INTERNATIONAL STANDARD

ISO 17757

First edition
2017-09

Earth-moving machinery and mining — Autonomous and semi-autonomous machine system safety

Engins de terrassement et exploitation minière — Sécurité de système de machine autonome et semi-autonome

Reference number
ISO 17757:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 2, *Safety, ergonomics and general requirements*.

Introduction

This document is a type-C standard as stated in ISO 12100.

The machinery concerned and the extent to which hazards, hazardous situations or hazardous events are covered are indicated in the Scope of this document.

When requirements of this type-C standard are different from those which are stated in type-A or -B standards, the requirements of this type-C standard take precedence over the requirements of the other standards for machines that have been designed and built according to the requirements of this type-C standard.

Mining input for this document was obtained through liaisons with the GMSG (global mining standards and guidelines group) and the Western Australia Mobile Autonomous Machine Systems Working Group.

Earth-moving machinery and mining — Autonomous and semi-autonomous machine system safety

1 Scope

This document provides safety requirements for autonomous machines and semi-autonomous machines used in earth-moving and mining operations, and their autonomous or semi-autonomous machine systems (ASAMS). It specifies safety criteria both for the machines and their associated systems and infrastructure, including hardware and software, and provides guidance on safe use in their defined functional environments during the machine and system life cycle. It also defines terms and definitions related to ASAMS.

It is applicable to autonomous and semi-autonomous versions of the earth-moving machinery (EMM) defined in ISO 6165 and of mobile mining machines used in either surface or underground applications. Its principles and many of its provisions can be applied to other types of autonomous or semi-autonomous machines used on the worksites.

Safety requirements for general mobile EMM and mining machines, as well as operators, trainers or passengers on the machine, are given by other International Standards (e.g. ISO 20474, ISO 19296). This document addresses additional hazards specific and relevant to ASAMS when used as intended.

It is not applicable to remote control capability (covered by ISO 15817) or function-specific automated features, except when those features are used as part of ASAMS.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 2867, *Earth-moving machinery — Access systems*

ISO 3450:2011, *Earth-moving machinery — Wheeled or high-speed rubber-tracked machines — Performance requirements and test procedures for braking systems*

ISO 5010:2007, *Earth-moving machinery — Rubber-tyred machines — Steering requirements*

ISO 6165, *Earth-moving machinery — Basic types — Identification and terms and definitions*

ISO 9533, *Earth-moving machinery — Machine-mounted audible travel alarms and forward horns — Test methods and performance criteria*

ISO 10265:2008, *Earth-moving machinery — Crawler machines — Performance requirements and test procedures for braking systems*

ISO 12100:2010, *Safety of machinery — General principles for design — Risk assessment and risk reduction*

ISO 19296, *Mining and earth-moving machinery — Mobile machines working underground — Machine Safety*[1)]

ISO 20474-1, *Earth-moving machinery — Safety — Part 1: General requirements*

1) Under preparation.

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO 6165, ISO 12100 and the following terms, definitions and abbreviated terms apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
autonomous or semi-autonomous machine system
ASAMS
machine and supporting systems and *infrastructure* (3.11) that enable the machine to operate in *autonomous mode* (3.3)

Note 1 to entry: An example of representative components of an ASAMS is shown in Figure 1. However, this document does not describe or provide detail for all the specific components identified in Figure 1.

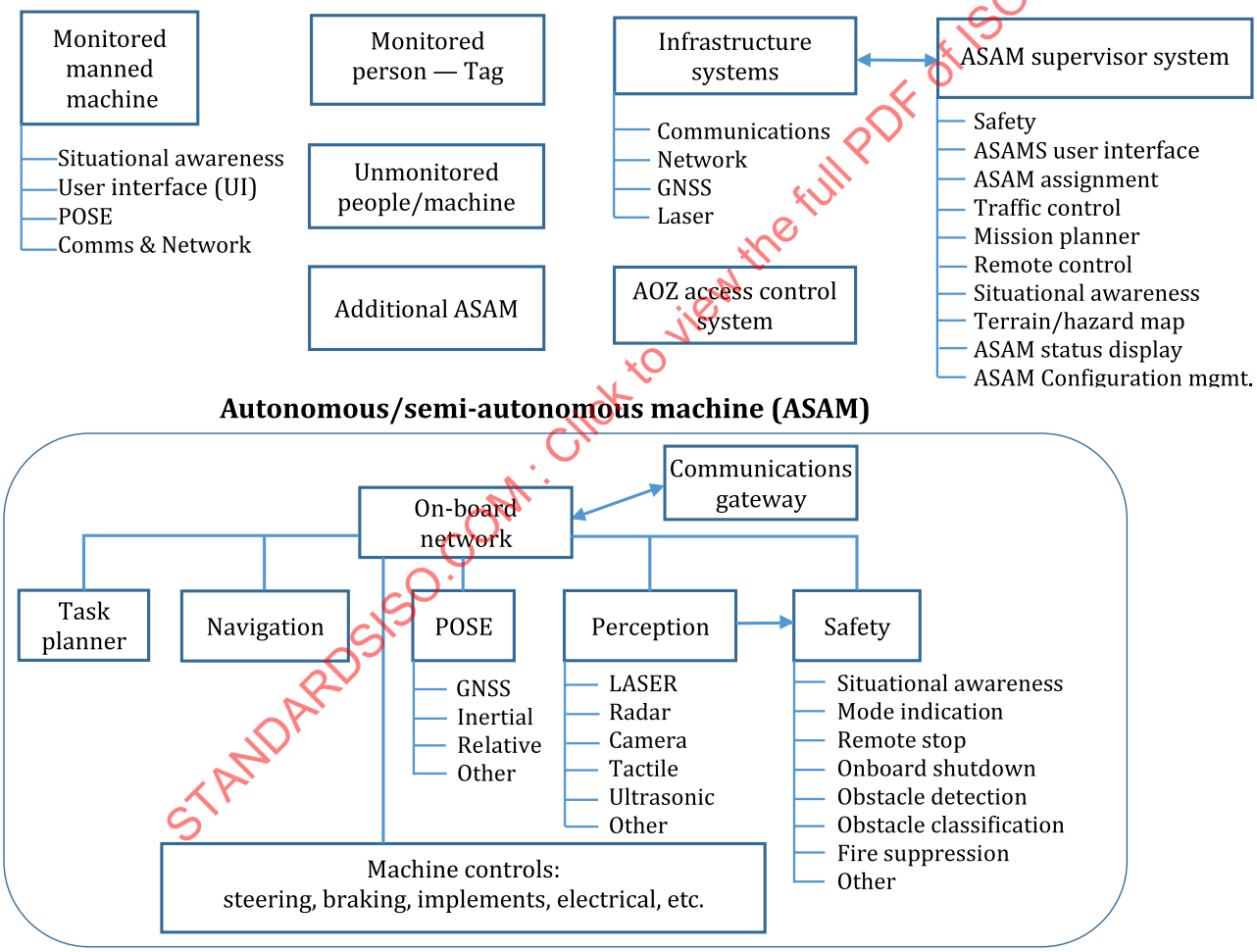

Figure 1 — Representative ASAMS components

3.2
autonomous or semi-autonomous machine supervisor system
ASAM supervisor system
system providing the primary user interface and "command and control centre" for operation in *autonomous mode* (3.3)

3.3
autonomous mode
mode of operation in which a mobile machine performs all machine safety-critical and earth-moving or mining functions related to its defined operations without operator interaction

Note 1 to entry: The operator could provide destination or navigation input, but is not needed to assert control during the defined operation.

