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.

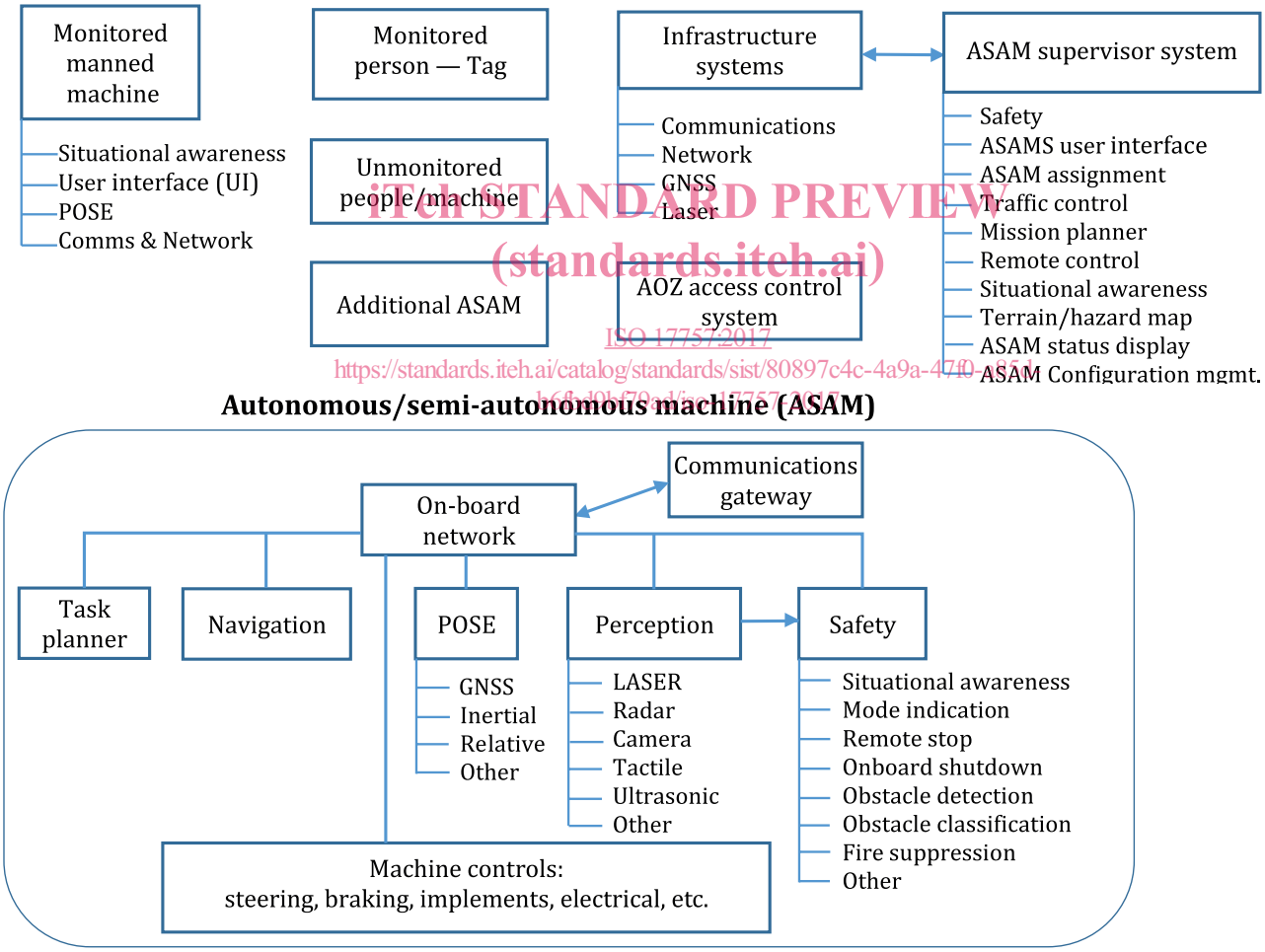

Figure 1 — Representative ASAMS components

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.