these standards and full standard numbers can be found in Section 15. Please note that for non-core standards, only the general sections of multi-part standards are cited unless otherwise specified.

B.1 Key Standards


This standard defines general terminology, principles, and methods of risk assessment associated with various types of fixed and mobile machinery. It provides a list of common hazards and is intended to be used in conjunction with other application-specific (i.e., Type B and Type C) safety standards.

ISO 13849 Safety of machinery – Safety-related parts of control systems (International Organization for Standardization, 2015b, 2012b)

This two-part standard provides guidance on the design, integration, and validation of safety-related control system hardware and software used in various types of machinery. It is primarily focused on fixed machinery, but it can also be applied to systems used in mobile equipment. Hazard assessment is used to establish required PLs of the control systems, and achieved PLs are analyzed through an evaluation of the system architecture, including reliability of the components used and fault detection capability. It references some concepts from other standards such as IEC 61508 and suggests using an application-specific risk graph for determining performance requirements.

ISO 17757 Earth-moving machinery and mining – Autonomous and semi-autonomous machine system safety (International Organization for Standardization, 2019)

This standard provides the general safety requirements and considerations for autonomous and semi-autonomous mobile machines used in earth-moving and mining applications.

ISO 19014 Earth-moving machinery – Functional safety (International Organization for Standardization, 2018c, 2018d)

This is a five-part standard that covers the application of functional safety to mobile machinery used in construction and mining applications. The first and third parts are published, and the other three are currently in development. Many concepts are similar to those in ISO 13849 and IEC 61508. This standard uses an industry-specific and risk-based approach to determine machine PLs of the safety-related control systems used. It addresses concerns with environmental conditions and provides further details on how to analyze complex embedded machine controls involving the use of integrated electrical, hydraulic, and pneumatic systems on earth-moving machinery.

ISO 31000 Risk management (International Organization for Standardization, 2018e)

This standard provides general principles and guidelines to establish a framework for managing process risk across an organization and explores various risk assessment concepts and methodologies.

IEC 31010 Risk management – Risk assessment techniques (International Electrotechnical Commission, 2019b)

This standard (a double logo standard with ISO) provides guidance on hazard identification and risk assessment techniques.


This is a broad seven-part standard covering various aspects to be considered when E/E/PE systems are used to carry out safety functions. It is particularly relevant to the principles of lifecycle management. It is intended to support the development of application or sector-specific functional safety standards and is only focused on electrical and electronic systems. It does not address concerns related to mechanical controls or human factor requirements related to the design of E/E/PE systems. System design requirements are expressed using SILs.


This is an adaptation of IEC 64508 that is specific to fixed machinery in which safety-related component design requirements are expressed using SILs.

B.2 Non-Core Standards


This standard defines general concepts and principles for hardware and software system developers to consider when developing a safety system. It uses some aspects similar to...
methodologies presented in IEC 61508 with a focus on contracts and the contractor’s responsibilities.

ISO 3450 Earth-moving machinery – Wheeled or high-speed rubber-tracked machines – Performance requirements and test procedures for brake systems (International Organization for Standardization, 2011a)

This standard specifies the performance requirements and test procedures for mobile machine braking systems.

ISO 5010 Earth-moving machinery – Rubber tyred machines – Steering requirements (International Organization for Standardization, 2007a)

This standard specifies the performance and testing criteria used to evaluate the steering capability of wheeled mobile machinery.


This standard covers the safety requirements associated with industrial robots, including the potential hazards and steps to reduce or eliminate them.

ISO 13766 Earth-moving and building construction machinery – Electromagnetic compatibility (EMC) of machines with internal electrical power supply (International Organization for Standardization, 2018a, 2018b)

This is a two-part standard focused on electromagnetic compatibility. The first part is around general equipment compatibility requirements. The second part is focused on the test methods and acceptance criteria for safety-related parts of control systems (functional safety) used on mobile machinery.

ISO / IEC/ IEEE 15288 - Systems and software engineering - System life cycle processes (International Organization for Standardization, 2015c)

This standard establishes a common framework of process controls that can be used by organizations when acquiring or supplying systems.

ISO 15817 Earth-moving machinery – Safety requirements for remote operator control systems (International Organization for Standardization, 2012a)

This standard specifies the essential safety requirements for remote operator control of mobile machinery. It is not applicable to autonomous systems that are capable of working without operator assistance.