3.3.1
autonomous machine
mobile machine that is intended to operate in *autonomous mode* (3.3) during its normal operating cycle

Note 1 to entry: The abbreviation "ASAM" is used throughout this document to refer both to autonomous machines and *semi-autonomous machines* (3.3.2) operating in autonomous mode.

3.3.2
semi-autonomous machine
mobile machine that is intended to operate in *autonomous mode* (3.3) during part of its operating cycle and which requires active control by an operator to complete some of the tasks assigned to the machine

Note 1 to entry: The abbreviation "ASAM" is used throughout this document to refer both to semi-autonomous machines operating in autonomous mode and *autonomous machines* (3.3.1).

3.4
autonomous operating zone
AOZ
autonomous area
designated area in which machines are authorized to operate in *autonomous mode* (3.3)

3.5
AOZ access control system
physical barrier or virtual or electronic system that monitors, authorizes and controls access, egress and transition of people and equipment between existing *autonomous operating zones* (3.4) and other areas

3.6
competent person
person who, in relation to the work undertaken, has the necessary knowledge, skill, training and experience to complete the work satisfactorily and without danger or injury to any person

[SOURCE: ISO 7240-19:2007, 3.1.5]

3.7
digital terrain map
DTM
topographical description of the site in digital format

3.8
function-specific automated feature
automated feature having a specific control function whereby the operator has overall control and is solely responsible for safe operation, but can cede limited authority over a manual control (e.g. grade control, auto-dig, antilock brakes, traction control)

Note 1 to entry: The feature can automatically assume limited authority over a machine function (e.g. electronic stability control).

3.9
halted state
condition in which all motion of a machine is stopped and an operator action is required to resume its operation

3.10
operator interaction
involvement of an operator to provide information to or control of an *ASAMS* (3.1), such as the transition between *autonomous mode* (3.3) and *manual mode* (3.13), or to provide any type of exception handling

3.11
infrastructure
work site equipment and facilities used in support of a machine's operation in *autonomous mode* (3.3)

EXAMPLE Communications network, solar power stations, GNSS base station, physical barrier systems.

3.12
layers of protection
independent processes or actions taken to prevent or address potential hazardous events leading to an unsafe consequence

3.13
manual mode
mode of operation in which a machine is controlled by an operator who is responsible for monitoring the surroundings and for safe operation of all machine controls

Note 1 to entry: Manually operated machines can have function-specific automated features.

3.14
approach mode
mode that allows access to the *ASAMS* (3.1)

3.15
mode indicator
means by which a machine shows whether it is in *manual mode* (3.13), *autonomous mode* (3.3) or remote-control mode

3.16
operator
system operator
person having control and responsibility for the operation of an *autonomous machine* (3.3.1) or a *semi-autonomous machine* (3.3.2) and the *ASAMS* (3.1)

3.17
remote-stop system
system that brings all *autonomous machines* (3.3.1) and *semi-autonomous machines* (3.3.2) within a defined range of a mobile stop device to a *halted state* (3.9) when initiated

3.18
all-stop system
system that brings all *autonomous machines* (3.3.1) and *semi-autonomous machines* (3.3.2) in the AOZ (3.4) to a *halted state* (3.9) when initiated

3.19
perception system
system comprising sensors used to detect, locate and recognize a potential feature of interest

3.20
remote control
operator control of a machine from a device not located on the machine

3.21
safe state
condition, whether or not an *autonomous machine* (3.3.1) or *semi-autonomous machine* (3.3.2) is operating or is shut down, such that a hazardous safety, health and environment event is at an acceptable level of risk based on a risk assessment

3.22
site manager
entity responsible for managing the entire work site, with overall responsibility for the operators and site operations

3.23
situational awareness
perception of elements in the environment, and a comprehension of their meaning, and could include a projection of the future status of perceived elements and the risk associated with that status

3.24
system integrator
entity responsible for design, installation and setup of the autonomous and semi-autonomous machine and system

3.25
risk assessment
overall process comprising a risk analysis and a risk evaluation

Note 1 to entry: See ISO 12100.

AOZ	autonomous operating zone
ASAM	autonomous or semi-autonomous machine
ASAMS	autonomous or semi-autonomous machine system
ECU	electronic control unit
ECM	electronic control module
GNSS	global navigation satellite system
IMU	inertial measurement unit
DTM	digital terrain map
UM	unmanned machine
POSE	positioning and orientation
RC	remote control

4 Safety requirements and/or protective/risk reduction measures

4.1 General

ASAMS shall comply with the safety requirements and/or protective/risk reduction measures of this clause.

A risk assessment process for ASAMS shall be completed according to the principles of ISO 12100. All identified risks shall be mitigated to acceptable risk levels as part of the risk assessment process. Annex B gives general information on risk assessment for ASAMS. The results of the risk assessment shall be formally documented.

Safety-related parts of control systems shall comply with the appropriate functional safety performance level. See, for example, ISO 13849, ISO 19014, IEC 62061 or IEC 61508.

The general safety requirements provided in ISO 20474 are applicable to earth-moving ASAM, and those given in ISO 19296 are applicable to underground mining ASAM. The requirements relating to an on-board operator where the machine is not equipped with an on-board operator's station do not apply.

4.2 Stop systems

4.2.1 General

All ASAM shall have a means to be stopped from a safe, remote distance.

4.2.2 All-stop system

If the ASAMS includes a remote ASAM supervisor system, that system shall have a means for the operator to stop all ASAM under his or her control: an *all-stop* system.

After an ASAM is stopped, operator intervention shall be required to restart machine motion.

The all-stop system performance criteria should be provided in the supplier's documentation.

The performance criteria should indicate the expected delay and maximum delay before the machine's braking system is activated.

4.2.3 Remote stop system

When risk assessment shows a need, ASAMS shall be equipped with an additional remote stop system which is distinct from the all-stop system specified in 4.2.2. The remote stop system shall enable a person to bring all ASAM within the required range (based on risk assessment) of the remote stop device to a halted state. Alternatively, the remote stop device may bring all ASAM in the AOZ to a halted state.

After a machine is stopped, operator intervention shall be required to restart machine motion.

