INTERNATIONAL STANDARD

ISO 22448

First edition
2010-10-01

Earth-moving machinery — Anti-theft systems — Classification and performance

Engins de terrassement — Systèmes antivol — Classification et performance

Reference number
ISO 22448:2010(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 22448 was prepared by Technical Committee ISO/TC 127, *Earth-moving machinery*, Subcommittee SC 3, *Machine characteristics, electrical and electronic systems, operation and maintenance*.

Earth-moving machinery — Anti-theft systems — Classification and performance

1 Scope

This International Standard specifies, and classifies at seven levels, systems for the protection against theft of earth-moving machinery as defined in ISO 6165, and gives performance criteria for each level.

It also gives recommendations for managing critical documentation and theft-sensitive spare parts in protection against theft.

It is not applicable to tracking systems that monitor the location of a machine.

2 Normative references

The following referenced documents are indispensable for the application 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 6165, *Earth moving machinery — Basic types — Identification and terms and definitions*

ISO 10264, *Earth-moving machinery — Key-locked starting systems*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
immobilizer
device that is intended to prevent normal operation of the machine

3.2
authentication device
device which allows identification of authorized user(s)

EXAMPLE Radio, satellite, cell phone, keypad, ultrasonic, magnetic wave, electronic key.

3.3
electronic control unit
electronic control module
ECU
ECM
electronic device (electronic programmable controller) used in a control system on earth-moving machinery

3.4
electronic key
wireless device used to aid authentication of the operator

3.5
token
unique and distinguishing code exchanged between ECM/ECUs

3.6
immobilizer software
software elements integrated into at least one machine ECM/ECU that require authentication before enabling operation of one or more machine functions

3.7
password
pass code, presented by means of, e.g. a keypad combination, electronic key ID or token

3.8
password process
means of providing a password through a human or an electronic interface

4 Classification

Theft protection systems for earth-moving machines are classified into seven levels, I to VII, as follows.

4.1 Level I — Universal key (with no combination)

A mechanical key, provided by the manufacturer, required by the user to start and operate the machine. This key is not unique to a particular machine and may operate other machines produced by the same manufacturer.

4.2 Level II — Mechanical restraint

A lockable mechanical device

— that restricts normal activation of one or several machine controls such as the power transmission, gear-shift and steering control, or

— that restricts normal movement of the machine or part of the machine by means of, for example, a steering cylinder lock, ground chains, cables or padlocks.

NOTE The mechanical restraint can be an aftermarket device.

4.3 Level III — Unique key

A mechanical key, matched specifically to a machine, required by the user to start and operate the machine.

4.4 Level IV — Add-on authentication system

An original equipment manufacturer's or third party add-on attachment that prevents unauthorized start-up or movement of the machine and which requires

— an authentication device, and

— a password process in order to be unlocked.

4.5 Level V — Manufacturer's authentication system

A system, designed by the machine manufacturer as part of the machine's electronic system, that prevents unauthorized start-up or movement of the machine and that requires

— an authentication device,

— a password process in order to be unlocked.

NOTE The system can be installed on a machine already in use, provided that the machine has been designed to receive such a system.

4.6 Level VI — Electronic immobilizer system

A system, designed by the machine manufacturer as a part of the machine's electronic system, that prevents unauthorized start-up or movement of the machine and that requires

— an authentication device,

— a password process in order to be unlocked,

— immobilizer software embedded in one of the machine's ECM/ECUs in order for the machine's starting or travel to be disabled.

The system shall be designed to be reprogrammed or serviced only by authorized service people (the machine manufacturer's dealer or manufacturer).

NOTE This system can be installed on a machine already in use, provided that the machine has been designed to receive such a system.

4.7 Level VII — Multiple-ECM/ECU immobilizer system

A system, designed by the machine manufacturer as part of the machine's electronic system, that prevents unauthorized start-up or movement of the machine and that requires

— an authentication device,

— a password process that is shared among the ECM/ECUs in order to be unlocked,

— immobilizer software embedded in more than one of the machine's ECM/ECUs in order for the machine's starting or travel to be disabled.

The system shall be designed to be reprogrammed or serviced only by authorized service personnel (the machine manufacturer's dealer or manufacturer).

NOTE This system can be installed on a machine already in use, provided that the machine has been designed to receive such a system.

5 Performance criteria

The performance criterion or criteria for each of the levels are as follows.