ISO 16001 Earth-moving machinery – Object detection systems and visibility aids – Performance requirements and tests (International Organization for Standardization, 2017a)

This standard specifies general requirements and methods for evaluating and testing the performance of object detection systems used on mobile machinery.

ISO 20474 Earth-moving machinery – Safety (International Organization for Standardization 2017b)

This 15-part standard specifies the general safety requirements for earth-moving machinery. The first part contains general requirements and the parts that follow are specific to individual types of machines and their specific functions and applications. It specifies the appropriate technical measures for eliminating or reducing risks from relevant hazards. It references use of ISO 17757 for autonomous systems.

ISO 21448 Road vehicles – Safety of the intended functionality (International Organization for Standardization, 2019c)

This standard complements ISO 26262; it is intended to be applied where situational awareness is critical to safety and is derived from complex sensor and processing algorithms (e.g., emergency intervention systems, advanced driver assistance systems) where it may not be possible to establish a SIL or PL rating.

ISO 26262 Road vehicles – Functional safety (International Organization for Standardization, 2018f)

This is a 10-part standard focused on the application of functional safety to automotive electrical and electronic systems. Many concepts are derived from IEC 61508 using an industry-specific and risk-based approach to determine automotive safety integrity levels (ASILs) of the safety-related control systems used.

IEC 61800 - Adjustable speed electrical power drive systems (International Electrotechnical Commission, 2016)

This is a nine-part standard focused on various aspects of AC and DC drive system design, including considerations for safety, interface requirements, electromagnetic compatibility, and energy efficiency. The most relevant document in this series is IEC 61800-5-2:2016, Adjustable speed electrical power drive systems - Part 5-2: Safety requirements – Functional.

IEC 62998 – Safety of machinery – Safety-related sensors used for the protection of persons (International Electrotechnical Commission, 2019b)

This is a technical specification of requirements for developing and integrating safety related sensor systems and protecting people.
APPENDIX C: EXAMPLE FUNCTIONAL SAFETY MANAGEMENT PLAN

Table C1 is an example outlining the contents to consider in a functional safety management plan. Please note that the details will vary depending on the context and that the contents of the functional safety management plan should be tailored to suit the specific product or application. Also note that a range of other processes may also fulfill the criteria of the functional safety management plan.

Note that the items contained in Table C1 may be embedded in an overall process rather than exist as a distinct functional safety management plan.

<table>
<thead>
<tr>
<th>Table C1. Functional Safety Management Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Introduction</strong></td>
</tr>
<tr>
<td>1.1 Scope</td>
</tr>
<tr>
<td>• Consider system and application</td>
</tr>
<tr>
<td>1.2 Standards</td>
</tr>
<tr>
<td>• Identify functional safety standards utilized</td>
</tr>
<tr>
<td><strong>2. Organization</strong></td>
</tr>
<tr>
<td>2.1 Roles and responsibilities</td>
</tr>
<tr>
<td>2.2 Competency</td>
</tr>
<tr>
<td>• Develop strategy for internal competency management</td>
</tr>
<tr>
<td>2.3 Communications</td>
</tr>
<tr>
<td>• Define interface points between OPS and mine operator, and set requirements for documentation exchanged</td>
</tr>
<tr>
<td>2.4 Supplier management</td>
</tr>
<tr>
<td><strong>3. Safety management</strong></td>
</tr>
<tr>
<td>3.1 Lifecycle</td>
</tr>
<tr>
<td>• Outline functional safety lifecycle to be followed</td>
</tr>
<tr>
<td>3.2 Phase activities</td>
</tr>
<tr>
<td>• Plan for each phase, including identifying inputs, outputs, and dependencies</td>
</tr>
<tr>
<td>3.3 Change management</td>
</tr>
<tr>
<td>3.4 Configuration management</td>
</tr>
<tr>
<td>3.5 Hazard log / risk register</td>
</tr>
<tr>
<td><strong>4. Technical delivery</strong></td>
</tr>
<tr>
<td>4.1 Design principles applied</td>
</tr>
<tr>
<td>• Structure software and hardware techniques employed (e.g., architecture)</td>
</tr>
<tr>
<td>4.2 Installation and commissioning</td>
</tr>
<tr>
<td>4.3 Verification</td>
</tr>
<tr>
<td>4.4 Validation</td>
</tr>
<tr>
<td>• Conduct site-specific safety validation exercise</td>
</tr>
<tr>
<td>4.5 Cybersecurity</td>
</tr>
<tr>
<td>4.6 Safety constraints</td>
</tr>
<tr>
<td><strong>5. Operations and maintenance</strong></td>
</tr>
<tr>
<td>5.1 Change management</td>
</tr>
<tr>
<td>• Detail how to maintain the risk register during production phase</td>
</tr>
<tr>
<td>5.2 Configuration management</td>
</tr>
<tr>
<td>• Define requirements for configuration management in operations and maintenance</td>
</tr>
<tr>
<td>5.3 In-service performance management</td>
</tr>
<tr>
<td>• Define requirements for ongoing safety management and continuous improvement</td>
</tr>
<tr>
<td>5.4 Management of actions</td>
</tr>
<tr>
<td>5.5 Emergency preparedness</td>
</tr>
<tr>
<td><strong>6. Assurance</strong></td>
</tr>
<tr>
<td>6.1 Audits</td>
</tr>
<tr>
<td>6.2 Functional safety assessments</td>
</tr>
<tr>
<td>• Define requirements for functional safety assessment</td>
</tr>
</tbody>
</table>
APPENDIX D: POTENTIAL ACTIVITIES FOR SOFTWARE DEVELOPMENT