The remote stop system performance criteria should be provided in the supplier's documentation.

The performance criteria should indicate the expected delay and maximum delay before the machine's braking system is activated.

4.3 Warning devices and safety signs

4.3.1 Visual indicators

The machine's operating mode shall be indicated. The indicators listed in Table 1 are recommended. An ASAM shall also have a means to indicate that the ASAM is in the approach mode, in which the ASAM will not move without on-board intervention.

Table 1 — Visual references

Mode	Light/pattern	Description/observation
Manual	Flashing green	Used to indicate that a machine is in manual mode. The manual indicator is included to ensure that there is always at least one indicator on an ASAM. If the manual light is not used, there shall be a method to diagnose failures of the other indicators.
Autonomous	Flashing blue	Indicates that an ASAM is operating in autonomous mode.

Where local practice does not allow these colours or patterns, all machines on an ASAMS site should use a consistent mode indication scheme. Where indicators are used, they shall be clearly visible so that the operating mode can be recognized a safe distance from the machine.

4.3.2 Audible alarms

ASAM should be capable of providing the same audible warnings that the work site is using for engine start, pre-movement and movement alarming on manned machines.

EXAMPLE The machine emits a configured number of horn blasts before undertaking a given action, a cyclic beeping pattern while moving.

If warning devices are provided, they shall be compliant with ISO 9533.

4.3.3 Safety signs

ISO 9244 applies for safety signs and warning labels.

4.4 Fire protection

A fire suppression system shall be provided if the risk assessment requires one. The means of its activation (i.e. automatically or remotely) shall be determined by the risk assessment.

4.5 Machine access systems

Access systems that comply with ISO 2867 shall be provided for all areas on ASAM that require access more frequently than every 30 days.

4.6 Braking and steering

4.6.1 General

The ability to maintain a safe speed and effective heading is a fundamental necessity for ASAM. With autonomous machines, electronic commands from the control system are used to control the brakes and steering system of the machine.

Because of the added complexity, additional safety criteria are necessary:

a) all ASAM shall have on-board capability to bring the machine to a stop;

b) when the ASAMS is operating within the specified operating environment, the control systems shall be able to cause the machine to brake while maintaining safe operation (e.g. braking under adverse conditions);

c) The ASAMS shall have provisions to ensure that safe operating temperatures and pressures in the braking and steering systems have been reached before the machine is put into operation in autonomous mode.

4.6.2 Braking

According to ISO 3450 or ISO 10265, the braking performance of a manned machine is measured from the time the on-board operator presses the brake pedal until the machine stops.

For an ASAM, the braking performance shall be measured from the time the on-board command is received by the machine brake subsystem until the machine stops.

The testing of the braking systems of wheeled ASAM shall meet the requirements of ISO 3450:2011, Clause 4, except where the requirements specifically apply to an on-board operator The warning device for stored energy sources specified in ISO 3450:2011, 4.9, shall alert the system operator.

The ASAMS shall maintain a safe state when a loss of brake stored energy is detected.

ISO 3450:2011, 4.12.2, which relates to the braking system and periodic verification instructions, applies for wheeled ASAM, except that manuals, labels or other means providing information on brakes shall be provided wherever the operator is located.

ISO 3450:2011, Clauses 5 and 6, apply for wheeled ASAM, except for ISO 3450:2011, 6.2, which is applicable only to those machines equipped with an on-board operator's station. Testing shall be carried out in both manual mode (on-board operator, when applicable) and autonomous mode. The measurement or reporting of control forces might not be necessary. The test report for a wheeled ASAM shall be in accordance with ISO 3450:2011, Clause 7.

The testing of the braking systems of crawler ASAM shall meet the requirements of ISO 10265:2008, Clause 4, except ISO 10265:2008, 4.2. The warning device for exhaustible energy sources specified in ISO 10265:2008, 4.4, shall readily attract the operator’s attention — independent of where the operator is physically located.

ISO 10265:2008, Clause 7, which relates to the braking system and periodic verification instructions, applies for crawler ASAM, except that manuals, labels or other means providing information on brakes shall be provided wherever the operator is located.

ISO 10265:2008, Clauses 5, 6 and 7, apply to crawler ASAM, except for the control forces described in ISO 10265:2008, 6.1.3, applicable only to those machines equipped with an on-board operator’s station. Testing shall be carried out in both manual mode (on-board operator, when applicable) and autonomous mode. The measurement or reporting of control forces is only applicable to machines equipped with an on-board operator’s station. The test report for the crawler ASAM shall be in accordance with ISO 10265:2008, Clause 8.

The braking systems of mobile mining ASAM working underground shall be in accordance with ISO 19296, except where the requirements specifically apply to an on board operator.

4.6.3 Steering

The steering systems of wheeled ASAM shall be in accordance with ISO 5010, with the following exceptions/modifications.

a) The general requirements of ISO 5010:2007, 4.1.1, 4.1.2 and 4.1.10, apply only to machines equipped with an on-board operator's station, with the exception of ISO 5010:2007, 4.1.1.3 and 4.1.1.4, which shall apply regardless of whether or not an on-board operator's station is present.

b) The steering control priority requirements of ISO 5010:2007, 4.2.1, only apply to manually operated machines. For ASAM operating in autonomous mode, the conventional steering wheel might not have any priority or ability to steer the machine while in autonomous mode, and this exception should be clearly explained in the operator’s manual.

c) The ergonomic requirements of ISO 5010:2007, Clause 5, apply only to machines equipped with an on-board operator's station.

d) The performance requirements of ISO 5010:2007, 6.4, apply to ASAM; those of ISO 5010:2007, 6.1, 6.2 and 6.3 apply only to machines with an on-board operator's station.

   In addition, the ASAMS shall alert the operator when any electronic steering system component has failed or is unable to maintain safe operation.

e) The provisions for steering tests given in ISO 5010:2007, Clause 10, apply, except for those of ISO 5010:2007, 10.3.1 and 10.3.7; the recording of the steering effort specified in ISO 5010:2007, 10.2.3 and 10.3.7, is not necessary for ASAM.

f) Replace ISO 5010:2007, 4.3, with the following requirement: In the case of a single electronic control system failure on the ASAM steering controller, the ASAM shall maintain a safe state as specified by the risk assessment of the ASAMS.

The ASAMS shall have a provision for periodically checking the steering capability. The check period and method (automatic or manual) shall be based on the risk assessment. If the steering system does not meet the steering performance requirements, then ASAM operation (e.g. speed, slope, load, autonomous mode) shall be limited to maintain a safe state.

This periodic check of the steering systems may be carried out by either the ASAMS or the operator.

4.7 Adaptation to environmental conditions

Based on the risk assessment, the ASAMS shall be capable of adapting to environmental conditions as long as any changes in the environmental conditions are within identified constraints. These may include the use of human operators or automated systems to make speed adjustments, disable operations, close off areas or other adjustments as needed to maintain safe operation.