5.1 Level I — Universal key (with no combination)

The key-locked starting system shall be in accordance with ISO 10264.

NOTE A single mechanical key from the same machine manufacturer can be used for the entire fleet, thereby simplifying the management of a fleet.

5.2 Level II — Mechanical restraints

The component(s) shall be designed to resist the force of a person using tools.

For mechanical constraint components that restrict the movement of the machine, the restraint component shall be capable of resisting the force of the machine itself, with an appropriate safety factor.

The key profile for the lock used with the mechanical restraint shall have at least 50 different permutations.

5.3 Level III — Unique key

The key-locked starting system shall be in accordance with ISO 10264.

The key profile shall have at least 50 different permutations.

5.4 Level IV — Add-on authentication system

The system shall not stop machine functions until the operator has shut down the engine.

The system shall provide a minimum of 10 000 possible passwords.

The password may be changed at any time by an authorized person.

When the engine is shut down, the system shall be capable of locking automatically after a certain period of time.

The possible number of wrong attempts shall be limited and, after this limit has been exceeded, the system shall remain locked for a certain period of time before allowing the next attempt.

5.5 Level V — Manufacturer's authentication system

The system shall not stop machine functions until the operator has shut down the engine.

The system shall provide a minimum of 10 000 possible passwords.

The password may be changed at any time by an authorized person.

When the engine is shut down, the system shall be capable of locking automatically after a certain period of time.

The possible number of wrong attempts shall be limited and, after this limit has been exceeded, the system shall remain locked for a certain period of time before allowing the next attempt.

5.6 Level VI — Electronic immobilizer system

An immobilizer shall be designed and built such that, when installed on a machine and in accordance with the manufacturer's instructions, it cannot rapidly or without attracting attention be rendered ineffective or be destroyed (for example, by the use of low-cost or easily concealed tools, equipment or fabrications readily available to the public at large). It shall be difficult and time-consuming to replace a major component or assembly in order to bypass the immobilizer.

Only the machine manufacturer, dealer or other authorized personnel shall be able to perform the authentication set-up and maintenance, using an authorized service tool that grants access to the immobilizer for set-up and configuration.

When the engine is shut down, the system shall be capable of locking automatically after a certain period of time.

The system shall not stop the machine functions until the operator has shut down the engine.

The system shall provide a minimum of 10 000 possible passwords.

The possible number of wrong attempts shall be limited and, after this limit has been exceeded, the system shall remain locked for a certain period of time before allowing the next attempt.

The password may be changed at any time by an authorized person.

5.7 Level VII — Multiple-ECM/ECU immobilizer system

An immobilizer shall be designed and built such that, when installed on a machine and according to the manufacturer's instructions, it cannot rapidly or without attracting attention be rendered ineffective or destroyed — for example, by the use of low-cost or easily concealed tools, equipment or fabrications readily available to the public at large. It shall be difficult and time-consuming to replace a major component or assembly in order to bypass the immobilizer.

Only the machine manufacturer, dealer or other authorized personnel shall be able to perform the authentication set-up and maintenance, using an authorized service tool that grants access to the immobilizer for set-up and configuration.

Two or more ECM/ECUs shall share unique information (ECM/ECU token information), so as to prevent the replacement of an ECM/ECU in an attempt to circumvent authentication.

A method of authentication shall be provided for the machine manufacturer dealer's service tool and customer configuration tool that grants access to the ECM/ECU for set-up and configuration.

The system shall not stop the machine functions until the operator has shut down the engine.

When the engine is shut down, the system shall be capable of locking automatically after a certain period of time.

The system shall provide a minimum of 10 000 possible passwords.

The password may be changed at any time by an authorized person.

The possible number of wrong attempts shall be limited and, after this limit has been exceeded, the system shall remain locked for a certain period of time before allowing the next attempt.

Table 1 — Summary of system levels

Level	Independent from original control/optional system	Single ECM/ECU	Multiple ECM/ECU	Entry/minimum requirement	Authentication set-up (token, password)
I	No	—	—	Key	—
II	Yes	—	—	Device-specific	—
III	No	—	—	Unique key	—
IV	Yes	—	—	Authentication device	User
V	No	—	—	Authentication device	Manufacturer, manufacturer's dealer, authorized user
VI	No	Yes	No	Authentication device	Manufacturer, manufacturer's dealer
VII	No	No	Yes	Authentication device	Manufacturer, manufacturer's dealer