Tables D.1 and D.2 list potential activities for software development and their relationship to PLs as they are defined in ISO 13849-1:2015. Please note that these tables are not for audit purposes because the activities and requirements will vary significantly depending on the development process. These can be used to help understand and identify some of the activities that may apply.

Please note that ISO 13849-1:2015 is under revision at the time of publication and this information will be outdated once the next version is released. Please also note that other approaches and standards for software development may be more appropriate for specific systems.

Table D.1. Safety-Related Embedded Software (SRESW)

<table>
<thead>
<tr>
<th>#</th>
<th>Activity</th>
<th>PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Software safety lifecycle with verification and validation activities</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>2</td>
<td>Documentation of specification and design</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>3</td>
<td>Modular and structured design and coding</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>4</td>
<td>Control of systematic failures</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>5</td>
<td>Where using software-based measures for control of random hardware failures, verification of correct implementation</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>6</td>
<td>Functional testing (e.g., black-box testing)</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>7</td>
<td>Appropriate software safety lifecycle activities after modifications</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>8</td>
<td>Project management and quality management system comparable to (e.g., ISO 9001)</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>9</td>
<td>Documentation of all relevant activities during software safety lifecycle</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>10</td>
<td>Configuration management to identify all configuration items and documents related to an SRESW release</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>11</td>
<td>Structured specification with safety requirements and design</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>12</td>
<td>Use of suitable programming languages and computer-based tools with confidence from use</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>13</td>
<td>Modular and structured programming, separation in non-safety-related software, limited module sizes with fully defined interfaces, use of design and coding standards</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>14</td>
<td>Coding verification by walk-through / review with control flow analysis</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>15</td>
<td>Extended functional testing (e.g., grey-box testing, performance testing, or simulation)</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>16</td>
<td>Impact analysis and appropriate software safety lifecycle activities after modifications</td>
<td>✓ ✓ ✓</td>
</tr>
<tr>
<td>17</td>
<td>Structural test coverage (statements) 100% (Note: in addition to ISO 13849 requirements)</td>
<td>✓ ✓ ✓</td>
</tr>
</tbody>
</table>
### Table D.2. Safety-Related Applied Software (SRASW)

<table>
<thead>
<tr>
<th>#</th>
<th>Activity</th>
<th>PL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>a</td>
</tr>
<tr>
<td>1</td>
<td>Software safety lifecycle with verification and validation activities</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>Documentation of specification and design</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>Modular and structured design and coding</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>Functional Testing</td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td>Appropriate development activities after modifications</td>
<td>✓</td>
</tr>
</tbody>
</table>

The safety-related software specification should be reviewed, made available to people involved in the lifecycle, and contain the description of:

6  Safety functions with required PL and associated operating modes               ✓ ✓ ✓ ✓ ✓
7  Performance criteria (e.g., reaction times)                                    ✓ ✓ ✓ ✓ ✓
8  Hardware architecture with external signal interfaces                          ✓ ✓ ✓ ✓ ✓
9  Detection and control of external failure                                      ✓ ✓ ✓ ✓ ✓