4.8 On-board electrical power

4.8.1 General

The on-board autonomy electronics of ASAM can place additional demands on the machine system beyond the needs of a non-autonomous machine. It is particularly important that the ASAMS manufacturer or integrator considers these extra electrical power needs.

4.8.2 Requirements

ASAM electrical and electronic systems shall conform with the general machine requirements for electrical and electronic systems in ISO 20474-1 or ISO 19296, as applicable.

Any sudden loss of electrical power to the machine electronics can lead to an undesirable and potentially hazardous outcome. ASAM shall have the capability to respond to electrical system failures, including the loss of electrical (supply) power to all controllers (ECM, ECU) that affect machine motion.

The electrical power source shall be capable of maintaining the power to the machine's systems in order to achieve a halted state and maintain a safe state.

ASAM shall have an adequate source of electrical power during operation in autonomous mode, including

a) sufficient battery reserve for the intended environmental conditions,

b) sufficient alternator capacity for additional autonomy related electronics, and

c) sufficiently gauged wiring for increased current carrying capability.

ASAM shall have sufficient reserve battery capacity to maintain all machine electronics, with the machine's engine off or when the alternator is not generating power, to maintain a safe state and complete an orderly shut-down of the machine for all intended environmental conditions.

When machine electrical power is unintentionally lost while operating, the ASAM shall maintain a safe state and, if required by risk assessment, should go to a halted state.

The ASAM shall have sufficient electrical capacity to support the additional loads required by the autonomy electronics (in addition to general machine requirements) for all intended operating and environmental conditions (e.g. low idle, night time).

5 Positioning and orientation (POSE)

5.1 General

The positioning and orientation (POSE) systems used by ASAM can include a wide variety of technologies, including GNSS, pseudolites, theodolites, IMUs, speed sensors, inclinometers, laser scanners, radar, wireless triangulation and vision systems. Each of these technologies can have unique characteristics. The requirements will also depend on the application. The positioning and orientation accuracy or measurement frequency required from such systems also depends on the machine's speed and location.

5.2 Risk and failure modes

The risks associated with incorrect POSE of the machine include collisions with other machines, damage to the ASAM or site damage due to erroneous navigation, lack of a situational awareness layer of protection and the creation of incorrect operational digital terrain models.

The failure modes for POSE systems include

a) inaccurate absolute position for systems that use a global coordinate system,

b) inaccurate relative position for systems that use a local coordinate system,

c) inaccurate orientation,

d) inaccurate registration to the digital terrain model, and

e) non-existent position, orientation or registration.

5.3 Requirements

The POSE systems of the ASAM shall have the means to detect the system status, e.g. measurement error probability, precision, resolution.

When the system status is not sufficient for positioning with the required precision and accuracy, which can change dynamically depending on the state of the ASAMS, the ASAM shall maintain a safe state.

The ASAMS should have sufficient independent means of detecting POSE to ensure that the ASAM can maintain a safe state in the event of a failure or deterioration of one positioning means.

6 Digital terrain map (DTM)

6.1 General

In applications where a digital terrain map (DTM) is used to maintain safe operating conditions, its validity should be monitored.

The ASAMS shall maintain a safe state in the event of insufficient accuracy of the DTM. Such failures and deteriorations can include

a) loss or deterioration of the accuracy of the DTM, its accuracy deteriorating due to road or site weathering, the altering of roads or other site work,

b) the DTM not being properly calibrated or aligned with the existing terrain, and

c) an obsolete version of the DTM being loaded or active on the ASAM.

NOTE The ASAM might not be able to respond to sudden terrain changes.

6.2 Requirements

In applications where a DTM is used to maintain safe operating conditions and is mapped by the ASAMS, the state of the POSE system shall be monitored during terrain map creation or area survey. The accuracy or accuracy state of the POSE system should be noted during any mapping to ensure that the map data are properly weighted during DTM creation and validation.

7 Perception

7.1 General

A perception system comprises perception sensors used to capture information about the ASAM's surroundings and then pass the information to algorithms for detecting, localizing and recognizing (classifying) a potential feature of interest. The purpose of the machine perception system is to provide the information necessary for the safe control of the machine, without the need for operator interaction.

If testing and calibration capability is required to ensure that the perception system is operating to system requirements, the ASAMS integrator shall provide such a capability.

7.2 Risk and failure modes

7.2.1 Failure to detect or late detection of an object

Examples of failure to detect an obstacle or late detection of an object are

a) objects occluded due to dust, fog, snow, rain or other obscurants,

b) perception results becoming unreliable due to poor lighting conditions,

c) obstacles hidden due to tilting of the ASAM,

d) uneven ground causing the scanning plane to vary, e.g. the laser beam could hit the ground or point to the sky when the machine is pitching down or up,

e) machine vibration or motion causing the misalignment of sensors,

f) objects moving too fast to be detected,

g) objects too small or not reflected back in the direction of the receiver — for example, the ability of the radar technology to identify an object might depend on the object's effective radar cross-section,

h) transparent or dark objects not reflecting the laser beam,

i) negative objects (holes in the terrain) not being detected, and

j) an increase in latency due to other applications or computation loading on the processor used for the object detection or classification system.

7.2.2 False detection of non-existent object

Examples of false detection are

a) dust or other obscurants reflect enough energy to be classified as an object, and

b) material on the transmitter or receiver is erroneously detected as objects.

7.2.3 Erroneous location of a detected object

Examples of erroneous location are

a) sensor misalignment causing inaccurate position estimate,

b) POSE system errors causing inaccurate machine position or orientation, and

c) vibration of the sensor mounting causing sensor motion that is not accounted for by the perception system, and

d) dust or obscurants blurring the edges.

7.2.4 Misclassification of an object

Examples of misclassification of an object are

a) dust or obscurants blurring the edges, and

b) inadequate training or validation of the classifier.

7.3 Requirements

a) System requirements of an on-board ASAM or ASAMS perception system shall be based on the risk assessment, the machine's characteristics (e.g. speed, visibility, normal operation) and the operating terrain (e.g. surface, underground, open area, tunnel).

b) The perception system shall maintain the safe state of the ASAM during any interaction with its intended operating environment (e.g. terrain, dust, weather conditions, lighting conditions).

c) The perception system shall be capable of detecting objects in the required area (e.g. the expected travel path) that are on either a positive or negative slope as required based on the risk assessment.

d) The ASAMS shall be capable of detecting when the perception system is not functioning to the minimum requirements based on the risk assessment and maintain the machine in a safe state.

e) When the perception system in not functioning properly, the operator or ASAM supervisor system should be notified.

f) When required, based on the risk assessment, the operational limits of the perception system shall be stated in the user manual, e.g. target size, shape and reflectivity, perception range, angular coverage.

