INTERNATIONAL STANDARD

ISO 17757

Second edition
2019-07

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 17757:2019(E)

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

Published in Switzerland

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 of the 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 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*, in collaboration with Technical Committee ISO/TC 82, *Mining*.

This second edition cancels and replaces the first edition (ISO 17757:2017), which has been technically revised.

The main changes compared to the previous edition are as follows:

— added EMC requirements;

— adapted braking and steering testing methods for autonomous operations;

— provided information on possible radio equipment restrictions;

— provided additional information for cyber security;

— provided an example of a form that can be used to show conformity to the individual requirements.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

This document is of relevance, in particular, for the following stakeholder groups representing the market players with regard to machinery safety:

— machine manufacturers (small, medium and large enterprises);

— health and safety bodies (regulators, accident prevention organisations, market surveillance, etc.).

Others can be affected by the level of machinery safety achieved with the means of the document by the above-mentioned stakeholder groups:

— machine users/employers (small, medium and large enterprises);

— machine users/employees (e.g. trade unions, organizations for people with special needs);

— service providers, e. g. for maintenance (small, medium and large enterprises);

— consumers (in case of machinery intended for use by consumers).

The above-mentioned stakeholder groups have been given the possibility to participate at the drafting process of this document.

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 GMG (global mining 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 (ASAM) 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 ASAM 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 brake 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 13766-1, *Earth-moving and building construction machinery — Electromagnetic compatibility (EMC) of machines with internal electrical power supply — Part 1: General EMC requirements under typical electromagnetic environmental conditions*

ISO 13766-2, *Earth-moving and building construction machinery — Electromagnetic compatibility (EMC) of machines with internal electrical power supply — Part 2: Additional EMC requirements for functional safety*

ISO 19296, *Mining — Mobile machines working underground — Machine safety*

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 6165 and 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/

3.1.1
autonomous or semi-autonomous machine system
ASAMS
machine and supporting systems and *infrastructure* (3.1.11) that enable the machine to operate in *autonomous mode* (3.1.3)

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.

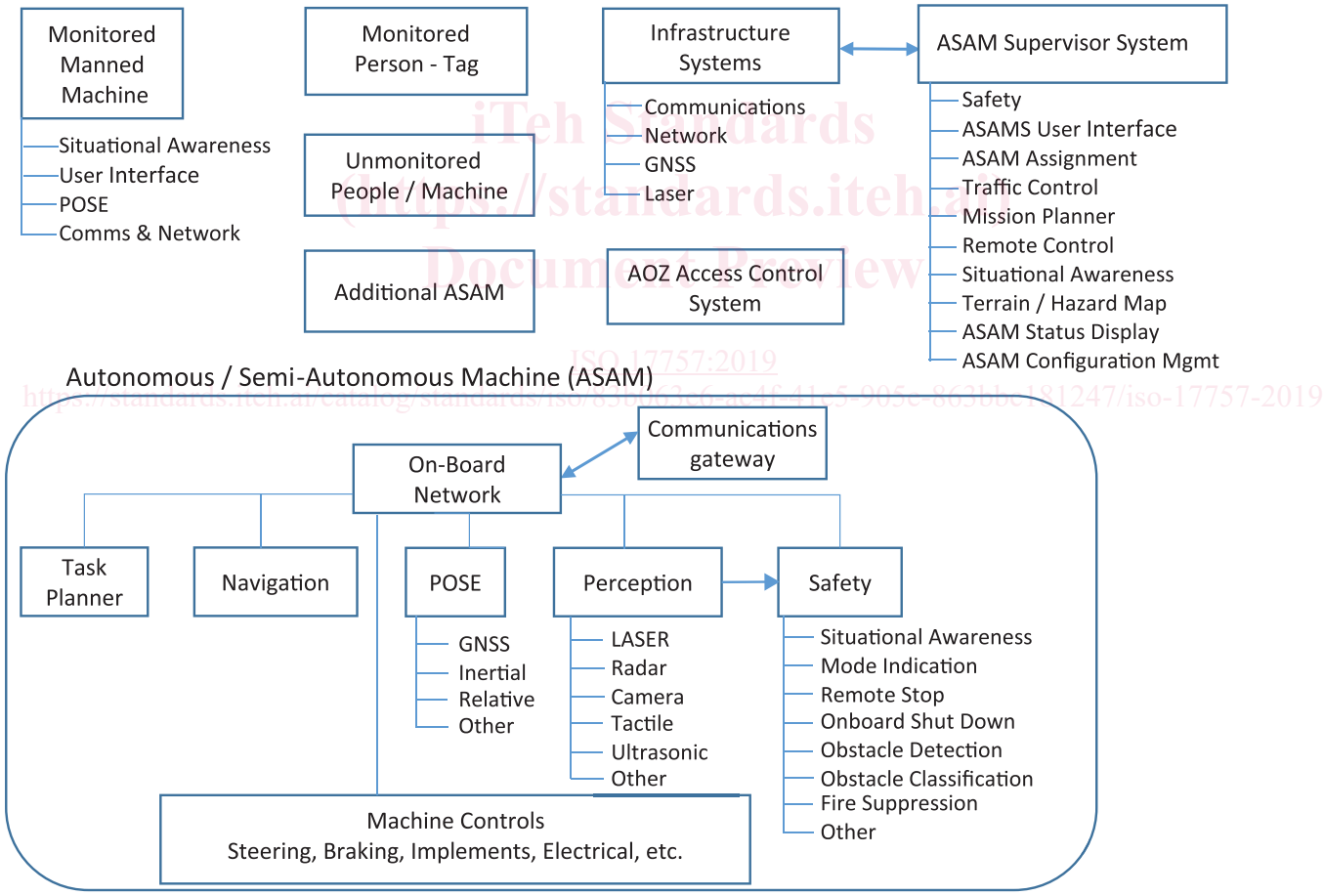

Figure 1 — Representative ASAMS components

3.1.2
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* (3.1.3)

3.1.3
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* (3.1.10)

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

3.1.3.1
autonomous machine
mobile machine that is intended to operate in *autonomous mode* (3.1.3) 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* (3.1.3.2) operating in autonomous mode.