**Selection of tools, libraries, languages:**

10 Suitable tools with “confidence from use.” The tool should comply with the appropriate safety standard; if two diverse components with diverse tools are used, confidence from use may be sufficient. Technical features that detect conditions that could cause systematic error (such as data type mismatch, ambiguous dynamic memory allocation, incomplete called interfaces, recursion, pointer arithmetic) should be used. ✓ ✓ ✓

11 Whenever reasonable and practicable, validated function block libraries should be used, either safety-related function block libraries provided by the tool manufacturer (highly recommended for PL = e) or validated application-specific FB libraries. ✓ ✓ ✓

12 A justified limited variability language (LVL) subset suitable for a modular approach should be used (e.g., the accepted subset of IEC 61131-3 languages). Graphical languages (e.g., function block diagram, ladder diagram) are highly recommended. ✓ ✓ ✓

**Software design should feature:**

13 Semi-formal methods to describe data and control flow (e.g., state diagram or program flow chart) ✓ ✓ ✓

14 Modular and structured programming predominantly realized by function blocks deriving from safety-related validated function block libraries ✓ ✓ ✓

15 Function blocks of limited size of coding ✓ ✓ ✓

16 Code execution inside function block that should have one entry and one exit point ✓ ✓ ✓

17 Architecture model of three stages: inputs, processing, outputs ✓ ✓ ✓

18 Assignment of a safety output at only one program location ✓ ✓ ✓

19 Use of techniques for detection of external failure and for defensive programming within input, processing, and output blocks that lead to a safe state ✓ ✓ ✓
Table D.2. Continued

<table>
<thead>
<tr>
<th>#</th>
<th>Activity</th>
<th>PL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>a</td>
</tr>
<tr>
<td>Where SRASW and non-SRASW are combined in one component:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>SRASW and non-SRASW should be coded in different function blocks with well-defined data links</td>
<td>✓</td>
</tr>
<tr>
<td>21</td>
<td>There should be no logical combination of non-safety-related and safety-related data that could lead to the downgrading of the integrity of safety-related signals (e.g., combining safety-related and non-safety-related signals by a logical “OR” where the result controls safety-related signals)</td>
<td>✓</td>
</tr>
<tr>
<td>Software implementation / coding:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Code should be readable, understandable and testable using symbolic variables instead of explicit hardware addresses</td>
<td>✓</td>
</tr>
<tr>
<td>23</td>
<td>Justified or accepted coding guidelines should be used</td>
<td>✓</td>
</tr>
<tr>
<td>24</td>
<td>Data integrity and plausibility checks (e.g., range checks) available on application layer (defensive programming) should be used</td>
<td>✓</td>
</tr>
<tr>
<td>25</td>
<td>Code should be tested by simulation</td>
<td>✓</td>
</tr>
<tr>
<td>26</td>
<td>Verification should be by control and data flow analysis for PLd or PLe</td>
<td>✓</td>
</tr>
<tr>
<td>Testing:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>The appropriate validation method is black-box testing of functional behavior and performance criteria (e.g., timing performance)</td>
<td>✓</td>
</tr>
<tr>
<td>28</td>
<td>For PLd and PLe, test case execution from boundary value analysis is recommended</td>
<td>✓</td>
</tr>
<tr>
<td>29</td>
<td>Test planning is recommended and should include test cases with completion criteria and required tools</td>
<td>✓</td>
</tr>
<tr>
<td>30</td>
<td>Input / output testing should confirm that safety-related signals are correctly used within SRASW</td>
<td>✓</td>
</tr>
<tr>
<td>31</td>
<td>Structural test coverage (statements) 100% (Note: in addition to ISO 13849 requirements)</td>
<td>✓</td>
</tr>
<tr>
<td>Documentation:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>All lifecycle and modification activities should be documented</td>
<td>✓</td>
</tr>
<tr>
<td>33</td>
<td>Documentation should be complete, available, readable, and understandable</td>
<td>✓</td>
</tr>
<tr>
<td>34</td>
<td>Code documentation within source text should contain module headers with legal entity, functional and I/O description, and version of used library function blocks, and sufficient comments on networks and declaration lines</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration management:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>It is highly recommended that procedures and data backup be established to identify and archive documents, software modules, verification/validation results, and tool configuration related to a specific SRASW version</td>
<td>✓</td>
</tr>
<tr>
<td>Modifications:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>After modifications of SRASW, impact analysis should be performed to confirm correct specification. Appropriate lifecycle activities should be performed after modifications. Access rights to modifications should be controlled, and modification history should be documented.</td>
<td>✓</td>
</tr>
</tbody>
</table>