8 Navigation system

8.1 General

The ASAM's navigation system can use either the absolute position or relative position of the ASAM to navigate a predetermined or dynamically determined path to meet the objectives of the ASAMS. System requirements will depend on the application and the risk assessment. The navigational accuracy can also depend on factors such as the machine's speed and location.

8.2 Risks

The risks associated with navigation of the ASAM include collisions with other machines, infrastructure and humans in the AOZ or damage to the ASAM. These can result from inaccurate POSE information, incompatible coordinate systems, imprecise navigation control, poor planning or an inaccurate DTM.

8.3 Requirements

a) The requirements relating the POSE system and DTM are covered in the POSE and DTM sections of this document.

b) ASAMS shall have the ability to maintain a safe heading and velocity when operated in accordance with their specified operating environment and conditions.

c) When operating within its specified environment, an ASAM navigation system shall have the means to detect that it is not meeting the specified requirements for the ASAM status and environment.

d) If the system status is not sufficient for meeting the required accuracy (this can be a dynamic requirement depending on the state of the ASAMS), the ASAM shall take action to maintain a safe state.

e) The operator should be notified of any errors in the navigation system that could lead to unacceptable risk as defined by the risk assessment.

f) All paths or areas used by ASAM shall be validated to ensure they are safely traversable under all reasonably expected operating conditions. Validation may be completed by either ASAMS or by a competent person.

9 Task planner

9.1 General

The function of task planners used by ASAMS varies significantly, depending on the type of machine and its application. This clause defines risks and provides general requirements for task planners.

9.2 Risks

a) The primary risk associated with the task planner is that the planner could direct the ASAM to go somewhere where it should not, e.g. traverse a non-existent or hazardous path.

b) The secondary risk of the task planner is that the planner could direct the ASAM to go somewhere it can cause a hazardous consequence, such as

— extracting material from a stockpile or load out point in a manner that creates a sudden or unexpected flow of material,

— extracting material in a manner that undercuts material under other machines or structures, or

— dumping material in a manner that causes a hazard to other machines or personnel, e.g. an autonomous dragline directed to dump material on top of adjacent machines.

9.3 Requirements

a) Based on the application, task planner requirements and the risk assessment itself, all risks shall be noted and mitigated as part of the risk assessment process.

b) The task planner shall avoid directing the ASAM onto a known hazardous path. The hazard level of the path may be determined either by the ASAMS or humans interacting with the ASAMS or some clearly defined combination of the two. If the ASAMS is responsible for determining the hazards

associated with a path, then the ASAMS shall be able to determine all reasonably anticipatable hazards and have a means to inform the task planner of the detected hazards.

The task planner shall not direct the ASAM to create hazardous conditions, e.g. extracting material from a stockpile in a manner that causes an unexpected flow of material, dumping material in a manner that causes a hazard to other machines.

10 Communications and networks

10.1 General

ASAMS can rely significantly on communications. Some design considerations include industry standards, system bandwidth and wireless coverage. Included in the bandwidth consideration will be the requirements for support machines and operator interaction. An important operational issue is the need to be aware of areas of potentially high levels of interference (e.g. queuing locations).

10.2 Risk and failure modes

10.2.1 Risks

Communications and network failures can result in the following safety risks:

a) the inability to stop the machine remotely or in an emergency,

b) a lack of access to situational awareness information,

c) inaccurate terrain data,

d) lost or delayed command input,

e) insufficient intersection control,

f) loss of machine coordination,

g) loss of derate information,

h) lost or delayed hazard information,

i) inaccurate position (due to loss of GNSS correction),

j) inaccurate planning information,

k) inaccurate personnel tracking, and

l) loss of remote ability to activate the fire protection system.

10.2.2 Failure modes

Communications-related failure modes include

a) loss of communications,

b) degraded communications, including losing one direction,

c) delayed communications,

d) misdirected communications,

e) altered communications, and

f) out-of-sequence communications.

10.2.3 Potential causes

Failure modes can be a result of any of the following:

a) noise issues (unintentional jamming);

b) network physical changes;

c) network configuration changes;

d) hardware issues;

e) environmental issues, e.g. weather-related, sun spots;

f) changing topology;

g) power issues;

h) intentional hacking or spoofing;

i) intentional jamming.

10.3 Communication systems requirements

10.3.1 Communication security

The ASAMS shall maintain safe operation in the event of any communications-related failure. Where risk assessment shows the need, ASAMS shall have a fail-safe means (e.g. via active monitoring, multiple independent communications channels) to remotely stop and maintain a safe state.

Where required by the risk assessment, ASAMS shall have a means of detecting a loss of communications, degraded communications or corrupted communications. This shall cover both single-direction and bi-directional loss of communications. Degraded communications can include dropping packets or out-of-sequence packets. The machine shall have means of activating a controlled stop and shall maintain a safe state in the event of lost, corrupted or delayed communications. The machine speed and current operating environment should be used in combination with the risk assessment to determine the maximum acceptable duration of a loss of communications or degraded communications.

10.3.2 Communication security

Means shall be provided to deter unauthorized control and spoofing or sabotage of the ASAMS. The acceptability of such means needs to be determined based on the risk assessment. Suitable means include restricting physical access, authentication, use of a firewall, data encryption and restricting external connection off the site.

10.4 Safety messages

Machines that operate in an AOZ should be managed on networks using the same communication protocol and should share the communication of safety-critical messages.

The following messages are considered to be safety-critical and shall be communicated as required by the risk assessment:

a) start-up warnings on an emergency channel;

b) performance parameters of network connection, e.g. quality of service,

c) positional and situational information, e.g. machine POSE and operation mode;

d) the site map.

Both the coverage (the required recipient and range) and frequency of the required messages should be specified. Elements of a networking protocol suite within the scope of network configuration include physical layer, protocol layer, application layer and content layer.

11 ASAM supervisor system

11.1 General

Supervisor systems contain sub-systems such as

a) ASAMS user interface and display,

b) ASAM assignment,

c) traffic control systems,

d) mission planner,

e) remote control,

f) situational awareness,

g) terrain / hazard map management,

h) ASAM status display, and

i) ASAM configuration management.

The risks associated with supervisor system error include wrong assignment, the human operator sending an incorrect command to an autonomous machine, operation using an incorrect/mismatched terrain map/operational area map or the use of incorrect machine parameters (dimensions, slope angles, etc.). The causes can be human error, hardware or software (system) failure, data corruption or supervisory system outage (e.g. computer freeze, loss of power).

11.2 Requirements

If the ASAMS includes a remote ASAM supervisor system, the following applies.

a) The ASAM supervisor system shall be able to communicate with any machines in the AOZ if required by the risk assessment.

b) The ASAM supervisor system shall periodically verify communication with the autonomous machines under its control. If communication is not verified, the ASAM supervisor system shall take the appropriate action, based on the risk assessment.

c) In the event of a control room outage, all autonomous machines shall maintain a safe state.

d) If required, based on the risk assessment, redundant systems shall be provided:

   — reserve or back-up power for control room;

   — backup storage of the terrain map or other safety critical data;

   — failover capability.