3.1.3.2
semi-autonomous machine
mobile machine that is intended to operate in *autonomous mode* (3.1.3) 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* (3.1.3.1).

3.1.4
autonomous operating zone
AOZ
autonomous area
designated area in which machines are authorized to operate in *autonomous mode* (3.1.3)

3.1.5
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* (3.1.4) and other areas

3.1.6
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, modified — The word training was added.]

3.1.7
digital terrain map
DTM
topographical description of the site in digital format

3.1.8
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

EXAMPLE 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).

3.1.9
halted state
condition in which all motion of a machine is stopped and an operator action is required to resume its operation

3.1.10
operator interaction
involvement of an operator to provide information to or control of an ASAM, such as the transition between *autonomous mode* (3.1.3) and *manual mode* (3.1.13), or to provide any type of exception handling

3.1.11
infrastructure
work site equipment and facilities used in support of a machine's operation in *autonomous mode* (3.1.3)

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

3.1.12
layers of protection
independent processes or actions taken to prevent or address potential hazardous events leading to an unsafe consequence

3.1.13
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* (3.1.8).

3.1.14
approach mode
mode that allows access to the ASAM

3.1.15
mode indicator
means by which a machine shows whether it is in *manual mode* (3.1.13), *autonomous mode* (3.1.3) or remote-control mode

3.1.16
operator
system operator
person having control and responsibility for the operation of an *autonomous machine* (3.1.3.1) or a *semi-autonomous machine* (3.1.3.2) and the *ASAMS* (3.1.1)

3.1.17
remote-stop system
system that brings all *autonomous machines* (3.1.3.1) and *semi-autonomous machines* (3.1.3.2) within a defined range of a mobile stop device to a *halted state* (3.1.9) when initiated

3.1.18
all-stop system
system that brings all *autonomous machines* (3.1.3.1) and *semi-autonomous machines* (3.1.3.2) under the operator's supervision to a *halted state* (3.1.9) when initiated

3.1.19
perception system
system comprising sensors used to detect, locate and recognize a potential feature of interest

3.1.20
remote control
RC
operator control of a machine from a device not located on the machine

3.1.21
safe state
condition, whether or not an *autonomous machine* (3.1.3.1) or *semi-autonomous machine* (3.1.3.2) 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

3.1.22
site manager
entity responsible for managing the entire work site, with overall responsibility for the operators and site operations

3.1.23
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

3.1.24
system integrator
entity responsible for the design, installation and setup of the ASAM and *ASAMS* (3.1.1)

3.1.25
risk assessment
overall process comprising a risk analysis and a risk evaluation

Note 1 to entry: See ISO 12100.

3.2 Abbreviated terms

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

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.

In addition, the ASAMS shall be designed according to the principles of ISO 12100:2010 for relevant but not significant hazards which are not dealt with by this document.

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 requirements. 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.

The ASAMS shall comply with the EMC requirements in ISO 13766-1 and 2, except for components in an environment with lower electromagnetic emissions, e.g. server room, office area, which shall comply with the appropriate IEC 61000 series EMC requirements.

4.2 Stop systems

4.2.1 General

All ASAM shall have a means to be placed into a halted state from a safe, remote distance.

4.2.2 All-stop system

If the ASAMS includes a remote ASAM supervisor system, that system shall have an all stop system for the operator to place all ASAM under supervision into a halted state.

After an ASAM is placed in the halted state, 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 any applicable AOZ to a halted state.

After an ASAM is placed in the halted state, 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 ASAMS. With ASAM, 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 ASAMS shall have on-board capability to bring the machine to a stop;

b) when the ASAM 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 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 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. If the ASAMS does not allow the machine to operate at the required test speeds according to ISO 3450, the maximum speed allowed by the ASAMS in those conditions may be used to demonstrate that the machine meets the required ISO 3450 performance. For example, if the ASAMS prevents the speed from exceeding 40 km/h on 8 % to 10 % slopes, then the test speed for ISO 3450:2011, 6.5.5 would be 40 km/h and the maximum stopping distance would be calculated from ISO 3450:2011, Table 3 using 40 km/h.

The test report for a wheeled ASAM shall be in accordance with ISO 3450:2011, Clause 7.

The braking systems of crawler ASAM shall meet the requirements of ISO 10265:2008, Clause 4, except ISO 10265:2008, 4.2 and 4.4. The ASAMS shall maintain the machine in a safe state if the exhaustible energy level drops below the level required to meet the secondary brake performance requirements, as defined in ISO 10265:2008, Clause 6.1.4.

ISO 10265:2008, Clause 7, which relates to the braking system and periodic evaluation 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.