12 AOZ access, permissions and security

12.1 Permissions and security

Based on the risk assessment, administrative or engineering controls shall be established to prevent unauthorized access to the AOZ and manage exit from the AOZ.

When required based on the risk assessment, each machine and person operating in the AOZ shall be monitored or escorted by a monitored person or vehicle. The following parameters should be taken into account by the risk assessment:

— the monitored person, vehicle and machine position and accuracy;

— the monitored person, vehicle and machine heading and velocity;

— the minimum separation distance between the monitored person or vehicle and an ASAM;

— the maximum separation distance from the monitored vehicle or person and monitored escort;

— the destination;

— the expected duration in the AOZ.

Means shall be provided to deter unauthorized access and control to the ASAMS. Acceptable means need to be determined based on the risk assessment

EXAMPLE Restricting physical access, user authentication.

12.2 AOZ access and warnings

A clear visual indication of the AOZ shall be provided at each designated entry and exit point. If an AOZ access control system (see Annex D) is used, then it should be monitored and appropriate action, based on the risk assessment, should be taken in case of failure.

12.3 Operational risks

Risk factors to consider as part of a comprehensive risk management strategy (see Annex B) for any ASAMS include

a) access into the AOZ by unauthorized personnel or equipment,

b) ergonomics or human factors that can lead to unexpected switching of operational mode with loss of control,

c) improper capture of changes to work areas, especially before switching work areas between manual and autonomous,

d) incomplete or improper system updates and changes to programming,

e) improper road design, area demarcation or other human errors,

f) natural phenomena,

g) malicious attacks, and

h) operational errors caused by poor integration with infrastructures or other existing systems.

12.4 Mode changes

Special care should be given to mode change events. A means to prevent mode changes that could result in an unsafe condition (e.g. unintentional, unexpected or unauthorized actions) shall be provided (e.g. physical switch, PIN system). The mode change procedure should consider the following:

— having the ability to physically disable all autonomous functions with a lockout process;

— having the capability to engage the autonomous mode from a safe position;

— preventing change to/from autonomous mode caused by a single human error.

13 ASAMS site operating procedures

13.1 General

Supervisory and operating personnel shall be instructed about system functionality and specific tasks to be undertaken, including the hazards and risks, the controls to be applied, and the job steps necessary to complete the tasks safely and correctly.

See Annex C for additional site planning information.

See Annex F for information on supervision.

13.2 Incident recording

Safety-related incident data shall be stored and recoverable.

NOTE Local or national regulations can exist that require incidents to be reported.

13.3 Commissioning

Commissioning for ASAMS should address the items presented in Annex G.

13.4 Documentation and training

Operators and supervisory personnel shall have the information and training necessary to complete tasks safely. Such information includes

— manuals, specifications and operating instructions provided by the system integrator,

— the operation's policies, procedures and plans, and

— applicable legislation, national and international standards, and other guidance material.

13.4.1 Documentation

The system integrator shall provide training documentation.

Operating procedures and processes (e.g. jobsite organization) for the ASAMS site shall be developed and implemented by the site manager, considering Annex C, Annex F and Annex G and the site risk assessment.

Instructional tools such as safe work instructions or procedures and standard operating procedures (SOP) should be used to document the ASAMS site operating procedures and should be reviewed and amended if there are any changes (e.g. equipment, conditions).

If there is to be a deviation from the safe work procedures, a job safety or hazard analysis should be undertaken to capture the hazards for the task and ensure that adequate controls are implemented.

The necessary documentation (user manual) for machine parameter setting or configuration shall be provided. This documentation should include known operational limitations.

It is recommended that instructional tools be formally approved by the supervisor or management.

13.4.2 Training

Personnel who interact with the ASAMS shall be trained to understand system functionality and specific tasks to be undertaken, including the hazards and risks, the controls to be applied, and the job steps necessary to complete the tasks safely and correctly. They shall successfully demonstrate understanding before working without supervision.

Training shall cover the various levels of operation in autonomous mode based on the job skills required, including training for ASAMS operators, support machine operators, supervisory personnel. Anyone entering the AOZ should receive the required training or be escorted.

Personnel who interact with ASAMS should understand the effects that their activities can have during commissioning, operation and maintenance of the ASAMS system. They should also understand

a) what to expect if environmental or operational conditions change,

b) site requirements for monitoring of machine performance,

c) how to recognize and take appropriate action when machines are not operating as intended, and

d) how to report incidents.

Assessment of competency should be evidence-based and verified before work commences. Methods for verification of competency include

— recognition of prior learning,

— on-site recognition or validation of current competency, or

— using the operation's training and development program.

Verifications of competency should include a documented assessment.

Whenever work procedures or plant and equipment change, there should be a process to ensure affected personnel are consulted, retrained as necessary and reassessed.

14 Operational hazard controls

Any additional personal protective equipment (PPE) required by the ASAMS shall be documented by system integrator.

The design and function of operational practices should adequately address matters such as those listed in Annex H.

15 Verification of safety requirements and/or protective/risk reduction measures

Either one or a combination of the following means shall be used to verify that the requirements of this document have been incorporated in the design and integration of the ASAMS:

a) measurement;

b) visual examination;

c) testing and analysis or simulation, as appropriate;

d) by assessment of the supplier's documentation of measurement, visual examination or testing.

16 Information for use

16.1 Safety labels and machine markings

Safety labels and machine markings shall meet the requirements of base machine safety standards such as ISO 20474-1 and ISO 19296.

16.2 User manual

The system integrator

a) shall provide information on ASAM and ASAMS operations (see ISO 6750 for guidance),

b) shall provide guidance on the range of environmental conditions in which the ASAMS is intended to operate, and

c) should provide guidance for operating within the range of environmental conditions.

Annex A
(informative)

List of significant hazards

The general hazards, hazardous situations and events are dealt with in ISO 20474-1 and ISO 19296. The specific risks for ASAMS are covered within the sections of this document as outlined in Table A.1.

Table A.1 — Additional hazards for autonomous machine systems

No.	Hazard	Subclause
1	**Mechanical hazards due to**	
1.1	Extraction of material from a stockpile or load out point in a manner that causes a sudden or unexpected flow of material	9.2
1.2	Extraction of material in a manner that undercuts material under other machines or structures	9.2
1.3	Dumping of material in a manner that causes a hazard to other machines or personnel	9.2
2	**Electrical hazards due to**	
2.1	Loss of electrical power	4.8.1, 4.8.2
3	**Navigational hazards due to**	
3.1	Loss or deterioration in the accuracy of the DTM	6.1
3.2	The DTM not being properly calibrated or aligned with the existing terrain	6.1
3.3	An obsolete version of the DTM loaded or active on ASAM	6.1
3.4	ASAM directed to go somewhere it should not	9.2
4	**Collision hazards due to**	
4.1	Inaccurate absolute position	5.2, 5.3
4.2	Inaccurate relative position	5.2, 5.3
4.3	Inaccurate orientation	5.2, 5.3
4.4	Non-existent position, orientation or registration	5.2, 5.3
4.5	Collisions with other machines and damage to the ASAM or site damage caused by erroneous navigation	8.2
4.6	Inaccurate personnel tracking	10.2.1
5	**Navigation and collision hazards due to**	
5.1	Failure to detect or late detection of an object	7.2.1
5.2	Objects occluded due to dust, fog, snow, rain or other obscurants	7.2.1
5.3	Perception results unreliable owing to poor lighting conditions	7.2.1
5.4	Obstacles hidden owing to tilted ASAM	7.2.1
5.5	Uneven ground causing scanning plane to vary	7.2.1
5.6	Machine vibration or motion causing misalignment of sensors	7.2.1
5.7	Objects moving too fast to be detected	7.2.1
5.8	Objects too small or which do not reflect back in the direction of the receiver	7.2.1
5.9	Transparent or dark objects not reflecting laser beam	7.2.1
5.10	Negative objects (holes in the terrain) not detected	7.2.1
5.11	Increased latency caused by other applications or computation loading on the processor being used for the object detection or classification system	7.2.1
5.12	False detection of non-existent objects	7.2.2
5.13	Dust or other obscurants reflecting enough energy to be classified as objects	7.2.2

Table A.1 *(continued)*

No.	Hazard	Subclause
5.14	Material on the transmitter or receiver erroneously detected as objects	7.2.2
5.15	Erroneous location of a detected object	7.2.3
5.16	Sensor misalignment causing inaccurate position estimate	7.2.3
5.17	POSE system errors causing inaccurate machine position or orientation	7.2.3
5.18	Vibration of the sensor mounting causing sensor motion not accounted for by the perception system	7.2.3
5.19	Dust or obscurants blurring edges	7.2.3, 7.2.4
5.20	Misclassification of an object	7.2.4
5.21	Inadequate training or validation of the classifier	7.2.4
5.22	Inability to stop the machine remotely or in an emergency	10.2.1
5.23	Lack of access to situational awareness information	10.2.1
5.24	Inaccurate terrain data	10.2.1
5.25	Lost or delayed command input	10.2.1
5.26	Insufficient intersection control	10.2.1
5.27	Loss of de-rate information	10.2.1
5.28	Inaccurate position (due to loss of GNSS correction)	10.2.1
5.29	Inaccurate planning information	10.2.1
5.30	Access to AOZ by unauthorized personnel or equipment	12.3
5.31	Ergonomic or human factors that can lead to unexpected switching of operational mode with loss of control	12.3
5.32	Improper capture of changes to work areas, especially before switching work areas between manual and autonomous	12.3
5.33	Incomplete or improper system updates and changes to programming	12.3
5.34	Improper road designs, area demarcation, or other human errors	12.3
5.35	Natural phenomena	12.3
5.36	Operational errors caused by poor integration with infrastructures and other existing systems	12.3
6	**Thermal hazard due to**	
6.1	Loss of remote ability to activate the fire protection system	10.2.1

Annex B
(informative)

Safety and the risk management process

B.1 Overview

ASAM can introduce hazardous situations not normally encountered on a conventional manned worksite.

The effective management of the risks associated with operating an ASAMS requires input from the system integrator, system operator and site manager, and potentially from diverse operational groups, ranging from system integrator, researchers, design engineers, project managers, team leaders and control room operators to safety and health representatives and other workers involved in the tasks, as well as emergency response personnel.

The risk management process should respond to the following questions:

— What are the potential scenarios for ASAMS incidents?

— What are their potential consequences in terms of safety and health?

— What controls are available and how effective are they?

Effective risk assessment for ASAMS may also require input from other subject-matter experts.

Information for risk management

Mining and earth-moving operations should be able to demonstrate that the hazards associated with ASAMS are being controlled so far as is reasonably practicable by considering issues such as

— any previous events or information (e.g. incident and injury reports, data from similar technology applications),

— reliability, maturity and available safety features of ASAMS,

— provision and frequency of validation processes (e.g. trials, functionality testing),

— suitability of established work procedures (e.g. separation, inspection and maintenance processes),

— whether established emergency procedures are sufficient,

— the provision and competency of operational and support personnel (e.g. assessment of knowledge and training needs), and

— identification of specific risks and provision for regular reviews of controls.

B.2 Risk identification

The use of autonomous technology in an operating worksite environment necessitates changes in established safety systems. It is important to identify these changes and the associated risks.

Hazard identification systems that can be implemented to ensure ASAMS risks are identified include

— hazard and operability study (HAZOP),

— layers of protection analysis (LOPA),

— functional safety analysis,

— change management,

— employee hazard identification and reporting procedures,

— workplace inspections,

— monitoring the working environment,

— incident investigations (e.g. ICAM, Taproot),

— monitoring (OEM) bulletins, recommendations and specifications, and

— regulators safety alerts.

Additional ASAMS risks are listed in Annex A.

B.3 Risk analysis

At the risk analysis stage, the nature of the risk is assessed and the risk level is determined. Factors to consider include

— the likelihood of an incident, and

— the potential severity of any injury or damage.

It is important that those undertaking the risk assessment have the necessary information, training, knowledge and experience of

a) the operational environment (e.g. scale, complexity and physical environment of mining activities),

b) the operational processes (e.g. maintenance systems, work practices, interaction, separation), and

c) the ASAMS (e.g. functionality, safety features)

involved.

B.4 Risk evaluation and management

All ASAMS hazards identified will need to be controlled. This is accomplished by applying a hierarchy of control. Higher-order control measures eliminate or reduce the risk more effectively than administrative controls or PPE.

Primary and contingency controls

For ASAMS, it is advisable to implement the following:

a) **primary controls**, which

   1) avoid the risk by determining whether or not to start or continue with the activity (e.g. cease operations during adverse weather),

   2) remove the source of the risk (e.g. isolate or provide alternative access for personnel not directly involved with the autonomous activity),

   3) change the likelihood (e.g. restrict specific functions to authorized personnel), and

   d) change the consequence (e.g. modify route, decrease speed);

b) **contingency controls**, which minimize the effects in case of an incident (e.g. layers of protection, systems that fail to the safe state).

Prevention and management controls

Prevention and management controls should be based on established processes and relevant standards by including

— safe design, construction and installation (according to specifications and design parameters),

— separation of the autonomous fleet from manned operations where possible,

— effective change management processes,

— operational and maintenance safe work procedures,

— competency-based training and assessment of workers, and

— supervision and management oversight.

B.5 Communication and consultation

Communication and consultation are fundamental for producing the most effective risk management. It is most essential that those with knowledge of the design, engineering, commissioning, operation and maintenance of the autonomous mining systems be involved in assessing and minimizing associated risks during the operational life cycle.

B.6 Monitoring and review

To ensure that the effectiveness of controls is maintained at the site, a monitoring and review programme should be implemented that includes control audits, verification and validation.

As part of the site's validation process, responsibilities and accountabilities should be clearly defined and assigned, and can include independent auditing. The findings should be used to

a) confirm that the recommendations of previous reviews have been actioned,

b) confirm that appropriate responses have been made to any incidents or issues arising,

c) verify compliance with specifications (e.g. inspection, monitoring, quality control), and

d) recommend any necessary operational or system design modifications, which are documented and managed through a formal change management process.

B.7 Documentation

The results of the risk assessment include

— locations of autonomous operating areas,

— size and complexity of operations,

— types of potential incidents,

— consequences and likelihood of each incident,

— controls used to mitigate each risk to a practicable minimum, and

— monitoring and reviewing outcomes and actions.

This information will form the basis of a site's ASAMS safety management plan.

Annex C
(informative)

Integration of ASAMS into the site planning process

C.1 Overview

The introduction of an ASAMS is typically a staged process that takes time to design and implement. ASAMS are complex systems, owing to the complexity of the processes themselves, their relation to people and the layers of safety that need to be built into them.

Work site operators should carefully evaluate *why* they wish to automate. They should evaluate their worksite design and undertake a comprehensive risk assessment of the processes with support from site representatives and subject-matter experts in order to satisfy regulators that there are sufficient and robust controls. Controls should seek to

a) minimize the start-up risks with new plant (e.g. "start simple and small" and gradually build up capacity), and

b) create an AOZ where ASAM and ASAMS are isolated or interactions with conventional, manned machines are managed (e.g. consider the implications for site design, plans and schedules).

Supporting infrastructure and area requirements should be identified early in the project, as automation systems can have specific needs (e.g. fuelling facilities, control rooms, communications network).

C.2 Principles

The following fundamental principles should be built into site design and planning processes:

a) risk management;

b) designing and planning for ASAMS;

c) managing and minimizing interaction;

d) autonomous infrastructure.

C.3 Risk management

Risk can be effectively addressed by applying the hierarchy of control. Mining operations should be able to demonstrate that the hazards associated with ASAMS are being controlled so far as is reasonably practicable. The introduction of autonomous mining systems is an opportunity, at the design stage, to adopt higher-order control measures that eliminate or reduce risks more effectively than administrative controls or PPE.

When considering the introduction of automation, the safety and risk management process described in Annex B should be used.

C.4 Designing and planning for autonomy

Site designers and planners should understand both the benefits and limitations of any technology being considered, including

a) the application of engineering and system controls to safety processes and practices,

b) modification of established planning and operational processes,

c) verification of system data (e.g. surveys) to validate site designs and plans,

d) the adaptability of planning and operational personnel, and

e) the application of positive outcomes to non-autonomous operations.

C.5 Managing and minimizing interactions

Site designers and planners should ensure work area design and construction are compatible with autonomy and minimize interaction with personnel and non-autonomous equipment, taking into account the following:

a) access controls and processes for exclusion and interface areas;

b) traffic management (e.g. road network, intersections, park-ups, load and dump locations;

c) placement within the autonomous area of infrastructure such as

- fuel facilities,
- crushers or ore passes,
- stockpiles,
- workshops and service areas,
- crib rooms, and
- services (e.g. electrical reticulation, dewatering bores).

C.6 Autonomous infrastructure

The design, location and integration of autonomous infrastructure should consider the following:

a) equipment specifications, fleet size and system capabilities (e.g. turning circle, road network layout, gradient);

b) communication systems (e.g. wireless, fixed);

c) autonomous signage and delineation.

Annex D
(informative)

Access control systems

D.1 General

The purpose of an access control system is to

a) prevent people from entering into the autonomous area, and

b) prevent ASAM from exiting the AOZ whether in a controlled or uncontrolled manner.

Access control systems can contain one or more of the following for protecting against or preventing people or equipment from entering an area where autonomous or semi-autonomous machines are operating:

— light curtains;

— laser beams;

— mechanical guards;

— physical chains and signs;

— geo fences;

— video imaging;

— tag-based technologies.

D.2 Hazards associated with access control systems

The following hazards are associated with the operation of machines operating in autonomous mode and should be considered during design and implementation, and when determining requirements for the access control system:

— undetected entrance after the access control is armed causing a hazard inside the AOZ,

— emergency situation requiring egress by persons through an autonomous area, and

— malfunction of ASAM crossing the access control and causing a hazard outside the AOZ.

An appropriate risk assessment should be completed to identify the risks associated with the access control system.

D.3 Mechanical barriers

In selecting an appropriate safeguard for a particular type of machinery or hazard zone, it needs to be considered that a fixed guard is simple and should be used where the access of an operator into a hazard zone is not required during the normal operation (operation without malfunction) of the machinery (from ISO 12100:2010, 6.3.2; see also ISO 12100:2010, 6.3.3).

D.4 Decision to use access control systems

The decision to use an access control system or other safety systems for the AOZ should be made on the basis of the risk assessment (see ISO 12100), and based on

a) machine characteristics (e.g. speed, visibility, normal operation),

b) operating environment (e.g. surface, underground, open area, tunnel),

c) frequency of changes to the hazard zone,

d) size of the danger hazard, and

e) frequency of the access to the hazard zone.

D.5 Access control placement

Consideration should be given to the ability of the access control to prevent the ASAM from inadvertent contact with a person. The requirements for the access control system (e.g. detection, safe separation distance, and safety gap) should be based on a risk assessment, taking into consideration items such as: type of machine, direction of travel, speed, stopping distance and level of protection required by the system.

D.6 Localized access controls

ISO 16001 specifies general requirements and describes methods for evaluating and testing the performance of hazard detection systems and visual aids used on the earth-moving machines defined in ISO 6165. It addresses detection of people in the detection zone, visual and audible warnings to the operator and to the persons in the detection zone, operational reliability of the system, compatibility and the environmental specifications of the system.

D.7 Infrastructure

Any fixed infrastructure that is related to the access control system should be well protected from damage as it is an integral part of the safety system.

D.8 Electronic access controls

If an electronic access control (e.g. light barriers, laser beams, video imaging, RFID) is used to isolate the AOZ, there should be a communication link between the access control system and the ASAMS while operating in autonomous mode. If communication is lost, the ASAM should be maintained in a safe state.

If the access control system is breached, the ASAM should be maintained in a safe state and the supervisor system should be alerted.

Communication latency times should be short enough such that the access control system is able to stop the ASAM before it creates a hazard, taking into consideration the type of ASAM, direction of travel, speed and level of protection required by the risk assessment.